网络安全与数据合规
法律法规汇编

宁波市律师协会互联网与数字化专业委员会

二0二四年七月

目 录

第一章 全国人大及常委会

中华人民共和国民法典(节选)

(2020 年 5 月 28 日第十三届全国人民代表大会第三次会议通过)

第一编 总 则

第五章 民事权利

第一百零九条 自然人的人身自由、人格尊严受法律保护。

第一百一十条 自然人享有生命权、身体权、健康权、姓名权、肖像权、名誉权、荣誉权、隐私权、婚姻自主权等权利。

法人、非法人组织享有名称权、名誉权和荣誉权。

第一百一十一条 自然人的个人信息受法律保护。任何组织或者个人需要获取他人个人信息的，应当依法取得并确保信息安全，不得非法收集、使用、加工、传输他人个人信息，不得非法买卖、提供或者公开他人个人信息。

第四编 人 格 权

第六章 隐私权和个人信息保护

第一千零三十二条 自然人享有隐私权。任何组织或者个人不得以刺探、侵扰、泄露、公开等方式侵害他人的隐私权。

隐私是自然人的私人生活安宁和不愿为他人知晓的私密空间、私密活动、私密信息。

第一千零三十三条 除法律另有规定或者权利人明确同意外，任何组织或者个人不得实施下列行为：

(一)以电话、短信、即时通讯工具、电子邮件、传单等方式侵扰他人的私人生活安宁；

(二)进入、拍摄、窥视他人的住宅、宾馆房间等私密空间；

(三)拍摄、窥视、窃听、公开他人的私密活动；

(四)拍摄、窥视他人身体的私密部位；

(五)处理他人的私密信息；

(六)以其他方式侵害他人的隐私权。

第一千零三十四条 自然人的个人信息受法律保护。

个人信息是以电子或者其他方式记录的能够单独或者与其他信息结合识别特定自然人的各种信息，包括自然人的姓名、出生日期、身份证件号码、生物识别信息、住址、电话号码、电子邮箱、健康信息、行踪信息等。

个人信息中的私密信息，适用有关隐私权的规定；没有规定的，适用有关个人信息保护的规定。

第一千零三十五条 处理个人信息的，应当遵循合法、正当、必要原则，不得过度处理，并符合下列条件：

(一)征得该自然人或者其监护人同意，但是法律、行政法规另有规定的除外；

(二)公开处理信息的规则；

(三)明示处理信息的目的、方式和范围；

(四)不违反法律、行政法规的规定和双方的约定。

个人信息的处理包括个人信息的收集、存储、使用、加工、传输、提供、公开等。

第一千零三十六条 处理个人信息，有下列情形之一的，行为人不承担民事责任：

(一)在该自然人或者其监护人同意的范围内合理实施的行为；

(二)合理处理该自然人自行公开的或者其他已经合法公开的信息，但是该自然人明确拒绝或者处理该信息侵害其重大利益的除外；

(三)为维护公共利益或者该自然人合法权益，合理实施的其他行为。

第一千零三十七条 自然人可以依法向信息处理者查阅或者复制其个人信息；发现信息有错误的，有权提出异议并请求及时采取更正等必要措施。

自然人发现信息处理者违反法律、行政法规的规定或者双方的约定处理其个人信息的，有权请求信息处理者及时删除。

第一千零三十八条 信息处理者不得泄露或者篡改其收集、存储的个人信息；未经自然人同意，不得向他人非法提供其个人信息，但是经过加工无法识别特定个人且不能复原的除外。

信息处理者应当采取技术措施和其他必要措施，确保其收集、存储的个人信息安全，防止信息泄露、篡改、丢失； 发生或者可能发生个人信息泄露、篡改、丢失的，应当及时采取补救措施，按照规定告知自然人并向有关主管部门报告。

第一千零三十九条 国家机关、承担行政职能的法定机构及其工作人员对于履行职责过程中知悉的自然人的隐私和个人信息，应当予以保密，不得泄露或者向他人非法提供。

第七编 侵权责任

第六章 医疗损害责任

第一千二百二十六条 医疗机构及其医务人员应当对患者的隐私和个人信息保密。泄露患者的隐私和个人信息， 或者未经患者同意公开其病历资料的，应当承担侵权责任。

中华人民共和国刑法(节选)

(1979 年 7 月 1 日第五届全国人民代表大会第二次会议通过 1997 年 3 月 14 日第八届全国人民代表大会第五次会议修订 根据 1998 年 12 月 29 日第九届全国人民代表大会常务委员会第六次会议通过的《全国人民代表大会常务委员会关于惩治骗购外汇、逃汇和非法买卖外汇犯罪的决定》、1999 年 12 月 25 日第九届全国人民代表大会常务委员会第十三次会议通过的《中华人民共和国刑法修正案》、2001 年 8 月 31 日第九届全国人民代表大会常务委员会第二十三次会议通过的《中华人民共和国刑法修正案(二)》、2001 年 12 月 29 日第九届全国人民代表大会常务委员会第二十五次会议通过的《中华人民共和国刑法修正案(三)》、2002 年 12 月 28 日第九届全国人民代表大会常务委员会第三十一次会议通过的《中华人民共和国刑法修正案(四)》、2005 年 2 月 28 日第十届全国人民代表大会常务委员会第十四次会议通过的《中华人民共和国刑法修正案(五)》、2006 年 6 月 29 日第十届全国人民代表大会常务委员会第二十二次会议通过的《中华人民共和国刑法修正案(六)》、2009 年 2 月 28 日第十一届全国人民代表大会常务委员会第七次会议通过的《中华人民共和国刑法修正案(七)》、2009 年 8 月 27 日第十一届全国人民代表大会常务委员会第十次会议通过的《全国人民代表大会常务委员会关于修改部分法律的决定》、2011 年 2 月 25 日第十一届全国人民代表大会常务委员会第十九次会议通过的《中华人民共和国刑法修正案(八)》、2015 年 8 月 29 日第十二届全国人民代表大会常务委员会第十六次会议通过的《中华人民共和国刑法修正案(九)》、2017 年 11 月 4 日第十二届全国人民代表大会常务委员会第三十次会议通过的《中华人民共和国刑法

修正案(十)》、2020 年 12 月 26 日第十三届全国人民代表大会常务委员会第二十四次会议通过的《中华人民共和国刑法修正案(十一)》和 2023 年 12 月 29 日第十四届全国人民代表大会常务委员会第七次会议通过的《中华人民共和国刑法修正案(十二)》修正)

第二百五十三条之一 违反国家有关规定，向他人出售或者提供公民个人信息，情节严重的，处三年以下有期徒刑或者拘役，并处或者单处罚金；情节特别严重的，处三年以上七年以下有期徒刑，并处罚金。

违反国家有关规定，将在履行职责或者提供服务过程中获得的公民个人信息，出售或者提供给他人的，依照前款的规定从重处罚。

窃取或者以其他方法非法获取公民个人信息的，依照第一款的规定处罚。

单位犯前三款罪的，对单位判处罚金，并对其直接负责的主管人员和其他直接责任人员，依照各该款的规定处罚。

第二百八十五条 违反国家规定，侵入国家事务、国防建设、尖端科学技术领域的计算机信息系统的，处三年以下有期徒刑或者拘役。

违反国家规定，侵入前款规定以外的计算机信息系统或者采用其他技术手段，获取该计算机信息系统中存储、处理或者传输的数据， 或者对该计算机信息系统实施非法控制，情节严重的，处三年以下有期徒刑或者拘役，并处或者单处罚金；情节特别严重的，处三年以上七年以下有期徒刑，并处罚金。

提供专门用于侵入、非法控制计算机信息系统的程序、工具， 或者明知他人实施侵入、非法控制计算机信息系统的违法犯罪行为而为其提供程序、工具， 情节严重的，依照前款的规定处罚。

单位犯前三款罪的，对单位判处罚金，并对其直接负责的主管人员和其他直接责任人员，依照各该款的规定处罚。

第二百八十六条 违反国家规定，对计算机信息系统功能进行删除、修改、增加、干扰， 造成计算机信息系统不能正常运行，后果严重的，处五年以下有期徒刑或者拘役；后果特别严重的，处五年以上有期徒刑。

违反国家规定，对计算机信息系统中存储、处理或者传输的数据和应用程序进行删除、修改、增加的操作，后果严重的，依照前款的规定处罚。

故意制作、传播计算机病毒等破坏性程序， 影响计算机系统正常运行，后果

严重的，依照第一款的规定处罚。

单位犯前三款罪的，对单位判处罚金，并对其直接负责的主管人员和其他直接责任人员，依照第一款的规定处罚。

第二百八十六条之一 网络服务提供者不履行法律、行政法规规定的信息网络安全管理义务，经监管部门责令采取改正措施而拒不改正，有下列情形之一的，处三年以下有期徒刑、拘役或者管制，并处或者单处罚金：

(一)致使违法信息大量传播的；

(二)致使用户信息泄露，造成严重后果的；

(三)致使刑事案件证据灭失，情节严重的；

(四)有其他严重情节的。

单位犯前款罪的，对单位判处罚金，并对其直接负责的主管人员和其他直接责任人员，依照前款的规定处罚。

有前两款行为，同时构成其他犯罪的，依照处罚较重的规定定罪处罚。

第二百八十七条 利用计算机实施金融诈骗、盗窃、贪污、挪用公款、窃取国家秘密或者其他犯罪的，依照本法有关规定定罪处罚。

第二百八十七条之一 利用信息网络实施下列行为之一，情节严重的，处三年以下有期徒刑或者拘役，并处或者单处罚金：

(一)设立用于实施诈骗、传授犯罪方法、制作或者销售违禁物品、管制物品等违法犯罪活动的网站、通讯群组的；

(二)发布有关制作或者销售毒品、枪支、淫秽物品等违禁物品、管制物品或者其他违法犯罪信息的；

(三)为实施诈骗等违法犯罪活动发布信息的。

单位犯前款罪的，对单位判处罚金，并对其直接负责的主管人员和其他直接责任人员，依照第一款的规定处罚。

有前两款行为，同时构成其他犯罪的，依照处罚较重的规定定罪处罚。

第二百八十七条之二 明知他人利用信息网络实施犯罪，为其犯罪提供互联网接入、服务器托管、网络存储、通讯传输等技术支持， 或者提供广告推广、支付结算等帮助，情节严重的，处三年以下有期徒刑或者拘役，并处或者单处罚金。

单位犯前款罪的，对单位判处罚金，并对其直接负责的主管人员和其他直接

责任人员，依照第一款的规定处罚。

有前两款行为，同时构成其他犯罪的，依照处罚较重的规定定罪处罚。

中华人民共和国保守国家秘密法

(1988 年 9 月 5 日第七届全国人民代表大会常务委员会第三次会议通过 2010 年 4 月 29 日第十一届全国人民代表大会常务委员会第十四次会议第一次修订 2024 年 2 月 27 日第十四届全国人民代表大会常务委员会第八次会议第二次修订)

目 录

第一章 总 则

第一条 为了保守国家秘密，维护国家安全和利益，保障改革开放和社会主义现代化建设事业的顺利进行，根据宪法，制定本法。

第二条 国家秘密是关系国家安全和利益，依照法定程序确定，在一定时间内只限一定范围的人员知悉的事项。

第三条 坚持中国共产党对保守国家秘密(以下简称保密)工作的领导。中央保密工作领导机构领导全国保密工作，研究制定、指导实施国家保密工作战略和重大方针政策，统筹协调国家保密重大事项和重要工作，推进国家保密法治建设。

第四条 保密工作坚持总体国家安全观，遵循党管保密、依法管理，积极防范、突出重点， 技管并重、创新发展的原则， 既确保国家秘密安全，又便利信息资源合理利用。

法律、行政法规规定公开的事项，应当依法公开。

第五条 国家秘密受法律保护。

一切国家机关和武装力量、各政党和各人民团体、企业事业组织和其他社会组织以及公民都有保密的义务。

任何危害国家秘密安全的行为，都必须受到法律追究。

第六条 国家保密行政管理部门主管全国的保密工作。县级以上地方各级保密行政管理部门主管本行政区域的保密工作。

第七条 国家机关和涉及国家秘密的单位(以下简称机关、单位)管理本机关和本单位的保密工作。

中央国家机关在其职权范围内管理或者指导本系统的保密工作。

第八条 机关、单位应当实行保密工作责任制，依法设置保密工作机构或者指定专人负责保密工作，健全保密管理制度，完善保密防护措施，开展保密宣传教育，加强保密监督检查。

第九条 国家采取多种形式加强保密宣传教育，将保密教育纳入国民教育体系和公务员教育培训体系，鼓励大众传播媒介面向社会进行保密宣传教育，普及保密知识，宣传保密法治，增强全社会的保密意识。

第十条 国家鼓励和支持保密科学技术研究和应用，提升自主创新能力，依法保护保密领域的知识产权。

第十一条 县级以上人民政府应当将保密工作纳入本级国民经济和社会发展规划，所需经费列入本级预算。

机关、单位开展保密工作所需经费应当列入本机关、本单位年度预算或者年度收支计划。

第十二条 国家加强保密人才培养和队伍建设，完善相关激励保障机制。

对在保守、保护国家秘密工作中做出突出贡献的组织和个人， 按照国家有关规定给予表彰和奖励。

第二章 国家秘密的范围和密级

第十三条 下列涉及国家安全和利益的事项，泄露后可能损害国家在政治、经济、国防、外交等领域的安全和利益的，应当确定为国家秘密：

(一)国家事务重大决策中的秘密事项；

(二)国防建设和武装力量活动中的秘密事项；

(三)外交和外事活动中的秘密事项以及对外承担保密义务的秘密事项；

(四)国民经济和社会发展中的秘密事项；

(五)科学技术中的秘密事项；

(六)维护国家安全活动和追查刑事犯罪中的秘密事项;

(七)经国家保密行政管理部门确定的其他秘密事项。

政党的秘密事项中符合前款规定的，属于国家秘密。

第十四条 国家秘密的密级分为绝密、机密、秘密三级。

绝密级国家秘密是最重要的国家秘密，泄露会使国家安全和利益遭受特别严重的损害；机密级国家秘密是重要的国家秘密，泄露会使国家安全和利益遭受严重的损害；秘密级国家秘密是一般的国家秘密，泄露会使国家安全和利益遭受损害。

第十五条 国家秘密及其密级的具体范围(以下简称保密事项范围)，由国家保密行政管理部门单独或者会同有关中央国家机关规定。

军事方面的保密事项范围，由中央军事委员会规定。

保密事项范围的确定应当遵循必要、合理原则， 科学论证评估，并根据情况变化及时调整。保密事项范围的规定应当在有关范围内公布。

第十六条 机关、单位主要负责人及其指定的人员为定密责任人，负责本机关、本单位的国家秘密确定、变更和解除工作。

机关、单位确定、变更和解除本机关、本单位的国家秘密， 应当由承办人提出具体意见，经定密责任人审核批准。

第十七条 确定国家秘密的密级，应当遵守定密权限。

中央国家机关、省级机关及其授权的机关、单位可以确定绝密级、机密级和秘密级国家秘密；设区的市级机关及其授权的机关、单位可以确定机密级和秘密级国家秘密；特殊情况下无法按照上述规定授权定密的，国家保密行政管理部门或者省、自治区、直辖市保密行政管理部门可以授予机关、单位定密权限。具体的定密权限、授权范围由国家保密行政管理部门规定。

下级机关、单位认为本机关、本单位产生的有关定密事项属于上级机关、单位的定密权限，应当先行采取保密措施，并立即报请上级机关、单位确定； 没有上级机关、单位的， 应当立即提请有相应定密权限的业务主管部门或者保密行政管理部门确定。

公安机关、国家安全机关在其工作范围内按照规定的权限确定国家秘密的密级。

第十八条 机关、单位执行上级确定的国家秘密事项或者办理其他机关、单位确定的国家秘密事项，需要派生定密的，应当根据所执行、办理的国家秘密事项的密级确定。

第十九条 机关、单位对所产生的国家秘密事项，应当按照保密事项范围的规定确定密级，同时确定保密期限和知悉范围；有条件的可以标注密点。

第二十条 国家秘密的保密期限，应当根据事项的性质和特点，按照维护国家安全和利益的需要，限定在必要的期限内；不能确定期限的，应当确定解密的条件。

国家秘密的保密期限，除另有规定外，绝密级不超过三十年，机密级不超过二十年，秘密级不超过十年。

机关、单位应当根据工作需要， 确定具体的保密期限、解密时间或者解密条件。

机关、单位对在决定和处理有关事项工作过程中确定需要保密的事项， 根据工作需要决定公开的，正式公布时即视为解密。

第二十一条 国家秘密的知悉范围，应当根据工作需要限定在最小范围。

国家秘密的知悉范围能够限定到具体人员的，限定到具体人员；不能限定到具体人员的，限定到机关、单位，由该机关、单位限定到具体人员。

国家秘密的知悉范围以外的人员，因工作需要知悉国家秘密的，应当经过机关、单位主要负责人或者其指定的人员批准。原定密机关、单位对扩大国家秘密的知悉范围有明确规定的，应当遵守其规定。

第二十二条 机关、单位对承载国家秘密的纸介质、光介质、电磁介质等载体(以下简称国家秘密载体)以及属于国家秘密的设备、产品， 应当作出国家秘密标志。

涉及国家秘密的电子文件应当按照国家有关规定作出国家秘密标志。

不属于国家秘密的，不得作出国家秘密标志。

第二十三条 国家秘密的密级、保密期限和知悉范围，应当根据情况变化及时变更。国家秘密的密级、保密期限和知悉范围的变更， 由原定密机关、单位决定，也可以由其上级机关决定。

国家秘密的密级、保密期限和知悉范围变更的， 应当及时书面通知知悉范围

内的机关、单位或者人员。

第二十四条 机关、单位应当每年审核所确定的国家秘密。

国家秘密的保密期限已满的，自行解密。在保密期限内因保密事项范围调整不再作为国家秘密，或者公开后不会损害国家安全和利益，不需要继续保密的，应当及时解密；需要延长保密期限的，应当在原保密期限届满前重新确定密级、保密期限和知悉范围。提前解密或者延长保密期限的，由原定密机关、单位决定，也可以由其上级机关决定。

第二十五条 机关、单位对是否属于国家秘密或者属于何种密级不明确或者有争议的，由国家保密行政管理部门或者省、自治区、直辖市保密行政管理部门按照国家保密规定确定。

第三章 保密制度

第二十六条 国家秘密载体的制作、收发、传递、使用、复制、保存、维修和销毁，应当符合国家保密规定。

绝密级国家秘密载体应当在符合国家保密标准的设施、设备中保存， 并指定专人管理；未经原定密机关、单位或者其上级机关批准，不得复制和摘抄；收发、传递和外出携带，应当指定人员负责，并采取必要的安全措施。

第二十七条 属于国家秘密的设备、产品的研制、生产、运输、使用、保存、维修和销毁，应当符合国家保密规定。

第二十八条 机关、单位应当加强对国家秘密载体的管理，任何组织和个人不得有下列行为：

(一)非法获取、持有国家秘密载体；

(二)买卖、转送或者私自销毁国家秘密载体；

(三)通过普通邮政、快递等无保密措施的渠道传递国家秘密载体；

(四)寄递、托运国家秘密载体出境；

(五)未经有关主管部门批准，携带、传递国家秘密载体出境；

(六)其他违反国家秘密载体保密规定的行为。

第二十九条 禁止非法复制、记录、存储国家秘密。

禁止未按照国家保密规定和标准采取有效保密措施，在互联网及其他公共信息网络或者有线和无线通信中传递国家秘密。

禁止在私人交往和通信中涉及国家秘密。

第三十条 存储、处理国家秘密的计算机信息系统(以下简称涉密信息系统)按照涉密程度实行分级保护。

涉密信息系统应当按照国家保密规定和标准规划、建设、运行、维护，并配备保密设施、设备。保密设施、设备应当与涉密信息系统同步规划、同步建设、同步运行。

涉密信息系统应当按照规定，经检查合格后，方可投入使用，并定期开展风险评估。

第三十一条 机关、单位应当加强对信息系统、信息设备的保密管理，建设保密自监管设施，及时发现并处置安全保密风险隐患。任何组织和个人不得有下列行为：

(一)未按照国家保密规定和标准采取有效保密措施，将涉密信息系统、涉密信息设备接入互联网及其他公共信息网络；

(二)未按照国家保密规定和标准采取有效保密措施，在涉密信息系统、涉密信息设备与互联网及其他公共信息网络之间进行信息交换；

(三)使用非涉密信息系统、非涉密信息设备存储或者处理国家秘密；

(四)擅自卸载、修改涉密信息系统的安全技术程序、管理程序；

(五)将未经安全技术处理的退出使用的涉密信息设备赠送、出售、丢弃或者改作其他用途；

(六)其他违反信息系统、信息设备保密规定的行为。

第三十二条 用于保护国家秘密的安全保密产品和保密技术装备应当符合国家保密规定和标准。

国家建立安全保密产品和保密技术装备抽检、复检制度， 由国家保密行政管理部门设立或者授权的机构进行检测。

第三十三条 报刊、图书、音像制品、电子出版物的编辑、出版、印制、发行，广播节目、电视节目、电影的制作和播放，网络信息的制作、复制、发布、传播，应当遵守国家保密规定。

第三十四条 网络运营者应当加强对其用户发布的信息的管理，配合监察机关、保密行政管理部门、公安机关、国家安全机关对涉嫌泄露国家秘密案件进行

调查处理；发现利用互联网及其他公共信息网络发布的信息涉嫌泄露国家秘密的，应当立即停止传输该信息，保存有关记录，向保密行政管理部门或者公安机关、国家安全机关报告；应当根据保密行政管理部门或者公安机关、国家安全机关的要求，删除涉及泄露国家秘密的信息，并对有关设备进行技术处理。

第三十五条 机关、单位应当依法对拟公开的信息进行保密审查，遵守国家保密规定。

第三十六条 开展涉及国家秘密的数据处理活动及其安全监管应当符合国家保密规定。

国家保密行政管理部门和省、自治区、直辖市保密行政管理部门会同有关主管部门建立安全保密防控机制，采取安全保密防控措施，防范数据汇聚、关联引发的泄密风险。

机关、单位应当对汇聚、关联后属于国家秘密事项的数据依法加强安全管理。

第三十七条 机关、单位向境外或者向境外在中国境内设立的组织、机构提供国家秘密，任用、聘用的境外人员因工作需要知悉国家秘密的， 按照国家有关规定办理。

第三十八条 举办会议或者其他活动涉及国家秘密的，主办单位应当采取保密措施，并对参加人员进行保密教育，提出具体保密要求。

第三十九条 机关、单位应当将涉及绝密级或者较多机密级、秘密级国家秘密的机构确定为保密要害部门，将集中制作、存放、保管国家秘密载体的专门场所确定为保密要害部位，按照国家保密规定和标准配备、使用必要的技术防护设施、设备。

第四十条 军事禁区、军事管理区和属于国家秘密不对外开放的其他场所、部位，应当采取保密措施，未经有关部门批准，不得擅自决定对外开放或者扩大开放范围。

涉密军事设施及其他重要涉密单位周边区域应当按照国家保密规定加强保密管理。

第四十一条 从事涉及国家秘密业务的企业事业单位，应当具备相应的保密管理能力，遵守国家保密规定。

从事国家秘密载体制作、复制、维修、销毁， 涉密信息系统集成，武器装备

科研生产，或者涉密军事设施建设等涉及国家秘密业务的企业事业单位，应当经过审查批准，取得保密资质。

第四十二条 采购涉及国家秘密的货物、服务的机关、单位， 直接涉及国家秘密的工程建设、设计、施工、监理等单位，应当遵守国家保密规定。

机关、单位委托企业事业单位从事涉及国家秘密的业务， 应当与其签订保密协议，提出保密要求，采取保密措施。

第四十三条 在涉密岗位工作的人员（以下简称涉密人员），按照涉密程度分为核心涉密人员、重要涉密人员和一般涉密人员，实行分类管理。

任用、聘用涉密人员应当按照国家有关规定进行审查。

涉密人员应当具有良好的政治素质和品行，经过保密教育培训，具备胜任涉密岗位的工作能力和保密知识技能，签订保密承诺书，严格遵守国家保密规定，承担保密责任。

涉密人员的合法权益受法律保护。对因保密原因合法权益受到影响和限制的涉密人员，按照国家有关规定给予相应待遇或者补偿。

第四十四条 机关、单位应当建立健全涉密人员管理制度，明确涉密人员的权利、岗位责任和要求，对涉密人员履行职责情况开展经常性的监督检查。

第四十五条 涉密人员出境应当经有关部门批准，有关机关认为涉密人员出境将对国家安全造成危害或者对国家利益造成重大损失的，不得批准出境。

第四十六条 涉密人员离岗离职应当遵守国家保密规定。机关、单位应当开展保密教育提醒，清退国家秘密载体，实行脱密期管理。涉密人员在脱密期内，不得违反规定就业和出境，不得以任何方式泄露国家秘密；脱密期结束后，应当遵守国家保密规定，对知悉的国家秘密继续履行保密义务。涉密人员严重违反离岗离职及脱密期国家保密规定的，机关、单位应当及时报告同级保密行政管理部门，由保密行政管理部门会同有关部门依法采取处置措施。

第四十七条 国家工作人员或者其他公民发现国家秘密已经泄露或者可能泄露时，应当立即采取补救措施并及时报告有关机关、单位。机关、单位接到报告后，应当立即作出处理，并及时向保密行政管理部门报告。

第四章 监督管理

第四十八条 国家保密行政管理部门依照法律、行政法规的规定，制定保密

规章和国家保密标准。

第四十九条 保密行政管理部门依法组织开展保密宣传教育、保密检查、保密技术防护、保密违法案件调查处理工作，对保密工作进行指导和监督管理。

第五十条 保密行政管理部门发现国家秘密确定、变更或者解除不当的，应当及时通知有关机关、单位予以纠正。

第五十一条 保密行政管理部门依法对机关、单位遵守保密法律法规和相关制度的情况进行检查；涉嫌保密违法的，应当及时调查处理或者组织、督促有关机关、单位调查处理；涉嫌犯罪的，应当依法移送监察机关、司法机关处理。

对严重违反国家保密规定的涉密人员，保密行政管理部门应当建议有关机关、单位将其调离涉密岗位。

有关机关、单位和个人应当配合保密行政管理部门依法履行职责。

第五十二条 保密行政管理部门在保密检查和案件调查处理中，可以依法查阅有关材料、询问人员、记录情况，先行登记保存有关设施、设备、文件资料等；必要时，可以进行保密技术检测。

保密行政管理部门对保密检查和案件调查处理中发现的非法获取、持有的国家秘密载体，应当予以收缴；发现存在泄露国家秘密隐患的，应当要求采取措施，限期整改；对存在泄露国家秘密隐患的设施、设备、场所，应当责令停止使用。

第五十三条 办理涉嫌泄露国家秘密案件的机关，需要对有关事项是否属于国家秘密、属于何种密级进行鉴定的，由国家保密行政管理部门或者省、自治区、直辖市保密行政管理部门鉴定。

第五十四条 机关、单位对违反国家保密规定的人员不依法给予处分的，保密行政管理部门应当建议纠正；对拒不纠正的，提请其上一级机关或者监察机关对该机关、单位负有责任的领导人员和直接责任人员依法予以处理。

第五十五条 设区的市级以上保密行政管理部门建立保密风险评估机制、监测预警制度、应急处置制度，会同有关部门开展信息收集、分析、通报工作。

第五十六条 保密协会等行业组织依照法律、行政法规的规定开展活动，推动行业自律，促进行业健康发展。

第五章 法律责任

第五十七条 违反本法规定，有下列情形之一，根据情节轻重，依法给予处

分；有违法所得的，没收违法所得：

(一)非法获取、持有国家秘密载体的；

(二)买卖、转送或者私自销毁国家秘密载体的；

(三)通过普通邮政、快递等无保密措施的渠道传递国家秘密载体的；

(四)寄递、托运国家秘密载体出境， 或者未经有关主管部门批准，携带、传递国家秘密载体出境的；

(五)非法复制、记录、存储国家秘密的；

(六)在私人交往和通信中涉及国家秘密的；

(七)未按照国家保密规定和标准采取有效保密措施，在互联网及其他公共信息网络或者有线和无线通信中传递国家秘密的；

(八)未按照国家保密规定和标准采取有效保密措施，将涉密信息系统、涉密信息设备接入互联网及其他公共信息网络的；

(九)未按照国家保密规定和标准采取有效保密措施，在涉密信息系统、涉密信息设备与互联网及其他公共信息网络之间进行信息交换的；

(十)使用非涉密信息系统、非涉密信息设备存储、处理国家秘密的；

(十一)擅自卸载、修改涉密信息系统的安全技术程序、管理程序的；

(十二)将未经安全技术处理的退出使用的涉密信息设备赠送、出售、丢弃或者改作其他用途的；

(十三)其他违反本法规定的情形。

有前款情形尚不构成犯罪，且不适用处分的人员，由保密行政管理部门督促其所在机关、单位予以处理。

第五十八条 机关、单位违反本法规定，发生重大泄露国家秘密案件的，依法对直接负责的主管人员和其他直接责任人员给予处分。不适用处分的人员， 由保密行政管理部门督促其主管部门予以处理。

机关、单位违反本法规定， 对应当定密的事项不定密，对不应当定密的事项定密，或者未履行解密审核责任，造成严重后果的，依法对直接负责的主管人员和其他直接责任人员给予处分。

第五十九条 网络运营者违反本法第三十四条规定的， 由公安机关、国家安全机关、电信主管部门、保密行政管理部门按照各自职责分工依法予以处罚。

第六十条 取得保密资质的企业事业单位违反国家保密规定的，由保密行政管理部门责令限期整改，给予警告或者通报批评；有违法所得的，没收违法所得；情节严重的，暂停涉密业务、降低资质等级；情节特别严重的，吊销保密资质。

未取得保密资质的企业事业单位违法从事本法第四十一条第二款规定的涉密业务的，由保密行政管理部门责令停止涉密业务，给予警告或者通报批评；有违法所得的，没收违法所得。

第六十一条 保密行政管理部门的工作人员在履行保密管理职责中滥用职权、玩忽职守、徇私舞弊的，依法给予处分。

第六十二条 违反本法规定，构成犯罪的，依法追究刑事责任。

第六章 附 则

第六十三条 中国人民解放军和中国人民武装警察部队开展保密工作的具体规定，由中央军事委员会根据本法制定。

第六十四条 机关、单位对履行职能过程中产生或者获取的不属于国家秘密但泄露后会造成一定不利影响的事项，适用工作秘密管理办法采取必要的保护措施。工作秘密管理办法另行规定。

第六十五条 本法自 2024 年 5 月 1 日起施行。

中华人民共和国未成年人保护法

（1991 年 9 月 4 日第七届全国人民代表大会常务委员会第二十一次会议通过 2006 年 12 月 29 日第十届全国人民代表大会常务委员会第二十五次会议第一次修订 根据 2012 年 10 月 26 日第十一届全国人民代表大会常务委员会第二十九次会议《关于修改〈中华人民共和国未成年人保护法〉的决定》修正 2020 年 10 月 17 日第十三届全国人民代表大会常务委员会第二十二次会议第二次修订）

第一章 总 则

第一条 为了保护未成年人身心健康，保障未成年人合法权益，促进未成年人德智体美劳全面发展，培养有理想、有道德、有文化、有纪律的社会主义建设者和接班人，培养担当民族复兴大任的时代新人，根据宪法，制定本法。

第二条 本法所称未成年人是指未满十八周岁的公民。

第三条 国家保障未成年人的生存权、发展权、受保护权、参与权等权利。

未成年人依法平等地享有各项权利，不因本人及其父母或者其他监护人的民

族、种族、性别、户籍、职业、宗教信仰、教育程度、家庭状况、身心健康状况等受到歧视。

第四条 保护未成年人，应当坚持最有利于未成年人的原则。处理涉及未成年人事项，应当符合下列要求：

(一)给予未成年人特殊、优先保护；

(二)尊重未成年人人格尊严；

(三)保护未成年人隐私权和个人信息；

(四)适应未成年人身心健康发展的规律和特点；

(五)听取未成年人的意见；

(六)保护与教育相结合。

第五条 国家、社会、学校和家庭应当对未成年人进行理想教育、道德教育、科学教育、文化教育、法治教育、国家安全教育、健康教育、劳动教育，加强爱国主义、集体主义和中国特色社会主义的教育，培养爱祖国、爱人民、爱劳动、爱科学、爱社会主义的公德，抵制资本主义、封建主义和其他腐朽思想的侵蚀，引导未成年人树立和践行社会主义核心价值观。

第六条 保护未成年人，是国家机关、武装力量、政党、人民团体、企业事业单位、社会组织、城乡基层群众性自治组织、未成年人的监护人以及其他成年人的共同责任。

国家、社会、学校和家庭应当教育和帮助未成年人维护自身合法权益， 增强自我保护的意识和能力。

第七条 未成年人的父母或者其他监护人依法对未成年人承担监护职责。

国家采取措施指导、支持、帮助和监督未成年人的父母或者其他监护人履行监护职责。

第八条 县级以上人民政府应当将未成年人保护工作纳入国民经济和社会发展规划，相关经费纳入本级政府预算。

第九条 县级以上人民政府应当建立未成年人保护工作协调机制，统筹、协调、督促和指导有关部门在各自职责范围内做好未成年人保护工作。协调机制具体工作由县级以上人民政府民政部门承担，省级人民政府也可以根据本地实际情况确定由其他有关部门承担。

第十条 共产主义青年团、妇女联合会、工会、残疾人联合会、关心下一代工作委员会、青年联合会、学生联合会、少年先锋队以及其他人民团体、有关社会组织，应当协助各级人民政府及其有关部门、人民检察院、人民法院做好未成年人保护工作，维护未成年人合法权益。

第十一条 任何组织或者个人发现不利于未成年人身心健康或者侵犯未成年人合法权益的情形，都有权劝阻、制止或者向公安、民政、教育等有关部门提出检举、控告。

国家机关、居民委员会、村民委员会、密切接触未成年人的单位及其工作人员，在工作中发现未成年人身心健康受到侵害、疑似受到侵害或者面临其他危险情形的，应当立即向公安、民政、教育等有关部门报告。

有关部门接到涉及未成年人的检举、控告或者报告， 应当依法及时受理、处置，并以适当方式将处理结果告知相关单位和人员。

第十二条 国家鼓励和支持未成年人保护方面的科学研究，建设相关学科、设置相关专业，加强人才培养。

第十三条 国家建立健全未成年人统计调查制度，开展未成年人健康、受教育等状况的统计、调查和分析，发布未成年人保护的有关信息。

第十四条 国家对保护未成年人有显著成绩的组织和个人给予表彰和奖励。

第二章 家庭保护

第十五条 未成年人的父母或者其他监护人应当学习家庭教育知识，接受家庭教育指导，创造良好、和睦、文明的家庭环境。

共同生活的其他成年家庭成员应当协助未成年人的父母或者其他监护人抚养、教育和保护未成年人。

第十六条 未成年人的父母或者其他监护人应当履行下列监护职责：

(一)为未成年人提供生活、健康、安全等方面的保障；

(二)关注未成年人的生理、心理状况和情感需求；

(三)教育和引导未成年人遵纪守法、勤俭节约， 养成良好的思想品德和行为习惯；

(四)对未成年人进行安全教育，提高未成年人的自我保护意识和能力；

(五)尊重未成年人受教育的权利，保障适龄未成年人依法接受并完成义务教

育；

(六)保障未成年人休息、娱乐和体育锻炼的时间， 引导未成年人进行有益身心健康的活动；

(七)妥善管理和保护未成年人的财产；

(八)依法代理未成年人实施民事法律行为；

(九)预防和制止未成年人的不良行为和违法犯罪行为，并进行合理管教；

(十)其他应当履行的监护职责。

第十七条 未成年人的父母或者其他监护人不得实施下列行为：

(一)虐待、遗弃、非法送养未成年人或者对未成年人实施家庭暴力；

(二)放任、教唆或者利用未成年人实施违法犯罪行为；

(三)放任、唆使未成年人参与邪教、迷信活动或者接受恐怖主义、分裂主义、极端主义等侵害；

(四)放任、唆使未成年人吸烟(含电子烟，下同)、饮酒、赌博、流浪乞讨或者欺凌他人；

(五)放任或者迫使应当接受义务教育的未成年人失学、辍学；

(六)放任未成年人沉迷网络，接触危害或者可能影响其身心健康的图书、报刊、电影、广播电视节目、音像制品、电子出版物和网络信息等；

(七)放任未成年人进入营业性娱乐场所、酒吧、互联网上网服务营业场所等不适宜未成年人活动的场所；

(八)允许或者迫使未成年人从事国家规定以外的劳动；

(九)允许、迫使未成年人结婚或者为未成年人订立婚约；

(十)违法处分、侵吞未成年人的财产或者利用未成年人牟取不正当利益；

(十一)其他侵犯未成年人身心健康、财产权益或者不依法履行未成年人保护义务的行为。

第十八条 未成年人的父母或者其他监护人应当为未成年人提供安全的家庭生活环境，及时排除引发触电、烫伤、跌落等伤害的安全隐患； 采取配备儿童安全座椅、教育未成年人遵守交通规则等措施，防止未成年人受到交通事故的伤害；提高户外安全保护意识，避免未成年人发生溺水、动物伤害等事故。

第十九条 未成年人的父母或者其他监护人应当根据未成年人的年龄和智力

发展状况，在作出与未成年人权益有关的决定前，听取未成年人的意见，充分考虑其真实意愿。

第二十条 未成年人的父母或者其他监护人发现未成年人身心健康受到侵害、疑似受到侵害或者其他合法权益受到侵犯的，应当及时了解情况并采取保护措施；情况严重的，应当立即向公安、民政、教育等部门报告。

第二十一条 未成年人的父母或者其他监护人不得使未满八周岁或者由于身体、心理原因需要特别照顾的未成年人处于无人看护状态， 或者将其交由无民事行为能力、限制民事行为能力、患有严重传染性疾病或者其他不适宜的人员临时照护。

未成年人的父母或者其他监护人不得使未满十六周岁的未成年人脱离监护单独生活。

第二十二条 未成年人的父母或者其他监护人因外出务工等原因在一定期限内不能完全履行监护职责的，应当委托具有照护能力的完全民事行为能力人代为照护；无正当理由的，不得委托他人代为照护。

未成年人的父母或者其他监护人在确定被委托人时，应当综合考虑其道德品质、家庭状况、身心健康状况、与未成年人生活情感上的联系等情况， 并听取有表达意愿能力未成年人的意见。

具有下列情形之一的，不得作为被委托人：

(一)曾实施性侵害、虐待、遗弃、拐卖、暴力伤害等违法犯罪行为；

(二)有吸毒、酗酒、赌博等恶习；

(三)曾拒不履行或者长期怠于履行监护、照护职责；

(四)其他不适宜担任被委托人的情形。

第二十三条 未成年人的父母或者其他监护人应当及时将委托照护情况书面告知未成年人所在学校、幼儿园和实际居住地的居民委员会、村民委员会， 加强和未成年人所在学校、幼儿园的沟通； 与未成年人、被委托人至少每周联系和交流一次， 了解未成年人的生活、学习、心理等情况，并给予未成年人亲情关爱。

未成年人的父母或者其他监护人接到被委托人、居民委员会、村民委员会、学校、幼儿园等关于未成年人心理、行为异常的通知后，应当及时采取干预措施。

第二十四条 未成年人的父母离婚时，应当妥善处理未成年子女的抚养、教

育、探望、财产等事宜， 听取有表达意愿能力未成年人的意见。不得以抢夺、藏匿未成年子女等方式争夺抚养权。

未成年人的父母离婚后，不直接抚养未成年子女的一方应当依照协议、人民法院判决或者调解确定的时间和方式，在不影响未成年人学习、生活的情况下探望未成年子女，直接抚养的一方应当配合，但被人民法院依法中止探望权的除外。

第三章 学校保护

第二十五条 学校应当全面贯彻国家教育方针，坚持立德树人，实施素质教育，提高教育质量，注重培养未成年学生认知能力、合作能力、创新能力和实践能力，促进未成年学生全面发展。

学校应当建立未成年学生保护工作制度，健全学生行为规范，培养未成年学生遵纪守法的良好行为习惯。

第二十六条 幼儿园应当做好保育、教育工作，遵循幼儿身心发展规律，实施启蒙教育，促进幼儿在体质、智力、品德等方面和谐发展。

第二十七条 学校、幼儿园的教职员工应当尊重未成年人人格尊严，不得对未成年人实施体罚、变相体罚或者其他侮辱人格尊严的行为。

第二十八条 学校应当保障未成年学生受教育的权利，不得违反国家规定开除、变相开除未成年学生。

学校应当对尚未完成义务教育的辍学未成年学生进行登记并劝返复学；劝返无效的，应当及时向教育行政部门书面报告。

第二十九条 学校应当关心、爱护未成年学生，不得因家庭、身体、心理、学习能力等情况歧视学生。对家庭困难、身心有障碍的学生， 应当提供关爱；对行为异常、学习有困难的学生，应当耐心帮助。

学校应当配合政府有关部门建立留守未成年学生、困境未成年学生的信息档案，开展关爱帮扶工作。

第三十条 学校应当根据未成年学生身心发展特点，进行社会生活指导、心理健康辅导、青春期教育和生命教育。

第三十一条 学校应当组织未成年学生参加与其年龄相适应的日常生活劳动、生产劳动和服务性劳动，帮助未成年学生掌握必要的劳动知识和技能，养成良好的劳动习惯。

第三十二条 学校、幼儿园应当开展勤俭节约、反对浪费、珍惜粮食、文明饮食等宣传教育活动，帮助未成年人树立浪费可耻、节约为荣的意识， 养成文明健康、绿色环保的生活习惯。

第三十三条 学校应当与未成年学生的父母或者其他监护人互相配合，合理安排未成年学生的学习时间，保障其休息、娱乐和体育锻炼的时间。

学校不得占用国家法定节假日、休息日及寒暑假期， 组织义务教育阶段的未成年学生集体补课，加重其学习负担。

幼儿园、校外培训机构不得对学龄前未成年人进行小学课程教育。

第三十四条 学校、幼儿园应当提供必要的卫生保健条件，协助卫生健康部门做好在校、在园未成年人的卫生保健工作。

第三十五条 学校、幼儿园应当建立安全管理制度，对未成年人进行安全教育，完善安保设施、配备安保人员， 保障未成年人在校、在园期间的人身和财产安全。

学校、幼儿园不得在危及未成年人人身安全、身心健康的校舍和其他设施、场所中进行教育教学活动。

学校、幼儿园安排未成年人参加文化娱乐、社会实践等集体活动， 应当保护未成年人的身心健康，防止发生人身伤害事故。

第三十六条 使用校车的学校、幼儿园应当建立健全校车安全管理制度，配备安全管理人员，定期对校车进行安全检查，对校车驾驶人进行安全教育，并向未成年人讲解校车安全乘坐知识，培养未成年人校车安全事故应急处理技能。

第三十七条 学校、幼儿园应当根据需要，制定应对自然灾害、事故灾难、公共卫生事件等突发事件和意外伤害的预案，配备相应设施并定期进行必要的演练。

未成年人在校内、园内或者本校、本园组织的校外、园外活动中发生人身伤害事故的，学校、幼儿园应当立即救护， 妥善处理，及时通知未成年人的父母或者其他监护人，并向有关部门报告。

第三十八条 学校、幼儿园不得安排未成年人参加商业性活动，不得向未成年人及其父母或者其他监护人推销或者要求其购买指定的商品和服务。

学校、幼儿园不得与校外培训机构合作为未成年人提供有偿课程辅导。

第三十九条 学校应当建立学生欺凌防控工作制度，对教职员工、学生等开展防治学生欺凌的教育和培训。

学校对学生欺凌行为应当立即制止，通知实施欺凌和被欺凌未成年学生的父母或者其他监护人参与欺凌行为的认定和处理；对相关未成年学生及时给予心理辅导、教育和引导； 对相关未成年学生的父母或者其他监护人给予必要的家庭教育指导。

对实施欺凌的未成年学生，学校应当根据欺凌行为的性质和程度，依法加强管教。对严重的欺凌行为， 学校不得隐瞒，应当及时向公安机关、教育行政部门报告，并配合相关部门依法处理。

第四十条 学校、幼儿园应当建立预防性侵害、性骚扰未成年人工作制度。对性侵害、性骚扰未成年人等违法犯罪行为， 学校、幼儿园不得隐瞒， 应当及时向公安机关、教育行政部门报告，并配合相关部门依法处理。

学校、幼儿园应当对未成年人开展适合其年龄的性教育， 提高未成年人防范性侵害、性骚扰的自我保护意识和能力。对遭受性侵害、性骚扰的未成年人， 学校、幼儿园应当及时采取相关的保护措施。

第四十一条 婴幼儿照护服务机构、早期教育服务机构、校外培训机构、校外托管机构等应当参照本章有关规定，根据不同年龄阶段未成年人的成长特点和规律，做好未成年人保护工作。

第四章 社会保护

第四十二条 全社会应当树立关心、爱护未成年人的良好风尚。

国家鼓励、支持和引导人民团体、企业事业单位、社会组织以及其他组织和个人，开展有利于未成年人健康成长的社会活动和服务。

第四十三条 居民委员会、村民委员会应当设置专人专岗负责未成年人保护工作，协助政府有关部门宣传未成年人保护方面的法律法规，指导、帮助和监督未成年人的父母或者其他监护人依法履行监护职责，建立留守未成年人、困境未成年人的信息档案并给予关爱帮扶。

居民委员会、村民委员会应当协助政府有关部门监督未成年人委托照护情况，发现被委托人缺乏照护能力、怠于履行照护职责等情况， 应当及时向政府有关部门报告，并告知未成年人的父母或者其他监护人，帮助、督促被委托人履行照护

职责。

第四十四条 爱国主义教育基地、图书馆、青少年宫、儿童活动中心、儿童之家应当对未成年人免费开放；博物馆、纪念馆、科技馆、展览馆、美术馆、文化馆、社区公益性互联网上网服务场所以及影剧院、体育场馆、动物园、植物园、公园等场所，应当按照有关规定对未成年人免费或者优惠开放。

国家鼓励爱国主义教育基地、博物馆、科技馆、美术馆等公共场馆开设未成年人专场，为未成年人提供有针对性的服务。

国家鼓励国家机关、企业事业单位、部队等开发自身教育资源， 设立未成年人开放日，为未成年人主题教育、社会实践、职业体验等提供支持。

国家鼓励科研机构和科技类社会组织对未成年人开展科学普及活动。

第四十五条 城市公共交通以及公路、铁路、水路、航空客运等应当按照有关规定对未成年人实施免费或者优惠票价。

第四十六条 国家鼓励大型公共场所、公共交通工具、旅游景区景点等设置母婴室、婴儿护理台以及方便幼儿使用的坐便器、洗手台等卫生设施， 为未成年人提供便利。

第四十七条 任何组织或者个人不得违反有关规定，限制未成年人应当享有的照顾或者优惠。

第四十八条 国家鼓励创作、出版、制作和传播有利于未成年人健康成长的图书、报刊、电影、广播电视节目、舞台艺术作品、音像制品、电子出版物和网络信息等。

第四十九条 新闻媒体应当加强未成年人保护方面的宣传，对侵犯未成年人合法权益的行为进行舆论监督。新闻媒体采访报道涉及未成年人事件应当客观、审慎和适度，不得侵犯未成年人的名誉、隐私和其他合法权益。

第五十条 禁止制作、复制、出版、发布、传播含有宣扬淫秽、色情、暴力、邪教、迷信、赌博、引诱自杀、恐怖主义、分裂主义、极端主义等危害未成年人身心健康内容的图书、报刊、电影、广播电视节目、舞台艺术作品、音像制品、电子出版物和网络信息等。

第五十一条 任何组织或者个人出版、发布、传播的图书、报刊、电影、广播电视节目、舞台艺术作品、音像制品、电子出版物或者网络信息， 包含可能影

响未成年人身心健康内容的，应当以显著方式作出提示。

第五十二条 禁止制作、复制、发布、传播或者持有有关未成年人的淫秽色情物品和网络信息。

第五十三条 任何组织或者个人不得刊登、播放、张贴或者散发含有危害未成年人身心健康内容的广告；不得在学校、幼儿园播放、张贴或者散发商业广告；不得利用校服、教材等发布或者变相发布商业广告。

第五十四条 禁止拐卖、绑架、虐待、非法收养未成年人，禁止对未成年人实施性侵害、性骚扰。

禁止胁迫、引诱、教唆未成年人参加黑社会性质组织或者从事违法犯罪活动。

禁止胁迫、诱骗、利用未成年人乞讨。

第五十五条 生产、销售用于未成年人的食品、药品、玩具、用具和游戏游艺设备、游乐设施等， 应当符合国家或者行业标准，不得危害未成年人的人身安全和身心健康。上述产品的生产者应当在显著位置标明注意事项， 未标明注意事项的不得销售。

第五十六条 未成年人集中活动的公共场所应当符合国家或者行业安全标准，并采取相应安全保护措施。对可能存在安全风险的设施， 应当定期进行维护，在显著位置设置安全警示标志并标明适龄范围和注意事项；必要时应当安排专门人员看管。

大型的商场、超市、医院、图书馆、博物馆、科技馆、游乐场、车站、码头、机场、旅游景区景点等场所运营单位应当设置搜寻走失未成年人的安全警报系统。场所运营单位接到求助后，应当立即启动安全警报系统，组织人员进行搜寻并向公安机关报告。

公共场所发生突发事件时，应当优先救护未成年人。

第五十七条 旅馆、宾馆、酒店等住宿经营者接待未成年人入住，或者接待未成年人和成年人共同入住时，应当询问父母或者其他监护人的联系方式、入住人员的身份关系等有关情况；发现有违法犯罪嫌疑的，应当立即向公安机关报告，并及时联系未成年人的父母或者其他监护人。

第五十八条 学校、幼儿园周边不得设置营业性娱乐场所、酒吧、互联网上网服务营业场所等不适宜未成年人活动的场所。营业性歌舞娱乐场所、酒吧、互

联网上网服务营业场所等不适宜未成年人活动场所的经营者，不得允许未成年人进入；游艺娱乐场所设置的电子游戏设备，除国家法定节假日外，不得向未成年人提供。经营者应当在显著位置设置未成年人禁入、限入标志； 对难以判明是否是未成年人的，应当要求其出示身份证件。

第五十九条 学校、幼儿园周边不得设置烟、酒、彩票销售网点。禁止向未成年人销售烟、酒、彩票或者兑付彩票奖金。烟、酒和彩票经营者应当在显著位置设置不向未成年人销售烟、酒或者彩票的标志；对难以判明是否是未成年人的，应当要求其出示身份证件。

任何人不得在学校、幼儿园和其他未成年人集中活动的公共场所吸烟、饮酒。

第六十条 禁止向未成年人提供、销售管制刀具或者其他可能致人严重伤害的器具等物品。经营者难以判明购买者是否是未成年人的， 应当要求其出示身份证件。

第六十一条 任何组织或者个人不得招用未满十六周岁未成年人，国家另有规定的除外。

营业性娱乐场所、酒吧、互联网上网服务营业场所等不适宜未成年人活动的场所不得招用已满十六周岁的未成年人。

招用已满十六周岁未成年人的单位和个人应当执行国家在工种、劳动时间、劳动强度和保护措施等方面的规定，不得安排其从事过重、有毒、有害等危害未成年人身心健康的劳动或者危险作业。

任何组织或者个人不得组织未成年人进行危害其身心健康的表演等活动。经未成年人的父母或者其他监护人同意，未成年人参与演出、节目制作等活动， 活动组织方应当根据国家有关规定，保障未成年人合法权益。

第六十二条 密切接触未成年人的单位招聘工作人员时，应当向公安机关、人民检察院查询应聘者是否具有性侵害、虐待、拐卖、暴力伤害等违法犯罪记录；发现其具有前述行为记录的，不得录用。

密切接触未成年人的单位应当每年定期对工作人员是否具有上述违法犯罪记录进行查询。通过查询或者其他方式发现其工作人员具有上述行为的， 应当及时解聘。

第六十三条 任何组织或者个人不得隐匿、毁弃、非法删除未成年人的信件、

日记、电子邮件或者其他网络通讯内容。

除下列情形外，任何组织或者个人不得开拆、查阅未成年人的信件、日记、电子邮件或者其他网络通讯内容：

(一)无民事行为能力未成年人的父母或者其他监护人代未成年人开拆、查阅；

(二)因国家安全或者追查刑事犯罪依法进行检查；

(三)紧急情况下为了保护未成年人本人的人身安全。

第五章　网络保护

第六十四条　国家、社会、学校和家庭应当加强未成年人网络素养宣传教育，培养和提高未成年人的网络素养，增强未成年人科学、文明、安全、合理使用网络的意识和能力，保障未成年人在网络空间的合法权益。

第六十五条　国家鼓励和支持有利于未成年人健康成长的网络内容的创作与传播，鼓励和支持专门以未成年人为服务对象、适合未成年人身心健康特点的网络技术、产品、服务的研发、生产和使用。

第六十六条　网信部门及其他有关部门应当加强对未成年人网络保护工作的监督检查，依法惩处利用网络从事危害未成年人身心健康的活动，为未成年人提供安全、健康的网络环境。

第六十七条　网信部门会同公安、文化和旅游、新闻出版、电影、广播电视等部门根据保护不同年龄阶段未成年人的需要，确定可能影响未成年人身心健康网络信息的种类、范围和判断标准。

第六十八条 新闻出版、教育、卫生健康、文化和旅游、网信等部门应当定期开展预防未成年人沉迷网络的宣传教育，监督网络产品和服务提供者履行预防未成年人沉迷网络的义务，指导家庭、学校、社会组织互相配合，　采取科学、合理的方式对未成年人沉迷网络进行预防和干预。

任何组织或者个人不得以侵害未成年人身心健康的方式对未成年人沉迷网络进行干预。

第六十九条 学校、社区、图书馆、文化馆、青少年宫等场所为未成年人提供的互联网上网服务设施，应当安装未成年人网络保护软件或者采取其他安全保护技术措施。

智能终端产品的制造者、销售者应当在产品上安装未成年人网络保护软件，

或者以显著方式告知用户未成年人网络保护软件的安装渠道和方法。

第七十条 学校应当合理使用网络开展教学活动。未经学校允许，未成年学生不得将手机等智能终端产品带入课堂，带入学校的应当统一管理。

学校发现未成年学生沉迷网络的，应当及时告知其父母或者其他监护人，共同对未成年学生进行教育和引导，帮助其恢复正常的学习生活。

第七十一条 未成年人的父母或者其他监护人应当提高网络素养，规范自身使用网络的行为，加强对未成年人使用网络行为的引导和监督。

未成年人的父母或者其他监护人应当通过在智能终端产品上安装未成年人网络保护软件、选择适合未成年人的服务模式和管理功能等方式， 避免未成年人接触危害或者可能影响其身心健康的网络信息，合理安排未成年人使用网络的时间，有效预防未成年人沉迷网络。

第七十二条 信息处理者通过网络处理未成年人个人信息的，应当遵循合法、正当和必要的原则。处理不满十四周岁未成年人个人信息的， 应当征得未成年人的父母或者其他监护人同意，但法律、行政法规另有规定的除外。

未成年人、父母或者其他监护人要求信息处理者更正、删除未成年人个人信息的，信息处理者应当及时采取措施予以更正、删除， 但法律、行政法规另有规定的除外。

第七十三条 网络服务提供者发现未成年人通过网络发布私密信息的，应当及时提示，并采取必要的保护措施。

第七十四条 网络产品和服务提供者不得向未成年人提供诱导其沉迷的产品和服务。

网络游戏、网络直播、网络音视频、网络社交等网络服务提供者应当针对未成年人使用其服务设置相应的时间管理、权限管理、消费管理等功能。

以未成年人为服务对象的在线教育网络产品和服务，不得插入网络游戏链接，不得推送广告等与教学无关的信息。

第七十五条 网络游戏经依法审批后方可运营。

国家建立统一的未成年人网络游戏电子身份认证系统。网络游戏服务提供者应当要求未成年人以真实身份信息注册并登录网络游戏。

网络游戏服务提供者应当按照国家有关规定和标准，对游戏产品进行分类，

作出适龄提示，并采取技术措施，不得让未成年人接触不适宜的游戏或者游戏功能。

网络游戏服务提供者不得在每日二十二时至次日八时向未成年人提供网络游戏服务。

第七十六条 网络直播服务提供者不得为未满十六周岁的未成年人提供网络直播发布者账号注册服务；为年满十六周岁的未成年人提供网络直播发布者账号注册服务时，应当对其身份信息进行认证，并征得其父母或者其他监护人同意。

第七十七条 任何组织或者个人不得通过网络以文字、图片、音视频等形式，对未成年人实施侮辱、诽谤、威胁或者恶意损害形象等网络欺凌行为。

遭受网络欺凌的未成年人及其父母或者其他监护人有权通知网络服务提供者采取删除、屏蔽、断开链接等措施。网络服务提供者接到通知后， 应当及时采取必要的措施制止网络欺凌行为，防止信息扩散。

第七十八条 网络产品和服务提供者应当建立便捷、合理、有效的投诉和举报渠道，公开投诉、举报方式等信息， 及时受理并处理涉及未成年人的投诉、举报。

第七十九条 任何组织或者个人发现网络产品、服务含有危害未成年人身心健康的信息，有权向网络产品和服务提供者或者网信、公安等部门投诉、举报。

第八十条 网络服务提供者发现用户发布、传播可能影响未成年人身心健康的信息且未作显著提示的，应当作出提示或者通知用户予以提示；未作出提示的，不得传输相关信息。

网络服务提供者发现用户发布、传播含有危害未成年人身心健康内容的信息的，应当立即停止传输相关信息，采取删除、屏蔽、断开链接等处置措施， 保存有关记录，并向网信、公安等部门报告。

网络服务提供者发现用户利用其网络服务对未成年人实施违法犯罪行为的，应当立即停止向该用户提供网络服务，保存有关记录，并向公安机关报告。

第六章 政府保护

第八十一条 县级以上人民政府承担未成年人保护协调机制具体工作的职能部门应当明确相关内设机构或者专门人员，负责承担未成年人保护工作。

乡镇人民政府和街道办事处应当设立未成年人保护工作站或者指定专门人

员，及时办理未成年人相关事务；支持、指导居民委员会、村民委员会设立专人专岗，做好未成年人保护工作。

第八十二条 各级人民政府应当将家庭教育指导服务纳入城乡公共服务体系，开展家庭教育知识宣传，鼓励和支持有关人民团体、企业事业单位、社会组织开展家庭教育指导服务。

第八十三条 各级人民政府应当保障未成年人受教育的权利，并采取措施保障留守未成年人、困境未成年人、残疾未成年人接受义务教育。

对尚未完成义务教育的辍学未成年学生，教育行政部门应当责令父母或者其他监护人将其送入学校接受义务教育。

第八十四条 各级人民政府应当发展托育、学前教育事业，办好婴幼儿照护服务机构、幼儿园， 支持社会力量依法兴办母婴室、婴幼儿照护服务机构、幼儿园。

县级以上地方人民政府及其有关部门应当培养和培训婴幼儿照护服务机构、幼儿园的保教人员，提高其职业道德素质和业务能力。

第八十五条 各级人民政府应当发展职业教育，保障未成年人接受职业教育或者职业技能培训，鼓励和支持人民团体、企业事业单位、社会组织为未成年人提供职业技能培训服务。

第八十六条 各级人民政府应当保障具有接受普通教育能力、能适应校园生活的残疾未成年人就近在普通学校、幼儿园接受教育； 保障不具有接受普通教育能力的残疾未成年人在特殊教育学校、幼儿园接受学前教育、义务教育和职业教育。

各级人民政府应当保障特殊教育学校、幼儿园的办学、办园条件， 鼓励和支持社会力量举办特殊教育学校、幼儿园。

第八十七条 地方人民政府及其有关部门应当保障校园安全，监督、指导学校、幼儿园等单位落实校园安全责任，建立突发事件的报告、处置和协调机制。

第八十八条 公安机关和其他有关部门应当依法维护校园周边的治安和交通秩序，设置监控设备和交通安全设施，预防和制止侵害未成年人的违法犯罪行为。

第八十九条 地方人民政府应当建立和改善适合未成年人的活动场所和设施，支持公益性未成年人活动场所和设施的建设和运行，鼓励社会力量兴办适合未成

年人的活动场所和设施，并加强管理。

地方人民政府应当采取措施，鼓励和支持学校在国家法定节假日、休息日及寒暑假期将文化体育设施对未成年人免费或者优惠开放。

地方人民政府应当采取措施，防止任何组织或者个人侵占、破坏学校、幼儿园、婴幼儿照护服务机构等未成年人活动场所的场地、房屋和设施。

第九十条 各级人民政府及其有关部门应当对未成年人进行卫生保健和营养指导，提供卫生保健服务。

卫生健康部门应当依法对未成年人的疫苗预防接种进行规范，防治未成年人常见病、多发病， 加强传染病防治和监督管理，做好伤害预防和干预，指导和监督学校、幼儿园、婴幼儿照护服务机构开展卫生保健工作。

教育行政部门应当加强未成年人的心理健康教育，建立未成年人心理问题的早期发现和及时干预机制。卫生健康部门应当做好未成年人心理治疗、心理危机干预以及精神障碍早期识别和诊断治疗等工作。

第九十一条 各级人民政府及其有关部门对困境未成年人实施分类保障，采取措施满足其生活、教育、安全、医疗康复、住房等方面的基本需要。

第九十二条 具有下列情形之一的，民政部门应当依法对未成年人进行临时监护：

(一)未成年人流浪乞讨或者身份不明，暂时查找不到父母或者其他监护人；

(二)监护人下落不明且无其他人可以担任监护人；

(三)监护人因自身客观原因或者因发生自然灾害、事故灾难、公共卫生事件等突发事件不能履行监护职责，导致未成年人监护缺失；

(四)监护人拒绝或者怠于履行监护职责，导致未成年人处于无人照料的状态；

(五)监护人教唆、利用未成年人实施违法犯罪行为， 未成年人需要被带离安置；

(六)未成年人遭受监护人严重伤害或者面临人身安全威胁，需要被紧急安置；

(七)法律规定的其他情形。

第九十三条 对临时监护的未成年人， 民政部门可以采取委托亲属抚养、家庭寄养等方式进行安置，也可以交由未成年人救助保护机构或者儿童福利机构进行收留、抚养。

临时监护期间，经民政部门评估，监护人重新具备履行监护职责条件的，民政部门可以将未成年人送回监护人抚养。

第九十四条 具有下列情形之一的，民政部门应当依法对未成年人进行长期监护：

(一)查找不到未成年人的父母或者其他监护人；

(二)监护人死亡或者被宣告死亡且无其他人可以担任监护人；

(三)监护人丧失监护能力且无其他人可以担任监护人；

(四)人民法院判决撤销监护人资格并指定由民政部门担任监护人；

(五)法律规定的其他情形。

第九十五条 民政部门进行收养评估后，可以依法将其长期监护的未成年人交由符合条件的申请人收养。收养关系成立后， 民政部门与未成年人的监护关系终止。

第九十六条 民政部门承担临时监护或者长期监护职责的，财政、教育、卫生健康、公安等部门应当根据各自职责予以配合。

县级以上人民政府及其民政部门应当根据需要设立未成年人救助保护机构、儿童福利机构，负责收留、抚养由民政部门监护的未成年人。

第九十七条 县级以上人民政府应当开通全国统一的未成年人保护热线，及时受理、转介侵犯未成年人合法权益的投诉、举报； 鼓励和支持人民团体、企业事业单位、社会组织参与建设未成年人保护服务平台、服务热线、服务站点， 提供未成年人保护方面的咨询、帮助。

第九十八条 国家建立性侵害、虐待、拐卖、暴力伤害等违法犯罪人员信息查询系统，向密切接触未成年人的单位提供免费查询服务。

第九十九条 地方人民政府应当培育、引导和规范有关社会组织、社会工作者参与未成年人保护工作，开展家庭教育指导服务，为未成年人的心理辅导、康复救助、监护及收养评估等提供专业服务。

第七章 司法保护

第一百条 公安机关、人民检察院、人民法院和司法行政部门应当依法履行职责，保障未成年人合法权益。

第一百零一条 公安机关、人民检察院、人民法院和司法行政部门应当确定

专门机构或者指定专门人员，负责办理涉及未成年人案件。办理涉及未成年人案件的人员应当经过专门培训，熟悉未成年人身心特点。专门机构或者专门人员中，应当有女性工作人员。

公安机关、人民检察院、人民法院和司法行政部门应当对上述机构和人员实行与未成年人保护工作相适应的评价考核标准。

第一百零二条 公安机关、人民检察院、人民法院和司法行政部门办理涉及未成年人案件，应当考虑未成年人身心特点和健康成长的需要，使用未成年人能够理解的语言和表达方式，听取未成年人的意见。

第一百零三条 公安机关、人民检察院、人民法院、司法行政部门以及其他组织和个人不得披露有关案件中未成年人的姓名、影像、住所、就读学校以及其他可能识别出其身份的信息，但查找失踪、被拐卖未成年人等情形除外。

第一百零四条 对需要法律援助或者司法救助的未成年人，法律援助机构或者公安机关、人民检察院、人民法院和司法行政部门应当给予帮助， 依法为其提供法律援助或者司法救助。

法律援助机构应当指派熟悉未成年人身心特点的律师为未成年人提供法律援助服务。

法律援助机构和律师协会应当对办理未成年人法律援助案件的律师进行指导和培训。

第一百零五条 人民检察院通过行使检察权，对涉及未成年人的诉讼活动等依法进行监督。

第一百零六条 未成年人合法权益受到侵犯，相关组织和个人未代为提起诉讼的，人民检察院可以督促、支持其提起诉讼； 涉及公共利益的，人民检察院有权提起公益诉讼。

第一百零七条 人民法院审理继承案件，应当依法保护未成年人的继承权和受遗赠权。

人民法院审理离婚案件，涉及未成年子女抚养问题的，应当尊重已满八周岁未成年子女的真实意愿，根据双方具体情况，按照最有利于未成年子女的原则依法处理。

第一百零八条 未成年人的父母或者其他监护人不依法履行监护职责或者严

重侵犯被监护的未成年人合法权益的，人民法院可以根据有关人员或者单位的申请，依法作出人身安全保护令或者撤销监护人资格。

被撤销监护人资格的父母或者其他监护人应当依法继续负担抚养费用。

第一百零九条 人民法院审理离婚、抚养、收养、监护、探望等案件涉及未成年人的，可以自行或者委托社会组织对未成年人的相关情况进行社会调查。

第一百一十条 公安机关、人民检察院、人民法院讯问未成年犯罪嫌疑人、被告人，询问未成年被害人、证人，应当依法通知其法定代理人或者其成年亲属、所在学校的代表等合适成年人到场，并采取适当方式，在适当场所进行，保障未成年人的名誉权、隐私权和其他合法权益。

人民法院开庭审理涉及未成年人案件，未成年被害人、证人一般不出庭作证；必须出庭的，应当采取保护其隐私的技术手段和心理干预等保护措施。

第一百一十一条 公安机关、人民检察院、人民法院应当与其他有关政府部门、人民团体、社会组织互相配合， 对遭受性侵害或者暴力伤害的未成年被害人及其家庭实施必要的心理干预、经济救助、法律援助、转学安置等保护措施。

第一百一十二条 公安机关、人民检察院、人民法院办理未成年人遭受性侵害或者暴力伤害案件，在询问未成年被害人、证人时， 应当采取同步录音录像等措施，尽量一次完成；未成年被害人、证人是女性的，应当由女性工作人员进行。

第一百一十三条 对违法犯罪的未成年人，实行教育、感化、挽救的方针，坚持教育为主、惩罚为辅的原则。

对违法犯罪的未成年人依法处罚后，在升学、就业等方面不得歧视。

第一百一十四条 公安机关、人民检察院、人民法院和司法行政部门发现有关单位未尽到未成年人教育、管理、救助、看护等保护职责的，应当向该单位提出建议。被建议单位应当在一个月内作出书面回复。

第一百一十五条 公安机关、人民检察院、人民法院和司法行政部门应当结合实际，根据涉及未成年人案件的特点，开展未成年人法治宣传教育工作。

第一百一十六条 国家鼓励和支持社会组织、社会工作者参与涉及未成年人案件中未成年人的心理干预、法律援助、社会调查、社会观护、教育矫治、社区矫正等工作。

第八章 法律责任

第一百一十七条 违反本法第十一条第二款规定，未履行报告义务造成严重后果的，由上级主管部门或者所在单位对直接负责的主管人员和其他直接责任人员依法给予处分。

第一百一十八条 未成年人的父母或者其他监护人不依法履行监护职责或者侵犯未成年人合法权益的，由其居住地的居民委员会、村民委员会予以劝诫、制止；情节严重的，居民委员会、村民委员会应当及时向公安机关报告。

公安机关接到报告或者公安机关、人民检察院、人民法院在办理案件过程中发现未成年人的父母或者其他监护人存在上述情形的，应当予以训诫，并可以责令其接受家庭教育指导。

第一百一十九条 学校、幼儿园、婴幼儿照护服务等机构及其教职员工违反本法第二十七条、第二十八条、第三十九条规定的，由公安、教育、卫生健康、市场监督管理等部门按照职责分工责令改正；拒不改正或者情节严重的，对直接负责的主管人员和其他直接责任人员依法给予处分。

第一百二十条 违反本法第四十四条、第四十五条、第四十七条规定，未给予未成年人免费或者优惠待遇的，由市场监督管理、文化和旅游、交通运输等部门按照职责分工责令限期改正，给予警告；拒不改正的，处一万元以上十万元以下罚款。

第一百二十一条 违反本法第五十条、第五十一条规定的，由新闻出版、广播电视、电影、网信等部门按照职责分工责令限期改正， 给予警告，没收违法所得，可以并处十万元以下罚款；拒不改正或者情节严重的，责令暂停相关业务、停产停业或者吊销营业执照、吊销相关许可证， 违法所得一百万元以上的，并处违法所得一倍以上十倍以下的罚款，没有违法所得或者违法所得不足一百万元的，并处十万元以上一百万元以下罚款。

第一百二十二条 场所运营单位违反本法第五十六条第二款规定、住宿经营者违反本法第五十七条规定的，由市场监督管理、应急管理、公安等部门按照职责分工责令限期改正，给予警告；拒不改正或者造成严重后果的，责令停业整顿或者吊销营业执照、吊销相关许可证，并处一万元以上十万元以下罚款。

第一百二十三条 相关经营者违反本法第五十八条、第五十九条第一款、第六十条规定的，由文化和旅游、市场监督管理、烟草专卖、公安等部门按照职责

分工责令限期改正，给予警告，没收违法所得，可以并处五万元以下罚款；拒不改正或者情节严重的，责令停业整顿或者吊销营业执照、吊销相关许可证， 可以并处五万元以上五十万元以下罚款。

第一百二十四条 违反本法第五十九条第二款规定，在学校、幼儿园和其他未成年人集中活动的公共场所吸烟、饮酒的， 由卫生健康、教育、市场监督管理等部门按照职责分工责令改正，给予警告，可以并处五百元以下罚款；场所管理者未及时制止的，由卫生健康、教育、市场监督管理等部门按照职责分工给予警告，并处一万元以下罚款。

第一百二十五条 违反本法第六十一条规定的，由文化和旅游、人力资源和社会保障、市场监督管理等部门按照职责分工责令限期改正， 给予警告，没收违法所得，可以并处十万元以下罚款；拒不改正或者情节严重的，责令停产停业或者吊销营业执照、吊销相关许可证，并处十万元以上一百万元以下罚款。

第一百二十六条 密切接触未成年人的单位违反本法第六十二条规定，未履行查询义务，或者招用、继续聘用具有相关违法犯罪记录人员的， 由教育、人力资源和社会保障、市场监督管理等部门按照职责分工责令限期改正，给予警告，并处五万元以下罚款；拒不改正或者造成严重后果的，责令停业整顿或者吊销营业执照、吊销相关许可证， 并处五万元以上五十万元以下罚款，对直接负责的主管人员和其他直接责任人员依法给予处分。

第一百二十七条 信息处理者违反本法第七十二条规定，或者网络产品和服务提供者违反本法第七十三条、第七十四条、第七十五条、第七十六条、第七十七条、第八十条规定的， 由公安、网信、电信、新闻出版、广播电视、文化和旅游等有关部门按照职责分工责令改正，给予警告，没收违法所得，违法所得一百万元以上的，并处违法所得一倍以上十倍以下罚款，没有违法所得或者违法所得不足一百万元的，并处十万元以上一百万元以下罚款，对直接负责的主管人员和其他责任人员处一万元以上十万元以下罚款；拒不改正或者情节严重的，并可以责令暂停相关业务、停业整顿、关闭网站、吊销营业执照或者吊销相关许可证。

第一百二十八条 国家机关工作人员玩忽职守、滥用职权、徇私舞弊，损害未成年人合法权益的，依法给予处分。

第一百二十九条 违反本法规定，侵犯未成年人合法权益，造成人身、财产

或者其他损害的，依法承担民事责任。

违反本法规定，构成违反治安管理行为的，依法给予治安管理处罚；构成犯罪的，依法追究刑事责任。

第九章 附 则

第一百三十条 本法中下列用语的含义：

(一)密切接触未成年人的单位，是指学校、幼儿园等教育机构； 校外培训机构；未成年人救助保护机构、儿童福利机构等未成年人安置、救助机构； 婴幼儿照护服务机构、早期教育服务机构；校外托管、临时看护机构；家政服务机构；为未成年人提供医疗服务的医疗机构；其他对未成年人负有教育、培训、监护、救助、看护、医疗等职责的企业事业单位、社会组织等。

(二)学校，是指普通中小学、特殊教育学校、中等职业学校、专门学校。

(三)学生欺凌，是指发生在学生之间，一方蓄意或者恶意通过肢体、语言及网络等手段实施欺压、侮辱， 造成另一方人身伤害、财产损失或者精神损害的行为。

第一百三十一条 对中国境内未满十八周岁的外国人、无国籍人，依照本法有关规定予以保护。

第一百三十二条 本法自 2021 年 6 月 1 日起施行。

中华人民共和国消费者权益保护法

(1993 年 10 月 31 日第八届全国人民代表大会常务委员会第四次会议通过 根据 2009 年 8 月 27 日第十一届全国人民代表大会常务委员会第十次会议《关于修改部分法律的决定》第一次修正 根据 2013 年 10 月 25 日第十二届全国人民代表大会常务委员会第五次会议《关于修改〈中华人民共和国消费者权益保护法〉的决定》第二次修正)

第一章 总 则

第一条 为保护消费者的合法权益，维护社会经济秩序，促进社会主义市场经济健康发展，制定本法。

第二条 消费者为生活消费需要购买、使用商品或者接受服务，其权益受本法保护；本法未作规定的，受其他有关法律、法规保护。

第三条 经营者为消费者提供其生产、销售的商品或者提供服务，应当遵守

本法；本法未作规定的，应当遵守其他有关法律、法规。

第四条 经营者与消费者进行交易，应当遵循自愿、平等、公平、诚实信用的原则。

第五条 国家保护消费者的合法权益不受侵害。

国家采取措施，保障消费者依法行使权利，维护消费者的合法权益。

国家倡导文明、健康、节约资源和保护环境的消费方式，反对浪费。

第六条 保护消费者的合法权益是全社会的共同责任。

国家鼓励、支持一切组织和个人对损害消费者合法权益的行为进行社会监督。

大众传播媒介应当做好维护消费者合法权益的宣传，对损害消费者合法权益的行为进行舆论监督。

第二章 消费者的权利

第七条 消费者在购买、使用商品和接受服务时享有人身、财产安全不受损害的权利。

消费者有权要求经营者提供的商品和服务，符合保障人身、财产安全的要求。

第八条 消费者享有知悉其购买、使用的商品或者接受的服务的真实情况的权利。

消费者有权根据商品或者服务的不同情况，要求经营者提供商品的价格、产地、生产者、用途、性能、规格、等级、主要成份、生产日期、有效期限、检验合格证明、使用方法说明书、售后服务， 或者服务的内容、规格、费用等有关情况。

第九条 消费者享有自主选择商品或者服务的权利。

消费者有权自主选择提供商品或者服务的经营者，自主选择商品品种或者服务方式，自主决定购买或者不购买任何一种商品、接受或者不接受任何一项服务。

消费者在自主选择商品或者服务时，有权进行比较、鉴别和挑选。

第十条 消费者享有公平交易的权利。

消费者在购买商品或者接受服务时，有权获得质量保障、价格合理、计量正确等公平交易条件，有权拒绝经营者的强制交易行为。

第十一条 消费者因购买、使用商品或者接受服务受到人身、财产损害的，享有依法获得赔偿的权利。

第十二条 消费者享有依法成立维护自身合法权益的社会组织的权利。

第十三条 消费者享有获得有关消费和消费者权益保护方面的知识的权利。

消费者应当努力掌握所需商品或者服务的知识和使用技能，正确使用商品，提高自我保护意识。

第十四条 消费者在购买、使用商品和接受服务时，享有人格尊严、民族风俗习惯得到尊重的权利，享有个人信息依法得到保护的权利。

第十五条 消费者享有对商品和服务以及保护消费者权益工作进行监督的权利。

消费者有权检举、控告侵害消费者权益的行为和国家机关及其工作人员在保护消费者权益工作中的违法失职行为，有权对保护消费者权益工作提出批评、建议。

第三章 经营者的义务

第十六条 经营者向消费者提供商品或者服务，应当依照本法和其他有关法律、法规的规定履行义务。

经营者和消费者有约定的，应当按照约定履行义务，但双方的约定不得违背法律、法规的规定。

经营者向消费者提供商品或者服务，应当恪守社会公德，诚信经营，保障消费者的合法权益；不得设定不公平、不合理的交易条件，不得强制交易。

第十七条 经营者应当听取消费者对其提供的商品或者服务的意见，接受消费者的监督。

第十八条 经营者应当保证其提供的商品或者服务符合保障人身、财产安全的要求。对可能危及人身、财产安全的商品和服务， 应当向消费者作出真实的说明和明确的警示，并说明和标明正确使用商品或者接受服务的方法以及防止危害发生的方法。

宾馆、商场、餐馆、银行、机场、车站、港口、影剧院等经营场所的经营者，应当对消费者尽到安全保障义务。

第十九条 经营者发现其提供的商品或者服务存在缺陷，有危及人身、财产安全危险的，应当立即向有关行政部门报告和告知消费者，并采取停止销售、警示、召回、无害化处理、销毁、停止生产或者服务等措施。采取召回措施的，经

营者应当承担消费者因商品被召回支出的必要费用。

第二十条 经营者向消费者提供有关商品或者服务的质量、性能、用途、有效期限等信息，应当真实、全面，不得作虚假或者引人误解的宣传。

经营者对消费者就其提供的商品或者服务的质量和使用方法等问题提出的询问，应当作出真实、明确的答复。

经营者提供商品或者服务应当明码标价。

第二十一条 经营者应当标明其真实名称和标记。

租赁他人柜台或者场地的经营者，应当标明其真实名称和标记。

第二十二条 经营者提供商品或者服务，应当按照国家有关规定或者商业惯例向消费者出具发票等购货凭证或者服务单据；消费者索要发票等购货凭证或者服务单据的，经营者必须出具。

第二十三条 经营者应当保证在正常使用商品或者接受服务的情况下其提供的商品或者服务应当具有的质量、性能、用途和有效期限； 但消费者在购买该商品或者接受该服务前已经知道其存在瑕疵，且存在该瑕疵不违反法律强制性规定的除外。

经营者以广告、产品说明、实物样品或者其他方式表明商品或者服务的质量状况的，应当保证其提供的商品或者服务的实际质量与表明的质量状况相符。

经营者提供的机动车、计算机、电视机、电冰箱、空调器、洗衣机等耐用商品或者装饰装修等服务，消费者自接受商品或者服务之日起六个月内发现瑕疵，发生争议的，由经营者承担有关瑕疵的举证责任。

第二十四条 经营者提供的商品或者服务不符合质量要求的，消费者可以依照国家规定、当事人约定退货， 或者要求经营者履行更换、修理等义务。没有国家规定和当事人约定的，消费者可以自收到商品之日起七日内退货；七日后符合法定解除合同条件的，消费者可以及时退货，不符合法定解除合同条件的，可以要求经营者履行更换、修理等义务。

依照前款规定进行退货、更换、修理的，经营者应当承担运输等必要费用。

第二十五条 经营者采用网络、电视、电话、邮购等方式销售商品，消费者有权自收到商品之日起七日内退货，且无需说明理由，但下列商品除外：

(一)消费者定作的；

(二)鲜活易腐的;

(三)在线下载或者消费者拆封的音像制品、计算机软件等数字化商品;

(四)交付的报纸、期刊。

除前款所列商品外,其他根据商品性质并经消费者在购买时确认不宜退货的商品,不适用无理由退货。

消费者退货的商品应当完好。经营者应当自收到退回商品之日起七日内返还消费者支付的商品价款。退回商品的运费由消费者承担; 经营者和消费者另有约定的,按照约定。

第二十六条 经营者在经营活动中使用格式条款的,应当以显著方式提请消费者注意商品或者服务的数量和质量、价款或者费用、履行期限和方式、安全注意事项和风险警示、售后服务、民事责任等与消费者有重大利害关系的内容, 并按照消费者的要求予以说明。

经营者不得以格式条款、通知、声明、店堂告示等方式,作出排除或者限制消费者权利、减轻或者免除经营者责任、加重消费者责任等对消费者不公平、不合理的规定,不得利用格式条款并借助技术手段强制交易。

格式条款、通知、声明、店堂告示等含有前款所列内容的,其内容无效。

第二十七条 经营者不得对消费者进行侮辱、诽谤,不得搜查消费者的身体及其携带的物品,不得侵犯消费者的人身自由。

第二十八条 采用网络、电视、电话、邮购等方式提供商品或者服务的经营者,以及提供证券、保险、银行等金融服务的经营者, 应当向消费者提供经营地址、联系方式、商品或者服务的数量和质量、价款或者费用、履行期限和方式、安全注意事项和风险警示、售后服务、民事责任等信息。

第二十九条 经营者收集、使用消费者个人信息,应当遵循合法、正当、必要的原则,明示收集、使用信息的目的、方式和范围, 并经消费者同意。经营者收集、使用消费者个人信息, 应当公开其收集、使用规则, 不得违反法律、法规的规定和双方的约定收集、使用信息。

经营者及其工作人员对收集的消费者个人信息必须严格保密,不得泄露、出售或者非法向他人提供。经营者应当采取技术措施和其他必要措施, 确保信息安全,防止消费者个人信息泄露、丢失。在发生或者可能发生信息泄露、丢失的情

况时，应当立即采取补救措施。

经营者未经消费者同意或者请求，或者消费者明确表示拒绝的，不得向其发送商业性信息。

第四章 国家对消费者合法权益的保护

第三十条 国家制定有关消费者权益的法律、法规、规章和强制性标准，应当听取消费者和消费者协会等组织的意见。

第三十一条 各级人民政府应当加强领导，组织、协调、督促有关行政部门做好保护消费者合法权益的工作，落实保护消费者合法权益的职责。

各级人民政府应当加强监督，预防危害消费者人身、财产安全行为的发生，及时制止危害消费者人身、财产安全的行为。

第三十二条 各级人民政府工商行政管理部门和其他有关行政部门应当依照法律、法规的规定，在各自的职责范围内，采取措施，保护消费者的合法权益。

有关行政部门应当听取消费者和消费者协会等组织对经营者交易行为、商品和服务质量问题的意见，及时调查处理。

第三十三条 有关行政部门在各自的职责范围内，应当定期或者不定期对经营者提供的商品和服务进行抽查检验，并及时向社会公布抽查检验结果。

有关行政部门发现并认定经营者提供的商品或者服务存在缺陷，有危及人身、财产安全危险的，应当立即责令经营者采取停止销售、警示、召回、无害化处理、销毁、停止生产或者服务等措施。

第三十四条 有关国家机关应当依照法律、法规的规定，惩处经营者在提供商品和服务中侵害消费者合法权益的违法犯罪行为。

第三十五条 人民法院应当采取措施，方便消费者提起诉讼。对符合《中华人民共和国民事诉讼法》起诉条件的消费者权益争议，必须受理，及时审理。

第五章 消费者组织

第三十六条 消费者协会和其他消费者组织是依法成立的对商品和服务进行社会监督的保护消费者合法权益的社会组织。

第三十七条 消费者协会履行下列公益性职责：

(一)向消费者提供消费信息和咨询服务，提高消费者维护自身合法权益的能力，引导文明、健康、节约资源和保护环境的消费方式；

(二)参与制定有关消费者权益的法律、法规、规章和强制性标准;

(三)参与有关行政部门对商品和服务的监督、检查;

(四)就有关消费者合法权益的问题，向有关部门反映、查询，提出建议;

(五)受理消费者的投诉，并对投诉事项进行调查、调解;

(六)投诉事项涉及商品和服务质量问题的，可以委托具备资格的鉴定人鉴定，鉴定人应当告知鉴定意见;

(七)就损害消费者合法权益的行为，支持受损害的消费者提起诉讼或者依照本法提起诉讼;

(八)对损害消费者合法权益的行为，通过大众传播媒介予以揭露、批评。

各级人民政府对消费者协会履行职责应当予以必要的经费等支持。

消费者协会应当认真履行保护消费者合法权益的职责，听取消费者的意见和建议，接受社会监督。

依法成立的其他消费者组织依照法律、法规及其章程的规定， 开展保护消费者合法权益的活动。

第三十八条 消费者组织不得从事商品经营和营利性服务，不得以收取费用或者其他牟取利益的方式向消费者推荐商品和服务。

第六章 争议的解决

第三十九条 消费者和经营者发生消费者权益争议的，可以通过下列途径解决:

(一)与经营者协商和解;

(二)请求消费者协会或者依法成立的其他调解组织调解;

(三)向有关行政部门投诉;

(四)根据与经营者达成的仲裁协议提请仲裁机构仲裁;

(五)向人民法院提起诉讼。

第四十条 消费者在购买、使用商品时，其合法权益受到损害的，可以向销售者要求赔偿。销售者赔偿后， 属于生产者的责任或者属于向销售者提供商品的其他销售者的责任的，销售者有权向生产者或者其他销售者追偿。

消费者或者其他受害人因商品缺陷造成人身、财产损害的， 可以向销售者要求赔偿，也可以向生产者要求赔偿。属于生产者责任的， 销售者赔偿后，有权向

生产者追偿。属于销售者责任的，生产者赔偿后，有权向销售者追偿。

消费者在接受服务时，其合法权益受到损害的，可以向服务者要求赔偿。

第四十一条 消费者在购买、使用商品或者接受服务时，其合法权益受到损害，因原企业分立、合并的，可以向变更后承受其权利义务的企业要求赔偿。

第四十二条 使用他人营业执照的违法经营者提供商品或者服务，损害消费者合法权益的，消费者可以向其要求赔偿，也可以向营业执照的持有人要求赔偿。

第四十三条 消费者在展销会、租赁柜台购买商品或者接受服务，其合法权益受到损害的，可以向销售者或者服务者要求赔偿。展销会结束或者柜台租赁期满后，也可以向展销会的举办者、柜台的出租者要求赔偿。展销会的举办者、柜台的出租者赔偿后，有权向销售者或者服务者追偿。

第四十四条 消费者通过网络交易平台购买商品或者接受服务，其合法权益受到损害的，可以向销售者或者服务者要求赔偿。网络交易平台提供者不能提供销售者或者服务者的真实名称、地址和有效联系方式的， 消费者也可以向网络交易平台提供者要求赔偿；网络交易平台提供者作出更有利于消费者的承诺的，应当履行承诺。网络交易平台提供者赔偿后，有权向销售者或者服务者追偿。

网络交易平台提供者明知或者应知销售者或者服务者利用其平台侵害消费者合法权益，未采取必要措施的，依法与该销售者或者服务者承担连带责任。

第四十五条 消费者因经营者利用虚假广告或者其他虚假宣传方式提供商品或者服务，其合法权益受到损害的，可以向经营者要求赔偿。广告经营者、发布者发布虚假广告的，消费者可以请求行政主管部门予以惩处。广告经营者、发布者不能提供经营者的真实名称、地址和有效联系方式的，应当承担赔偿责任。

广告经营者、发布者设计、制作、发布关系消费者生命健康商品或者服务的虚假广告，造成消费者损害的，应当与提供该商品或者服务的经营者承担连带责任。

社会团体或者其他组织、个人在关系消费者生命健康商品或者服务的虚假广告或者其他虚假宣传中向消费者推荐商品或者服务，造成消费者损害的，应当与提供该商品或者服务的经营者承担连带责任。

第四十六条 消费者向有关行政部门投诉的，该部门应当自收到投诉之日起七个工作日内，予以处理并告知消费者。

第四十七条 对侵害众多消费者合法权益的行为，中国消费者协会以及在省、自治区、直辖市设立的消费者协会，可以向人民法院提起诉讼。

第七章 法律责任

第四十八条 经营者提供商品或者服务有下列情形之一的，除本法另有规定外，应当依照其他有关法律、法规的规定，承担民事责任：

(一)商品或者服务存在缺陷的；

(二)不具备商品应当具备的使用性能而出售时未作说明的；

(三)不符合在商品或者其包装上注明采用的商品标准的；

(四)不符合商品说明、实物样品等方式表明的质量状况的；

(五)生产国家明令淘汰的商品或者销售失效、变质的商品的；

(六)销售的商品数量不足的；

(七)服务的内容和费用违反约定的；

(八)对消费者提出的修理、重作、更换、退货、补足商品数量、退还货款和服务费用或者赔偿损失的要求，故意拖延或者无理拒绝的；

(九)法律、法规规定的其他损害消费者权益的情形。

经营者对消费者未尽到安全保障义务，造成消费者损害的，应当承担侵权责任。

第四十九条 经营者提供商品或者服务，造成消费者或者其他受害人人身伤害的，应当赔偿医疗费、护理费、交通费等为治疗和康复支出的合理费用， 以及因误工减少的收入。造成残疾的，还应当赔偿残疾生活辅助具费和残疾赔偿金。造成死亡的，还应当赔偿丧葬费和死亡赔偿金。

第五十条 经营者侵害消费者的人格尊严、侵犯消费者人身自由或者侵害消费者个人信息依法得到保护的权利的，应当停止侵害、恢复名誉、消除影响、赔礼道歉，并赔偿损失。

第五十一条 经营者有侮辱诽谤、搜查身体、侵犯人身自由等侵害消费者或者其他受害人人身权益的行为，造成严重精神损害的，受害人可以要求精神损害赔偿。

第五十二条 经营者提供商品或者服务，造成消费者财产损害的，应当依照法律规定或者当事人约定承担修理、重作、更换、退货、补足商品数量、退还货

款和服务费用或者赔偿损失等民事责任。

第五十三条 经营者以预收款方式提供商品或者服务的，应当按照约定提供。未按照约定提供的，应当按照消费者的要求履行约定或者退回预付款；并应当承担预付款的利息、消费者必须支付的合理费用。

第五十四条 依法经有关行政部门认定为不合格的商品，消费者要求退货的，经营者应当负责退货。

第五十五条 经营者提供商品或者服务有欺诈行为的，应当按照消费者的要求增加赔偿其受到的损失，增加赔偿的金额为消费者购买商品的价款或者接受服务的费用的三倍；增加赔偿的金额不足五百元的，为五百元。法律另有规定的，依照其规定。

经营者明知商品或者服务存在缺陷，仍然向消费者提供，造成消费者或者其他受害人死亡或者健康严重损害的，受害人有权要求经营者依照本法第四十九条、第五十一条等法律规定赔偿损失，并有权要求所受损失二倍以下的惩罚性赔偿。

第五十六条 经营者有下列情形之一，除承担相应的民事责任外，其他有关法律、法规对处罚机关和处罚方式有规定的，依照法律、法规的规定执行；法律、法规未作规定的，由工商行政管理部门或者其他有关行政部门责令改正，可以根据情节单处或者并处警告、没收违法所得、处以违法所得一倍以上十倍以下的罚款，没有违法所得的，处以五十万元以下的罚款；情节严重的，责令停业整顿、吊销营业执照：

(一)提供的商品或者服务不符合保障人身、财产安全要求的；

(二)在商品中掺杂、掺假， 以假充真，以次充好，或者以不合格商品冒充合格商品的；

(三)生产国家明令淘汰的商品或者销售失效、变质的商品的；

(四)伪造商品的产地，伪造或者冒用他人的厂名、厂址， 篡改生产日期，伪造或者冒用认证标志等质量标志的；

(五)销售的商品应当检验、检疫而未检验、检疫或者伪造检验、检疫结果的；

(六)对商品或者服务作虚假或者引人误解的宣传的；

(七)拒绝或者拖延有关行政部门责令对缺陷商品或者服务采取停止销售、警示、召回、无害化处理、销毁、停止生产或者服务等措施的；

(八)对消费者提出的修理、重作、更换、退货、补足商品数量、退还货款和服务费用或者赔偿损失的要求，故意拖延或者无理拒绝的；

(九)侵害消费者人格尊严、侵犯消费者人身自由或者侵害消费者个人信息依法得到保护的权利的；

(十)法律、法规规定的对损害消费者权益应当予以处罚的其他情形。

经营者有前款规定情形的，除依照法律、法规规定予以处罚外， 处罚机关应当记入信用档案，向社会公布。

第五十七条 经营者违反本法规定提供商品或者服务，侵害消费者合法权益，构成犯罪的，依法追究刑事责任。

第五十八条 经营者违反本法规定，应当承担民事赔偿责任和缴纳罚款、罚金，其财产不足以同时支付的，先承担民事赔偿责任。

第五十九条 经营者对行政处罚决定不服的，可以依法申请行政复议或者提起行政诉讼。

第六十条 以暴力、威胁等方法阻碍有关行政部门工作人员依法执行职务的，依法追究刑事责任；拒绝、阻碍有关行政部门工作人员依法执行职务， 未使用暴力、威胁方法的， 由公安机关依照《中华人民共和国治安管理处罚法》的规定处罚。

第六十一条 国家机关工作人员玩忽职守或者包庇经营者侵害消费者合法权益的行为的，由其所在单位或者上级机关给予行政处分；情节严重，构成犯罪的，依法追究刑事责任。

第八章 附 则

第六十二条 农民购买、使用直接用于农业生产的生产资料，参照本法执行。

第六十三条 本法自 1994 年 1 月 1 日起施行。

中华人民共和国消费者权益保护法实施条例

中华人民共和国国务院令第 778 号

《中华人民共和国消费者权益保护法实施条例》已经 2024 年 2 月 23 日国务院第 26 次常务会议通过，现予公布，自 2024 年 7 月 1 日起施行。

总理 李强

2024 年 3 月 15 日

中华人民共和国消费者权益保护法实施条例

第一章 总 则

第一条 根据《中华人民共和国消费者权益保护法》(以下简称消费者权益保护法)等法律，制定本条例。

第二条 消费者权益保护工作坚持中国共产党的领导，坚持以人民为中心，遵循合法、公平、高效的原则。

第三条 国家加大消费者合法权益保护力度，建立和完善经营者守法、行业自律、消费者参与、政府监管和社会监督相结合的消费者权益保护共同治理体系。

第四条 国家统筹推进消费环境建设，营造安全放心的消费环境，增强消费对经济发展的基础性作用。

第五条 国家加强消费商品和服务的标准体系建设，鼓励经营者制定实施严于国家标准或者行业标准的企业标准，不断提升商品和服务质量。

第六条 国家倡导文明、健康、绿色的消费理念和消费方式，反对奢侈浪费。

第二章 消费者的权利和经营者的义务

第七条 消费者在购买商品、使用商品或者接受服务时，依法享有人身和财产安全不受损害的权利。

经营者向消费者提供商品或者服务(包括以奖励、赠送、试用等形式向消费者免费提供商品或者服务)，应当保证商品或者服务符合保障人身、财产安全的要求。免费提供的商品或者服务存在瑕疵但不违反法律强制性规定且不影响正常使用性能的，经营者应当在提供商品或者服务前如实告知消费者。

经营者应当保证其经营场所及设施符合保障人身、财产安全的要求， 采取必要的安全防护措施，并设置相应的警示标识。消费者在经营场所遇到危险或者受到侵害时，经营者应当给予及时、必要的救助。

第八条 消费者认为经营者提供的商品或者服务可能存在缺陷，有危及人身、财产安全危险的，可以向经营者或者有关行政部门反映情况或者提出建议。

经营者发现其提供的商品或者服务可能存在缺陷，有危及人身、财产安全危险的，应当依照消费者权益保护法第十九条的规定及时采取相关措施。采取召回措施的，生产或者进口商品的经营者应当制定召回计划，发布召回信息，明确告知消费者享有的相关权利，保存完整的召回记录，并承担消费者因商品被召回所

支出的必要费用。商品销售、租赁、修理、零部件生产供应、受委托生产等相关经营者应当依法履行召回相关协助和配合义务。

第九条 经营者应当采用通俗易懂的方式，真实、全面地向消费者提供商品或者服务相关信息，不得通过虚构经营者资质、资格或者所获荣誉， 虚构商品或者服务交易信息、经营数据， 篡改、编造、隐匿用户评价等方式，进行虚假或者引人误解的宣传，欺骗、误导消费者。

经营者不得在消费者不知情的情况下，对同一商品或者服务在同等交易条件下设置不同的价格或者收费标准。

第十条 经营者应当按照国家有关规定，以显著方式标明商品的品名、价格和计价单位或者服务的项目、内容、价格和计价方法等信息，做到价签价目齐全、内容真实准确、标识清晰醒目。

经营者采取自动展期、自动续费等方式提供服务的， 应当在消费者接受服务前和自动展期、自动续费等日期前，以显著方式提请消费者注意。

第十一条 消费者享有自主选择商品或者服务的权利。经营者不得以暴力、胁迫、限制人身自由等方式或者利用技术手段， 强制或者变相强制消费者购买商品或者接受服务，或者排除、限制消费者选择其他经营者提供的商品或者服务。经营者通过搭配、组合等方式提供商品或者服务的， 应当以显著方式提请消费者注意。

第十二条 经营者以商业宣传、产品推荐、实物展示或者通知、声明、店堂告示等方式提供商品或者服务，对商品或者服务的数量、质量、价格、售后服务、责任承担等作出承诺的，应当向购买商品或者接受服务的消费者履行其所承诺的内容。

第十三条 经营者应当在其经营场所的显著位置标明其真实名称和标记。

经营者通过网络、电视、电话、邮购等方式提供商品或者服务的， 应当在其首页、视频画面、语音、商品目录等处以显著方式标明或者说明其真实名称和标记。由其他经营者实际提供商品或者服务的， 还应当向消费者提供该经营者的名称、经营地址、联系方式等信息。

经营者租赁他人柜台或者场地提供商品或者服务，或者通过宣讲、抽奖、集中式体验等方式提供商品或者服务的，应当以显著方式标明其真实名称和标记。

柜台、场地的出租者应当建立场内经营管理制度， 核验、更新、公示经营者的相关信息，供消费者查询。

第十四条 经营者通过网络直播等方式提供商品或者服务的，应当依法履行消费者权益保护相关义务。

直播营销平台经营者应当建立健全消费者权益保护制度，明确消费争议解决机制。发生消费争议的， 直播营销平台经营者应当根据消费者的要求提供直播间运营者、直播营销人员相关信息以及相关经营活动记录等必要信息。

直播间运营者、直播营销人员发布的直播内容构成商业广告的，应当依照《中华人民共和国广告法》的有关规定履行广告发布者、广告经营者或者广告代言人的义务。

第十五条 经营者不得通过虚假或者引人误解的宣传，虚构或者夸大商品或者服务的治疗、保健、养生等功效， 诱导老年人等消费者购买明显不符合其实际需求的商品或者服务。

第十六条 经营者提供网络游戏服务的，应当符合国家关于网络游戏服务相关时段、时长、功能和内容等方面的规定和标准， 针对未成年人设置相应的时间管理、权限管理、消费管理等功能， 在注册、登录等环节严格进行用户核验， 依法保护未成年人身心健康。

第十七条 经营者使用格式条款的，应当遵守消费者权益保护法第二十六条的规定。经营者不得利用格式条款不合理地免除或者减轻其责任、加重消费者的责任或者限制消费者依法变更或者解除合同、选择诉讼或者仲裁解决消费争议、选择其他经营者的商品或者服务等权利。

第十八条 经营者与消费者约定承担退货、更换、修理等义务的有效期限不得低于国家有关规定的要求。有效期限自经营者向消费者交付商品或者提供服务完结之日起计算，需要经营者另行安装的商品，有效期限自商品安装完成之日起计算。经营者向消费者履行更换义务后， 承担更换、修理等义务的有效期限自更换完成之日起重新计算。经营者修理的时间不计入上述有效期限。

经营者依照国家有关规定或者与消费者约定履行退货义务的，应当按照发票等购货凭证或者服务单据上显示的价格一次性退清相关款项。经营者能够证明消费者实际支付的价格与发票等购货凭证或者服务单据上显示的价格不一致的，按

照消费者实际支付的价格退清相关款项。

第十九条 经营者通过网络、电视、电话、邮购等方式销售商品的，应当遵守消费者权益保护法第二十五条规定，不得擅自扩大不适用无理由退货的商品范围。

经营者应当以显著方式对不适用无理由退货的商品进行标注，提示消费者在购买时进行确认，不得将不适用无理由退货作为消费者默认同意的选项。未经消费者确认，经营者不得拒绝无理由退货。

消费者退货的商品应当完好。消费者基于查验需要打开商品包装， 或者为确认商品的品质和功能进行合理调试而不影响商品原有品质、功能和外观的， 经营者应当予以退货。

消费者无理由退货应当遵循诚实信用原则，不得利用无理由退货规则损害经营者和其他消费者的合法权益。

第二十条 经营者提供商品或者服务时收取押金的，应当事先与消费者约定退还押金的方式、程序和时限，不得对退还押金设置不合理条件。

消费者要求退还押金，符合押金退还条件的，经营者应当及时退还。

第二十一条 经营者决定停业或者迁移服务场所的，应当提前 30 日在其经营场所、网站、网店首页等的醒目位置公告经营者的有效联系方式等信息。

第二十二条 经营者以收取预付款方式提供商品或者服务的，应当与消费者订立书面合同，约定商品或者服务的具体内容、价款或者费用、预付款退还方式、违约责任等事项。

经营者收取预付款后，应当按照与消费者的约定提供商品或者服务，不得降低商品或者服务质量，不得任意加价。经营者未按照约定提供商品或者服务的，应当按照消费者的要求履行约定或者退还预付款。

经营者出现重大经营风险，有可能影响经营者按照合同约定或者交易习惯正常提供商品或者服务的，应当停止收取预付款。经营者决定停业或者迁移服务场所的，应当提前告知消费者，并履行本条例第二十一条规定的义务。消费者依照国家有关规定或者合同约定，有权要求经营者继续履行提供商品或者服务的义务，或者要求退还未消费的预付款余额。

第二十三条 经营者应当依法保护消费者的个人信息。经营者在提供商品或

者服务时，不得过度收集消费者个人信息，不得采用一次概括授权、默认授权等方式，强制或者变相强制消费者同意收集、使用与经营活动无直接关系的个人信息。

经营者处理包含消费者的生物识别、宗教信仰、特定身份、医疗健康、金融账户、行踪轨迹等信息以及不满十四周岁未成年人的个人信息等敏感个人信息的，应当符合有关法律、行政法规的规定。

第二十四条 未经消费者同意，经营者不得向消费者发送商业性信息或者拨打商业性电话。消费者同意接收商业性信息或者商业性电话的， 经营者应当提供明确、便捷的取消方式。消费者选择取消的， 经营者应当立即停止发送商业性信息或者拨打商业性电话。

第三章 国家对消费者合法权益的保护

第二十五条 各级人民政府应当加强对消费者权益保护工作的指导，组织、协调、督促有关行政部门落实消费者权益保护工作职责， 提升消费者权益保护工作的法治化水平。

第二十六条 消费者与经营者发生消费者权益争议的，可以向市场监督管理部门或者其他有关行政部门投诉。

自然人、法人或者其他组织可以向市场监督管理部门或者其他有关行政部门举报，反映经营者涉嫌违法的线索。

第二十七条 市场监督管理部门或者其他有关行政部门应当畅通和规范消费者投诉、举报渠道，完善投诉、举报处理流程，依法及时受理和处理投诉、举报，加强对投诉、举报信息的分析应用，开展消费预警和风险提示。

投诉、举报应当遵守法律、法规和有关规定， 不得利用投诉、举报牟取不正当利益，侵害经营者的合法权益，扰乱市场经济秩序。

第二十八条 市场监督管理部门和其他有关行政部门应当加强消费者权益保护工作的协同配合和信息共享，依照法律、法规的规定，在各自的职责范围内，对经营者提供的商品和服务实施抽查检验等监管措施，及时查处侵害消费者合法权益的行为。

第二十九条 市场监督管理部门和其他有关行政部门应当加强消费领域信用体系建设，依法公示有关行政许可、行政处罚、抽查检验结果、消费投诉等信息，

依法对违法失信经营者实施惩戒。

第三十条 有关行政部门应当加强消费知识的宣传普及，倡导文明、健康、绿色消费，提高消费者依法、理性维权的意识和能力；加强对经营者的普法宣传、行政指导和合规指引，提高经营者依法经营的意识。

第三十一条 国家完善绿色消费的标准、认证和信息披露体系，鼓励经营者对商品和服务作出绿色消费方面的信息披露或者承诺，依法查处虚假信息披露和承诺的行为。

第三十二条 行业协会商会等组织应当加强行业自律，引导、督促经营者守法诚信经营，制定的行业规则、自律规则、示范合同和相关标准等应当有利于保护消费者合法权益。

第三十三条 国家鼓励、支持一切组织和个人对损害消费者合法权益的行为进行社会监督。

大众传播媒介应当真实、客观、公正地报道涉及消费者权益的相关事项， 加强消费者维权相关知识的宣传普及，对损害消费者合法权益的行为进行舆论监督。

第四章 消费者组织

第三十四条 消费者协会和其他依法成立的消费者组织应当按照消费者权益保护法的规定履行职责。

第三十五条 各级人民政府应当加强消费者协会组织建设，对消费者协会履行职责予以必要的经费等支持。

第三十六条 有关行政部门应当认真听取消费者协会的意见和建议。对于消费者协会向有关行政部门反映的侵害消费者合法权益的问题，有关行政部门应当及时调查处理并予以回复；对于立案查处的案件，有关行政部门应当将处理结果告知消费者协会。

第三十七条 消费者协会应当加强消费普法宣传和消费引导， 向消费者提供消费维权服务与支持，提高消费者维护自身合法权益的能力。

消费者协会应当及时总结、推广保护消费者合法权益的典型案例和经验做法，引导、支持经营者依法合规开展经营活动。

第三十八条 消费者协会可以组织开展比较试验、消费调查、消费评议、投诉信息公示、对投诉商品提请鉴定、发布消费提示警示等，反映商品和服务状况、

消费者意见和消费维权情况。

第三十九条 消费者协会可以就消费者权益保护事项向有关经营者、行业组织提出改进意见或者进行指导谈话，加强消费者、经营者、行业组织、专业机构、有关行政部门等各相关方的组织协调，推动解决涉及消费者合法权益保护的重要问题。

第四十条 消费者协会可以就消费者投诉的损害消费者合法权益的行为开展调查，与有关经营者核实情况，约请有关经营者到场陈述事实意见、提供证据资料等。

第四十一条 对侵害众多消费者合法权益的行为，中国消费者协会以及在省、自治区、直辖市设立的消费者协会，可以向人民法院提起诉讼。

第五章 争议的解决

第四十二条 消费者应当文明、理性消费，提高自我保护意识，依法维护自身合法权益，在发生消费争议时依法维权。

第四十三条 各级人民政府市场监督管理部门和其他有关行政部门应当推动、健全消费争议多元化解决机制，引导消费者依法通过协商、调解、投诉、仲裁、诉讼等方式维护自身合法权益。

第四十四条 经营者应当建立便捷、高效的投诉处理机制，及时解决消费争议。

鼓励和引导经营者建立健全首问负责、先行赔付、在线争议解决等制度， 及时预防和解决消费争议。

第四十五条 消费者和经营者发生消费争议，请求消费者协会或者依法成立的其他调解组织进行调解的，相关组织应当及时处理。

第四十六条 消费者和经营者发生消费争议向市场监督管理部门或者其他有关行政部门投诉的，应当提供真实身份信息，有明确的被投诉人、具体的投诉请求和事实依据。

有关行政部门应当自收到投诉之日起 7 个工作日内，予以处理并告知消费者。对不符合规定的投诉决定不予受理的， 应当告知消费者不予受理的理由和其他解决争议的途径。

有关行政部门受理投诉后，消费者和经营者同意调解的，有关行政部门应当

依据职责及时调解，并在受理之日起 60 日内调解完毕；调解不成的应当终止调解。调解过程中需要鉴定、检测的，鉴定、检测时间不计算在 60 日内。

有关行政部门经消费者和经营者同意，可以依法将投诉委托消费者协会或者依法成立的其他调解组织调解。

第四十七条 因消费争议需要对商品或者服务质量进行鉴定、检测的，消费者和经营者可以协商确定鉴定、检测机构。无法协商一致的，受理消费者投诉的市场监督管理部门或者其他有关行政部门可以指定鉴定、检测机构。

对于重大、复杂、涉及众多消费者合法权益的消费争议， 可以由市场监督管理部门或者其他有关行政部门纳入抽查检验程序，委托具备相应资质的机构进行鉴定、检测。

第六章 法律责任

第四十八条 经营者提供商品或者服务，违反消费者权益保护法和本条例有关规定，侵害消费者合法权益的，依法承担民事责任。

第四十九条 经营者提供商品或者服务有欺诈行为的，消费者有权根据消费者权益保护法第五十五条第一款的规定要求经营者予以赔偿。但是， 商品或者服务的标签标识、说明书、宣传材料等存在不影响商品或者服务质量且不会对消费者造成误导的瑕疵的除外。

通过夹带、掉包、造假、篡改商品生产日期、捏造事实等方式骗取经营者的赔偿或者对经营者进行敲诈勒索的，不适用消费者权益保护法第五十五条第一款的规定，依照《中华人民共和国治安管理处罚法》等有关法律、法规处理； 构成犯罪的，依法追究刑事责任。

第五十条 经营者违反本条例第十条至第十四条、第十六条、第十七条、第十九条至第二十一条规定，其他有关法律、法规对处罚机关和处罚方式有规定的，依照法律、法规的规定执行； 法律、法规未作规定的， 由市场监督管理部门或者其他有关行政部门责令改正，可以根据情节单处或者并处警告、没收违法所得、处以违法所得 1 倍以上 5 倍以下的罚款，没有违法所得的，处以 30 万元以下的罚款；情节严重的，责令停业整顿、吊销营业执照。

经营者违反本条例第二十二条规定的，由有关行政部门责令改正，可以根据情节单处或者并处警告、没收违法所得、处以违法所得 1 倍以上 10 倍以下的罚

款，没有违法所得的，处以 50 万元以下的罚款；情节严重的，责令停业整顿、吊销营业执照。

经营者违反本条例其他规定的，依照消费者权益保护法第五十六条的规定予以处罚。

第五十一条 经营者主动消除或者减轻违法行为危害后果的，违法行为轻微并及时改正且没有造成危害后果的，或者初次违法且危害后果轻微并及时改正的，依照《中华人民共和国行政处罚法》的规定从轻、减轻或者不予处罚。

第五十二条 有关行政部门工作人员未按照本条例规定履行消费者权益保护职责，玩忽职守或者包庇经营者侵害消费者合法权益的行为的，依法给予处分；构成犯罪的，依法追究刑事责任。

第七章 附 则

第五十三条 本条例自 2024 年 7 月 1 日起施行。

中华人民共和国安全生产法

(2002 年 6 月 29 日第九届全国人民代表大会常务委员会第二十八次会议通过 根据 2009 年 8 月 27 日第十一届全国人民代表大会常务委员会第十次会议关于《关于修改部分法律的决定》第一次修正 根据 2014 年 8 月 31 日第十二届全国人民代表大会常务委员会第十次会议《关于修改〈中华人民共和国安全生产法〉的决定》第二次修正 根据 2021 年 6 月 10 日第十三届全国人民代表大会常务委员会第二十九次会议《关于修改〈中华人民共和国安全生产法〉的决定》第三次修正)

第一章 总 则

第一条 为了加强安全生产工作，防止和减少生产安全事故，保障人民群众生命和财产安全，促进经济社会持续健康发展，制定本法。

第二条 在中华人民共和国领域内从事生产经营活动的单位(以下统称生产经营单位)的安全生产，适用本法；有关法律、行政法规对消防安全和道路交通安全、铁路交通安全、水上交通安全、民用航空安全以及核与辐射安全、特种设备安全另有规定的，适用其规定。

第三条 安全生产工作坚持中国共产党的领导。

安全生产工作应当以人为本，坚持人民至上、生命至上，把保护人民生命

安全摆在首位，树牢安全发展理念，坚持安全第一、预防为主、综合治理的方针，从源头上防范化解重大安全风险。

安全生产工作实行管行业必须管安全、管业务必须管安全、管生产经营必须管安全，强化和落实生产经营单位主体责任与政府监管责任，建立生产经营单位负责、职工参与、政府监管、行业自律和社会监督的机制。

第四条 生产经营单位必须遵守本法和其他有关安全生产的法律、法规，加强安全生产管理，建立健全全员安全生产责任制和安全生产规章制度，加大对安全生产资金、物资、技术、人员的投入保障力度，改善安全生产条件，加强安全生产标准化、信息化建设，构建安全风险分级管控和隐患排查治理双重预防机制，健全风险防范化解机制，提高安全生产水平，确保安全生产。

平台经济等新兴行业、领域的生产经营单位应当根据本行业、领域的特点，建立健全并落实全员安全生产责任制，加强从业人员安全生产教育和培训，履行本法和其他法律、法规规定的有关安全生产义务。

第五条 生产经营单位的主要负责人是本单位安全生产第一责任人，对本单位的安全生产工作全面负责。其他负责人对职责范围内的安全生产工作负责。

第六条 生产经营单位的从业人员有依法获得安全生产保障的权利，并应当依法履行安全生产方面的义务。

第七条 工会依法对安全生产工作进行监督。

生产经营单位的工会依法组织职工参加本单位安全生产工作的民主管理和民主监督，维护职工在安全生产方面的合法权益。生产经营单位制定或者修改有关安全生产的规章制度，应当听取工会的意见。

第八条 国务院和县级以上地方各级人民政府应当根据国民经济和社会发展规划制定安全生产规划，并组织实施。安全生产规划应当与国土空间规划等相关规划相衔接。

各级人民政府应当加强安全生产基础设施建设和安全生产监管能力建设，所需经费列入本级预算。

县级以上地方各级人民政府应当组织有关部门建立完善安全风险评估与论证机制，按照安全风险管控要求，进行产业规划和空间布局，并对位置相邻、

行业相近、业态相似的生产经营单位实施重大安全风险联防联控。

第九条 国务院和县级以上地方各级人民政府应当加强对安全生产工作的领导，建立健全安全生产工作协调机制，支持、督促各有关部门依法履行安全生产监督管理职责，及时协调、解决安全生产监督管理中存在的重大问题。

乡镇人民政府和街道办事处，以及开发区、工业园区、港区、风景区等应当明确负责安全生产监督管理的有关工作机构及其职责，加强安全生产监管力量建设，按照职责对本行政区域或者管理区域内生产经营单位安全生产状况进行监督检查，协助人民政府有关部门或者按照授权依法履行安全生产监督管理职责。

第十条 国务院应急管理部门依照本法，对全国安全生产工作实施综合监督管理；县级以上地方各级人民政府应急管理部门依照本法，对本行政区域内安全生产工作实施综合监督管理。

国务院交通运输、住房和城乡建设、水利、民航等有关部门依照本法和其他有关法律、行政法规的规定，在各自的职责范围内对有关行业、领域的安全生产工作实施监督管理；县级以上地方各级人民政府有关部门依照本法和其他有关法律、法规的规定，在各自的职责范围内对有关行业、领域的安全生产工作实施监督管理。对新兴行业、领域的安全生产监督管理职责不明确的，由县级以上地方各级人民政府按照业务相近的原则确定监督管理部门。

应急管理部门和对有关行业、领域的安全生产工作实施监督管理的部门，统称负有安全生产监督管理职责的部门。负有安全生产监督管理职责的部门应当相互配合、齐抓共管、信息共享、资源共用，依法加强安全生产监督管理工作。

第十一条 国务院有关部门应当按照保障安全生产的要求，依法及时制定有关的国家标准或者行业标准，并根据科技进步和经济发展适时修订。

生产经营单位必须执行依法制定的保障安全生产的国家标准或者行业标准。

第十二条 国务院有关部门按照职责分工负责安全生产强制性国家标准的项目提出、组织起草、征求意见、技术审查。国务院应急管理部门统筹提出安全生产强制性国家标准的立项计划。国务院标准化行政主管部门负责安全生产

强制性国家标准的立项、编号、对外通报和授权批准发布工作。国务院标准化行政主管部门、有关部门依据法定职责对安全生产强制性国家标准的实施进行监督检查。

第十三条 各级人民政府及其有关部门应当采取多种形式，加强对有关安全生产的法律、法规和安全生产知识的宣传，增强全社会的安全生产意识。

第十四条 有关协会组织依照法律、行政法规和章程，为生产经营单位提供安全生产方面的信息、培训等服务，发挥自律作用，促进生产经营单位加强安全生产管理。

第十五条 依法设立的为安全生产提供技术、管理服务的机构，依照法律、行政法规和执业准则，接受生产经营单位的委托为其安全生产工作提供技术、管理服务。

生产经营单位委托前款规定的机构提供安全生产技术、管理服务的，保证安全生产的责任仍由本单位负责。

第十六条 国家实行生产安全事故责任追究制度，依照本法和有关法律、法规的规定，追究生产安全事故责任单位和责任人员的法律责任。

第十七条 县级以上各级人民政府应当组织负有安全生产监督管理职责的部门依法编制安全生产权力和责任清单，公开并接受社会监督。

第十八条 国家鼓励和支持安全生产科学技术研究和安全生产先进技术的推广应用，提高安全生产水平。

第十九条 国家对在改善安全生产条件、防止生产安全事故、参加抢险救护等方面取得显著成绩的单位和个人，给予奖励。

第二章 生产经营单位的安全生产保障

第二十条 生产经营单位应当具备本法和有关法律、行政法规和国家标准或者行业标准规定的安全生产条件；不具备安全生产条件的，不得从事生产经营活动。

第二十一条 生产经营单位的主要负责人对本单位安全生产工作负有下列职责：

(一)建立健全并落实本单位全员安全生产责任制，加强安全生产标准化建设；

(二)组织制定并实施本单位安全生产规章制度和操作规程;

(三)组织制定并实施本单位安全生产教育和培训计划;

(四)保证本单位安全生产投入的有效实施;

(五)组织建立并落实安全风险分级管控和隐患排查治理双重预防工作机制,督促、检查本单位的安全生产工作,及时消除生产安全事故隐患;

(六)组织制定并实施本单位的生产安全事故应急救援预案;

(七)及时、如实报告生产安全事故。

第二十二条 生产经营单位的全员安全生产责任制应当明确各岗位的责任人员、责任范围和考核标准等内容。

生产经营单位应当建立相应的机制,加强对全员安全生产责任制落实情况的监督考核,保证全员安全生产责任制的落实。

第二十三条 生产经营单位应当具备的安全生产条件所必需的资金投入,由生产经营单位的决策机构、主要负责人或者个人经营的投资人予以保证,并对由于安全生产所必需的资金投入不足导致的后果承担责任。

有关生产经营单位应当按照规定提取和使用安全生产费用,专门用于改善安全生产条件。安全生产费用在成本中据实列支。安全生产费用提取、使用和监督管理的具体办法由国务院财政部门会同国务院应急管理部门征求国务院有关部门意见后制定。

第二十四条 矿山、金属冶炼、建筑施工、运输单位和危险物品的生产、经营、储存、装卸单位,应当设置安全生产管理机构或者配备专职安全生产管理人员。

前款规定以外的其他生产经营单位,从业人员超过一百人的,应当设置安全生产管理机构或者配备专职安全生产管理人员;从业人员在一百人以下的,应当配备专职或者兼职的安全生产管理人员。

第二十五条 生产经营单位的安全生产管理机构以及安全生产管理人员履行下列职责:

(一)组织或者参与拟订本单位安全生产规章制度、操作规程和生产安全事故应急救援预案;

(二)组织或者参与本单位安全生产教育和培训,如实记录安全生产教育和

培训情况；

(三)组织开展危险源辨识和评估，督促落实本单位重大危险源的安全管理措施；

(四)组织或者参与本单位应急救援演练；

(五)检查本单位的安全生产状况，及时排查生产安全事故隐患，提出改进安全生产管理的建议；

(六)制止和纠正违章指挥、强令冒险作业、违反操作规程的行为；

(七)督促落实本单位安全生产整改措施。

生产经营单位可以设置专职安全生产分管负责人，协助本单位主要负责人履行安全生产管理职责。

第二十六条 生产经营单位的安全生产管理机构以及安全生产管理人员应当恪尽职守，依法履行职责。

生产经营单位作出涉及安全生产的经营决策，应当听取安全生产管理机构以及安全生产管理人员的意见。

生产经营单位不得因安全生产管理人员依法履行职责而降低其工资、福利等待遇或者解除与其订立的劳动合同。

危险物品的生产、储存单位以及矿山、金属冶炼单位的安全生产管理人员的任免，应当告知主管的负有安全生产监督管理职责的部门。

第二十七条 生产经营单位的主要负责人和安全生产管理人员必须具备与本单位所从事的生产经营活动相应的安全生产知识和管理能力。

危险物品的生产、经营、储存、装卸单位以及矿山、金属冶炼、建筑施工、运输单位的主要负责人和安全生产管理人员，应当由主管的负有安全生产监督管理职责的部门对其安全生产知识和管理能力考核合格。考核不得收费。

危险物品的生产、储存、装卸单位以及矿山、金属冶炼单位应当有注册安全工程师从事安全生产管理工作。鼓励其他生产经营单位聘用注册安全工程师从事安全生产管理工作。注册安全工程师按专业分类管理，具体办法由国务院人力资源和社会保障部门、国务院应急管理部门会同国务院有关部门制定。

第二十八条 生产经营单位应当对从业人员进行安全生产教育和培训，保证从业人员具备必要的安全生产知识，熟悉有关的安全生产规章制度和安全操

作规程，掌握本岗位的安全操作技能，了解事故应急处理措施，知悉自身在安全生产方面的权利和义务。未经安全生产教育和培训合格的从业人员，不得上岗作业。

生产经营单位使用被派遣劳动者的，应当将被派遣劳动者纳入本单位从业人员统一管理，对被派遣劳动者进行岗位安全操作规程和安全操作技能的教育和培训。劳务派遣单位应当对被派遣劳动者进行必要的安全生产教育和培训。

生产经营单位接收中等职业学校、高等学校学生实习的，应当对实习学生进行相应的安全生产教育和培训，提供必要的劳动防护用品。学校应当协助生产经营单位对实习学生进行安全生产教育和培训。

生产经营单位应当建立安全生产教育和培训档案，如实记录安全生产教育和培训的时间、内容、参加人员以及考核结果等情况。

第二十九条 生产经营单位采用新工艺、新技术、新材料或者使用新设备，必须了解、掌握其安全技术特性，采取有效的安全防护措施，并对从业人员进行专门的安全生产教育和培训。

第三十条 生产经营单位的特种作业人员必须按照国家有关规定经专门的安全作业培训，取得相应资格，方可上岗作业。

特种作业人员的范围由国务院应急管理部门会同国务院有关部门确定。

第三十一条 生产经营单位新建、改建、扩建工程项目(以下统称建设项目)的安全设施，必须与主体工程同时设计、同时施工、同时投入生产和使用。安全设施投资应当纳入建设项目概算。

第三十二条 矿山、金属冶炼建设项目和用于生产、储存、装卸危险物品的建设项目，应当按照国家有关规定进行安全评价。

第三十三条 建设项目安全设施的设计人、设计单位应当对安全设施设计负责。

矿山、金属冶炼建设项目和用于生产、储存、装卸危险物品的建设项目的安全设施设计应当按照国家有关规定报经有关部门审查，审查部门及其负责审查的人员对审查结果负责。

第三十四条 矿山、金属冶炼建设项目和用于生产、储存、装卸危险物品的建设项目的施工单位必须按照批准的安全设施设计施工，并对安全设施的工

程质量负责。

矿山、金属冶炼建设项目和用于生产、储存、装卸危险物品的建设项目竣工投入生产或者使用前，应当由建设单位负责组织对安全设施进行验收；验收合格后，方可投入生产和使用。负有安全生产监督管理职责的部门应当加强对建设单位验收活动和验收结果的监督核查。

第三十五条 生产经营单位应当在有较大危险因素的生产经营场所和有关设施、设备上，设置明显的安全警示标志。

第三十六条 安全设备的设计、制造、安装、使用、检测、维修、改造和报废，应当符合国家标准或者行业标准。

生产经营单位必须对安全设备进行经常性维护、保养，并定期检测，保证正常运转。维护、保养、检测应当作好记录，并由有关人员签字。

生产经营单位不得关闭、破坏直接关系生产安全的监控、报警、防护、救生设备、设施，或者篡改、隐瞒、销毁其相关数据、信息。

餐饮等行业的生产经营单位使用燃气的，应当安装可燃气体报警装置，并保障其正常使用。

第三十七条 生产经营单位使用的危险物品的容器、运输工具，以及涉及人身安全、危险性较大的海洋石油开采特种设备和矿山井下特种设备，必须按照国家有关规定，由专业生产单位生产，并经具有专业资质的检测、检验机构检测、检验合格，取得安全使用证或者安全标志，方可投入使用。检测、检验机构对检测、检验结果负责。

第三十八条 国家对严重危及生产安全的工艺、设备实行淘汰制度，具体目录由国务院应急管理部门会同国务院有关部门制定并公布。法律、行政法规对目录的制定另有规定的，适用其规定。

省、自治区、直辖市人民政府可以根据本地区实际情况制定并公布具体目录，对前款规定以外的危及生产安全的工艺、设备予以淘汰。

生产经营单位不得使用应当淘汰的危及生产安全的工艺、设备。

第三十九条 生产、经营、运输、储存、使用危险物品或者处置废弃危险物品的，由有关主管部门依照有关法律、法规的规定和国家标准或者行业标准审批并实施监督管理。

生产经营单位生产、经营、运输、储存、使用危险物品或者处置废弃危险物品，必须执行有关法律、法规和国家标准或者行业标准，建立专门的安全管理制度，采取可靠的安全措施，接受有关主管部门依法实施的监督管理。

第四十条 生产经营单位对重大危险源应当登记建档，进行定期检测、评估、监控，并制定应急预案，告知从业人员和相关人员在紧急情况下应当采取的应急措施。

生产经营单位应当按照国家有关规定将本单位重大危险源及有关安全措施、应急措施报有关地方人民政府应急管理部门和有关部门备案。有关地方人民政府应急管理部门和有关部门应当通过相关信息系统实现信息共享。

第四十一条 生产经营单位应当建立安全风险分级管控制度，按照安全风险分级采取相应的管控措施。

生产经营单位应当建立健全并落实生产安全事故隐患排查治理制度，采取技术、管理措施，及时发现并消除事故隐患。事故隐患排查治理情况应当如实记录，并通过职工大会或者职工代表大会、信息公示栏等方式向从业人员通报。其中，重大事故隐患排查治理情况应当及时向负有安全生产监督管理职责的部门和职工大会或者职工代表大会报告。

县级以上地方各级人民政府负有安全生产监督管理职责的部门应当将重大事故隐患纳入相关信息系统，建立健全重大事故隐患治理督办制度，督促生产经营单位消除重大事故隐患。

第四十二条 生产、经营、储存、使用危险物品的车间、商店、仓库不得与员工宿舍在同一座建筑物内，并应当与员工宿舍保持安全距离。

生产经营场所和员工宿舍应当设有符合紧急疏散要求、标志明显、保持畅通的出口、疏散通道。禁止占用、锁闭、封堵生产经营场所或者员工宿舍的出口、疏散通道。

第四十三条 生产经营单位进行爆破、吊装、动火、临时用电以及国务院应急管理部门会同国务院有关部门规定的其他危险作业，应当安排专门人员进行现场安全管理，确保操作规程的遵守和安全措施的落实。

第四十四条 生产经营单位应当教育和督促从业人员严格执行本单位的安全生产规章制度和安全操作规程；并向从业人员如实告知作业场所和工作岗位

存在的危险因素、防范措施以及事故应急措施。

生产经营单位应当关注从业人员的身体、心理状况和行为习惯，加强对从业人员的心理疏导、精神慰藉，严格落实岗位安全生产责任，防范从业人员行为异常导致事故发生。

第四十五条 生产经营单位必须为从业人员提供符合国家标准或者行业标准的劳动防护用品，并监督、教育从业人员按照使用规则佩戴、使用。

第四十六条 生产经营单位的安全生产管理人员应当根据本单位的生产经营特点，对安全生产状况进行经常性检查；对检查中发现的安全问题，应当立即处理；不能处理的，应当及时报告本单位有关负责人，有关负责人应当及时处理。检查及处理情况应当如实记录在案。

生产经营单位的安全生产管理人员在检查中发现重大事故隐患，依照前款规定向本单位有关负责人报告，有关负责人不及时处理的，安全生产管理人员可以向主管的负有安全生产监督管理职责的部门报告，接到报告的部门应当依法及时处理。

第四十七条 生产经营单位应当安排用于配备劳动防护用品、进行安全生产培训的经费。

第四十八条 两个以上生产经营单位在同一作业区域内进行生产经营活动，可能危及对方生产安全的，应当签订安全生产管理协议，明确各自的安全生产管理职责和应当采取的安全措施，并指定专职安全生产管理人员进行安全检查与协调。

第四十九条 生产经营单位不得将生产经营项目、场所、设备发包或者出租给不具备安全生产条件或者相应资质的单位或者个人。

生产经营项目、场所发包或者出租给其他单位的，生产经营单位应当与承包单位、承租单位签订专门的安全生产管理协议，或者在承包合同、租赁合同中约定各自的安全生产管理职责；生产经营单位对承包单位、承租单位的安全生产工作统一协调、管理，定期进行安全检查，发现安全问题的，应当及时督促整改。

矿山、金属冶炼建设项目和用于生产、储存、装卸危险物品的建设项目的施工单位应当加强对施工项目的安全管理，不得倒卖、出租、出借、挂靠或者

以其他形式非法转让施工资质，不得将其承包的全部建设工程转包给第三人或者将其承包的全部建设工程支解以后以分包的名义分别转包给第三人，不得将工程分包给不具备相应资质条件的单位。

第五十条 生产经营单位发生生产安全事故时，单位的主要负责人应当立即组织抢救，并不得在事故调查处理期间擅离职守。

第五十一条 生产经营单位必须依法参加工伤保险，为从业人员缴纳保险费。

国家鼓励生产经营单位投保安全生产责任保险；属于国家规定的高危行业、领域的生产经营单位，应当投保安全生产责任保险。具体范围和实施办法由国务院应急管理部门会同国务院财政部门、国务院保险监督管理机构和相关行业主管部门制定。

第三章 从业人员的安全生产权利义务

第五十二条 生产经营单位与从业人员订立的劳动合同，应当载明有关保障从业人员劳动安全、防止职业危害的事项，以及依法为从业人员办理工伤保险的事项。

生产经营单位不得以任何形式与从业人员订立协议，免除或者减轻其对从业人员因生产安全事故伤亡依法应承担的责任。

第五十三条 生产经营单位的从业人员有权了解其作业场所和工作岗位存在的危险因素、防范措施及事故应急措施，有权对本单位的安全生产工作提出建议。

第五十四条 从业人员有权对本单位安全生产工作中存在的问题提出批评、检举、控告；有权拒绝违章指挥和强令冒险作业。

生产经营单位不得因从业人员对本单位安全生产工作提出批评、检举、控告或者拒绝违章指挥、强令冒险作业而降低其工资、福利等待遇或者解除与其订立的劳动合同。

第五十五条 从业人员发现直接危及人身安全的紧急情况时，有权停止作业或者在采取可能的应急措施后撤离作业场所。

生产经营单位不得因从业人员在前款紧急情况下停止作业或者采取紧急撤离措施而降低其工资、福利等待遇或者解除与其订立的劳动合同。

第五十六条 生产经营单位发生生产安全事故后，应当及时采取措施救治有关人员。

因生产安全事故受到损害的从业人员，除依法享有工伤保险外，依照有关民事法律尚有获得赔偿的权利的，有权提出赔偿要求。

第五十七条 从业人员在作业过程中，应当严格落实岗位安全责任，遵守本单位的安全生产规章制度和操作规程，服从管理，正确佩戴和使用劳动防护用品。

第五十八条 从业人员应当接受安全生产教育和培训，掌握本职工作所需的安全生产知识，提高安全生产技能，增强事故预防和应急处理能力。

第五十九条 从业人员发现事故隐患或者其他不安全因素，应当立即向现场安全生产管理人员或者本单位负责人报告；接到报告的人员应当及时予以处理。

第六十条 工会有权对建设项目的安全设施与主体工程同时设计、同时施工、同时投入生产和使用进行监督，提出意见。

工会对生产经营单位违反安全生产法律、法规，侵犯从业人员合法权益的行为，有权要求纠正；发现生产经营单位违章指挥、强令冒险作业或者发现事故隐患时，有权提出解决的建议，生产经营单位应当及时研究答复；发现危及从业人员生命安全的情况时，有权向生产经营单位建议组织从业人员撤离危险场所，生产经营单位必须立即作出处理。

工会有权依法参加事故调查，向有关部门提出处理意见，并要求追究有关人员的责任。

第六十一条 生产经营单位使用被派遣劳动者的，被派遣劳动者享有本法规定的从业人员的权利，并应当履行本法规定的从业人员的义务。

第四章 安全生产的监督管理

第六十二条 县级以上地方各级人民政府应当根据本行政区域内的安全生产状况，组织有关部门按照职责分工，对本行政区域内容易发生重大生产安全事故的生产经营单位进行严格检查。

应急管理部门应当按照分类分级监督管理的要求，制定安全生产年度监督检查计划，并按照年度监督检查计划进行监督检查，发现事故隐患，应当及时

处理。

第六十三条 负有安全生产监督管理职责的部门依照有关法律、法规的规定，对涉及安全生产的事项需要审查批准(包括批准、核准、许可、注册、认证、颁发证照等，下同)或者验收的，必须严格依照有关法律、法规和国家标准或者行业标准规定的安全生产条件和程序进行审查；不符合有关法律、法规和国家标准或者行业标准规定的安全生产条件的，不得批准或者验收通过。对未依法取得批准或者验收合格的单位擅自从事有关活动的，负责行政审批的部门发现或者接到举报后应当立即予以取缔，并依法予以处理。对已经依法取得批准的单位，负责行政审批的部门发现其不再具备安全生产条件的，应当撤销原批准。

第六十四条 负有安全生产监督管理职责的部门对涉及安全生产的事项进行审查、验收，不得收取费用；不得要求接受审查、验收的单位购买其指定品牌或者指定生产、销售单位的安全设备、器材或者其他产品。

第六十五条 应急管理部门和其他负有安全生产监督管理职责的部门依法开展安全生产行政执法工作，对生产经营单位执行有关安全生产的法律、法规和国家标准或者行业标准的情况进行监督检查，行使以下职权：

(一)进入生产经营单位进行检查，调阅有关资料，向有关单位和人员了解情况；

(二)对检查中发现的安全生产违法行为，当场予以纠正或者要求限期改正；对依法应当给予行政处罚的行为，依照本法和其他有关法律、行政法规的规定作出行政处罚决定；

(三)对检查中发现的事故隐患，应当责令立即排除；重大事故隐患排除前或者排除过程中无法保证安全的，应当责令从危险区域内撤出作业人员，责令暂时停产停业或者停止使用相关设施、设备；重大事故隐患排除后，经审查同意，方可恢复生产经营和使用；

(四)对有根据认为不符合保障安全生产的国家标准或者行业标准的设施、设备、器材以及违法生产、储存、使用、经营、运输的危险物品予以查封或者扣押，对违法生产、储存、使用、经营危险物品的作业场所予以查封，并依法作出处理决定。

监督检查不得影响被检查单位的正常生产经营活动。

第六十六条 生产经营单位对负有安全生产监督管理职责的部门的监督检查人员(以下统称安全生产监督检查人员)依法履行监督检查职责，应当予以配合，不得拒绝、阻挠。

第六十七条 安全生产监督检查人员应当忠于职守，坚持原则，秉公执法。

安全生产监督检查人员执行监督检查任务时，必须出示有效的行政执法证件；对涉及被检查单位的技术秘密和业务秘密，应当为其保密。

第六十八条 安全生产监督检查人员应当将检查的时间、地点、内容、发现的问题及其处理情况，作出书面记录，并由检查人员和被检查单位的负责人签字；被检查单位的负责人拒绝签字的，检查人员应当将情况记录在案，并向负有安全生产监督管理职责的部门报告。

第六十九条 负有安全生产监督管理职责的部门在监督检查中，应当互相配合，实行联合检查；确需分别进行检查的，应当互通情况，发现存在的安全问题应当由其他有关部门进行处理的，应当及时移送其他有关部门并形成记录备查，接受移送的部门应当及时进行处理。

第七十条 负有安全生产监督管理职责的部门依法对存在重大事故隐患的生产经营单位作出停产停业、停止施工、停止使用相关设施或者设备的决定，生产经营单位应当依法执行，及时消除事故隐患。生产经营单位拒不执行，有发生生产安全事故的现实危险的，在保证安全的前提下，经本部门主要负责人批准，负有安全生产监督管理职责的部门可以采取通知有关单位停止供电、停止供应民用爆炸物品等措施，强制生产经营单位履行决定。通知应当采用书面形式，有关单位应当予以配合。

负有安全生产监督管理职责的部门依照前款规定采取停止供电措施，除有危及生产安全的紧急情形外，应当提前二十四小时通知生产经营单位。生产经营单位依法履行行政决定、采取相应措施消除事故隐患的，负有安全生产监督管理职责的部门应当及时解除前款规定的措施。

第七十一条 监察机关依照监察法的规定，对负有安全生产监督管理职责的部门及其工作人员履行安全生产监督管理职责实施监察。

第七十二条 承担安全评价、认证、检测、检验职责的机构应当具备国家规定的资质条件，并对其作出的安全评价、认证、检测、检验结果的合法性、真实性负责。资质条件由国务院应急管理部门会同国务院有关部门制定。

承担安全评价、认证、检测、检验职责的机构应当建立并实施服务公开和报告公开制度，不得租借资质、挂靠、出具虚假报告。

第七十三条 负有安全生产监督管理职责的部门应当建立举报制度，公开举报电话、信箱或者电子邮件地址等网络举报平台，受理有关安全生产的举报；受理的举报事项经调查核实后，应当形成书面材料；需要落实整改措施的，报经有关负责人签字并督促落实。对不属于本部门职责，需要由其他有关部门进行调查处理的，转交其他有关部门处理。

涉及人员死亡的举报事项，应当由县级以上人民政府组织核查处理。

第七十四条 任何单位或者个人对事故隐患或者安全生产违法行为，均有权向负有安全生产监督管理职责的部门报告或者举报。

因安全生产违法行为造成重大事故隐患或者导致重大事故，致使国家利益或者社会公共利益受到侵害的，人民检察院可以根据民事诉讼法、行政诉讼法的相关规定提起公益诉讼。

第七十五条 居民委员会、村民委员会发现其所在区域内的生产经营单位存在事故隐患或者安全生产违法行为时，应当向当地人民政府或者有关部门报告。

第七十六条 县级以上各级人民政府及其有关部门对报告重大事故隐患或者举报安全生产违法行为的有功人员，给予奖励。具体奖励办法由国务院应急管理部门会同国务院财政部门制定。

第七十七条 新闻、出版、广播、电影、电视等单位有进行安全生产公益宣传教育的义务，有对违反安全生产法律、法规的行为进行舆论监督的权利。

第七十八条 负有安全生产监督管理职责的部门应当建立安全生产违法行为信息库，如实记录生产经营单位及其有关从业人员的安全生产违法行为信息；对违法行为情节严重的生产经营单位及其有关从业人员，应当及时向社会公告，并通报行业主管部门、投资主管部门、自然资源主管部门、生态环境主管部门、证券监督管理机构以及有关金融机构。有关部门和机构应当对存在失

信行为的生产经营单位及其有关从业人员采取加大执法检查频次、暂停项目审批、上调有关保险费率、行业或者职业禁入等联合惩戒措施，并向社会公示。

负有安全生产监督管理职责的部门应当加强对生产经营单位行政处罚信息的及时归集、共享、应用和公开，对生产经营单位作出处罚决定后七个工作日内在监督管理部门公示系统予以公开曝光，强化对违法失信生产经营单位及其有关从业人员的社会监督，提高全社会安全生产诚信水平。

第五章 生产安全事故的应急救援与调查处理

第七十九条 国家加强生产安全事故应急能力建设，在重点行业、领域建立应急救援基地和应急救援队伍，并由国家安全生产应急救援机构统一协调指挥；鼓励生产经营单位和其他社会力量建立应急救援队伍，配备相应的应急救援装备和物资，提高应急救援的专业化水平。

国务院应急管理部门牵头建立全国统一的生产安全事故应急救援信息系统，国务院交通运输、住房和城乡建设、水利、民航等有关部门和县级以上地方人民政府建立健全相关行业、领域、地区的生产安全事故应急救援信息系统，实现互联互通、信息共享，通过推行网上安全信息采集、安全监管和监测预警，提升监管的精准化、智能化水平。

第八十条 县级以上地方各级人民政府应当组织有关部门制定本行政区域内生产安全事故应急救援预案，建立应急救援体系。

乡镇人民政府和街道办事处，以及开发区、工业园区、港区、风景区等应当制定相应的生产安全事故应急救援预案，协助人民政府有关部门或者按照授权依法履行生产安全事故应急救援工作职责。

第八十一条 生产经营单位应当制定本单位生产安全事故应急救援预案，与所在地县级以上地方人民政府组织制定的生产安全事故应急救援预案相衔接，并定期组织演练。

第八十二条 危险物品的生产、经营、储存单位以及矿山、金属冶炼、城市轨道交通运营、建筑施工单位应当建立应急救援组织；生产经营规模较小的，可以不建立应急救援组织，但应当指定兼职的应急救援人员。

危险物品的生产、经营、储存、运输单位以及矿山、金属冶炼、城市轨道交通运营、建筑施工单位应当配备必要的应急救援器材、设备和物资，并进行

经常性维护、保养，保证正常运转。

第八十三条 生产经营单位发生生产安全事故后，事故现场有关人员应当立即报告本单位负责人。

单位负责人接到事故报告后，应当迅速采取有效措施，组织抢救，防止事故扩大，减少人员伤亡和财产损失，并按照国家有关规定立即如实报告当地负有安全生产监督管理职责的部门，不得隐瞒不报、谎报或者迟报，不得故意破坏事故现场、毁灭有关证据。

第八十四条 负有安全生产监督管理职责的部门接到事故报告后，应当立即按照国家有关规定上报事故情况。负有安全生产监督管理职责的部门和有关地方人民政府对事故情况不得隐瞒不报、谎报或者迟报。

第八十五条 有关地方人民政府和负有安全生产监督管理职责的部门的负责人接到生产安全事故报告后，应当按照生产安全事故应急救援预案的要求立即赶到事故现场，组织事故抢救。

参与事故抢救的部门和单位应当服从统一指挥，加强协同联动，采取有效的应急救援措施，并根据事故救援的需要采取警戒、疏散等措施，防止事故扩大和次生灾害的发生，减少人员伤亡和财产损失。

事故抢救过程中应当采取必要措施，避免或者减少对环境造成的危害。

任何单位和个人都应当支持、配合事故抢救，并提供一切便利条件。

第八十六条 事故调查处理应当按照科学严谨、依法依规、实事求是、注重实效的原则，及时、准确地查清事故原因，查明事故性质和责任，评估应急处置工作，总结事故教训，提出整改措施，并对事故责任单位和人员提出处理建议。事故调查报告应当依法及时向社会公布。事故调查和处理的具体办法由国务院制定。

事故发生单位应当及时全面落实整改措施，负有安全生产监督管理职责的部门应当加强监督检查。

负责事故调查处理的国务院有关部门和地方人民政府应当在批复事故调查报告后一年内，组织有关部门对事故整改和防范措施落实情况进行评估，并及时向社会公开评估结果；对不履行职责导致事故整改和防范措施没有落实的有关单位和人员，应当按照有关规定追究责任。

第八十七条 生产经营单位发生生产安全事故，经调查确定为责任事故的，除了应当查明事故单位的责任并依法予以追究外，还应当查明对安全生产的有关事项负有审查批准和监督职责的行政部门的责任，对有失职、渎职行为的，依照本法第九十条的规定追究法律责任。

第八十八条 任何单位和个人不得阻挠和干涉对事故的依法调查处理。

第八十九条 县级以上地方各级人民政府应急管理部门应当定期统计分析本行政区域内发生生产安全事故的情况，并定期向社会公布。

第六章 法律责任

第九十条 负有安全生产监督管理职责的部门的工作人员，有下列行为之一的，给予降级或者撤职的处分；构成犯罪的，依照刑法有关规定追究刑事责任：

(一)对不符合法定安全生产条件的涉及安全生产的事项予以批准或者验收通过的；

(二)发现未依法取得批准、验收的单位擅自从事有关活动或者接到举报后不予取缔或者不依法予以处理的；

(三)对已经依法取得批准的单位不履行监督管理职责，发现其不再具备安全生产条件而不撤销原批准或者发现安全生产违法行为不予查处的；

(四)在监督检查中发现重大事故隐患，不依法及时处理的。

负有安全生产监督管理职责的部门的工作人员有前款规定以外的滥用职权、玩忽职守、徇私舞弊行为的，依法给予处分；构成犯罪的，依照刑法有关规定追究刑事责任。

第九十一条 负有安全生产监督管理职责的部门，要求被审查、验收的单位购买其指定的安全设备、器材或者其他产品的，在对安全生产事项的审查、验收中收取费用的，由其上级机关或者监察机关责令改正，责令退还收取的费用；情节严重的，对直接负责的主管人员和其他直接责任人员依法给予处分。

第九十二条 承担安全评价、认证、检测、检验职责的机构出具失实报告的，责令停业整顿，并处三万元以上十万元以下的罚款；给他人造成损害的，依法承担赔偿责任。

承担安全评价、认证、检测、检验职责的机构租借资质、挂靠、出具虚假

报告的，没收违法所得；违法所得在十万元以上的，并处违法所得二倍以上五倍以下的罚款，没有违法所得或者违法所得不足十万元的，单处或者并处十万元以上二十万元以下的罚款；对其直接负责的主管人员和其他直接责任人员处五万元以上十万元以下的罚款；给他人造成损害的，与生产经营单位承担连带赔偿责任；构成犯罪的，依照刑法有关规定追究刑事责任。

对有前款违法行为的机构及其直接责任人员，吊销其相应资质和资格，五年内不得从事安全评价、认证、检测、检验等工作；情节严重的，实行终身行业和职业禁入。

第九十三条 生产经营单位的决策机构、主要负责人或者个人经营的投资人不依照本法规定保证安全生产所必需的资金投入，致使生产经营单位不具备安全生产条件的，责令限期改正，提供必需的资金；逾期未改正的，责令生产经营单位停产停业整顿。

有前款违法行为，导致发生生产安全事故的，对生产经营单位的主要负责人给予撤职处分，对个人经营的投资人处二万元以上二十万元以下的罚款；构成犯罪的，依照刑法有关规定追究刑事责任。

第九十四条 生产经营单位的主要负责人未履行本法规定的安全生产管理职责的，责令限期改正，处二万元以上五万元以下的罚款；逾期未改正的，处五万元以上十万元以下的罚款，责令生产经营单位停产停业整顿。

生产经营单位的主要负责人有前款违法行为，导致发生生产安全事故的，给予撤职处分；构成犯罪的，依照刑法有关规定追究刑事责任。

生产经营单位的主要负责人依照前款规定受刑事处罚或者撤职处分的，自刑罚执行完毕或者受处分之日起，五年内不得担任任何生产经营单位的主要负责人；对重大、特别重大生产安全事故负有责任的，终身不得担任本行业生产经营单位的主要负责人。

第九十五条 生产经营单位的主要负责人未履行本法规定的安全生产管理职责，导致发生生产安全事故的，由应急管理部门依照下列规定处以罚款：

(一)发生一般事故的，处上一年年收入百分之四十的罚款；

(二)发生较大事故的，处上一年年收入百分之六十的罚款；

(三)发生重大事故的，处上一年年收入百分之八十的罚款；

(四)发生特别重大事故的，处上一年年收入百分之一百的罚款。

第九十六条 生产经营单位的其他负责人和安全生产管理人员未履行本法规定的安全生产管理职责的，责令限期改正，处一万元以上三万元以下的罚款；导致发生生产安全事故的，暂停或者吊销其与安全生产有关的资格，并处上一年年收入百分之二十以上百分之五十以下的罚款；构成犯罪的，依照刑法有关规定追究刑事责任。

第九十七条 生产经营单位有下列行为之一的，责令限期改正，处十万元以下的罚款；逾期未改正的，责令停产停业整顿，并处十万元以上二十万元以下的罚款，对其直接负责的主管人员和其他直接责任人员处二万元以上五万元以下的罚款：

(一)未按照规定设置安全生产管理机构或者配备安全生产管理人员、注册安全工程师的；

(二)危险物品的生产、经营、储存、装卸单位以及矿山、金属冶炼、建筑施工、运输单位的主要负责人和安全生产管理人员未按照规定经考核合格的；

(三)未按照规定对从业人员、被派遣劳动者、实习学生进行安全生产教育和培训，或者未按照规定如实告知有关的安全生产事项的；

(四)未如实记录安全生产教育和培训情况的；

(五)未将事故隐患排查治理情况如实记录或者未向从业人员通报的；

(六)未按照规定制定生产安全事故应急救援预案或者未定期组织演练的；

(七)特种作业人员未按照规定经专门的安全作业培训并取得相应资格，上岗作业的。

第九十八条 生产经营单位有下列行为之一的，责令停止建设或者停产停业整顿，限期改正，并处十万元以上五十万元以下的罚款，对其直接负责的主管人员和其他直接责任人员处二万元以上五万元以下的罚款；逾期未改正的，处五十万元以上一百万元以下的罚款，对其直接负责的主管人员和其他直接责任人员处五万元以上十万元以下的罚款；构成犯罪的，依照刑法有关规定追究刑事责任：

(一)未按照规定对矿山、金属冶炼建设项目或者用于生产、储存、装卸危险物品的建设项目进行安全评价的；

(二)矿山、金属冶炼建设项目或者用于生产、储存、装卸危险物品的建设项目没有安全设施设计或者安全设施设计未按照规定报经有关部门审查同意的;

(三)矿山、金属冶炼建设项目或者用于生产、储存、装卸危险物品的建设项目的施工单位未按照批准的安全设施设计施工的;

(四)矿山、金属冶炼建设项目或者用于生产、储存、装卸危险物品的建设项目竣工投入生产或者使用前,安全设施未经验收合格的。

第九十九条 生产经营单位有下列行为之一的,责令限期改正,处五万元以下的罚款;逾期未改正的,处五万元以上二十万元以下的罚款,对其直接负责的主管人员和其他直接责任人员处一万元以上二万元以下的罚款;情节严重的,责令停产停业整顿;构成犯罪的,依照刑法有关规定追究刑事责任:

(一)未在有较大危险因素的生产经营场所和有关设施、设备上设置明显的安全警示标志的;

(二)安全设备的安装、使用、检测、改造和报废不符合国家标准或者行业标准的;

(三)未对安全设备进行经常性维护、保养和定期检测的;

(四)关闭、破坏直接关系生产安全的监控、报警、防护、救生设备、设施,或者篡改、隐瞒、销毁其相关数据、信息的;

(五)未为从业人员提供符合国家标准或者行业标准的劳动防护用品的;

(六)危险物品的容器、运输工具,以及涉及人身安全、危险性较大的海洋石油开采特种设备和矿山井下特种设备未经具有专业资质的机构检测、检验合格,取得安全使用证或者安全标志,投入使用的;

(七)使用应当淘汰的危及生产安全的工艺、设备的。

(八)餐饮等行业的生产经营单位使用燃气未安装可燃气体报警装置的。

第一百条 未经依法批准,擅自生产、经营、运输、储存、使用危险物品或者处置废弃危险物品的,依照有关危险物品安全管理的法律、行政法规的规定予以处罚;构成犯罪的,依照刑法有关规定追究刑事责任。

第一百零一条 生产经营单位有下列行为之一的,责令限期改正,处十万元以下的罚款;逾期未改正的,责令停产停业整顿,并处十万元以上二十万元

以下的罚款，对其直接负责的主管人员和其他直接责任人员处二万元以上五万元以下的罚款；构成犯罪的，依照刑法有关规定追究刑事责任：

(一)生产、经营、运输、储存、使用危险物品或者处置废弃危险物品，未建立专门安全管理制度、未采取可靠的安全措施的；

(二)对重大危险源未登记建档，未进行定期检测、评估、监控，未制定应急预案，或者未告知应急措施的；

(三)进行爆破、吊装、动火、临时用电以及国务院应急管理部门会同国务院有关部门规定的其他危险作业，未安排专门人员进行现场安全管理的；

(四)未建立安全风险分级管控制度或者未按照安全风险分级采取相应管控措施的；

(五)未建立事故隐患排查治理制度，或者重大事故隐患排查治理情况未按照规定报告的。

第一百零二条 生产经营单位未采取措施消除事故隐患的，责令立即消除或者限期消除，处五万元以下的罚款；生产经营单位拒不执行的，责令停产停业整顿，对其直接负责的主管人员和其他直接责任人员处五万元以上十万元以下的罚款；构成犯罪的，依照刑法有关规定追究刑事责任。

第一百零三条 生产经营单位将生产经营项目、场所、设备发包或者出租给不具备安全生产条件或者相应资质的单位或者个人的，责令限期改正，没收违法所得；违法所得十万元以上的，并处违法所得二倍以上五倍以下的罚款；没有违法所得或者违法所得不足十万元的，单处或者并处十万元以上二十万元以下的罚款；对其直接负责的主管人员和其他直接责任人员处一万元以上二万元以下的罚款；导致发生生产安全事故给他人造成损害的，与承包方、承租方承担连带赔偿责任。

生产经营单位未与承包单位、承租单位签订专门的安全生产管理协议或者未在承包合同、租赁合同中明确各自的安全生产管理职责，或者未对承包单位、承租单位的安全生产统一协调、管理的，责令限期改正，处五万元以下的罚款，对其直接负责的主管人员和其他直接责任人员处一万元以下的罚款；逾期未改正的，责令停产停业整顿。

矿山、金属冶炼建设项目和用于生产、储存、装卸危险物品的建设项目的

施工单位未按照规定对施工项目进行安全管理的，责令限期改正，处十万元以下的罚款，对其直接负责的主管人员和其他直接责任人员处二万元以下的罚款；逾期未改正的，责令停产停业整顿。以上施工单位倒卖、出租、出借、挂靠或者以其他形式非法转让施工资质的，责令停产停业整顿，吊销资质证书，没收违法所得；违法所得十万元以上的，并处违法所得二倍以上五倍以下的罚款，没有违法所得或者违法所得不足十万元的，单处或者并处十万元以上二十万元以下的罚款；对其直接负责的主管人员和其他直接责任人员处五万元以上十万元以下的罚款；构成犯罪的，依照刑法有关规定追究刑事责任。

第一百零四条 两个以上生产经营单位在同一作业区域内进行可能危及对方安全生产的生产经营活动，未签订安全生产管理协议或者未指定专职安全生产管理人员进行安全检查与协调的，责令限期改正，处五万元以下的罚款，对其直接负责的主管人员和其他直接责任人员处一万元以下的罚款；逾期未改正的，责令停产停业。

第一百零五条 生产经营单位有下列行为之一的，责令限期改正，处五万元以下的罚款，对其直接负责的主管人员和其他直接责任人员处一万元以下的罚款；逾期未改正的，责令停产停业整顿；构成犯罪的，依照刑法有关规定追究刑事责任：

(一)生产、经营、储存、使用危险物品的车间、商店、仓库与员工宿舍在同一座建筑内，或者与员工宿舍的距离不符合安全要求的；

(二)生产经营场所和员工宿舍未设有符合紧急疏散需要、标志明显、保持畅通的出口、疏散通道，或者占用、锁闭、封堵生产经营场所或者员工宿舍出口、疏散通道的。

第一百零六条 生产经营单位与从业人员订立协议，免除或者减轻其对从业人员因生产安全事故伤亡依法应承担的责任的，该协议无效；对生产经营单位的主要负责人、个人经营的投资人处二万元以上十万元以下的罚款。

第一百零七条 生产经营单位的从业人员不落实岗位安全责任，不服从管理，违反安全生产规章制度或者操作规程的，由生产经营单位给予批评教育，依照有关规章制度给予处分；构成犯罪的，依照刑法有关规定追究刑事责任。

第一百零八条 违反本法规定，生产经营单位拒绝、阻碍负有安全生产监

督管理职责的部门依法实施监督检查的，责令改正；拒不改正的，处二万元以上二十万元以下的罚款；对其直接负责的主管人员和其他直接责任人员处一万元以上二万元以下的罚款；构成犯罪的，依照刑法有关规定追究刑事责任。

第一百零九条 高危行业、领域的生产经营单位未按照国家规定投保安全生产责任保险的，责令限期改正，处五万元以上十万元以下的罚款；逾期未改正的，处十万元以上二十万元以下的罚款。

第一百一十条 生产经营单位的主要负责人在本单位发生生产安全事故时，不立即组织抢救或者在事故调查处理期间擅离职守或者逃匿的，给予降级、撤职的处分，并由应急管理部门处上一年年收入百分之六十至百分之一百的罚款；对逃匿的处十五日以下拘留；构成犯罪的，依照刑法有关规定追究刑事责任。

生产经营单位的主要负责人对生产安全事故隐瞒不报、谎报或者迟报的，依照前款规定处罚。

第一百一十一条 有关地方人民政府、负有安全生产监督管理职责的部门，对生产安全事故隐瞒不报、谎报或者迟报的，对直接负责的主管人员和其他直接责任人员依法给予处分；构成犯罪的，依照刑法有关规定追究刑事责任。

第一百一十二条 生产经营单位违反本法规定，被责令改正且受到罚款处罚，拒不改正的，负有安全生产监督管理职责的部门可以自作出责令改正之日的次日起，按照原处罚数额按日连续处罚。

第一百一十三条 生产经营单位存在下列情形之一的，负有安全生产监督管理职责的部门应当提请地方人民政府予以关闭，有关部门应当依法吊销其有关证照。生产经营单位主要负责人五年内不得担任任何生产经营单位的主要负责人；情节严重的，终身不得担任本行业生产经营单位的主要负责人：

(一)存在重大事故隐患，一百八十日内三次或者一年内四次受到本法规定的行政处罚的；

(二)经停产停业整顿，仍不具备法律、行政法规和国家标准或者行业标准规定的安全生产条件的；

(三)不具备法律、行政法规和国家标准或者行业标准规定的安全生产条

件，导致发生重大、特别重大生产安全事故的；

(四)拒不执行负有安全生产监督管理职责的部门作出的停产停业整顿决定的。

第一百一十四条 发生生产安全事故，对负有责任的生产经营单位除要求其依法承担相应的赔偿等责任外，由应急管理部门依照下列规定处以罚款：

(一)发生一般事故的，处三十万元以上一百万元以下的罚款；

(二)发生较大事故的，处一百万元以上二百万元以下的罚款；

(三)发生重大事故的，处二百万元以上一千万元以下的罚款；

(四)发生特别重大事故的，处一千万元以上二千万元以下的罚款。

发生生产安全事故，情节特别严重、影响特别恶劣的，应急管理部门可以按照前款罚款数额的二倍以上五倍以下对负有责任的生产经营单位处以罚款。

第一百一十五条 本法规定的行政处罚，由应急管理部门和其他负有安全生产监督管理职责的部门按照职责分工决定；其中，根据本法第九十五条、第一百一十条、第一百一十四条的规定应当给予民航、铁路、电力行业的生产经营单位及其主要负责人行政处罚的，也可以由主管的负有安全生产监督管理职责的部门进行处罚。予以关闭的行政处罚，由负有安全生产监督管理职责的部门报请县级以上人民政府按照国务院规定的权限决定；给予拘留的行政处罚，由公安机关依照治安管理处罚的规定决定。

第一百一十六条 生产经营单位发生生产安全事故造成人员伤亡、他人财产损失的，应当依法承担赔偿责任；拒不承担或者其负责人逃匿的，由人民法院依法强制执行。

生产安全事故的责任人未依法承担赔偿责任，经人民法院依法采取执行措施后，仍不能对受害人给予足额赔偿的，应当继续履行赔偿义务；受害人发现责任人有其他财产的，可以随时请求人民法院执行。

第七章 附 则

第一百一十七条 本法下列用语的含义：

危险物品，是指易燃易爆物品、危险化学品、放射性物品等能够危及人身安全和财产安全的物品。

重大危险源，是指长期地或者临时地生产、搬运、使用或者储存危险物

品，且危险物品的数量等于或者超过临界量的单元(包括场所和设施)。

第一百一十八条 本法规定的生产安全一般事故、较大事故、重大事故、特别重大事故的划分标准由国务院规定。

国务院应急管理部门和其他负有安全生产监督管理职责的部门应当根据各自的职责分工，制定相关行业、领域重大危险源的辨识标准和重大事故隐患的判定标准。

第一百一十九条 本法自 2002 年 11 月 1 日起施行。

中华人民共和国电子签名法

(2004 年 8 月 28 日第十届全国人民代表大会常务委员会第十一次会议通过 根据 2015 年 4 月 24 日第十二届全国人民代表大会常务委员会第十四次会议《关于修改〈中华人民共和国电力法〉等六部法律的决定》第一次修正 根据 2019 年 4 月 23 日第十三届全国人民代表大会常务委员会第十次会议《关于修改〈中华人民共和国建筑法〉等八部法律的决定》第二次修正)

第一章 总 则

第一条 为了规范电子签名行为，确立电子签名的法律效力，维护有关各方的合法权益，制定本法。

第二条 本法所称电子签名，是指数据电文中以电子形式所含、所附用于识别签名人身份并表明签名人认可其中内容的数据。

本法所称数据电文，是指以电子、光学、磁或者类似手段生成、发送、接收或者储存的信息。

第三条 民事活动中的合同或者其他文件、单证等文书，当事人可以约定使用或者不使用电子签名、数据电文。

当事人约定使用电子签名、数据电文的文书，不得仅因为其采用电子签名、数据电文的形式而否定其法律效力。

前款规定不适用下列文书：

(一)涉及婚姻、收养、继承等人身关系的；

(二)涉及停止供水、供热、供气等公用事业服务的；

(三)法律、行政法规规定的不适用电子文书的其他情形。

第二章 数据电文

第四条 能够有形地表现所载内容，并可以随时调取查用的数据电文，视为符合法律、法规要求的书面形式。

第五条 符合下列条件的数据电文，视为满足法律、法规规定的原件形式要求：

(一)能够有效地表现所载内容并可供随时调取查用；

(二)能够可靠地保证自最终形成时起，内容保持完整、未被更改。但是， 在数据电文上增加背书以及数据交换、储存和显示过程中发生的形式变化不影响数据电文的完整性。

第六条 符合下列条件的数据电文，视为满足法律、法规规定的文件保存要求：

(一)能够有效地表现所载内容并可供随时调取查用；

(二)数据电文的格式与其生成、发送或者接收时的格式相同， 或者格式不相同但是能够准确表现原来生成、发送或者接收的内容；

(三)能够识别数据电文的发件人、收件人以及发送、接收的时间。

第七条 数据电文不得仅因为其是以电子、光学、磁或者类似手段生成、发送、接收或者储存的而被拒绝作为证据使用。

第八条 审查数据电文作为证据的真实性，应当考虑以下因素：

(一)生成、储存或者传递数据电文方法的可靠性；

(二)保持内容完整性方法的可靠性；

(三)用以鉴别发件人方法的可靠性；

(四)其他相关因素。

第九条 数据电文有下列情形之一的，视为发件人发送：

(一)经发件人授权发送的；

(二)发件人的信息系统自动发送的；

(三)收件人按照发件人认可的方法对数据电文进行验证后结果相符的。

当事人对前款规定的事项另有约定的，从其约定。

第十条 法律、行政法规规定或者当事人约定数据电文需要确认收讫的，应当确认收讫。发件人收到收件人的收讫确认时，数据电文视为已经收到。

第十一条 数据电文进入发件人控制之外的某个信息系统的时间，视为该数

据电文的发送时间。

收件人指定特定系统接收数据电文的，数据电文进入该特定系统的时间，视为该数据电文的接收时间；未指定特定系统的，数据电文进入收件人的任何系统的首次时间，视为该数据电文的接收时间。

当事人对数据电文的发送时间、接收时间另有约定的，从其约定。

第十二条 发件人的主营业地为数据电文的发送地点，收件人的主营业地为数据电文的接收地点。没有主营业地的，其经常居住地为发送或者接收地点。

当事人对数据电文的发送地点、接收地点另有约定的，从其约定。

第三章 电子签名与认证

第十三条 电子签名同时符合下列条件的，视为可靠的电子签名：

(一)电子签名制作数据用于电子签名时，属于电子签名人专有；

(二)签署时电子签名制作数据仅由电子签名人控制；

(三)签署后对电子签名的任何改动能够被发现；

(四)签署后对数据电文内容和形式的任何改动能够被发现。

当事人也可以选择使用符合其约定的可靠条件的电子签名。

第十四条 可靠的电子签名与手写签名或者盖章具有同等的法律效力。

第十五条 电子签名人应当妥善保管电子签名制作数据。电子签名人知悉电子签名制作数据已经失密或者可能已经失密时，应当及时告知有关各方，并终止使用该电子签名制作数据。

第十六条 电子签名需要第三方认证的，由依法设立的电子认证服务提供者提供认证服务。

第十七条 提供电子认证服务，应当具备下列条件：

(一)取得企业法人资格；

(二)具有与提供电子认证服务相适应的专业技术人员和管理人员；

(三)具有与提供电子认证服务相适应的资金和经营场所；

(四)具有符合国家安全标准的技术和设备；

(五)具有国家密码管理机构同意使用密码的证明文件；

(六)法律、行政法规规定的其他条件。

第十八条 从事电子认证服务，应当向国务院信息产业主管部门提出申请，

并提交符合本法第十七条规定条件的相关材料。国务院信息产业主管部门接到申请后经依法审查，征求国务院商务主管部门等有关部门的意见后，自接到申请之日起四十五日内作出许可或者不予许可的决定。予以许可的，颁发电子认证许可证书；不予许可的，应当书面通知申请人并告知理由。

取得认证资格的电子认证服务提供者，应当按照国务院信息产业主管部门的规定在互联网上公布其名称、许可证号等信息。

第十九条 电子认证服务提供者应当制定、公布符合国家有关规定的电子认证业务规则，并向国务院信息产业主管部门备案。

电子认证业务规则应当包括责任范围、作业操作规范、信息安全保障措施等事项。

第二十条 电子签名人向电子认证服务提供者申请电子签名认证证书，应当提供真实、完整和准确的信息。

电子认证服务提供者收到电子签名认证证书申请后，应当对申请人的身份进行查验，并对有关材料进行审查。

第二十一条 电子认证服务提供者签发的电子签名认证证书应当准确无误，并应当载明下列内容：

(一)电子认证服务提供者名称；

(二)证书持有人名称；

(三)证书序列号；

(四)证书有效期；

(五)证书持有人的电子签名验证数据；

(六)电子认证服务提供者的电子签名；

(七)国务院信息产业主管部门规定的其他内容。

第二十二条 电子认证服务提供者应当保证电子签名认证证书内容在有效期内完整、准确，并保证电子签名依赖方能够证实或者了解电子签名认证证书所载内容及其他有关事项。

第二十三条 电子认证服务提供者拟暂停或者终止电子认证服务的，应当在暂停或者终止服务九十日前，就业务承接及其他有关事项通知有关各方。

电子认证服务提供者拟暂停或者终止电子认证服务的，应当在暂停或者终止

服务六十日前向国务院信息产业主管部门报告，并与其他电子认证服务提供者就业务承接进行协商，作出妥善安排。

电子认证服务提供者未能就业务承接事项与其他电子认证服务提供者达成协议的，应当申请国务院信息产业主管部门安排其他电子认证服务提供者承接其业务。

电子认证服务提供者被依法吊销电子认证许可证书的，其业务承接事项的处理按照国务院信息产业主管部门的规定执行。

第二十四条 电子认证服务提供者应当妥善保存与认证相关的信息，信息保存期限至少为电子签名认证证书失效后五年。

第二十五条 国务院信息产业主管部门依照本法制定电子认证服务业的具体管理办法，对电子认证服务提供者依法实施监督管理。

第二十六条 经国务院信息产业主管部门根据有关协议或者对等原则核准后，中华人民共和国境外的电子认证服务提供者在境外签发的电子签名认证证书与依照本法设立的电子认证服务提供者签发的电子签名认证证书具有同等的法律效力。

第四章 法律责任

第二十七条 电子签名人知悉电子签名制作数据已经失密或者可能已经失密未及时告知有关各方、并终止使用电子签名制作数据， 未向电子认证服务提供者提供真实、完整和准确的信息， 或者有其他过错，给电子签名依赖方、电子认证服务提供者造成损失的，承担赔偿责任。

第二十八条 电子签名人或者电子签名依赖方因依据电子认证服务提供者提供的电子签名认证服务从事民事活动遭受损失，电子认证服务提供者不能证明自己无过错的，承担赔偿责任。

第二十九条 未经许可提供电子认证服务的， 由国务院信息产业主管部门责令停止违法行为；有违法所得的，没收违法所得；违法所得三十万元以上的，处违法所得一倍以上三倍以下的罚款；没有违法所得或者违法所得不足三十万元的，处十万元以上三十万元以下的罚款。

第三十条 电子认证服务提供者暂停或者终止电子认证服务，未在暂停或者终止服务六十日前向国务院信息产业主管部门报告的，由国务院信息产业主管部

门对其直接负责的主管人员处一万元以上五万元以下的罚款。

第三十一条 电子认证服务提供者不遵守认证业务规则、未妥善保存与认证相关的信息，或者有其他违法行为的，由国务院信息产业主管部门责令限期改正；逾期未改正的，吊销电子认证许可证书，其直接负责的主管人员和其他直接责任人员十年内不得从事电子认证服务。吊销电子认证许可证书的， 应当予以公告并通知工商行政管理部门。

第三十二条 伪造、冒用、盗用他人的电子签名，构成犯罪的，依法追究刑事责任；给他人造成损失的，依法承担民事责任。

第三十三条 依照本法负责电子认证服务业监督管理工作的部门的工作人员，不依法履行行政许可、监督管理职责的， 依法给予行政处分；构成犯罪的，依法追究刑事责任。

第五章 附 则

第三十四条 本法中下列用语的含义：

(一)电子签名人，是指持有电子签名制作数据并以本人身份或者以其所代表的人的名义实施电子签名的人；

(二)电子签名依赖方，是指基于对电子签名认证证书或者电子签名的信赖从事有关活动的人；

(三)电子签名认证证书，是指可证实电子签名人与电子签名制作数据有联系的数据电文或者其他电子记录；

(四)电子签名制作数据，是指在电子签名过程中使用的，将电子签名与电子签名人可靠地联系起来的字符、编码等数据；

(五)电子签名验证数据，是指用于验证电子签名的数据，包括代码、口令、算法或者公钥等。

第三十五条 国务院或者国务院规定的部门可以依据本法制定政务活动和其他社会活动中使用电子签名、数据电文的具体办法。

第三十六条 本法自 2005 年 4 月 1 日起施行。

中华人民共和国治安管理处罚法

(2005 年 8 月 28 日第十届全国人民代表大会常务委员会第十七次会议通过 根据 2012 年 10 月 26 日第十一届全国人民代表大会常务委员会第二十九次会议

《关于修改〈中华人民共和国治安管理处罚法〉的决定》修正)

第一章 总 则

第一条 为维护社会治安秩序，保障公共安全，保护公民、法人和其他组织的合法权益，规范和保障公安机关及其人民警察依法履行治安管理职责，制定本法。

第二条 扰乱公共秩序，妨害公共安全，侵犯人身权利、财产权利，妨害社会管理，具有社会危害性，依照《中华人民共和国刑法》的规定构成犯罪的， 依法追究刑事责任；尚不够刑事处罚的， 由公安机关依照本法给予治安管理处罚。

第三条 治安管理处罚的程序，适用本法的规定；本法没有规定的，适用《中华人民共和国行政处罚法》的有关规定。

第四条 在中华人民共和国领域内发生的违反治安管理行为，除法律有特别规定的外，适用本法。

在中华人民共和国船舶和航空器内发生的违反治安管理行为，除法律有特别规定的外，适用本法。

第五条 治安管理处罚必须以事实为依据，与违反治安管理行为的性质、情节以及社会危害程度相当。

实施治安管理处罚，应当公开、公正， 尊重和保障人权，保护公民的人格尊严。

办理治安案件应当坚持教育与处罚相结合的原则。

第六条 各级人民政府应当加强社会治安综合治理，采取有效措施，化解社会矛盾，增进社会和谐，维护社会稳定。

第七条 国务院公安部门负责全国的治安管理工作。县级以上地方各级人民政府公安机关负责本行政区域内的治安管理工作。

治安案件的管辖由国务院公安部门规定。

第八条 违反治安管理的行为对他人造成损害的，行为人或者其监护人应当依法承担民事责任。

第九条 对于因民间纠纷引起的打架斗殴或者损毁他人财物等违反治安管理行为，情节较轻的，公安机关可以调解处理。经公安机关调解， 当事人达成协议的，不予处罚。经调解未达成协议或者达成协议后不履行的， 公安机关应当依照

本法的规定对违反治安管理行为人给予处罚，并告知当事人可以就民事争议依法向人民法院提起民事诉讼。

第二章 处罚的种类和适用

第十条 治安管理处罚的种类分为：

(一)警告；

(二)罚款；

(三)行政拘留；

(四)吊销公安机关发放的许可证。

对违反治安管理的外国人，可以附加适用限期出境或者驱逐出境。

第十一条 办理治安案件所查获的毒品、淫秽物品等违禁品，赌具、赌资，吸食、注射毒品的用具以及直接用于实施违反治安管理行为的本人所有的工具，应当收缴，按照规定处理。

违反治安管理所得的财物，追缴退还被侵害人；没有被侵害人的，登记造册，公开拍卖或者按照国家有关规定处理，所得款项上缴国库。

第十二条 已满十四周岁不满十八周岁的人违反治安管理的，从轻或者减轻处罚；不满十四周岁的人违反治安管理的，不予处罚，但是应当责令其监护人严加管教。

第十三条 精神病人在不能辨认或者不能控制自己行为的时候违反治安管理的，不予处罚，但是应当责令其监护人严加看管和治疗。间歇性的精神病人在精神正常的时候违反治安管理的，应当给予处罚。

第十四条 盲人或者又聋又哑的人违反治安管理的，可以从轻、减轻或者不予处罚。

第十五条 醉酒的人违反治安管理的，应当给予处罚。

醉酒的人在醉酒状态中，对本人有危险或者对他人的人身、财产或者公共安全有威胁的，应当对其采取保护性措施约束至酒醒。

第十六条 有两种以上违反治安管理行为的，分别决定，合并执行。行政拘留处罚合并执行的，最长不超过二十日。

第十七条 共同违反治安管理的，根据违反治安管理行为人在违反治安管理行为中所起的作用，分别处罚。

教唆、胁迫、诱骗他人违反治安管理的， 按照其教唆、胁迫、诱骗的行为处罚。

第十八条 单位违反治安管理的，对其直接负责的主管人员和其他直接责任人员依照本法的规定处罚。其他法律、行政法规对同一行为规定给予单位处罚的，依照其规定处罚。

第十九条 违反治安管理有下列情形之一的，减轻处罚或者不予处罚：

(一)情节特别轻微的；

(二)主动消除或者减轻违法后果，并取得被侵害人谅解的；

(三)出于他人胁迫或者诱骗的；

(四)主动投案，向公安机关如实陈述自己的违法行为的；

(五)有立功表现的。

第二十条 违反治安管理有下列情形之一的，从重处罚：

(一)有较严重后果的；

(二)教唆、胁迫、诱骗他人违反治安管理的；

(三)对报案人、控告人、举报人、证人打击报复的；

(四)六个月内曾受过治安管理处罚的。

第二十一条 违反治安管理行为人有下列情形之一，依照本法应当给予行政拘留处罚的，不执行行政拘留处罚：

(一)已满十四周岁不满十六周岁的；

(二)已满十六周岁不满十八周岁，初次违反治安管理的；

(三)七十周岁以上的；

(四)怀孕或者哺乳自己不满一周岁婴儿的。

第二十二条 违反治安管理行为在六个月内没有被公安机关发现的，不再处罚。

前款规定的期限，从违反治安管理行为发生之日起计算；违反治安管理行为有连续或者继续状态的，从行为终了之日起计算。

第三章 违反治安管理的行为和处罚

第一节 扰乱公共秩序的行为和处罚

第二十三条 有下列行为之一的，处警告或者二百元以下罚款；情节较重的，

处五日以上十日以下拘留，可以并处五百元以下罚款：

(一)扰乱机关、团体、企业、事业单位秩序， 致使工作、生产、营业、医疗、教学、科研不能正常进行，尚未造成严重损失的；

(二)扰乱车站、港口、码头、机场、商场、公园、展览馆或者其他公共场所秩序的；

(三)扰乱公共汽车、电车、火车、船舶、航空器或者其他公共交通工具上的秩序的；

(四)非法拦截或者强登、扒乘机动车、船舶、航空器以及其他交通工具， 影响交通工具正常行驶的；

(五)破坏依法进行的选举秩序的。

聚众实施前款行为的，对首要分子处十日以上十五日以下拘留，可以并处一千元以下罚款。

第二十四条 有下列行为之一，扰乱文化、体育等大型群众性活动秩序的，处警告或者二百元以下罚款；情节严重的，处五日以上十日以下拘留，可以并处五百元以下罚款：

(一)强行进入场内的；

(二)违反规定，在场内燃放烟花爆竹或者其他物品的；

(三)展示侮辱性标语、条幅等物品的；

(四)围攻裁判员、运动员或者其他工作人员的；

(五)向场内投掷杂物，不听制止的；

(六)扰乱大型群众性活动秩序的其他行为。

因扰乱体育比赛秩序被处以拘留处罚的，可以同时责令其十二个月内不得进入体育场馆观看同类比赛；违反规定进入体育场馆的，强行带离现场。

第二十五条 有下列行为之一的，处五日以上十日以下拘留，可以并处五百元以下罚款；情节较轻的，处五日以下拘留或者五百元以下罚款：

(一)散布谣言，谎报险情、疫情、警情或者以其他方法故意扰乱公共秩序的；

(二)投放虚假的爆炸性、毒害性、放射性、腐蚀性物质或者传染病病原体等危险物质扰乱公共秩序的；

(三)扬言实施放火、爆炸、投放危险物质扰乱公共秩序的。

第二十六条 有下列行为之一的，处五日以上十日以下拘留，可以并处五百元以下罚款；情节较重的，处十日以上十五日以下拘留，可以并处一千元以下罚款：

(一)结伙斗殴的；

(二)追逐、拦截他人的；

(三)强拿硬要或者任意损毁、占用公私财物的；

(四)其他寻衅滋事行为。

第二十七条 有下列行为之一的，处十日以上十五日以下拘留，可以并处一千元以下罚款；情节较轻的，处五日以上十日以下拘留，可以并处五百元以下罚款：

(一)组织、教唆、胁迫、诱骗、煽动他人从事邪教、会道门活动或者利用邪教、会道门、迷信活动，扰乱社会秩序、损害他人身体健康的；

(二)冒用宗教、气功名义进行扰乱社会秩序、损害他人身体健康活动的。

第二十八条 违反国家规定，故意干扰无线电业务正常进行的，或者对正常运行的无线电台(站)产生有害干扰，经有关主管部门指出后，拒不采取有效措施消除的，处五日以上十日以下拘留；情节严重的，处十日以上十五日以下拘留。

第二十九条 有下列行为之一的，处五日以下拘留；情节较重的，处五日以上十日以下拘留：

(一)违反国家规定，侵入计算机信息系统，造成危害的；

(二)违反国家规定，对计算机信息系统功能进行删除、修改、增加、干扰，造成计算机信息系统不能正常运行的；

(三)违反国家规定，对计算机信息系统中存储、处理、传输的数据和应用程序进行删除、修改、增加的；

(四)故意制作、传播计算机病毒等破坏性程序， 影响计算机信息系统正常运行的。

第二节 妨害公共安全的行为和处罚

第三十条 违反国家规定，制造、买卖、储存、运输、邮寄、携带、使用、提供、处置爆炸性、毒害性、放射性、腐蚀性物质或者传染病病原体等危险物质的，处十日以上十五日以下拘留；情节较轻的，处五日以上十日以下拘留。

第三十一条 爆炸性、毒害性、放射性、腐蚀性物质或者传染病病原体等危险物质被盗、被抢或者丢失， 未按规定报告的，处五日以下拘留；故意隐瞒不报的，处五日以上十日以下拘留。

第三十二条 非法携带枪支、弹药或者弩、匕首等国家规定的管制器具的，处五日以下拘留，可以并处五百元以下罚款；情节较轻的，处警告或者二百元以下罚款。

非法携带枪支、弹药或者弩、匕首等国家规定的管制器具进入公共场所或者公共交通工具的，处五日以上十日以下拘留，可以并处五百元以下罚款。

第三十三条 有下列行为之一的，处十日以上十五日以下拘留：

(一)盗窃、损毁油气管道设施、电力电信设施、广播电视设施、水利防汛工程设施或者水文监测、测量、气象测报、环境监测、地质监测、地震监测等公共设施的；

(二)移动、损毁国家边境的界碑、界桩以及其他边境标志、边境设施或者领土、领海标志设施的；

(三)非法进行影响国(边)界线走向的活动或者修建有碍国(边)境管理的设施的。

第三十四条 盗窃、损坏、擅自移动使用中的航空设施，或者强行进入航空器驾驶舱的，处十日以上十五日以下拘留。

在使用中的航空器上使用可能影响导航系统正常功能的器具、工具， 不听劝阻的，处五日以下拘留或者五百元以下罚款。

第三十五条 有下列行为之一的，处五日以上十日以下拘留，可以并处五百元以下罚款；情节较轻的，处五日以下拘留或者五百元以下罚款：

(一)盗窃、损毁或者擅自移动铁路设施、设备、机车车辆配件或者安全标志的；

(二)在铁路线路上放置障碍物，或者故意向列车投掷物品的；

(三)在铁路线路、桥梁、涵洞处挖掘坑穴、采石取沙的；

(四)在铁路线路上私设道口或者平交过道的。

第三十六条 擅自进入铁路防护网或者火车来临时在铁路线路上行走坐卧、抢越铁路，影响行车安全的，处警告或者二百元以下罚款。

第三十七条 有下列行为之一的，处五日以下拘留或者五百元以下罚款；情节严重的，处五日以上十日以下拘留，可以并处五百元以下罚款：

(一)未经批准，安装、使用电网的，或者安装、使用电网不符合安全规定的；

(二)在车辆、行人通行的地方施工， 对沟井坎穴不设覆盖物、防围和警示标志的，或者故意损毁、移动覆盖物、防围和警示标志的；

(三)盗窃、损毁路面井盖、照明等公共设施的。

第三十八条 举办文化、体育等大型群众性活动，违反有关规定，有发生安全事故危险的，责令停止活动，立即疏散；对组织者处五日以上十日以下拘留，并处二百元以上五百元以下罚款；情节较轻的，处五日以下拘留或者五百元以下罚款。

第三十九条 旅馆、饭店、影剧院、娱乐场、运动场、展览馆或者其他供社会公众活动的场所的经营管理人员，违反安全规定，致使该场所有发生安全事故危险，经公安机关责令改正，拒不改正的，处五日以下拘留。

第三节 侵犯人身权利、财产权利的行为和处罚

第四十条 有下列行为之一的，处十日以上十五日以下拘留，并处五百元以上一千元以下罚款；情节较轻的，处五日以上十日以下拘留，并处二百元以上五百元以下罚款：

(一)组织、胁迫、诱骗不满十六周岁的人或者残疾人进行恐怖、残忍表演的；

(二)以暴力、威胁或者其他手段强迫他人劳动的；

(三)非法限制他人人身自由、非法侵入他人住宅或者非法搜查他人身体的。

第四十一条 胁迫、诱骗或者利用他人乞讨的，处十日以上十五日以下拘留，可以并处一千元以下罚款。

反复纠缠、强行讨要或者以其他滋扰他人的方式乞讨的， 处五日以下拘留或者警告。

第四十二条 有下列行为之一的，处五日以下拘留或者五百元以下罚款；情节较重的，处五日以上十日以下拘留，可以并处五百元以下罚款：

(一)写恐吓信或者以其他方法威胁他人人身安全的；

(二)公然侮辱他人或者捏造事实诽谤他人的；

(三)捏造事实诬告陷害他人，企图使他人受到刑事追究或者受到治安管理处

罚的；

(四)对证人及其近亲属进行威胁、侮辱、殴打或者打击报复的；

(五)多次发送淫秽、侮辱、恐吓或者其他信息，干扰他人正常生活的；

(六)偷窥、偷拍、窃听、散布他人隐私的。

第四十三条 殴打他人的，或者故意伤害他人身体的，处五日以上十日以下拘留，并处二百元以上五百元以下罚款；情节较轻的，处五日以下拘留或者五百元以下罚款。

有下列情形之一的，处十日以上十五日以下拘留，并处五百元以上一千元以下罚款：

(一)结伙殴打、伤害他人的；

(二)殴打、伤害残疾人、孕妇、不满十四周岁的人或者六十周岁以上的人的；

(三)多次殴打、伤害他人或者一次殴打、伤害多人的。

第四十四条 猥亵他人的，或者在公共场所故意裸露身体，情节恶劣的，处五日以上十日以下拘留；猥亵智力残疾人、精神病人、不满十四周岁的人或者有其他严重情节的，处十日以上十五日以下拘留。

第四十五条 有下列行为之一的，处五日以下拘留或者警告：

(一)虐待家庭成员，被虐待人要求处理的；

(二)遗弃没有独立生活能力的被扶养人的。

第四十六条 强买强卖商品，强迫他人提供服务或者强迫他人接受服务的，处五日以上十日以下拘留，并处二百元以上五百元以下罚款；情节较轻的，处五日以下拘留或者五百元以下罚款。

第四十七条 煽动民族仇恨、民族歧视，或者在出版物、计算机信息网络中刊载民族歧视、侮辱内容的， 处十日以上十五日以下拘留，可以并处一千元以下罚款。

第四十八条 冒领、隐匿、毁弃、私自开拆或者非法检查他人邮件的，处五日以下拘留或者五百元以下罚款。

第四十九条 盗窃、诈骗、哄抢、抢夺、敲诈勒索或者故意损毁公私财物的，处五日以上十日以下拘留，可以并处五百元以下罚款；情节较重的，处十日以上十五日以下拘留，可以并处一千元以下罚款。

第四节 妨害社会管理的行为和处罚

第五十条 有下列行为之一的，处警告或者二百元以下罚款；情节严重的，处五日以上十日以下拘留，可以并处五百元以下罚款：

(一)拒不执行人民政府在紧急状态情况下依法发布的决定、命令的；

(二)阻碍国家机关工作人员依法执行职务的；

(三)阻碍执行紧急任务的消防车、救护车、工程抢险车、警车等车辆通行的；

(四)强行冲闯公安机关设置的警戒带、警戒区的。

阻碍人民警察依法执行职务的，从重处罚。

第五十一条 冒充国家机关工作人员或者以其他虚假身份招摇撞骗的，处五日以上十日以下拘留，可以并处五百元以下罚款；情节较轻的，处五日以下拘留或者五百元以下罚款。

冒充军警人员招摇撞骗的，从重处罚。

第五十二条 有下列行为之一的，处十日以上十五日以下拘留，可以并处一千元以下罚款；情节较轻的，处五日以上十日以下拘留，可以并处五百元以下罚款：

(一)伪造、变造或者买卖国家机关、人民团体、企业、事业单位或者其他组织的公文、证件、证明文件、印章的；

(二)买卖或者使用伪造、变造的国家机关、人民团体、企业、事业单位或者其他组织的公文、证件、证明文件的；

(三)伪造、变造、倒卖车票、船票、航空客票、文艺演出票、体育比赛入场券或者其他有价票证、凭证的；

(四)伪造、变造船舶户牌， 买卖或者使用伪造、变造的船舶户牌， 或者涂改船舶发动机号码的。

第五十三条 船舶擅自进入、停靠国家禁止、限制进入的水域或者岛屿的，对船舶负责人及有关责任人员处五百元以上一千元以下罚款；情节严重的，处五日以下拘留，并处五百元以上一千元以下罚款。

第五十四条 有下列行为之一的，处十日以上十五日以下拘留，并处五百元以上一千元以下罚款；情节较轻的，处五日以下拘留或者五百元以下罚款：

(一)违反国家规定，未经注册登记，以社会团体名义进行活动，被取缔后，

仍进行活动的；

(二)被依法撤销登记的社会团体，仍以社会团体名义进行活动的；

(三)未经许可，擅自经营按照国家规定需要由公安机关许可的行业的。

有前款第三项行为的，予以取缔。

取得公安机关许可的经营者，违反国家有关管理规定，情节严重的，公安机关可以吊销许可证。

第五十五条 煽动、策划非法集会、游行、示威，不听劝阻的，处十日以上十五日以下拘留。

第五十六条 旅馆业的工作人员对住宿的旅客不按规定登记姓名、身份证件种类和号码的，或者明知住宿的旅客将危险物质带入旅馆，不予制止的，处二百元以上五百元以下罚款。

旅馆业的工作人员明知住宿的旅客是犯罪嫌疑人员或者被公安机关通缉的人员，不向公安机关报告的，处二百元以上五百元以下罚款；情节严重的，处五日以下拘留，可以并处五百元以下罚款。

第五十七条 房屋出租人将房屋出租给无身份证件的人居住的，或者不按规定登记承租人姓名、身份证件种类和号码的，处二百元以上五百元以下罚款。

房屋出租人明知承租人利用出租房屋进行犯罪活动，不向公安机关报告的，处二百元以上五百元以下罚款；情节严重的，处五日以下拘留，可以并处五百元以下罚款。

第五十八条 违反关于社会生活噪声污染防治的法律规定，制造噪声干扰他人正常生活的，处警告；警告后不改正的，处二百元以上五百元以下罚款。

第五十九条 有下列行为之一的，处五百元以上一千元以下罚款；情节严重的，处五日以上十日以下拘留，并处五百元以上一千元以下罚款：

(一)典当业工作人员承接典当的物品，不查验有关证明、不履行登记手续，或者明知是违法犯罪嫌疑人、赃物，不向公安机关报告的；

(二)违反国家规定，收购铁路、油田、供电、电信、矿山、水利、测量和城市公用设施等废旧专用器材的；

(三)收购公安机关通报寻查的赃物或者有赃物嫌疑的物品的；

(四)收购国家禁止收购的其他物品的。

第六十条 有下列行为之一的，处五日以上十日以下拘留，并处二百元以上五百元以下罚款：

(一)隐藏、转移、变卖或者损毁行政执法机关依法扣押、查封、冻结的财物的；

(二)伪造、隐匿、毁灭证据或者提供虚假证言、谎报案情， 影响行政执法机关依法办案的；

(三)明知是赃物而窝藏、转移或者代为销售的；

(四)被依法执行管制、剥夺政治权利或者在缓刑、暂予监外执行中的罪犯或者被依法采取刑事强制措施的人，有违反法律、行政法规或者国务院有关部门的监督管理规定的行为。

第六十一条 协助组织或者运送他人偷越国(边)境的，处十日以上十五日以下拘留，并处一千元以上五千元以下罚款。

第六十二条 为偷越国(边)境人员提供条件的，处五日以上十日以下拘留，并处五百元以上二千元以下罚款。

偷越国(边)境的，处五日以下拘留或者五百元以下罚款。

第六十三条 有下列行为之一的，处警告或者二百元以下罚款；情节较重的，处五日以上十日以下拘留，并处二百元以上五百元以下罚款：

(一)刻划、涂污或者以其他方式故意损坏国家保护的文物、名胜古迹的；

(二)违反国家规定，在文物保护单位附近进行爆破、挖掘等活动， 危及文物安全的。

第六十四条 有下列行为之一的，处五百元以上一千元以下罚款；情节严重的，处十日以上十五日以下拘留，并处五百元以上一千元以下罚款：

(一)偷开他人机动车的；

(二)未取得驾驶证驾驶或者偷开他人航空器、机动船舶的。

第六十五条 有下列行为之一的，处五日以上十日以下拘留；情节严重的，处十日以上十五日以下拘留，可以并处一千元以下罚款：

(一)故意破坏、污损他人坟墓或者毁坏、丢弃他人尸骨、骨灰的；

(二)在公共场所停放尸体或者因停放尸体影响他人正常生活、工作秩序， 不听劝阻的。

第六十六条 卖淫、嫖娼的，处十日以上十五日以下拘留，可以并处五千元以下罚款；情节较轻的，处五日以下拘留或者五百元以下罚款。

在公共场所拉客招嫖的，处五日以下拘留或者五百元以下罚款。

第六十七条 引诱、容留、介绍他人卖淫的，处十日以上十五日以下拘留，可以并处五千元以下罚款；情节较轻的，处五日以下拘留或者五百元以下罚款。

第六十八条 制作、运输、复制、出售、出租淫秽的书刊、图片、影片、音像制品等淫秽物品或者利用计算机信息网络、电话以及其他通讯工具传播淫秽信息的，处十日以上十五日以下拘留，可以并处三千元以下罚款；情节较轻的，处五日以下拘留或者五百元以下罚款。

第六十九条 有下列行为之一的，处十日以上十五日以下拘留，并处五百元以上一千元以下罚款：

(一)组织播放淫秽音像的；

(二)组织或者进行淫秽表演的；

(三)参与聚众淫乱活动的。

明知他人从事前款活动，为其提供条件的，依照前款的规定处罚。

第七十条 以营利为目的，为赌博提供条件的，或者参与赌博赌资较大的，处五日以下拘留或者五百元以下罚款；情节严重的，处十日以上十五日以下拘留，并处五百元以上三千元以下罚款。

第七十一条 有下列行为之一的，处十日以上十五日以下拘留，可以并处三千元以下罚款；情节较轻的，处五日以下拘留或者五百元以下罚款：

(一)非法种植罂粟不满五百株或者其他少量毒品原植物的；

(二)非法买卖、运输、携带、持有少量未经灭活的罂粟等毒品原植物种子或者幼苗的；

(三)非法运输、买卖、储存、使用少量罂粟壳的。

有前款第一项行为，在成熟前自行铲除的，不予处罚。

第七十二条 有下列行为之一的，处十日以上十五日以下拘留，可以并处二千元以下罚款；情节较轻的，处五日以下拘留或者五百元以下罚款：

(一)非法持有鸦片不满二百克、海洛因或者甲基苯丙胺不满十克或者其他少量毒品的；

(二)向他人提供毒品的;

(三)吸食、注射毒品的;

(四)胁迫、欺骗医务人员开具麻醉药品、精神药品的。

第七十三条 教唆、引诱、欺骗他人吸食、注射毒品的,处十日以上十五日以下拘留,并处五百元以上二千元以下罚款。

第七十四条 旅馆业、饮食服务业、文化娱乐业、出租汽车业等单位的人员,在公安机关查处吸毒、赌博、卖淫、嫖娼活动时,为违法犯罪行为人通风报信的,处十日以上十五日以下拘留。

第七十五条 饲养动物,干扰他人正常生活的,处警告;警告后不改正的,或者放任动物恐吓他人的,处二百元以上五百元以下罚款。

驱使动物伤害他人的,依照本法第四十三条第一款的规定处罚。

第七十六条 有本法第六十七条、第六十八条、第七十条的行为,屡教不改的,可以按照国家规定采取强制性教育措施。

第四章 处罚程序

第一节 调查

第七十七条 公安机关对报案、控告、举报或者违反治安管理行为人主动投案,以及其他行政主管部门、司法机关移送的违反治安管理案件,应当及时受理,并进行登记。

第七十八条 公安机关受理报案、控告、举报、投案后,认为属于违反治安管理行为的,应当立即进行调查;认为不属于违反治安管理行为的,应当告知报案人、控告人、举报人、投案人,并说明理由。

第七十九条 公安机关及其人民警察对治安案件的调查,应当依法进行。严禁刑讯逼供或者采用威胁、引诱、欺骗等非法手段收集证据。

以非法手段收集的证据不得作为处罚的根据。

第八十条 公安机关及其人民警察在办理治安案件时,对涉及的国家秘密、商业秘密或者个人隐私,应当予以保密。

第八十一条 人民警察在办理治安案件过程中,遇有下列情形之一的,应当回避;违反治安管理行为人、被侵害人或者其法定代理人也有权要求他们回避:

(一)是本案当事人或者当事人的近亲属的;

(二)本人或者其近亲属与本案有利害关系的;

(三)与本案当事人有其他关系，可能影响案件公正处理的。

人民警察的回避，由其所属的公安机关决定；公安机关负责人的回避，由上一级公安机关决定。

第八十二条 需要传唤违反治安管理行为人接受调查的，经公安机关办案部门负责人批准，使用传唤证传唤。对现场发现的违反治安管理行为人， 人民警察经出示工作证件，可以口头传唤，但应当在询问笔录中注明。

公安机关应当将传唤的原因和依据告知被传唤人。对无正当理由不接受传唤或者逃避传唤的人，可以强制传唤。

第八十三条 对违反治安管理行为人，公安机关传唤后应当及时询问查证，询问查证的时间不得超过八小时；情况复杂，依照本法规定可能适用行政拘留处罚的，询问查证的时间不得超过二十四小时。

公安机关应当及时将传唤的原因和处所通知被传唤人家属。

第八十四条 询问笔录应当交被询问人核对；对没有阅读能力的，应当向其宣读。记载有遗漏或者差错的， 被询问人可以提出补充或者更正。被询问人确认笔录无误后，应当签名或者盖章，询问的人民警察也应当在笔录上签名。

被询问人要求就被询问事项自行提供书面材料的，应当准许；必要时，人民警察也可以要求被询问人自行书写。

询问不满十六周岁的违反治安管理行为人，应当通知其父母或者其他监护人到场。

第八十五条 人民警察询问被侵害人或者其他证人，可以到其所在单位或者住处进行；必要时，也可以通知其到公安机关提供证言。

人民警察在公安机关以外询问被侵害人或者其他证人，应当出示工作证件。

询问被侵害人或者其他证人，同时适用本法第八十四条的规定。

第八十六条 询问聋哑的违反治安管理行为人、被侵害人或者其他证人，应当有通晓手语的人提供帮助，并在笔录上注明。

询问不通晓当地通用的语言文字的违反治安管理行为人、被侵害人或者其他证人，应当配备翻译人员，并在笔录上注明。

第八十七条 公安机关对与违反治安管理行为有关的场所、物品、人身可以

进行检查。检查时， 人民警察不得少于二人，并应当出示工作证件和县级以上人民政府公安机关开具的检查证明文件。对确有必要立即进行检查的， 人民警察经出示工作证件，可以当场检查，但检查公民住所应当出示县级以上人民政府公安机关开具的检查证明文件。

检查妇女的身体，应当由女性工作人员进行。

第八十八条 检查的情况应当制作检查笔录， 由检查人、被检查人和见证人签名或者盖章；被检查人拒绝签名的，人民警察应当在笔录上注明。

第八十九条 公安机关办理治安案件，对与案件有关的需要作为证据的物品，可以扣押；对被侵害人或者善意第三人合法占有的财产，不得扣押，应当予以登记。对与案件无关的物品，不得扣押。

对扣押的物品，应当会同在场见证人和被扣押物品持有人查点清楚，当场开列清单一式二份，由调查人员、见证人和持有人签名或者盖章，一份交给持有人，另一份附卷备查。

对扣押的物品，应当妥善保管，不得挪作他用；对不宜长期保存的物品，按照有关规定处理。经查明与案件无关的， 应当及时退还；经核实属于他人合法财产的，应当登记后立即退还；满六个月无人对该财产主张权利或者无法查清权利人的，应当公开拍卖或者按照国家有关规定处理，所得款项上缴国库。

第九十条 为了查明案情，需要解决案件中有争议的专门性问题的，应当指派或者聘请具有专门知识的人员进行鉴定；鉴定人鉴定后，应当写出鉴定意见，并且签名。

第二节 决定

第九十一条 治安管理处罚由县级以上人民政府公安机关决定；其中警告、五百元以下的罚款可以由公安派出所决定。

第九十二条 对决定给予行政拘留处罚的人，在处罚前已经采取强制措施限制人身自由的时间，应当折抵。限制人身自由一日，折抵行政拘留一 日。

第九十三条 公安机关查处治安案件，对没有本人陈述，但其他证据能够证明案件事实的，可以作出治安管理处罚决定。但是， 只有本人陈述，没有其他证据证明的，不能作出治安管理处罚决定。

第九十四条 公安机关作出治安管理处罚决定前，应当告知违反治安管理行

为人作出治安管理处罚的事实、理由及依据， 并告知违反治安管理行为人依法享有的权利。

违反治安管理行为人有权陈述和申辩。公安机关必须充分听取违反治安管理行为人的意见，对违反治安管理行为人提出的事实、理由和证据，应当进行复核；违反治安管理行为人提出的事实、理由或者证据成立的，公安机关应当采纳。

公安机关不得因违反治安管理行为人的陈述、申辩而加重处罚。

第九十五条 治安案件调查结束后，公安机关应当根据不同情况，分别作出以下处理：

(一)确有依法应当给予治安管理处罚的违法行为的，根据情节轻重及具体情况，作出处罚决定；

(二)依法不予处罚的，或者违法事实不能成立的，作出不予处罚决定；

(三)违法行为已涉嫌犯罪的，移送主管机关依法追究刑事责任；

(四)发现违反治安管理行为人有其他违法行为的，在对违反治安管理行为作出处罚决定的同时，通知有关行政主管部门处理。

第九十六条 公安机关作出治安管理处罚决定的，应当制作治安管理处罚决定书。决定书应当载明下列内容：

(一)被处罚人的姓名、性别、年龄、身份证件的名称和号码、住址；

(二)违法事实和证据；

(三)处罚的种类和依据；

(四)处罚的执行方式和期限；

(五)对处罚决定不服，申请行政复议、提起行政诉讼的途径和期限；

(六)作出处罚决定的公安机关的名称和作出决定的日期。

决定书应当由作出处罚决定的公安机关加盖印章。

第九十七条 公安机关应当向被处罚人宣告治安管理处罚决定书，并当场交付被处罚人；无法当场向被处罚人宣告的，应当在二日内送达被处罚人。决定给予行政拘留处罚的，应当及时通知被处罚人的家属。

有被侵害人的，公安机关应当将决定书副本抄送被侵害人。

第九十八条 公安机关作出吊销许可证以及处二千元以上罚款的治安管理处罚决定前，应当告知违反治安管理行为人有权要求举行听证；违反治安管理行为

人要求听证的，公安机关应当及时依法举行听证。

第九十九条 公安机关办理治安案件的期限，自受理之日起不得超过三十日；案情重大、复杂的，经上一级公安机关批准，可以延长三十日。

为了查明案情进行鉴定的期间，不计入办理治安案件的期限。

第一百条 违反治安管理行为事实清楚，证据确凿，处警告或者二百元以下罚款的，可以当场作出治安管理处罚决定。

第一百零一条 当场作出治安管理处罚决定的，人民警察应当向违反治安管理行为人出示工作证件，并填写处罚决定书。处罚决定书应当当场交付被处罚人；有被侵害人的，并将决定书副本抄送被侵害人。

前款规定的处罚决定书，应当载明被处罚人的姓名、违法行为、处罚依据、罚款数额、时间、地点以及公安机关名称，并由经办的人民警察签名或者盖章。

当场作出治安管理处罚决定的，经办的人民警察应当在二十四小时内报所属公安机关备案。

第一百零二条 被处罚人对治安管理处罚决定不服的，可以依法申请行政复议或者提起行政诉讼。

第三节 执行

第一百零三条 对被决定给予行政拘留处罚的人，由作出决定的公安机关送达拘留所执行。

第一百零四条 受到罚款处罚的人应当自收到处罚决定书之日起十五日内，到指定的银行缴纳罚款。但是，有下列情形之一的，人民警察可以当场收缴罚款：

(一)被处五十元以下罚款，被处罚人对罚款无异议的；

(二)在边远、水上、交通不便地区， 公安机关及其人民警察依照本法的规定作出罚款决定后，被处罚人向指定的银行缴纳罚款确有困难，经被处罚人提出的；

(三)被处罚人在当地没有固定住所，不当场收缴事后难以执行的。

第一百零五条 人民警察当场收缴的罚款，应当自收缴罚款之日起二日内，交至所属的公安机关；在水上、旅客列车上当场收缴的罚款， 应当自抵岸或者到站之日起二日内，交至所属的公安机关；公安机关应当自收到罚款之日起二日内将罚款缴付指定的银行。

第一百零六条 人民警察当场收缴罚款的，应当向被处罚人出具省、自治区、

直辖市人民政府财政部门统一制发的罚款收据；不出具统一制发的罚款收据的，被处罚人有权拒绝缴纳罚款。

第一百零七条 被处罚人不服行政拘留处罚决定，申请行政复议、提起行政诉讼的，可以向公安机关提出暂缓执行行政拘留的申请。公安机关认为暂缓执行行政拘留不致发生社会危险的，由被处罚人或者其近亲属提出符合本法第一百零八条规定条件的担保人，或者按每日行政拘留二百元的标准交纳保证金，行政拘留的处罚决定暂缓执行。

第一百零八条 担保人应当符合下列条件：

(一)与本案无牵连；

(二)享有政治权利，人身自由未受到限制；

(三)在当地有常住户口和固定住所；

(四)有能力履行担保义务。

第一百零九条 担保人应当保证被担保人不逃避行政拘留处罚的执行。

担保人不履行担保义务，致使被担保人逃避行政拘留处罚的执行的，由公安机关对其处三千元以下罚款。

第一百一十条 被决定给予行政拘留处罚的人交纳保证金，暂缓行政拘留后，逃避行政拘留处罚的执行的，保证金予以没收并上缴国库，已经作出的行政拘留决定仍应执行。

第一百一十一条 行政拘留的处罚决定被撤销，或者行政拘留处罚开始执行的，公安机关收取的保证金应当及时退还交纳人。

第五章 执法监督

第一百一十二条 公安机关及其人民警察应当依法、公正、严格、高效办理治安案件，文明执法，不得徇私舞弊。

第一百一十三条 公安机关及其人民警察办理治安案件，禁止对违反治安管理行为人打骂、虐待或者侮辱。

第一百一十四条 公安机关及其人民警察办理治安案件，应当自觉接受社会和公民的监督。

公安机关及其人民警察办理治安案件，不严格执法或者有违法违纪行为的，任何单位和个人都有权向公安机关或者人民检察院、行政监察机关检举、控告；

收到检举、控告的机关，应当依据职责及时处理。

第一百一十五条 公安机关依法实施罚款处罚，应当依照有关法律、行政法规的规定，实行罚款决定与罚款收缴分离；收缴的罚款应当全部上缴国库。

第一百一十六条 人民警察办理治安案件，有下列行为之一的，依法给予行政处分；构成犯罪的，依法追究刑事责任：

(一)刑讯逼供、体罚、虐待、侮辱他人的；

(二)超过询问查证的时间限制人身自由的；

(三)不执行罚款决定与罚款收缴分离制度或者不按规定将罚没的财物上缴国库或者依法处理的；

(四)私分、侵占、挪用、故意损毁收缴、扣押的财物的；

(五)违反规定使用或者不及时返还被侵害人财物的；

(六)违反规定不及时退还保证金的；

(七)利用职务上的便利收受他人财物或者谋取其他利益的；

(八)当场收缴罚款不出具罚款收据或者不如实填写罚款数额的；

(九)接到要求制止违反治安管理行为的报警后，不及时出警的；

(十)在查处违反治安管理活动时，为违法犯罪行为人通风报信的；

(十一)有徇私舞弊、滥用职权，不依法履行法定职责的其他情形的。

办理治安案件的公安机关有前款所列行为的，对直接负责的主管人员和其他直接责任人员给予相应的行政处分。

第一百一十七条 公安机关及其人民警察违法行使职权，侵犯公民、法人和其他组织合法权益的，应当赔礼道歉；造成损害的，应当依法承担赔偿责任。

第六章 附 则

第一百一十八条 本法所称以上、以下、以内，包括本数。

第一百一十九条 本法自 2006 年 3 月 1 日起施行。1986 年 9 月 5 日公布、1994 年 5 月 12 日修订公布的《中华人民共和国治安管理处罚条例》同时废止。

中华人民共和国突发事件应对法

中华人民共和国主席令第二十五号

《中华人民共和国突发事件应对法》已由中华人民共和国第十四届全国人民代表大会常务委员会第十次会议于 2024 年 6 月 28 日修订通过，现予公布，自

2024 年 11 月 1 日起施行。

中华人民共和国主席 习近平

2024 年 6 月 28 日

中华人民共和国突发事件应对法

（2007 年 8 月 30 日第十届全国人民代表大会常务委员会第二十九次会议通过 2024 年 6 月 28 日第十四届全国人民代表大会常务委员会第十次会议修订）

第一章 总 则

第一条 为了预防和减少突发事件的发生，控制、减轻和消除突发事件引起的严重社会危害，提高突发事件预防和应对能力，规范突发事件应对活动，保护人民生命财产安全，维护国家安全、公共安全、生态环境安全和社会秩序， 根据宪法，制定本法。

第二条 本法所称突发事件，是指突然发生，造成或者可能造成严重社会危害，需要采取应急处置措施予以应对的自然灾害、事故灾难、公共卫生事件和社会安全事件。

突发事件的预防与应急准备、监测与预警、应急处置与救援、事后恢复与重建等应对活动，适用本法。

《中华人民共和国传染病防治法》等有关法律对突发公共卫生事件应对作出规定的，适用其规定。有关法律没有规定的，适用本法。

第三条 按照社会危害程度、影响范围等因素，突发自然灾害、事故灾难、公共卫生事件分为特别重大、重大、较大和一般四级。法律、行政法规或者国务院另有规定的，从其规定。

突发事件的分级标准由国务院或者国务院确定的部门制定。

第四条 突发事件应对工作坚持中国共产党的领导，坚持以马克思列宁主义、毛泽东思想、邓小平理论、“三个代表”重要思想、科学发展观、习近平新时代中国特色社会主义思想为指导，建立健全集中统一、高效权威的中国特色突发事件应对工作领导体制，完善党委领导、政府负责、部门联动、军地联合、社会协同、公众参与、科技支撑、法治保障的治理体系。

第五条 突发事件应对工作应当坚持总体国家安全观，统筹发展与安全；坚持人民至上、生命至上；坚持依法科学应对，尊重和保障人权；坚持预防为主、

预防与应急相结合。

第六条 国家建立有效的社会动员机制，组织动员企业事业单位、社会组织、志愿者等各方力量依法有序参与突发事件应对工作，增强全民的公共安全和防范风险的意识，提高全社会的避险救助能力。

第七条 国家建立健全突发事件信息发布制度。有关人民政府和部门应当及时向社会公布突发事件相关信息和有关突发事件应对的决定、命令、措施等信息。

任何单位和个人不得编造、故意传播有关突发事件的虚假信息。有关人民政府和部门发现影响或者可能影响社会稳定、扰乱社会和经济管理秩序的虚假或者不完整信息的，应当及时发布准确的信息予以澄清。

第八条 国家建立健全突发事件新闻采访报道制度。有关人民政府和部门应当做好新闻媒体服务引导工作，支持新闻媒体开展采访报道和舆论监督。

新闻媒体采访报道突发事件应当及时、准确、客观、公正。

新闻媒体应当开展突发事件应对法律法规、预防与应急、自救与互救知识等的公益宣传。

第九条 国家建立突发事件应对工作投诉、举报制度，公布统一的投诉、举报方式。

对于不履行或者不正确履行突发事件应对工作职责的行为，任何单位和个人有权向有关人民政府和部门投诉、举报。

接到投诉、举报的人民政府和部门应当依照规定立即组织调查处理， 并将调查处理结果以适当方式告知投诉人、举报人；投诉、举报事项不属于其职责的，应当及时移送有关机关处理。

有关人民政府和部门对投诉人、举报人的相关信息应当予以保密， 保护投诉人、举报人的合法权益。

第十条 突发事件应对措施应当与突发事件可能造成的社会危害的性质、程度和范围相适应；有多种措施可供选择的，应当选择有利于最大程度地保护公民、法人和其他组织权益，且对他人权益损害和生态环境影响较小的措施，并根据情况变化及时调整，做到科学、精准、有效。

第十一条 国家在突发事件应对工作中，应当对未成年人、老年人、残疾人、孕产期和哺乳期的妇女、需要及时就医的伤病人员等群体给予特殊、优先保护。

第十二条 县级以上人民政府及其部门为应对突发事件的紧急需要，可以征用单位和个人的设备、设施、场地、交通工具等财产。被征用的财产在使用完毕或者突发事件应急处置工作结束后，应当及时返还。财产被征用或者征用后毁损、灭失的，应当给予公平、合理的补偿。

第十三条 因依法采取突发事件应对措施，致使诉讼、监察调查、行政复议、仲裁、国家赔偿等活动不能正常进行的，适用有关时效中止和程序中止的规定，法律另有规定的除外。

第十四条 中华人民共和国政府在突发事件的预防与应急准备、监测与预警、应急处置与救援、事后恢复与重建等方面， 同外国政府和有关国际组织开展合作与交流。

第十五条 对在突发事件应对工作中做出突出贡献的单位和个人，按照国家有关规定给予表彰、奖励。

第二章 管理与指挥体制

第十六条 国家建立统一指挥、专常兼备、反应灵敏、上下联动的应急管理体制和综合协调、分类管理、分级负责、属地管理为主的工作体系。

第十七条 县级人民政府对本行政区域内突发事件的应对管理工作负责。突发事件发生后，发生地县级人民政府应当立即采取措施控制事态发展，组织开展应急救援和处置工作，并立即向上一级人民政府报告，必要时可以越级上报，具备条件的，应当进行网络直报或者自动速报。

突发事件发生地县级人民政府不能消除或者不能有效控制突发事件引起的严重社会危害的，应当及时向上级人民政府报告。上级人民政府应当及时采取措施，统一领导应急处置工作。

法律、行政法规规定由国务院有关部门对突发事件应对管理工作负责的， 从其规定；地方人民政府应当积极配合并提供必要的支持。

第十八条 突发事件涉及两个以上行政区域的，其应对管理工作由有关行政区域共同的上一级人民政府负责，或者由各有关行政区域的上一级人民政府共同负责。共同负责的人民政府应当按照国家有关规定， 建立信息共享和协调配合机制。根据共同应对突发事件的需要，地方人民政府之间可以建立协同应对机制。

第十九条 县级以上人民政府是突发事件应对管理工作的行政领导机关。

国务院在总理领导下研究、决定和部署特别重大突发事件的应对工作； 根据实际需要，设立国家突发事件应急指挥机构，负责突发事件应对工作；必要时，国务院可以派出工作组指导有关工作。

县级以上地方人民政府设立由本级人民政府主要负责人、相关部门负责人、国家综合性消防救援队伍和驻当地中国人民解放军、中国人民武装警察部队有关负责人等组成的突发事件应急指挥机构，统一领导、协调本级人民政府各有关部门和下级人民政府开展突发事件应对工作；根据实际需要，设立相关类别突发事件应急指挥机构，组织、协调、指挥突发事件应对工作。

第二十条 突发事件应急指挥机构在突发事件应对过程中可以依法发布有关突发事件应对的决定、命令、措施。突发事件应急指挥机构发布的决定、命令、措施与设立它的人民政府发布的决定、命令、措施具有同等效力， 法律责任由设立它的人民政府承担。

第二十一条 县级以上人民政府应急管理部门和卫生健康、公安等有关部门应当在各自职责范围内做好有关突发事件应对管理工作，并指导、协助下级人民政府及其相应部门做好有关突发事件的应对管理工作。

第二十二条 乡级人民政府、街道办事处应当明确专门工作力量，负责突发事件应对有关工作。

居民委员会、村民委员会依法协助人民政府和有关部门做好突发事件应对工作。

第二十三条 公民、法人和其他组织有义务参与突发事件应对工作。

第二十四条 中国人民解放军、中国人民武装警察部队和民兵组织依照本法和其他有关法律、行政法规、军事法规的规定以及国务院、中央军事委员会的命令，参加突发事件的应急救援和处置工作。

第二十五条 县级以上人民政府及其设立的突发事件应急指挥机构发布的有关突发事件应对的决定、命令、措施， 应当及时报本级人民代表大会常务委员会备案；突发事件应急处置工作结束后，应当向本级人民代表大会常务委员会作出专项工作报告。

第三章 预防与应急准备

第二十六条 国家建立健全突发事件应急预案体系。

国务院制定国家突发事件总体应急预案，组织制定国家突发事件专项应急预案；国务院有关部门根据各自的职责和国务院相关应急预案，制定国家突发事件部门应急预案并报国务院备案。

地方各级人民政府和县级以上地方人民政府有关部门根据有关法律、法规、规章、上级人民政府及其有关部门的应急预案以及本地区、本部门的实际情况，制定相应的突发事件应急预案并按国务院有关规定备案。

第二十七条 县级以上人民政府应急管理部门指导突发事件应急预案体系建设，综合协调应急预案衔接工作，增强有关应急预案的衔接性和实效性。

第二十八条 应急预案应当根据本法和其他有关法律、法规的规定，针对突发事件的性质、特点和可能造成的社会危害， 具体规定突发事件应对管理工作的组织指挥体系与职责和突发事件的预防与预警机制、处置程序、应急保障措施以及事后恢复与重建措施等内容。

应急预案制定机关应当广泛听取有关部门、单位、专家和社会各方面意见，增强应急预案的针对性和可操作性，并根据实际需要、情势变化、应急演练中发现的问题等及时对应急预案作出修订。

应急预案的制定、修订、备案等工作程序和管理办法由国务院规定。

第二十九条 县级以上人民政府应当将突发事件应对工作纳入国民经济和社会发展规划。县级以上人民政府有关部门应当制定突发事件应急体系建设规划。

第三十条 国土空间规划等规划应当符合预防、处置突发事件的需要，统筹安排突发事件应对工作所必需的设备和基础设施建设，合理确定应急避难、封闭隔离、紧急医疗救治等场所，实现日常使用和应急使用的相互转换。

第三十一条 国务院应急管理部门会同卫生健康、自然资源、住房城乡建设等部门统筹、指导全国应急避难场所的建设和管理工作， 建立健全应急避难场所标准体系。县级以上地方人民政府负责本行政区域内应急避难场所的规划、建设和管理工作。

第三十二条 国家建立健全突发事件风险评估体系，对可能发生的突发事件进行综合性评估，有针对性地采取有效防范措施，减少突发事件的发生，最大限度减轻突发事件的影响。

第三十三条 县级人民政府应当对本行政区域内容易引发自然灾害、事故灾

难和公共卫生事件的危险源、危险区域进行调查、登记、风险评估， 定期进行检查、监控，并责令有关单位采取安全防范措施。

省级和设区的市级人民政府应当对本行政区域内容易引发特别重大、重大突发事件的危险源、危险区域进行调查、登记、风险评估，组织进行检查、监控，并责令有关单位采取安全防范措施。

县级以上地方人民政府应当根据情况变化，及时调整危险源、危险区域的登记。登记的危险源、危险区域及其基础信息， 应当按照国家有关规定接入突发事件信息系统，并及时向社会公布。

第三十四条 县级人民政府及其有关部门、乡级人民政府、街道办事处、居民委员会、村民委员会应当及时调解处理可能引发社会安全事件的矛盾纠纷。

第三十五条 所有单位应当建立健全安全管理制度，定期开展危险源辨识评估，制定安全防范措施；定期检查本单位各项安全防范措施的落实情况，及时消除事故隐患；掌握并及时处理本单位存在的可能引发社会安全事件的问题，防止矛盾激化和事态扩大；对本单位可能发生的突发事件和采取安全防范措施的情况，应当按照规定及时向所在地人民政府或者有关部门报告。

第三十六条 矿山、金属冶炼、建筑施工单位和易燃易爆物品、危险化学品、放射性物品等危险物品的生产、经营、运输、储存、使用单位， 应当制定具体应急预案，配备必要的应急救援器材、设备和物资， 并对生产经营场所、有危险物品的建筑物、构筑物及周边环境开展隐患排查， 及时采取措施管控风险和消除隐患，防止发生突发事件。

第三十七条 公共交通工具、公共场所和其他人员密集场所的经营单位或者管理单位应当制定具体应急预案，为交通工具和有关场所配备报警装置和必要的应急救援设备、设施， 注明其使用方法，并显著标明安全撤离的通道、路线， 保证安全通道、出口的畅通。

有关单位应当定期检测、维护其报警装置和应急救援设备、设施， 使其处于良好状态，确保正常使用。

第三十八条 县级以上人民政府应当建立健全突发事件应对管理培训制度，对人民政府及其有关部门负有突发事件应对管理职责的工作人员以及居民委员会、村民委员会有关人员定期进行培训。

第三十九条 国家综合性消防救援队伍是应急救援的综合性常备骨干力量，按照国家有关规定执行综合应急救援任务。县级以上人民政府有关部门可以根据实际需要设立专业应急救援队伍。

县级以上人民政府及其有关部门可以建立由成年志愿者组成的应急救援队伍。乡级人民政府、街道办事处和有条件的居民委员会、村民委员会可以建立基层应急救援队伍，及时、就近开展应急救援。单位应当建立由本单位职工组成的专职或者兼职应急救援队伍。

国家鼓励和支持社会力量建立提供社会化应急救援服务的应急救援队伍。社会力量建立的应急救援队伍参与突发事件应对工作应当服从履行统一领导职责或者组织处置突发事件的人民政府、突发事件应急指挥机构的统一指挥。

县级以上人民政府应当推动专业应急救援队伍与非专业应急救援队伍联合培训、联合演练，提高合成应急、协同应急的能力。

第四十条 地方各级人民政府、县级以上人民政府有关部门、有关单位应当为其组建的应急救援队伍购买人身意外伤害保险，配备必要的防护装备和器材，防范和减少应急救援人员的人身伤害风险。

专业应急救援人员应当具备相应的身体条件、专业技能和心理素质， 取得国家规定的应急救援职业资格，具体办法由国务院应急管理部门会同国务院有关部门制定。

第四十一条 中国人民解放军、中国人民武装警察部队和民兵组织应当有计划地组织开展应急救援的专门训练。

第四十二条 县级人民政府及其有关部门、乡级人民政府、街道办事处应当组织开展面向社会公众的应急知识宣传普及活动和必要的应急演练。

居民委员会、村民委员会、企业事业单位、社会组织应当根据所在地人民政府的要求，结合各自的实际情况，开展面向居民、村民、职工等的应急知识宣传普及活动和必要的应急演练。

第四十三条 各级各类学校应当把应急教育纳入教育教学计划，对学生及教职工开展应急知识教育和应急演练，培养安全意识，提高自救与互救能力。

教育主管部门应当对学校开展应急教育进行指导和监督，应急管理等部门应当给予支持。

第四十四条 各级人民政府应当将突发事件应对工作所需经费纳入本级预算，并加强资金管理，提高资金使用绩效。

第四十五条 国家按照集中管理、统一调拨、平时服务、灾时应急、采储结合、节约高效的原则， 建立健全应急物资储备保障制度，动态更新应急物资储备品种目录，完善重要应急物资的监管、生产、采购、储备、调拨和紧急配送体系，促进安全应急产业发展，优化产业布局。

国家储备物资品种目录、总体发展规划， 由国务院发展改革部门会同国务院有关部门拟订。国务院应急管理等部门依据职责制定应急物资储备规划、品种目录，并组织实施。应急物资储备规划应当纳入国家储备总体发展规划。

第四十六条 设区的市级以上人民政府和突发事件易发、多发地区的县级人民政府应当建立应急救援物资、生活必需品和应急处置装备的储备保障制度。

县级以上地方人民政府应当根据本地区的实际情况和突发事件应对工作的需要，依法与有条件的企业签订协议，保障应急救援物资、生活必需品和应急处置装备的生产、供给。有关企业应当根据协议，按照县级以上地方人民政府要求，进行应急救援物资、生活必需品和应急处置装备的生产、供给， 并确保符合国家有关产品质量的标准和要求。

国家鼓励公民、法人和其他组织储备基本的应急自救物资和生活必需品。有关部门可以向社会公布相关物资、物品的储备指南和建议清单。

第四十七条 国家建立健全应急运输保障体系，统筹铁路、公路、水运、民航、邮政、快递等运输和服务方式， 制定应急运输保障方案，保障应急物资、装备和人员及时运输。

县级以上地方人民政府和有关主管部门应当根据国家应急运输保障方案，结合本地区实际做好应急调度和运力保障，确保运输通道和客货运枢纽畅通。

国家发挥社会力量在应急运输保障中的积极作用。社会力量参与突发事件应急运输保障，应当服从突发事件应急指挥机构的统一指挥。

第四十八条 国家建立健全能源应急保障体系，提高能源安全保障能力，确保受突发事件影响地区的能源供应。

第四十九条 国家建立健全应急通信、应急广播保障体系，加强应急通信系统、应急广播系统建设，确保突发事件应对工作的通信、广播安全畅通。

第五十条 国家建立健全突发事件卫生应急体系，组织开展突发事件中的医疗救治、卫生学调查处置和心理援助等卫生应急工作，有效控制和消除危害。

第五十一条 县级以上人民政府应当加强急救医疗服务网络的建设，配备相应的医疗救治物资、设施设备和人员， 提高医疗卫生机构应对各类突发事件的救治能力。

第五十二条 国家鼓励公民、法人和其他组织为突发事件应对工作提供物资、资金、技术支持和捐赠。

接受捐赠的单位应当及时公开接受捐赠的情况和受赠财产的使用、管理情况，接受社会监督。

第五十三条 红十字会在突发事件中，应当对伤病人员和其他受害者提供紧急救援和人道救助，并协助人民政府开展与其职责相关的其他人道主义服务活动。有关人民政府应当给予红十字会支持和资助，保障其依法参与应对突发事件。

慈善组织在发生重大突发事件时开展募捐和救助活动，应当在有关人民政府的统筹协调、有序引导下依法进行。有关人民政府应当通过提供必要的需求信息、政府购买服务等方式，对慈善组织参与应对突发事件、开展应急慈善活动予以支持。

第五十四条 有关单位应当加强应急救援资金、物资的管理，提高使用效率。

任何单位和个人不得截留、挪用、私分或者变相私分应急救援资金、物资。

第五十五条 国家发展保险事业，建立政府支持、社会力量参与、市场化运作的巨灾风险保险体系，并鼓励单位和个人参加保险。

第五十六条 国家加强应急管理基础科学、重点行业领域关键核心技术的研究，加强互联网、云计算、大数据、人工智能等现代技术手段在突发事件应对工作中的应用，鼓励、扶持有条件的教学科研机构、企业培养应急管理人才和科技人才，研发、推广新技术、新材料、新设备和新工具，提高突发事件应对能力。

第五十七条 县级以上人民政府及其有关部门应当建立健全突发事件专家咨询论证制度，发挥专业人员在突发事件应对工作中的作用。

第四章 监测与预警

第五十八条 国家建立健全突发事件监测制度。

县级以上人民政府及其有关部门应当根据自然灾害、事故灾难和公共卫生事

件的种类和特点，建立健全基础信息数据库，完善监测网络，划分监测区域，确定监测点，明确监测项目，提供必要的设备、设施， 配备专职或者兼职人员，对可能发生的突发事件进行监测。

第五十九条 国务院建立全国统一的突发事件信息系统。

县级以上地方人民政府应当建立或者确定本地区统一的突发事件信息系统，汇集、储存、分析、传输有关突发事件的信息，并与上级人民政府及其有关部门、下级人民政府及其有关部门、专业机构、监测网点和重点企业的突发事件信息系统实现互联互通，加强跨部门、跨地区的信息共享与情报合作。

第六十条 县级以上人民政府及其有关部门、专业机构应当通过多种途径收集突发事件信息。

县级人民政府应当在居民委员会、村民委员会和有关单位建立专职或者兼职信息报告员制度。

公民、法人或者其他组织发现发生突发事件， 或者发现可能发生突发事件的异常情况，应当立即向所在地人民政府、有关主管部门或者指定的专业机构报告。接到报告的单位应当按照规定立即核实处理，对于不属于其职责的，应当立即移送相关单位核实处理。

第六十一条 地方各级人民政府应当按照国家有关规定向上级人民政府报送突发事件信息。县级以上人民政府有关主管部门应当向本级人民政府相关部门通报突发事件信息，并报告上级人民政府主管部门。专业机构、监测网点和信息报告员应当及时向所在地人民政府及其有关主管部门报告突发事件信息。

有关单位和人员报送、报告突发事件信息， 应当做到及时、客观、真实， 不得迟报、谎报、瞒报、漏报， 不得授意他人迟报、谎报、瞒报， 不得阻碍他人报告。

第六十二条 县级以上地方人民政府应当及时汇总分析突发事件隐患和监测信息，必要时组织相关部门、专业技术人员、专家学者进行会商， 对发生突发事件的可能性及其可能造成的影响进行评估；认为可能发生重大或者特别重大突发事件的，应当立即向上级人民政府报告，并向上级人民政府有关部门、当地驻军和可能受到危害的毗邻或者相关地区的人民政府通报，及时采取预防措施。

第六十三条 国家建立健全突发事件预警制度。

可以预警的自然灾害、事故灾难和公共卫生事件的预警级别，按照突发事件发生的紧急程度、发展势态和可能造成的危害程度分为一级、二级、三级和四级，分别用红色、橙色、黄色和蓝色标示，一级为最高级别。

预警级别的划分标准由国务院或者国务院确定的部门制定。

第六十四条 可以预警的自然灾害、事故灾难或者公共卫生事件即将发生或者发生的可能性增大时，县级以上地方人民政府应当根据有关法律、行政法规和国务院规定的权限和程序，发布相应级别的警报，决定并宣布有关地区进入预警期，同时向上一级人民政府报告，必要时可以越级上报；具备条件的，应当进行网络直报或者自动速报；同时向当地驻军和可能受到危害的毗邻或者相关地区的人民政府通报。

发布警报应当明确预警类别、级别、起始时间、可能影响的范围、警示事项、应当采取的措施、发布单位和发布时间等。

第六十五条 国家建立健全突发事件预警发布平台，按照有关规定及时、准确向社会发布突发事件预警信息。

广播、电视、报刊以及网络服务提供者、电信运营商应当按照国家有关规定，建立突发事件预警信息快速发布通道，及时、准确、无偿播发或者刊载突发事件预警信息。

公共场所和其他人员密集场所，应当指定专门人员负责突发事件预警信息接收和传播工作，做好相关设备、设施维护，确保突发事件预警信息及时、准确接收和传播。

第六十六条 发布三级、四级警报，宣布进入预警期后，县级以上地方人民政府应当根据即将发生的突发事件的特点和可能造成的危害，采取下列措施：

(一)启动应急预案；

(二)责令有关部门、专业机构、监测网点和负有特定职责的人员及时收集、报告有关信息，向社会公布反映突发事件信息的渠道，加强对突发事件发生、发展情况的监测、预报和预警工作；

(三)组织有关部门和机构、专业技术人员、有关专家学者，随时对突发事件信息进行分析评估，预测发生突发事件可能性的大小、影响范围和强度以及可能发生的突发事件的级别；

(四)定时向社会发布与公众有关的突发事件预测信息和分析评估结果，并对相关信息的报道工作进行管理；

(五)及时按照有关规定向社会发布可能受到突发事件危害的警告，宣传避免、减轻危害的常识，公布咨询或者求助电话等联络方式和渠道。

第六十七条 发布一级、二级警报，宣布进入预警期后，县级以上地方人民政府除采取本法第六十六条规定的措施外，还应当针对即将发生的突发事件的特点和可能造成的危害，采取下列一项或者多项措施：

(一)责令应急救援队伍、负有特定职责的人员进入待命状态， 并动员后备人员做好参加应急救援和处置工作的准备；

(二)调集应急救援所需物资、设备、工具， 准备应急设施和应急避难、封闭隔离、紧急医疗救治等场所，并确保其处于良好状态、随时可以投入正常使用；

(三)加强对重点单位、重要部位和重要基础设施的安全保卫， 维护社会治安秩序；

(四)采取必要措施，确保交通、通信、供水、排水、供电、供气、供热、医疗卫生、广播电视、气象等公共设施的安全和正常运行；

(五)及时向社会发布有关采取特定措施避免或者减轻危害的建议、劝告；

(六)转移、疏散或者撤离易受突发事件危害的人员并予以妥善安置， 转移重要财产；

(七)关闭或者限制使用易受突发事件危害的场所，控制或者限制容易导致危害扩大的公共场所的活动；

(八)法律、法规、规章规定的其他必要的防范性、保护性措施。

第六十八条 发布警报，宣布进入预警期后，县级以上人民政府应当对重要商品和服务市场情况加强监测，根据实际需要及时保障供应、稳定市场。必要时，国务院和省、自治区、直辖市人民政府可以按照《中华人民共和国价格法》等有关法律规定采取相应措施。

第六十九条 对即将发生或者已经发生的社会安全事件，县级以上地方人民政府及其有关主管部门应当按照规定向上一级人民政府及其有关主管部门报告，必要时可以越级上报，具备条件的，应当进行网络直报或者自动速报。

第七十条 发布突发事件警报的人民政府应当根据事态的发展，按照有关规

定适时调整预警级别并重新发布。

有事实证明不可能发生突发事件或者危险已经解除的，发布警报的人民政府应当立即宣布解除警报，终止预警期，并解除已经采取的有关措施。

第五章 应急处置与救援

第七十一条 国家建立健全突发事件应急响应制度。

突发事件的应急响应级别，按照突发事件的性质、特点、可能造成的危害程度和影响范围等因素分为一级、二级、三级和四级，一级为最高级别。

突发事件应急响应级别划分标准由国务院或者国务院确定的部门制定。县级以上人民政府及其有关部门应当在突发事件应急预案中确定应急响应级别。

第七十二条 突发事件发生后，履行统一领导职责或者组织处置突发事件的人民政府应当针对其性质、特点、危害程度和影响范围等，立即启动应急响应，组织有关部门，调动应急救援队伍和社会力量，依照法律、法规、规章和应急预案的规定，采取应急处置措施，并向上级人民政府报告；必要时，可以设立现场指挥部，负责现场应急处置与救援，统一指挥进入突发事件现场的单位和个人。

启动应急响应，应当明确响应事项、级别、预计期限、应急处置措施等。

履行统一领导职责或者组织处置突发事件的人民政府，应当建立协调机制，提供需求信息，引导志愿服务组织和志愿者等社会力量及时有序参与应急处置与救援工作。

第七十三条 自然灾害、事故灾难或者公共卫生事件发生后，履行统一领导职责的人民政府应当采取下列一项或者多项应急处置措施：

(一)组织营救和救治受害人员，转移、疏散、撤离并妥善安置受到威胁的人员以及采取其他救助措施；

(二)迅速控制危险源，标明危险区域，封锁危险场所，划定警戒区，实行交通管制、限制人员流动、封闭管理以及其他控制措施；

(三)立即抢修被损坏的交通、通信、供水、排水、供电、供气、供热、医疗卫生、广播电视、气象等公共设施， 向受到危害的人员提供避难场所和生活必需品，实施医疗救护和卫生防疫以及其他保障措施；

(四)禁止或者限制使用有关设备、设施， 关闭或者限制使用有关场所，中止人员密集的活动或者可能导致危害扩大的生产经营活动以及采取其他保护措施；

(五)启用本级人民政府设置的财政预备费和储备的应急救援物资，必要时调用其他急需物资、设备、设施、工具；

(六)组织公民、法人和其他组织参加应急救援和处置工作， 要求具有特定专长的人员提供服务；

(七)保障食品、饮用水、药品、燃料等基本生活必需品的供应；

(八)依法从严惩处囤积居奇、哄抬价格、牟取暴利、制假售假等扰乱市场秩序的行为，维护市场秩序；

(九)依法从严惩处哄抢财物、干扰破坏应急处置工作等扰乱社会秩序的行为，维护社会治安；

(十)开展生态环境应急监测，保护集中式饮用水水源地等环境敏感目标，控制和处置污染物；

(十一)采取防止发生次生、衍生事件的必要措施。

第七十四条 社会安全事件发生后，组织处置工作的人民政府应当立即启动应急响应，组织有关部门针对事件的性质和特点，依照有关法律、行政法规和国家其他有关规定，采取下列一项或者多项应急处置措施：

(一)强制隔离使用器械相互对抗或者以暴力行为参与冲突的当事人，妥善解决现场纠纷和争端，控制事态发展；

(二)对特定区域内的建筑物、交通工具、设备、设施以及燃料、燃气、电力、水的供应进行控制；

(三)封锁有关场所、道路， 查验现场人员的身份证件，限制有关公共场所内的活动；

(四)加强对易受冲击的核心机关和单位的警卫，在国家机关、军事机关、国家通讯社、广播电台、电视台、外国驻华使领馆等单位附近设置临时警戒线；

(五)法律、行政法规和国务院规定的其他必要措施。

第七十五条 发生突发事件，严重影响国民经济正常运行时，国务院或者国务院授权的有关主管部门可以采取保障、控制等必要的应急措施， 保障人民群众的基本生活需要，最大限度地减轻突发事件的影响。

第七十六条 履行统一领导职责或者组织处置突发事件的人民政府及其有关部门，必要时可以向单位和个人征用应急救援所需设备、设施、场地、交通工具

和其他物资，请求其他地方人民政府及其有关部门提供人力、物力、财力或者技术支援，要求生产、供应生活必需品和应急救援物资的企业组织生产、保证供给，要求提供医疗、交通等公共服务的组织提供相应的服务。

履行统一领导职责或者组织处置突发事件的人民政府和有关主管部门，应当组织协调运输经营单位，优先运送处置突发事件所需物资、设备、工具、应急救援人员和受到突发事件危害的人员。

履行统一领导职责或者组织处置突发事件的人民政府及其有关部门，应当为受突发事件影响无人照料的无民事行为能力人、限制民事行为能力人提供及时有效帮助；建立健全联系帮扶应急救援人员家庭制度，帮助解决实际困难。

第七十七条 突发事件发生地的居民委员会、村民委员会和其他组织应当按照当地人民政府的决定、命令， 进行宣传动员，组织群众开展自救与互救，协助维护社会秩序；情况紧急的，应当立即组织群众开展自救与互救等先期处置工作。

第七十八条 受到自然灾害危害或者发生事故灾难、公共卫生事件的单位，应当立即组织本单位应急救援队伍和工作人员营救受害人员，疏散、撤离、安置受到威胁的人员，控制危险源，标明危险区域，封锁危险场所，并采取其他防止危害扩大的必要措施，同时向所在地县级人民政府报告；对因本单位的问题引发的或者主体是本单位人员的社会安全事件，有关单位应当按照规定上报情况，并迅速派出负责人赶赴现场开展劝解、疏导工作。

突发事件发生地的其他单位应当服从人民政府发布的决定、命令， 配合人民政府采取的应急处置措施，做好本单位的应急救援工作，并积极组织人员参加所在地的应急救援和处置工作。

第七十九条 突发事件发生地的个人应当依法服从人民政府、居民委员会、村民委员会或者所属单位的指挥和安排，配合人民政府采取的应急处置措施，积极参加应急救援工作，协助维护社会秩序。

第八十条 国家支持城乡社区组织健全应急工作机制，强化城乡社区综合服务设施和信息平台应急功能，加强与突发事件信息系统数据共享，增强突发事件应急处置中保障群众基本生活和服务群众能力。

第八十一条 国家采取措施，加强心理健康服务体系和人才队伍建设，支持引导心理健康服务人员和社会工作者对受突发事件影响的各类人群开展心理健

康教育、心理评估、心理疏导、心理危机干预、心理行为问题诊治等心理援助工作。

第八十二条 对于突发事件遇难人员的遗体，应当按照法律和国家有关规定，科学规范处置，加强卫生防疫，维护逝者尊严。对于逝者的遗物应当妥善保管。

第八十三条 县级以上人民政府及其有关部门根据突发事件应对工作需要，在履行法定职责所必需的范围和限度内，可以要求公民、法人和其他组织提供应急处置与救援需要的信息。公民、法人和其他组织应当予以提供， 法律另有规定的除外。县级以上人民政府及其有关部门对获取的相关信息， 应当严格保密，并依法保护公民的通信自由和通信秘密。

第八十四条 在突发事件应急处置中，有关单位和个人因依照本法规定配合突发事件应对工作或者履行相关义务，需要获取他人个人信息的，应当依照法律规定的程序和方式取得并确保信息安全，不得非法收集、使用、加工、传输他人个人信息，不得非法买卖、提供或者公开他人个人信息。

第八十五条 因依法履行突发事件应对工作职责或者义务获取的个人信息，只能用于突发事件应对，并在突发事件应对工作结束后予以销毁。确因依法作为证据使用或者调查评估需要留存或者延期销毁的，应当按照规定进行合法性、必要性、安全性评估，并采取相应保护和处理措施，严格依法使用。

第六章 事后恢复与重建

第八十六条 突发事件的威胁和危害得到控制或者消除后，履行统一领导职责或者组织处置突发事件的人民政府应当宣布解除应急响应，停止执行依照本法规定采取的应急处置措施，同时采取或者继续实施必要措施，防止发生自然灾害、事故灾难、公共卫生事件的次生、衍生事件或者重新引发社会安全事件， 组织受影响地区尽快恢复社会秩序。

第八十七条 突发事件应急处置工作结束后，履行统一领导职责的人民政府应当立即组织对突发事件造成的影响和损失进行调查评估，制定恢复重建计划，并向上一级人民政府报告。

受突发事件影响地区的人民政府应当及时组织和协调应急管理、卫生健康、公安、交通、铁路、民航、邮政、电信、建设、生态环境、水利、能源、广播电视等有关部门恢复社会秩序，尽快修复被损坏的交通、通信、供水、排水、供电、

供气、供热、医疗卫生、水利、广播电视等公共设施。

第八十八条 受突发事件影响地区的人民政府开展恢复重建工作需要上一级人民政府支持的，可以向上一级人民政府提出请求。上一级人民政府应当根据受影响地区遭受的损失和实际情况，提供资金、物资支持和技术指导， 组织协调其他地区和有关方面提供资金、物资和人力支援。

第八十九条 国务院根据受突发事件影响地区遭受损失的情况，制定扶持该地区有关行业发展的优惠政策。

受突发事件影响地区的人民政府应当根据本地区遭受的损失和采取应急处置措施的情况，制定救助、补偿、抚慰、抚恤、安置等善后工作计划并组织实施，妥善解决因处置突发事件引发的矛盾纠纷。

第九十条 公民参加应急救援工作或者协助维护社会秩序期间，其所在单位应当保证其工资待遇和福利不变，并可以按照规定给予相应补助。

第九十一条 县级以上人民政府对在应急救援工作中伤亡的人员依法落实工伤待遇、抚恤或者其他保障政策， 并组织做好应急救援工作中致病人员的医疗救治工作。

第九十二条 履行统一领导职责的人民政府在突发事件应对工作结束后，应当及时查明突发事件的发生经过和原因，总结突发事件应急处置工作的经验教训，制定改进措施，并向上一级人民政府提出报告。

第九十三条 突发事件应对工作中有关资金、物资的筹集、管理、分配、拨付和使用等情况，应当依法接受审计机关的审计监督。

第九十四条 国家档案主管部门应当建立健全突发事件应对工作相关档案收集、整理、保护、利用工作机制。突发事件应对工作中形成的材料， 应当按照国家规定归档，并向相关档案馆移交。

第七章 法律责任

第九十五条 地方各级人民政府和县级以上人民政府有关部门违反本法规定，不履行或者不正确履行法定职责的，由其上级行政机关责令改正；有下列情形之一，由有关机关综合考虑突发事件发生的原因、后果、应对处置情况、行为人过错等因素，对负有责任的领导人员和直接责任人员依法给予处分：

(一)未按照规定采取预防措施，导致发生突发事件，或者未采取必要的防范

措施，导致发生次生、衍生事件的；

(二)迟报、谎报、瞒报、漏报或者授意他人迟报、谎报、瞒报以及阻碍他人报告有关突发事件的信息，或者通报、报送、公布虚假信息，造成后果的；

(三)未按照规定及时发布突发事件警报、采取预警期的措施， 导致损害发生的；

(四)未按照规定及时采取措施处置突发事件或者处置不当，造成后果的；

(五)违反法律规定采取应对措施，侵犯公民生命健康权益的；

(六)不服从上级人民政府对突发事件应急处置工作的统一领导、指挥和协调的；

(七)未及时组织开展生产自救、恢复重建等善后工作的；

(八)截留、挪用、私分或者变相私分应急救援资金、物资的；

(九)不及时归还征用的单位和个人的财产，或者对被征用财产的单位和个人不按照规定给予补偿的。

第九十六条 有关单位有下列情形之一，由所在地履行统一领导职责的人民政府有关部门责令停产停业，暂扣或者吊销许可证件，并处五万元以上二十万元以下的罚款；情节特别严重的，并处二十万元以上一百万元以下的罚款：

(一)未按照规定采取预防措施，导致发生较大以上突发事件的；

(二)未及时消除已发现的可能引发突发事件的隐患，导致发生较大以上突发事件的；

(三)未做好应急物资储备和应急设备、设施日常维护、检测工作， 导致发生较大以上突发事件或者突发事件危害扩大的；

(四)突发事件发生后，不及时组织开展应急救援工作，造成严重后果的。

其他法律对前款行为规定了处罚的，依照较重的规定处罚。

第九十七条 违反本法规定，编造并传播有关突发事件的虚假信息，或者明知是有关突发事件的虚假信息而进行传播的，责令改正，给予警告；造成严重后果的，依法暂停其业务活动或者吊销其许可证件；负有直接责任的人员是公职人员的，还应当依法给予处分。

第九十八条 单位或者个人违反本法规定，不服从所在地人民政府及其有关部门依法发布的决定、命令或者不配合其依法采取的措施的， 责令改正；造成严

重后果的，依法给予行政处罚；负有直接责任的人员是公职人员的，还应当依法给予处分。

第九十九条 单位或者个人违反本法第八十四条、第八十五条关于个人信息保护规定的，由主管部门依照有关法律规定给予处罚。

第一百条 单位或者个人违反本法规定，导致突发事件发生或者危害扩大，造成人身、财产或者其他损害的，应当依法承担民事责任。

第一百零一条 为了使本人或者他人的人身、财产免受正在发生的危险而采取避险措施的，依照《中华人民共和国民法典》、《中华人民共和国刑法》等法律关于紧急避险的规定处理。

第一百零二条 违反本法规定，构成违反治安管理行为的，依法给予治安管理处罚；构成犯罪的，依法追究刑事责任。

第八章 附 则

第一百零三条 发生特别重大突发事件，对人民生命财产安全、国家安全、公共安全、生态环境安全或者社会秩序构成重大威胁，采取本法和其他有关法律、法规、规章规定的应急处置措施不能消除或者有效控制、减轻其严重社会危害，需要进入紧急状态的，由全国人民代表大会常务委员会或者国务院依照宪法和其他有关法律规定的权限和程序决定。

紧急状态期间采取的非常措施，依照有关法律规定执行或者由全国人民代表大会常务委员会另行规定。

第一百零四条 中华人民共和国领域外发生突发事件，造成或者可能造成中华人民共和国公民、法人和其他组织人身伤亡、财产损失的， 由国务院外交部门会同国务院其他有关部门、有关地方人民政府，按照国家有关规定做好应对工作。

第一百零五条 在中华人民共和国境内的外国人、无国籍人应当遵守本法，服从所在地人民政府及其有关部门依法发布的决定、命令， 并配合其依法采取的措施。

第一百零六条 本法自 2024 年 11 月 1 日起施行。

中华人民共和国国家安全法

(2015 年 7 月 1 日第十二届全国人民代表大会常务委员会第十五次会议通过)

第一章 总 则

第一条 为了维护国家安全，保卫人民民主专政的政权和中国特色社会主义制度，保护人民的根本利益，保障改革开放和社会主义现代化建设的顺利进行，实现中华民族伟大复兴，根据宪法，制定本法。

第二条 国家安全是指国家政权、主权、统一和领土完整、人民福祉、经济社会可持续发展和国家其他重大利益相对处于没有危险和不受内外威胁的状态，以及保障持续安全状态的能力。

第三条 国家安全工作应当坚持总体国家安全观，以人民安全为宗旨，以政治安全为根本，以经济安全为基础，以军事、文化、社会安全为保障， 以促进国际安全为依托，维护各领域国家安全，构建国家安全体系，走中国特色国家安全道路。

第四条 坚持中国共产党对国家安全工作的领导，建立集中统一、高效权威的国家安全领导体制。

第五条 中央国家安全领导机构负责国家安全工作的决策和议事协调，研究制定、指导实施国家安全战略和有关重大方针政策， 统筹协调国家安全重大事项和重要工作，推动国家安全法治建设。

第六条 国家制定并不断完善国家安全战略，全面评估国际、国内安全形势，明确国家安全战略的指导方针、中长期目标、重点领域的国家安全政策、工作任务和措施。

第七条 维护国家安全，应当遵守宪法和法律，坚持社会主义法治原则，尊重和保障人权，依法保护公民的权利和自由。

第八条 维护国家安全，应当与经济社会发展相协调。

国家安全工作应当统筹内部安全和外部安全、国土安全和国民安全、传统安全和非传统安全、自身安全和共同安全。

第九条 维护国家安全，应当坚持预防为主、标本兼治，专门工作与群众路线相结合，充分发挥专门机关和其他有关机关维护国家安全的职能作用，广泛动员公民和组织，防范、制止和依法惩治危害国家安全的行为。

第十条 维护国家安全，应当坚持互信、互利、平等、协作， 积极同外国政府和国际组织开展安全交流合作，履行国际安全义务，促进共同安全，维护世界和平。

第十一条　中华人民共和国公民、一切国家机关和武装力量、各政党和各人民团体、企业事业组织和其他社会组织，都有维护国家安全的责任和义务。

中国的主权和领土完整不容侵犯和分割。维护国家主权、统一和领土完整是包括港澳同胞和台湾同胞在内的全中国人民的共同义务。

第十二条　国家对在维护国家安全工作中作出突出贡献的个人和组织给予表彰和奖励。

第十三条　国家机关工作人员在国家安全工作和涉及国家安全活动中，滥用职权、玩忽职守、徇私舞弊的，依法追究法律责任。

任何个人和组织违反本法和有关法律，不履行维护国家安全义务或者从事危害国家安全活动的，依法追究法律责任。

第十四条　每年 4 月 15 日为全民国家安全教育日。

第二章　维护国家安全的任务

第十五条　国家坚持中国共产党的领导，维护中国特色社会主义制度，发展社会主义民主政治，健全社会主义法治，强化权力运行制约和监督机制，保障人民当家作主的各项权利。

国家防范、制止和依法惩治任何叛国、分裂国家、煽动叛乱、颠覆或者煽动颠覆人民民主专政政权的行为；防范、制止和依法惩治窃取、泄露国家秘密等危害国家安全的行为；防范、制止和依法惩治境外势力的渗透、破坏、颠覆、分裂活动。

第十六条　国家维护和发展最广大人民的根本利益，保卫人民安全，创造良好生存发展条件和安定工作生活环境，保障公民的生命财产安全和其他合法权益。

第十七条　国家加强边防、海防和空防建设，采取一切必要的防卫和管控措施，保卫领陆、内水、领海和领空安全，维护国家领土主权和海洋权益。

第十八条　国家加强武装力量革命化、现代化、正规化建设，建设与保卫国家安全和发展利益需要相适应的武装力量；实施积极防御军事战略方针，防备和抵御侵略，制止武装颠覆和分裂；开展国际军事安全合作，实施联合国维和、国际救援、海上护航和维护国家海外利益的军事行动，　维护国家主权、安全、领土完整、发展利益和世界和平。

第十九条　国家维护国家基本经济制度和社会主义市场经济秩序，健全预防

和化解经济安全风险的制度机制，保障关系国民经济命脉的重要行业和关键领域、重点产业、重大基础设施和重大建设项目以及其他重大经济利益安全。

第二十条　国家健全金融宏观审慎管理和金融风险防范、处置机制，加强金融基础设施和基础能力建设，防范和化解系统性、区域性金融风险， 防范和抵御外部金融风险的冲击。

第二十一条　国家合理利用和保护资源能源，有效管控战略资源能源的开发，加强战略资源能源储备，完善资源能源运输战略通道建设和安全保护措施，加强国际资源能源合作，全面提升应急保障能力，保障经济社会发展所需的资源能源持续、可靠和有效供给。

第二十二条　国家健全粮食安全保障体系，保护和提高粮食综合生产能力，完善粮食储备制度、流通体系和市场调控机制， 健全粮食安全预警制度，保障粮食供给和质量安全。

第二十三条　国家坚持社会主义先进文化前进方向，继承和弘扬中华民族优秀传统文化，培育和践行社会主义核心价值观，防范和抵制不良文化的影响，掌握意识形态领域主导权，增强文化整体实力和竞争力。

第二十四条　国家加强自主创新能力建设，加快发展自主可控的战略高新技术和重要领域核心关键技术，加强知识产权的运用、保护和科技保密能力建设，保障重大技术和工程的安全。

第二十五条　国家建设网络与信息安全保障体系，提升网络与信息安全保护能力，加强网络和信息技术的创新研究和开发应用，实现网络和信息核心技术、关键基础设施和重要领域信息系统及数据的安全可控；加强网络管理，防范、制止和依法惩治网络攻击、网络入侵、网络窃密、散布违法有害信息等网络违法犯罪行为，维护国家网络空间主权、安全和发展利益。

第二十六条　国家坚持和完善民族区域自治制度，巩固和发展平等团结互助和谐的社会主义民族关系。坚持各民族一律平等，加强民族交往、交流、交融，防范、制止和依法惩治民族分裂活动， 维护国家统一、民族团结和社会和谐， 实现各民族共同团结奋斗、共同繁荣发展。

第二十七条　国家依法保护公民宗教信仰自由和正常宗教活动，坚持宗教独立自主自办的原则，防范、制止和依法惩治利用宗教名义进行危害国家安全的违

法犯罪活动，反对境外势力干涉境内宗教事务，维护正常宗教活动秩序。

国家依法取缔邪教组织，防范、制止和依法惩治邪教违法犯罪活动。

第二十八条 国家反对一切形式的恐怖主义和极端主义，加强防范和处置恐怖主义的能力建设，依法开展情报、调查、防范、处置以及资金监管等工作， 依法取缔恐怖活动组织和严厉惩治暴力恐怖活动。

第二十九条 国家健全有效预防和化解社会矛盾的体制机制，健全公共安全体系，积极预防、减少和化解社会矛盾， 妥善处置公共卫生、社会安全等影响国家安全和社会稳定的突发事件，促进社会和谐，维护公共安全和社会安定。

第三十条 国家完善生态环境保护制度体系，加大生态建设和环境保护力度，划定生态保护红线，强化生态风险的预警和防控，妥善处置突发环境事件，保障人民赖以生存发展的大气、水、土壤等自然环境和条件不受威胁和破坏， 促进人与自然和谐发展。

第三十一条 国家坚持和平利用核能和核技术，加强国际合作，防止核扩散，完善防扩散机制，加强对核设施、核材料、核活动和核废料处置的安全管理、监管和保护，加强核事故应急体系和应急能力建设，防止、控制和消除核事故对公民生命健康和生态环境的危害，不断增强有效应对和防范核威胁、核攻击的能力。

第三十二条 国家坚持和平探索和利用外层空间、国际海底区域和极地，增强安全进出、科学考察、开发利用的能力，加强国际合作，维护我国在外层空间、国际海底区域和极地的活动、资产和其他利益的安全。

第三十三条 国家依法采取必要措施，保护海外中国公民、组织和机构的安全和正当权益，保护国家的海外利益不受威胁和侵害。

第三十四条 国家根据经济社会发展和国家发展利益的需要，不断完善维护国家安全的任务。

第三章 维护国家安全的职责

第三十五条 全国人民代表大会依照宪法规定，决定战争和和平的问题，行使宪法规定的涉及国家安全的其他职权。

全国人民代表大会常务委员会依照宪法规定，决定战争状态的宣布，决定全国总动员或者局部动员，决定全国或者个别省、自治区、直辖市进入紧急状态，行使宪法规定的和全国人民代表大会授予的涉及国家安全的其他职权。

第三十六条 中华人民共和国主席根据全国人民代表大会的决定和全国人民代表大会常务委员会的决定，宣布进入紧急状态，宣布战争状态，发布动员令，行使宪法规定的涉及国家安全的其他职权。

第三十七条 国务院根据宪法和法律，制定涉及国家安全的行政法规，规定有关行政措施，发布有关决定和命令；实施国家安全法律法规和政策；依照法律规定决定省、自治区、直辖市的范围内部分地区进入紧急状态； 行使宪法法律规定的和全国人民代表大会及其常务委员会授予的涉及国家安全的其他职权。

第三十八条 中央军事委员会领导全国武装力量，决定军事战略和武装力量的作战方针，统一指挥维护国家安全的军事行动，制定涉及国家安全的军事法规，发布有关决定和命令。

第三十九条 中央国家机关各部门按照职责分工，贯彻执行国家安全方针政策和法律法规，管理指导本系统、本领域国家安全工作。

第四十条 地方各级人民代表大会和县级以上地方各级人民代表大会常务委员会在本行政区域内，保证国家安全法律法规的遵守和执行。

地方各级人民政府依照法律法规规定管理本行政区域内的国家安全工作。

香港特别行政区、澳门特别行政区应当履行维护国家安全的责任。

第四十一条 人民法院依照法律规定行使审判权，人民检察院依照法律规定行使检察权，惩治危害国家安全的犯罪。

第四十二条 国家安全机关、公安机关依法搜集涉及国家安全的情报信息，在国家安全工作中依法行使侦查、拘留、预审和执行逮捕以及法律规定的其他职权。

有关军事机关在国家安全工作中依法行使相关职权。

第四十三条 国家机关及其工作人员在履行职责时，应当贯彻维护国家安全的原则。

国家机关及其工作人员在国家安全工作和涉及国家安全活动中，应当严格依法履行职责，不得超越职权、滥用职权，不得侵犯个人和组织的合法权益。

第四章 国家安全制度

第一节 一般规定

第四十四条 中央国家安全领导机构实行统分结合、协调高效的国家安全制

度与工作机制。

第四十五条 国家建立国家安全重点领域工作协调机制，统筹协调中央有关职能部门推进相关工作。

第四十六条 国家建立国家安全工作督促检查和责任追究机制，确保国家安全战略和重大部署贯彻落实。

第四十七条 各部门、各地区应当采取有效措施，贯彻实施国家安全战略。

第四十八条 国家根据维护国家安全工作需要，建立跨部门会商工作机制，就维护国家安全工作的重大事项进行会商研判，提出意见和建议。

第四十九条 国家建立中央与地方之间、部门之间、军地之间以及地区之间关于国家安全的协同联动机制。

第五十条 国家建立国家安全决策咨询机制，组织专家和有关方面开展对国家安全形势的分析研判，推进国家安全的科学决策。

第二节 情报信息

第五十一条 国家健全统一归口、反应灵敏、准确高效、运转顺畅的情报信息收集、研判和使用制度， 建立情报信息工作协调机制，实现情报信息的及时收集、准确研判、有效使用和共享。

第五十二条 国家安全机关、公安机关、有关军事机关根据职责分工，依法搜集涉及国家安全的情报信息。

国家机关各部门在履行职责过程中，对于获取的涉及国家安全的有关信息应当及时上报。

第五十三条 开展情报信息工作，应当充分运用现代科学技术手段，加强对情报信息的鉴别、筛选、综合和研判分析。

第五十四条 情报信息的报送应当及时、准确、客观， 不得迟报、漏报、瞒报和谎报。

第三节 风险预防、评估和预警

第五十五条 国家制定完善应对各领域国家安全风险预案。

第五十六条 国家建立国家安全风险评估机制，定期开展各领域国家安全风险调查评估。

有关部门应当定期向中央国家安全领导机构提交国家安全风险评估报告。

第五十七条 国家健全国家安全风险监测预警制度，根据国家安全风险程度，及时发布相应风险预警。

第五十八条 对可能即将发生或者已经发生的危害国家安全的事件，县级以上地方人民政府及其有关主管部门应当立即按照规定向上一级人民政府及其有关主管部门报告，必要时可以越级上报。

第四节 审查监管

第五十九条 国家建立国家安全审查和监管的制度和机制，对影响或者可能影响国家安全的外商投资、特定物项和关键技术、网络信息技术产品和服务、涉及国家安全事项的建设项目，以及其他重大事项和活动，进行国家安全审查，有效预防和化解国家安全风险。

第六十条 中央国家机关各部门依照法律、行政法规行使国家安全审查职责，依法作出国家安全审查决定或者提出安全审查意见并监督执行。

第六十一条 省、自治区、直辖市依法负责本行政区域内有关国家安全审查和监管工作。

第五节 危机管控

第六十二条 国家建立统一领导、协同联动、有序高效的国家安全危机管控制度。

第六十三条 发生危及国家安全的重大事件，中央有关部门和有关地方根据中央国家安全领导机构的统一部署，依法启动应急预案，采取管控处置措施。

第六十四条 发生危及国家安全的特别重大事件，需要进入紧急状态、战争状态或者进行全国总动员、局部动员的，由全国人民代表大会、全国人民代表大会常务委员会或者国务院依照宪法和有关法律规定的权限和程序决定。

第六十五条 国家决定进入紧急状态、战争状态或者实施国防动员后，履行国家安全危机管控职责的有关机关依照法律规定或者全国人民代表大会常务委员会规定，有权采取限制公民和组织权利、增加公民和组织义务的特别措施。

第六十六条 履行国家安全危机管控职责的有关机关依法采取处置国家安全危机的管控措施，应当与国家安全危机可能造成的危害的性质、程度和范围相适应；有多种措施可供选择的，应当选择有利于最大程度保护公民、组织权益的措施。

第六十七条 国家健全国家安全危机的信息报告和发布机制。

国家安全危机事件发生后，履行国家安全危机管控职责的有关机关，应当按照规定准确、及时报告， 并依法将有关国家安全危机事件发生、发展、管控处置及善后情况统一向社会发布。

第六十八条 国家安全威胁和危害得到控制或者消除后，应当及时解除管控处置措施，做好善后工作。

第五章 国家安全保障

第六十九条 国家健全国家安全保障体系，增强维护国家安全的能力。

第七十条 国家健全国家安全法律制度体系，推动国家安全法治建设。

第七十一条 国家加大对国家安全各项建设的投入，保障国家安全工作所需经费和装备。

第七十二条 承担国家安全战略物资储备任务的单位，应当按照国家有关规定和标准对国家安全物资进行收储、保管和维护， 定期调整更换，保证储备物资的使用效能和安全。

第七十三条 鼓励国家安全领域科技创新，发挥科技在维护国家安全中的作用。

第七十四条 国家采取必要措施，招录、培养和管理国家安全工作专门人才和特殊人才。

根据维护国家安全工作的需要，国家依法保护有关机关专门从事国家安全工作人员的身份和合法权益，加大人身保护和安置保障力度。

第七十五条 国家安全机关、公安机关、有关军事机关开展国家安全专门工作，可以依法采取必要手段和方式，有关部门和地方应当在职责范围内提供支持和配合。

第七十六条 国家加强国家安全新闻宣传和舆论引导，通过多种形式开展国家安全宣传教育活动，将国家安全教育纳入国民教育体系和公务员教育培训体系，增强全民国家安全意识。

第六章 公民、组织的义务和权利

第七十七条 公民和组织应当履行下列维护国家安全的义务：

(一)遵守宪法、法律法规关于国家安全的有关规定；

(二)及时报告危害国家安全活动的线索;

(三)如实提供所知悉的涉及危害国家安全活动的证据;

(四)为国家安全工作提供便利条件或者其他协助;

(五)向国家安全机关、公安机关和有关军事机关提供必要的支持和协助;

(六)保守所知悉的国家秘密;

(七)法律、行政法规规定的其他义务。

任何个人和组织不得有危害国家安全的行为,不得向危害国家安全的个人或者组织提供任何资助或者协助。

第七十八条 机关、人民团体、企业事业组织和其他社会组织应当对本单位的人员进行维护国家安全的教育,动员、组织本单位的人员防范、制止危害国家安全的行为。

第七十九条 企业事业组织根据国家安全工作的要求,应当配合有关部门采取相关安全措施。

第八十条 公民和组织支持、协助国家安全工作的行为受法律保护。

因支持、协助国家安全工作, 本人或者其近亲属的人身安全面临危险的,可以向公安机关、国家安全机关请求予以保护。公安机关、国家安全机关应当会同有关部门依法采取保护措施。

第八十一条 公民和组织因支持、协助国家安全工作导致财产损失的,按照国家有关规定给予补偿;造成人身伤害或者死亡的,按照国家有关规定给予抚恤优待。

第八十二条 公民和组织对国家安全工作有向国家机关提出批评建议的权利,对国家机关及其工作人员在国家安全工作中的违法失职行为有提出申诉、控告和检举的权利。

第八十三条 在国家安全工作中,需要采取限制公民权利和自由的特别措施时,应当依法进行,并以维护国家安全的实际需要为限度。

第七章 附 则

第八十四条 本法自公布之日起施行。

中华人民共和国网络安全法

(2016 年 11 月 7 日第十二届全国人民代表大会常务委员会第二十四次会议通

过)

第一章 总 则

第一条 为了保障网络安全，维护网络空间主权和国家安全、社会公共利益，保护公民、法人和其他组织的合法权益， 促进经济社会信息化健康发展，制定本法。

第二条 在中华人民共和国境内建设、运营、维护和使用网络，以及网络安全的监督管理，适用本法。

第三条 国家坚持网络安全与信息化发展并重，遵循积极利用、科学发展、依法管理、确保安全的方针， 推进网络基础设施建设和互联互通，鼓励网络技术创新和应用，支持培养网络安全人才，建立健全网络安全保障体系，提高网络安全保护能力。

第四条 国家制定并不断完善网络安全战略，明确保障网络安全的基本要求和主要目标，提出重点领域的网络安全政策、工作任务和措施。

第五条 国家采取措施，监测、防御、处置来源于中华人民共和国境内外的网络安全风险和威胁，保护关键信息基础设施免受攻击、侵入、干扰和破坏， 依法惩治网络违法犯罪活动，维护网络空间安全和秩序。

第六条 国家倡导诚实守信、健康文明的网络行为，推动传播社会主义核心价值观，采取措施提高全社会的网络安全意识和水平，形成全社会共同参与促进网络安全的良好环境。

第七条 国家积极开展网络空间治理、网络技术研发和标准制定、打击网络违法犯罪等方面的国际交流与合作，推动构建和平、安全、开放、合作的网络空间，建立多边、民主、透明的网络治理体系。

第八条 国家网信部门负责统筹协调网络安全工作和相关监督管理工作。国务院电信主管部门、公安部门和其他有关机关依照本法和有关法律、行政法规的规定，在各自职责范围内负责网络安全保护和监督管理工作。

县级以上地方人民政府有关部门的网络安全保护和监督管理职责，按照国家有关规定确定。

第九条 网络运营者开展经营和服务活动，必须遵守法律、行政法规，尊重社会公德，遵守商业道德，诚实信用，履行网络安全保护义务，接受政府和社会

的监督，承担社会责任。

第十条 建设、运营网络或者通过网络提供服务，应当依照法律、行政法规的规定和国家标准的强制性要求，采取技术措施和其他必要措施，保障网络安全、稳定运行，有效应对网络安全事件，防范网络违法犯罪活动，维护网络数据的完整性、保密性和可用性。

第十一条 网络相关行业组织按照章程，加强行业自律，制定网络安全行为规范，指导会员加强网络安全保护，提高网络安全保护水平，促进行业健康发展。

第十二条 国家保护公民、法人和其他组织依法使用网络的权利，促进网络接入普及，提升网络服务水平，为社会提供安全、便利的网络服务， 保障网络信息依法有序自由流动。

任何个人和组织使用网络应当遵守宪法法律，遵守公共秩序，尊重社会公德，不得危害网络安全，不得利用网络从事危害国家安全、荣誉和利益， 煽动颠覆国家政权、推翻社会主义制度， 煽动分裂国家、破坏国家统一，宣扬恐怖主义、极端主义，宣扬民族仇恨、民族歧视， 传播暴力、淫秽色情信息， 编造、传播虚假信息扰乱经济秩序和社会秩序，以及侵害他人名誉、隐私、知识产权和其他合法权益等活动。

第十三条 国家支持研究开发有利于未成年人健康成长的网络产品和服务，依法惩治利用网络从事危害未成年人身心健康的活动，为未成年人提供安全、健康的网络环境。

第十四条 任何个人和组织有权对危害网络安全的行为向网信、电信、公安等部门举报。收到举报的部门应当及时依法作出处理； 不属于本部门职责的，应当及时移送有权处理的部门。

有关部门应当对举报人的相关信息予以保密，保护举报人的合法权益。

第二章 网络安全支持与促进

第十五条 国家建立和完善网络安全标准体系。国务院标准化行政主管部门和国务院其他有关部门根据各自的职责，组织制定并适时修订有关网络安全管理以及网络产品、服务和运行安全的国家标准、行业标准。

国家支持企业、研究机构、高等学校、网络相关行业组织参与网络安全国家标准、行业标准的制定。

第十六条 国务院和省、自治区、直辖市人民政府应当统筹规划，加大投入，扶持重点网络安全技术产业和项目，支持网络安全技术的研究开发和应用，推广安全可信的网络产品和服务，保护网络技术知识产权，支持企业、研究机构和高等学校等参与国家网络安全技术创新项目。

第十七条 国家推进网络安全社会化服务体系建设，鼓励有关企业、机构开展网络安全认证、检测和风险评估等安全服务。

第十八条 国家鼓励开发网络数据安全保护和利用技术，促进公共数据资源开放，推动技术创新和经济社会发展。

国家支持创新网络安全管理方式，运用网络新技术，提升网络安全保护水平。

第十九条 各级人民政府及其有关部门应当组织开展经常性的网络安全宣传教育，并指导、督促有关单位做好网络安全宣传教育工作。

大众传播媒介应当有针对性地面向社会进行网络安全宣传教育。

第二十条 国家支持企业和高等学校、职业学校等教育培训机构开展网络安全相关教育与培训，采取多种方式培养网络安全人才，促进网络安全人才交流。

第三章 网络运行安全

第一节 一般规定

第二十一条 国家实行网络安全等级保护制度。网络运营者应当按照网络安全等级保护制度的要求，履行下列安全保护义务，保障网络免受干扰、破坏或者未经授权的访问，防止网络数据泄露或者被窃取、篡改：

(一)制定内部安全管理制度和操作规程，确定网络安全负责人，落实网络安全保护责任；

(二)采取防范计算机病毒和网络攻击、网络侵入等危害网络安全行为的技术措施；

(三)采取监测、记录网络运行状态、网络安全事件的技术措施， 并按照规定留存相关的网络日志不少于六个月；

(四)采取数据分类、重要数据备份和加密等措施；

(五)法律、行政法规规定的其他义务。

第二十二条 网络产品、服务应当符合相关国家标准的强制性要求。网络产品、服务的提供者不得设置恶意程序； 发现其网络产品、服务存在安全缺陷、漏

洞等风险时，应当立即采取补救措施，按照规定及时告知用户并向有关主管部门报告。

网络产品、服务的提供者应当为其产品、服务持续提供安全维护； 在规定或者当事人约定的期限内，不得终止提供安全维护。

网络产品、服务具有收集用户信息功能的， 其提供者应当向用户明示并取得同意；涉及用户个人信息的，还应当遵守本法和有关法律、行政法规关于个人信息保护的规定。

第二十三条 网络关键设备和网络安全专用产品应当按照相关国家标准的强制性要求，由具备资格的机构安全认证合格或者安全检测符合要求后，方可销售或者提供。国家网信部门会同国务院有关部门制定、公布网络关键设备和网络安全专用产品目录，并推动安全认证和安全检测结果互认，避免重复认证、检测。

第二十四条 网络运营者为用户办理网络接入、域名注册服务，办理固定电话、移动电话等入网手续， 或者为用户提供信息发布、即时通讯等服务， 在与用户签订协议或者确认提供服务时，应当要求用户提供真实身份信息。用户不提供真实身份信息的，网络运营者不得为其提供相关服务。

国家实施网络可信身份战略，支持研究开发安全、方便的电子身份认证技术，推动不同电子身份认证之间的互认。

第二十五条 网络运营者应当制定网络安全事件应急预案，及时处置系统漏洞、计算机病毒、网络攻击、网络侵入等安全风险； 在发生危害网络安全的事件时，立即启动应急预案，采取相应的补救措施，并按照规定向有关主管部门报告。

第二十六条 开展网络安全认证、检测、风险评估等活动，向社会发布系统漏洞、计算机病毒、网络攻击、网络侵入等网络安全信息， 应当遵守国家有关规定。

第二十七条 任何个人和组织不得从事非法侵入他人网络、干扰他人网络正常功能、窃取网络数据等危害网络安全的活动；不得提供专门用于从事侵入网络、干扰网络正常功能及防护措施、窃取网络数据等危害网络安全活动的程序、工具；明知他人从事危害网络安全的活动的，不得为其提供技术支持、广告推广、支付结算等帮助。

第二十八条 网络运营者应当为公安机关、国家安全机关依法维护国家安全

和侦查犯罪的活动提供技术支持和协助。

第二十九条 国家支持网络运营者之间在网络安全信息收集、分析、通报和应急处置等方面进行合作，提高网络运营者的安全保障能力。

有关行业组织建立健全本行业的网络安全保护规范和协作机制，加强对网络安全风险的分析评估，定期向会员进行风险警示，支持、协助会员应对网络安全风险。

第三十条 网信部门和有关部门在履行网络安全保护职责中获取的信息，只能用于维护网络安全的需要，不得用于其他用途。

第二节 关键信息基础设施的运行安全

第三十一条 国家对公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务等重要行业和领域， 以及其他一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的关键信息基础设施， 在网络安全等级保护制度的基础上，实行重点保护。关键信息基础设施的具体范围和安全保护办法由国务院制定。

国家鼓励关键信息基础设施以外的网络运营者自愿参与关键信息基础设施保护体系。

第三十二条 按照国务院规定的职责分工，负责关键信息基础设施安全保护工作的部门分别编制并组织实施本行业、本领域的关键信息基础设施安全规划，指导和监督关键信息基础设施运行安全保护工作。

第三十三条 建设关键信息基础设施应当确保其具有支持业务稳定、持续运行的性能，并保证安全技术措施同步规划、同步建设、同步使用。

第三十四条 除本法第二十一条的规定外，关键信息基础设施的运营者还应当履行下列安全保护义务：

(一)设置专门安全管理机构和安全管理负责人，并对该负责人和关键岗位的人员进行安全背景审查；

(二)定期对从业人员进行网络安全教育、技术培训和技能考核；

(三)对重要系统和数据库进行容灾备份；

(四)制定网络安全事件应急预案，并定期进行演练；

(五)法律、行政法规规定的其他义务。

第三十五条 关键信息基础设施的运营者采购网络产品和服务，可能影响国家安全的，应当通过国家网信部门会同国务院有关部门组织的国家安全审查。

第三十六条 关键信息基础设施的运营者采购网络产品和服务，应当按照规定与提供者签订安全保密协议，明确安全和保密义务与责任。

第三十七条 关键信息基础设施的运营者在中华人民共和国境内运营中收集和产生的个人信息和重要数据应当在境内存储。因业务需要，确需向境外提供的，应当按照国家网信部门会同国务院有关部门制定的办法进行安全评估；法律、行政法规另有规定的，依照其规定。

第三十八条 关键信息基础设施的运营者应当自行或者委托网络安全服务机构对其网络的安全性和可能存在的风险每年至少进行一次检测评估，并将检测评估情况和改进措施报送相关负责关键信息基础设施安全保护工作的部门。

第三十九条 国家网信部门应当统筹协调有关部门对关键信息基础设施的安全保护采取下列措施：

(一)对关键信息基础设施的安全风险进行抽查检测，提出改进措施，必要时可以委托网络安全服务机构对网络存在的安全风险进行检测评估；

(二)定期组织关键信息基础设施的运营者进行网络安全应急演练，提高应对网络安全事件的水平和协同配合能力；

(三)促进有关部门、关键信息基础设施的运营者以及有关研究机构、网络安全服务机构等之间的网络安全信息共享；

(四)对网络安全事件的应急处置与网络功能的恢复等，提供技术支持和协助。

第四章 网络信息安全

第四十条 网络运营者应当对其收集的用户信息严格保密，并建立健全用户信息保护制度。

第四十一条 网络运营者收集、使用个人信息，应当遵循合法、正当、必要的原则，公开收集、使用规则，明示收集、使用信息的目的、方式和范围，并经被收集者同意。

网络运营者不得收集与其提供的服务无关的个人信息，不得违反法律、行政法规的规定和双方的约定收集、使用个人信息， 并应当依照法律、行政法规的规定和与用户的约定，处理其保存的个人信息。

第四十二条 网络运营者不得泄露、篡改、毁损其收集的个人信息；未经被收集者同意，不得向他人提供个人信息。但是， 经过处理无法识别特定个人且不能复原的除外。

网络运营者应当采取技术措施和其他必要措施，确保其收集的个人信息安全，防止信息泄露、毁损、丢失。在发生或者可能发生个人信息泄露、毁损、丢失的情况时，应当立即采取补救措施，按照规定及时告知用户并向有关主管部门报告。

第四十三条 个人发现网络运营者违反法律、行政法规的规定或者双方的约定收集、使用其个人信息的， 有权要求网络运营者删除其个人信息；发现网络运营者收集、存储的其个人信息有错误的， 有权要求网络运营者予以更正。网络运营者应当采取措施予以删除或者更正。

第四十四条 任何个人和组织不得窃取或者以其他非法方式获取个人信息，不得非法出售或者非法向他人提供个人信息。

第四十五条 依法负有网络安全监督管理职责的部门及其工作人员，必须对在履行职责中知悉的个人信息、隐私和商业秘密严格保密， 不得泄露、出售或者非法向他人提供。

第四十六条 任何个人和组织应当对其使用网络的行为负责，不得设立用于实施诈骗，传授犯罪方法，制作或者销售违禁物品、管制物品等违法犯罪活动的网站、通讯群组， 不得利用网络发布涉及实施诈骗，制作或者销售违禁物品、管制物品以及其他违法犯罪活动的信息。

第四十七条 网络运营者应当加强对其用户发布的信息的管理，发现法律、行政法规禁止发布或者传输的信息的，应当立即停止传输该信息，采取消除等处置措施，防止信息扩散，保存有关记录，并向有关主管部门报告。

第四十八条 任何个人和组织发送的电子信息、提供的应用软件，不得设置恶意程序，不得含有法律、行政法规禁止发布或者传输的信息。

电子信息发送服务提供者和应用软件下载服务提供者，应当履行安全管理义务，知道其用户有前款规定行为的，应当停止提供服务，采取消除等处置措施，保存有关记录，并向有关主管部门报告。

第四十九条 网络运营者应当建立网络信息安全投诉、举报制度，公布投诉、举报方式等信息，及时受理并处理有关网络信息安全的投诉和举报。

网络运营者对网信部门和有关部门依法实施的监督检查，应当予以配合。

第五十条 国家网信部门和有关部门依法履行网络信息安全监督管理职责，发现法律、行政法规禁止发布或者传输的信息的，应当要求网络运营者停止传输，采取消除等处置措施，保存有关记录；对来源于中华人民共和国境外的上述信息，应当通知有关机构采取技术措施和其他必要措施阻断传播。

第五章 监测预警与应急处置

第五十一条 国家建立网络安全监测预警和信息通报制度。国家网信部门应当统筹协调有关部门加强网络安全信息收集、分析和通报工作， 按照规定统一发布网络安全监测预警信息。

第五十二条 负责关键信息基础设施安全保护工作的部门，应当建立健全本行业、本领域的网络安全监测预警和信息通报制度， 并按照规定报送网络安全监测预警信息。

第五十三条 国家网信部门协调有关部门建立健全网络安全风险评估和应急工作机制，制定网络安全事件应急预案，并定期组织演练。

负责关键信息基础设施安全保护工作的部门应当制定本行业、本领域的网络安全事件应急预案，并定期组织演练。

网络安全事件应急预案应当按照事件发生后的危害程度、影响范围等因素对网络安全事件进行分级，并规定相应的应急处置措施。

第五十四条 网络安全事件发生的风险增大时，省级以上人民政府有关部门应当按照规定的权限和程序，并根据网络安全风险的特点和可能造成的危害，采取下列措施：

(一)要求有关部门、机构和人员及时收集、报告有关信息， 加强对网络安全风险的监测；

(二)组织有关部门、机构和专业人员，对网络安全风险信息进行分析评估，预测事件发生的可能性、影响范围和危害程度；

(三)向社会发布网络安全风险预警，发布避免、减轻危害的措施。

第五十五条 发生网络安全事件，应当立即启动网络安全事件应急预案，对网络安全事件进行调查和评估，要求网络运营者采取技术措施和其他必要措施，消除安全隐患，防止危害扩大，并及时向社会发布与公众有关的警示信息。

第五十六条 省级以上人民政府有关部门在履行网络安全监督管理职责中，发现网络存在较大安全风险或者发生安全事件的，可以按照规定的权限和程序对该网络的运营者的法定代表人或者主要负责人进行约谈。网络运营者应当按照要求采取措施，进行整改，消除隐患。

第五十七条 因网络安全事件，发生突发事件或者生产安全事故的，应当依照《中华人民共和国突发事件应对法》、《中华人民共和国安全生产法》等有关法律、行政法规的规定处置。

第五十八条 因维护国家安全和社会公共秩序，处置重大突发社会安全事件的需要，经国务院决定或者批准，可以在特定区域对网络通信采取限制等临时措施。

第六章 法律责任

第五十九条 网络运营者不履行本法第二十一条、第二十五条规定的网络安全保护义务的，由有关主管部门责令改正，给予警告；拒不改正或者导致危害网络安全等后果的，处一万元以上十万元以下罚款，对直接负责的主管人员处五千元以上五万元以下罚款。

关键信息基础设施的运营者不履行本法第三十三条、第三十四条、第三十六条、第三十八条规定的网络安全保护义务的， 由有关主管部门责令改正，给予警告；拒不改正或者导致危害网络安全等后果的，处十万元以上一百万元以下罚款，对直接负责的主管人员处一万元以上十万元以下罚款。

第六十条 违反本法第二十二条第一款、第二款和第四十八条第一款规定，有下列行为之一的，由有关主管部门责令改正，给予警告；拒不改正或者导致危害网络安全等后果的，处五万元以上五十万元以下罚款，对直接负责的主管人员处一万元以上十万元以下罚款：

(一)设置恶意程序的；

(二)对其产品、服务存在的安全缺陷、漏洞等风险未立即采取补救措施， 或者未按照规定及时告知用户并向有关主管部门报告的；

(三)擅自终止为其产品、服务提供安全维护的。

第六十一条 网络运营者违反本法第二十四条第一款规定，未要求用户提供真实身份信息，或者对不提供真实身份信息的用户提供相关服务的，由有关主管

部门责令改正；拒不改正或者情节严重的，处五万元以上五十万元以下罚款，并可以由有关主管部门责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照，对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。

第六十二条 违反本法第二十六条规定，开展网络安全认证、检测、风险评估等活动，或者向社会发布系统漏洞、计算机病毒、网络攻击、网络侵入等网络安全信息的，由有关主管部门责令改正，给予警告；拒不改正或者情节严重的，处一万元以上十万元以下罚款，并可以由有关主管部门责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照， 对直接负责的主管人员和其他直接责任人员处五千元以上五万元以下罚款。

第六十三条 违反本法第二十七条规定，从事危害网络安全的活动，或者提供专门用于从事危害网络安全活动的程序、工具， 或者为他人从事危害网络安全的活动提供技术支持、广告推广、支付结算等帮助， 尚不构成犯罪的，由公安机关没收违法所得，处五日以下拘留，可以并处五万元以上五十万元以下罚款；情节较重的，处五日以上十五日以下拘留，可以并处十万元以上一百万元以下罚款。

单位有前款行为的，由公安机关没收违法所得，处十万元以上一百万元以下罚款，并对直接负责的主管人员和其他直接责任人员依照前款规定处罚。

违反本法第二十七条规定，受到治安管理处罚的人员，五年内不得从事网络安全管理和网络运营关键岗位的工作；受到刑事处罚的人员，终身不得从事网络安全管理和网络运营关键岗位的工作。

第六十四条 网络运营者、网络产品或者服务的提供者违反本法第二十二条第三款、第四十一条至第四十三条规定，侵害个人信息依法得到保护的权利的，由有关主管部门责令改正，可以根据情节单处或者并处警告、没收违法所得、处违法所得一倍以上十倍以下罚款，没有违法所得的，处一百万元以下罚款，对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款；情节严重的，并可以责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照。

违反本法第四十四条规定，窃取或者以其他非法方式获取、非法出售或者非法向他人提供个人信息，尚不构成犯罪的，由公安机关没收违法所得，并处违法

所得一倍以上十倍以下罚款，没有违法所得的，处一百万元以下罚款。

第六十五条 关键信息基础设施的运营者违反本法第三十五条规定，使用未经安全审查或者安全审查未通过的网络产品或者服务的，由有关主管部门责令停止使用，处采购金额一倍以上十倍以下罚款；对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。

第六十六条 关键信息基础设施的运营者违反本法第三十七条规定，在境外存储网络数据，或者向境外提供网络数据的，由有关主管部门责令改正，给予警告，没收违法所得，处五万元以上五十万元以下罚款，并可以责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照； 对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。

第六十七条 违反本法第四十六条规定，设立用于实施违法犯罪活动的网站、通讯群组，或者利用网络发布涉及实施违法犯罪活动的信息，尚不构成犯罪的，由公安机关处五日以下拘留，可以并处一万元以上十万元以下罚款；情节较重的，处五日以上十五日以下拘留，可以并处五万元以上五十万元以下罚款。关闭用于实施违法犯罪活动的网站、通讯群组。

单位有前款行为的，由公安机关处十万元以上五十万元以下罚款，并对直接负责的主管人员和其他直接责任人员依照前款规定处罚。

第六十八条 网络运营者违反本法第四十七条规定，对法律、行政法规禁止发布或者传输的信息未停止传输、采取消除等处置措施、保存有关记录的， 由有关主管部门责令改正，给予警告，没收违法所得；拒不改正或者情节严重的，处十万元以上五十万元以下罚款，并可以责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照，对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。

电子信息发送服务提供者、应用软件下载服务提供者， 不履行本法第四十八条第二款规定的安全管理义务的，依照前款规定处罚。

第六十九条 网络运营者违反本法规定，有下列行为之一的， 由有关主管部门责令改正；拒不改正或者情节严重的，处五万元以上五十万元以下罚款，对直接负责的主管人员和其他直接责任人员，处一万元以上十万元以下罚款：

(一)不按照有关部门的要求对法律、行政法规禁止发布或者传输的信息， 采

取停止传输、消除等处置措施的；

(二)拒绝、阻碍有关部门依法实施的监督检查的；

(三)拒不向公安机关、国家安全机关提供技术支持和协助的。

第七十条 发布或者传输本法第十二条第二款和其他法律、行政法规禁止发布或者传输的信息的，依照有关法律、行政法规的规定处罚。

第七十一条 有本法规定的违法行为的，依照有关法律、行政法规的规定记入信用档案，并予以公示。

第七十二条 国家机关政务网络的运营者不履行本法规定的网络安全保护义务的，由其上级机关或者有关机关责令改正；对直接负责的主管人员和其他直接责任人员依法给予处分。

第七十三条 网信部门和有关部门违反本法第三十条规定，将在履行网络安全保护职责中获取的信息用于其他用途的，对直接负责的主管人员和其他直接责任人员依法给予处分。

网信部门和有关部门的工作人员玩忽职守、滥用职权、徇私舞弊， 尚不构成犯罪的，依法给予处分。

第七十四条 违反本法规定，给他人造成损害的，依法承担民事责任。

违反本法规定，构成违反治安管理行为的，依法给予治安管理处罚；构成犯罪的，依法追究刑事责任。

第七十五条 境外的机构、组织、个人从事攻击、侵入、干扰、破坏等危害中华人民共和国的关键信息基础设施的活动，造成严重后果的，依法追究法律责任；国务院公安部门和有关部门并可以决定对该机构、组织、个人采取冻结财产或者其他必要的制裁措施。

第七章 附 则

第七十六条 本法下列用语的含义：

(一)网络，是指由计算机或者其他信息终端及相关设备组成的按照一定的规则和程序对信息进行收集、存储、传输、交换、处理的系统。

(二)网络安全，是指通过采取必要措施，防范对网络的攻击、侵入、干扰、破坏和非法使用以及意外事故，使网络处于稳定可靠运行的状态，以及保障网络数据的完整性、保密性、可用性的能力。

(三)网络运营者，是指网络的所有者、管理者和网络服务提供者。

(四)网络数据，是指通过网络收集、存储、传输、处理和产生的各种电子数据。

(五)个人信息，是指以电子或者其他方式记录的能够单独或者与其他信息结合识别自然人个人身份的各种信息，包括但不限于自然人的姓名、出生日期、身份证件号码、个人生物识别信息、住址、电话号码等。

第七十七条 存储、处理涉及国家秘密信息的网络的运行安全保护，除应当遵守本法外，还应当遵守保密法律、行政法规的规定。

第七十八条 军事网络的安全保护，由中央军事委员会另行规定。

第七十九条 本法自 2017 年 6 月 1 日起施行。

中华人民共和国电子商务法

(2018 年 8 月 31 日第十三届全国人民代表大会常务委员会第五次会议通过)

第一章 总 则

第一条 为了保障电子商务各方主体的合法权益，规范电子商务行为，维护市场秩序，促进电子商务持续健康发展，制定本法。

第二条 中华人民共和国境内的电子商务活动，适用本法。

本法所称电子商务，是指通过互联网等信息网络销售商品或者提供服务的经营活动。

法律、行政法规对销售商品或者提供服务有规定的， 适用其规定。金融类产品和服务，利用信息网络提供新闻信息、音视频节目、出版以及文化产品等内容方面的服务，不适用本法。

第三条 国家鼓励发展电子商务新业态，创新商业模式，促进电子商务技术研发和推广应用，推进电子商务诚信体系建设，营造有利于电子商务创新发展的市场环境，充分发挥电子商务在推动高质量发展、满足人民日益增长的美好生活需要、构建开放型经济方面的重要作用。

第四条 国家平等对待线上线下商务活动，促进线上线下融合发展，各级人民政府和有关部门不得采取歧视性的政策措施，不得滥用行政权力排除、限制市场竞争。

第五条 电子商务经营者从事经营活动，应当遵循自愿、平等、公平、诚信

的原则，遵守法律和商业道德，公平参与市场竞争，履行消费者权益保护、环境保护、知识产权保护、网络安全与个人信息保护等方面的义务， 承担产品和服务质量责任，接受政府和社会的监督。

第六条 国务院有关部门按照职责分工负责电子商务发展促进、监督管理等工作。县级以上地方各级人民政府可以根据本行政区域的实际情况， 确定本行政区域内电子商务的部门职责划分。

第七条 国家建立符合电子商务特点的协同管理体系，推动形成有关部门、电子商务行业组织、电子商务经营者、消费者等共同参与的电子商务市场治理体系。

第八条 电子商务行业组织按照本组织章程开展行业自律，建立健全行业规范，推动行业诚信建设，监督、引导本行业经营者公平参与市场竞争。

第二章 电子商务经营者

第一节 一般规定

第九条 本法所称电子商务经营者，是指通过互联网等信息网络从事销售商品或者提供服务的经营活动的自然人、法人和非法人组织， 包括电子商务平台经营者、平台内经营者以及通过自建网站、其他网络服务销售商品或者提供服务的电子商务经营者。

本法所称电子商务平台经营者，是指在电子商务中为交易双方或者多方提供网络经营场所、交易撮合、信息发布等服务， 供交易双方或者多方独立开展交易活动的法人或者非法人组织。

本法所称平台内经营者，是指通过电子商务平台销售商品或者提供服务的电子商务经营者。

第十条 电子商务经营者应当依法办理市场主体登记。但是， 个人销售自产农副产品、家庭手工业产品， 个人利用自己的技能从事依法无须取得许可的便民劳务活动和零星小额交易活动，以及依照法律、行政法规不需要进行登记的除外。

第十一条 电子商务经营者应当依法履行纳税义务，并依法享受税收优惠。

依照前条规定不需要办理市场主体登记的电子商务经营者在首次纳税义务发生后，应当依照税收征收管理法律、行政法规的规定申请办理税务登记， 并如实申报纳税。

第十二条 电子商务经营者从事经营活动，依法需要取得相关行政许可的，应当依法取得行政许可。

第十三条 电子商务经营者销售的商品或者提供的服务应当符合保障人身、财产安全的要求和环境保护要求，不得销售或者提供法律、行政法规禁止交易的商品或者服务。

第十四条 电子商务经营者销售商品或者提供服务应当依法出具纸质发票或者电子发票等购货凭证或者服务单据。电子发票与纸质发票具有同等法律效力。

第十五条 电子商务经营者应当在其首页显著位置，持续公示营业执照信息、与其经营业务有关的行政许可信息、属于依照本法第十条规定的不需要办理市场主体登记情形等信息，或者上述信息的链接标识。

前款规定的信息发生变更的，电子商务经营者应当及时更新公示信息。

第十六条 电子商务经营者自行终止从事电子商务的，应当提前三十日在首页显著位置持续公示有关信息。

第十七条 电子商务经营者应当全面、真实、准确、及时地披露商品或者服务信息，保障消费者的知情权和选择权。电子商务经营者不得以虚构交易、编造用户评价等方式进行虚假或者引人误解的商业宣传，欺骗、误导消费者。

第十八条 电子商务经营者根据消费者的兴趣爱好、消费习惯等特征向其提供商品或者服务的搜索结果的，应当同时向该消费者提供不针对其个人特征的选项，尊重和平等保护消费者合法权益。

电子商务经营者向消费者发送广告的，应当遵守《中华人民共和国广告法》的有关规定。

第十九条 电子商务经营者搭售商品或者服务，应当以显著方式提请消费者注意，不得将搭售商品或者服务作为默认同意的选项。

第二十条 电子商务经营者应当按照承诺或者与消费者约定的方式、时限向消费者交付商品或者服务，并承担商品运输中的风险和责任。但是， 消费者另行选择快递物流服务提供者的除外。

第二十一条 电子商务经营者按照约定向消费者收取押金的，应当明示押金退还的方式、程序， 不得对押金退还设置不合理条件。消费者申请退还押金， 符合押金退还条件的，电子商务经营者应当及时退还。

第二十二条 电子商务经营者因其技术优势、用户数量、对相关行业的控制能力以及其他经营者对该电子商务经营者在交易上的依赖程度等因素而具有市场支配地位的，不得滥用市场支配地位，排除、限制竞争。

第二十三条 电子商务经营者收集、使用其用户的个人信息，应当遵守法律、行政法规有关个人信息保护的规定。

第二十四条 电子商务经营者应当明示用户信息查询、更正、删除以及用户注销的方式、程序， 不得对用户信息查询、更正、删除以及用户注销设置不合理条件。

电子商务经营者收到用户信息查询或者更正、删除的申请的， 应当在核实身份后及时提供查询或者更正、删除用户信息。用户注销的， 电子商务经营者应当立即删除该用户的信息；依照法律、行政法规的规定或者双方约定保存的， 依照其规定。

第二十五条 有关主管部门依照法律、行政法规的规定要求电子商务经营者提供有关电子商务数据信息的，电子商务经营者应当提供。有关主管部门应当采取必要措施保护电子商务经营者提供的数据信息的安全，并对其中的个人信息、隐私和商业秘密严格保密，不得泄露、出售或者非法向他人提供。

第二十六条 电子商务经营者从事跨境电子商务，应当遵守进出口监督管理的法律、行政法规和国家有关规定。

第二节 电子商务平台经营者

第二十七条 电子商务平台经营者应当要求申请进入平台销售商品或者提供服务的经营者提交其身份、地址、联系方式、行政许可等真实信息，进行核验、登记，建立登记档案，并定期核验更新。

电子商务平台经营者为进入平台销售商品或者提供服务的非经营用户提供服务，应当遵守本节有关规定。

第二十八条 电子商务平台经营者应当按照规定向市场监督管理部门报送平台内经营者的身份信息，提示未办理市场主体登记的经营者依法办理登记，并配合市场监督管理部门，针对电子商务的特点，为应当办理市场主体登记的经营者办理登记提供便利。

电子商务平台经营者应当依照税收征收管理法律、行政法规的规定， 向税务

部门报送平台内经营者的身份信息和与纳税有关的信息，并应当提示依照本法第十条规定不需要办理市场主体登记的电子商务经营者依照本法第十一条第二款的规定办理税务登记。

第二十九条 电子商务平台经营者发现平台内的商品或者服务信息存在违反本法第十二条、第十三条规定情形的， 应当依法采取必要的处置措施，并向有关主管部门报告。

第三十条 电子商务平台经营者应当采取技术措施和其他必要措施保证其网络安全、稳定运行， 防范网络违法犯罪活动，有效应对网络安全事件，保障电子商务交易安全。

电子商务平台经营者应当制定网络安全事件应急预案，发生网络安全事件时，应当立即启动应急预案，采取相应的补救措施，并向有关主管部门报告。

第三十一条 电子商务平台经营者应当记录、保存平台上发布的商品和服务信息、交易信息， 并确保信息的完整性、保密性、可用性。商品和服务信息、交易信息保存时间自交易完成之日起不少于三年；法律、行政法规另有规定的， 依照其规定。

第三十二条 电子商务平台经营者应当遵循公开、公平、公正的原则，制定平台服务协议和交易规则，明确进入和退出平台、商品和服务质量保障、消费者权益保护、个人信息保护等方面的权利和义务。

第三十三条 电子商务平台经营者应当在其首页显著位置持续公示平台服务协议和交易规则信息或者上述信息的链接标识，并保证经营者和消费者能够便利、完整地阅览和下载。

第三十四条 电子商务平台经营者修改平台服务协议和交易规则，应当在其首页显著位置公开征求意见，采取合理措施确保有关各方能够及时充分表达意见。修改内容应当至少在实施前七日予以公示。

平台内经营者不接受修改内容，要求退出平台的，电子商务平台经营者不得阻止，并按照修改前的服务协议和交易规则承担相关责任。

第三十五条 电子商务平台经营者不得利用服务协议、交易规则以及技术等手段，对平台内经营者在平台内的交易、交易价格以及与其他经营者的交易等进行不合理限制或者附加不合理条件，或者向平台内经营者收取不合理费用。

第三十六条 电子商务平台经营者依据平台服务协议和交易规则对平台内经营者违反法律、法规的行为实施警示、暂停或者终止服务等措施的， 应当及时公示。

第三十七条 电子商务平台经营者在其平台上开展自营业务的，应当以显著方式区分标记自营业务和平台内经营者开展的业务，不得误导消费者。

电子商务平台经营者对其标记为自营的业务依法承担商品销售者或者服务提供者的民事责任。

第三十八条 电子商务平台经营者知道或者应当知道平台内经营者销售的商品或者提供的服务不符合保障人身、财产安全的要求， 或者有其他侵害消费者合法权益行为，未采取必要措施的，依法与该平台内经营者承担连带责任。

对关系消费者生命健康的商品或者服务，电子商务平台经营者对平台内经营者的资质资格未尽到审核义务，或者对消费者未尽到安全保障义务，造成消费者损害的，依法承担相应的责任。

第三十九条 电子商务平台经营者应当建立健全信用评价制度，公示信用评价规则，为消费者提供对平台内销售的商品或者提供的服务进行评价的途径。

电子商务平台经营者不得删除消费者对其平台内销售的商品或者提供的服务的评价。

第四十条 电子商务平台经营者应当根据商品或者服务的价格、销量、信用等以多种方式向消费者显示商品或者服务的搜索结果；对于竞价排名的商品或者服务，应当显著标明“广告”。

第四十一条 电子商务平台经营者应当建立知识产权保护规则，与知识产权权利人加强合作，依法保护知识产权。

第四十二条 知识产权权利人认为其知识产权受到侵害的，有权通知电子商务平台经营者采取删除、屏蔽、断开链接、终止交易和服务等必要措施。通知应当包括构成侵权的初步证据。

电子商务平台经营者接到通知后，应当及时采取必要措施，并将该通知转送平台内经营者；未及时采取必要措施的，对损害的扩大部分与平台内经营者承担连带责任。

因通知错误造成平台内经营者损害的，依法承担民事责任。恶意发出错误通

知，造成平台内经营者损失的，加倍承担赔偿责任。

第四十三条 平台内经营者接到转送的通知后，可以向电子商务平台经营者提交不存在侵权行为的声明。声明应当包括不存在侵权行为的初步证据。

电子商务平台经营者接到声明后，应当将该声明转送发出通知的知识产权权利人，并告知其可以向有关主管部门投诉或者向人民法院起诉。电子商务平台经营者在转送声明到达知识产权权利人后十五日内，未收到权利人已经投诉或者起诉通知的，应当及时终止所采取的措施。

第四十四条 电子商务平台经营者应当及时公示收到的本法第四十二条、第四十三条规定的通知、声明及处理结果。

第四十五条 电子商务平台经营者知道或者应当知道平台内经营者侵犯知识产权的，应当采取删除、屏蔽、断开链接、终止交易和服务等必要措施；未采取必要措施的，与侵权人承担连带责任。

第四十六条 除本法第九条第二款规定的服务外，电子商务平台经营者可以按照平台服务协议和交易规则，为经营者之间的电子商务提供仓储、物流、支付结算、交收等服务。电子商务平台经营者为经营者之间的电子商务提供服务， 应当遵守法律、行政法规和国家有关规定， 不得采取集中竞价、做市商等集中交易方式进行交易，不得进行标准化合约交易。

第三章 电子商务合同的订立与履行

第四十七条 电子商务当事人订立和履行合同，适用本章和《中华人民共和国民法总则》《中华人民共和国合同法》《中华人民共和国电子签名法》等法律的规定。

第四十八条 电子商务当事人使用自动信息系统订立或者履行合同的行为对使用该系统的当事人具有法律效力。

在电子商务中推定当事人具有相应的民事行为能力。但是， 有相反证据足以推翻的除外。

第四十九条 电子商务经营者发布的商品或者服务信息符合要约条件的，用户选择该商品或者服务并提交订单成功，合同成立。当事人另有约定的， 从其约定。

电子商务经营者不得以格式条款等方式约定消费者支付价款后合同不成立；

格式条款等含有该内容的，其内容无效。

第五十条 电子商务经营者应当清晰、全面、明确地告知用户订立合同的步骤、注意事项、下载方法等事项，并保证用户能够便利、完整地阅览和下载。

电子商务经营者应当保证用户在提交订单前可以更正输入错误。

第五十一条 合同标的为交付商品并采用快递物流方式交付的，收货人签收时间为交付时间。合同标的为提供服务的， 生成的电子凭证或者实物凭证中载明的时间为交付时间；前述凭证没有载明时间或者载明时间与实际提供服务时间不一致的，实际提供服务的时间为交付时间。

合同标的为采用在线传输方式交付的，合同标的进入对方当事人指定的特定系统并且能够检索识别的时间为交付时间。

合同当事人对交付方式、交付时间另有约定的，从其约定。

第五十二条 电子商务当事人可以约定采用快递物流方式交付商品。

快递物流服务提供者为电子商务提供快递物流服务，应当遵守法律、行政法规，并应当符合承诺的服务规范和时限。快递物流服务提供者在交付商品时， 应当提示收货人当面查验；交由他人代收的，应当经收货人同意。

快递物流服务提供者应当按照规定使用环保包装材料，实现包装材料的减量化和再利用。

快递物流服务提供者在提供快递物流服务的同时，可以接受电子商务经营者的委托提供代收货款服务。

第五十三条 电子商务当事人可以约定采用电子支付方式支付价款。

电子支付服务提供者为电子商务提供电子支付服务，应当遵守国家规定，告知用户电子支付服务的功能、使用方法、注意事项、相关风险和收费标准等事项，不得附加不合理交易条件。电子支付服务提供者应当确保电子支付指令的完整性、一致性、可跟踪稽核和不可篡改。

电子支付服务提供者应当向用户免费提供对账服务以及最近三年的交易记录。

第五十四条 电子支付服务提供者提供电子支付服务不符合国家有关支付安全管理要求，造成用户损失的，应当承担赔偿责任。

第五十五条 用户在发出支付指令前，应当核对支付指令所包含的金额、收

款人等完整信息。

支付指令发生错误的，电子支付服务提供者应当及时查找原因，并采取相关措施予以纠正。造成用户损失的， 电子支付服务提供者应当承担赔偿责任，但能够证明支付错误非自身原因造成的除外。

第五十六条 电子支付服务提供者完成电子支付后，应当及时准确地向用户提供符合约定方式的确认支付的信息。

第五十七条 用户应当妥善保管交易密码、电子签名数据等安全工具。用户发现安全工具遗失、被盗用或者未经授权的支付的， 应当及时通知电子支付服务提供者。

未经授权的支付造成的损失，由电子支付服务提供者承担；电子支付服务提供者能够证明未经授权的支付是因用户的过错造成的，不承担责任。

电子支付服务提供者发现支付指令未经授权，或者收到用户支付指令未经授权的通知时，应当立即采取措施防止损失扩大。电子支付服务提供者未及时采取措施导致损失扩大的，对损失扩大部分承担责任。

第四章 电子商务争议解决

第五十八条 国家鼓励电子商务平台经营者建立有利于电子商务发展和消费者权益保护的商品、服务质量担保机制。

电子商务平台经营者与平台内经营者协议设立消费者权益保证金的，双方应当就消费者权益保证金的提取数额、管理、使用和退还办法等作出明确约定。

消费者要求电子商务平台经营者承担先行赔偿责任以及电子商务平台经营者赔偿后向平台内经营者的追偿，适用《中华人民共和国消费者权益保护法》的有关规定。

第五十九条 电子商务经营者应当建立便捷、有效的投诉、举报机制，公开投诉、举报方式等信息，及时受理并处理投诉、举报。

第六十条 电子商务争议可以通过协商和解，请求消费者组织、行业协会或者其他依法成立的调解组织调解，向有关部门投诉，提请仲裁，或者提起诉讼等方式解决。

第六十一条 消费者在电子商务平台购买商品或者接受服务，与平台内经营者发生争议时，电子商务平台经营者应当积极协助消费者维护合法权益。

第六十二条 在电子商务争议处理中，电子商务经营者应当提供原始合同和交易记录。因电子商务经营者丢失、伪造、篡改、销毁、隐匿或者拒绝提供前述资料，致使人民法院、仲裁机构或者有关机关无法查明事实的， 电子商务经营者应当承担相应的法律责任。

第六十三条 电子商务平台经营者可以建立争议在线解决机制，制定并公示争议解决规则，根据自愿原则，公平、公正地解决当事人的争议。

第五章 电子商务促进

第六十四条 国务院和省、自治区、直辖市人民政府应当将电子商务发展纳入国民经济和社会发展规划，制定科学合理的产业政策，促进电子商务创新发展。

第六十五条 国务院和县级以上地方人民政府及其有关部门应当采取措施，支持、推动绿色包装、仓储、运输，促进电子商务绿色发展。

第六十六条 国家推动电子商务基础设施和物流网络建设，完善电子商务统计制度，加强电子商务标准体系建设。

第六十七条 国家推动电子商务在国民经济各个领域的应用，支持电子商务与各产业融合发展。

第六十八条 国家促进农业生产、加工、流通等环节的互联网技术应用，鼓励各类社会资源加强合作，促进农村电子商务发展，发挥电子商务在精准扶贫中的作用。

第六十九条 国家维护电子商务交易安全，保护电子商务用户信息，鼓励电子商务数据开发应用，保障电子商务数据依法有序自由流动。

国家采取措施推动建立公共数据共享机制，促进电子商务经营者依法利用公共数据。

第七十条 国家支持依法设立的信用评价机构开展电子商务信用评价，向社会提供电子商务信用评价服务。

第七十一条 国家促进跨境电子商务发展，建立健全适应跨境电子商务特点的海关、税收、进出境检验检疫、支付结算等管理制度， 提高跨境电子商务各环节便利化水平，支持跨境电子商务平台经营者等为跨境电子商务提供仓储物流、报关、报检等服务。

国家支持小型微型企业从事跨境电子商务。

第七十二条 国家进出口管理部门应当推进跨境电子商务海关申报、纳税、检验检疫等环节的综合服务和监管体系建设，优化监管流程，推动实现信息共享、监管互认、执法互助， 提高跨境电子商务服务和监管效率。跨境电子商务经营者可以凭电子单证向国家进出口管理部门办理有关手续。

第七十三条 国家推动建立与不同国家、地区之间跨境电子商务的交流合作，参与电子商务国际规则的制定，促进电子签名、电子身份等国际互认。

国家推动建立与不同国家、地区之间的跨境电子商务争议解决机制。

第六章 法律责任

第七十四条 电子商务经营者销售商品或者提供服务，不履行合同义务或者履行合同义务不符合约定，或者造成他人损害的，依法承担民事责任。

第七十五条 电子商务经营者违反本法第十二条、第十三条规定，未取得相关行政许可从事经营活动，或者销售、提供法律、行政法规禁止交易的商品、服务，或者不履行本法第二十五条规定的信息提供义务，电子商务平台经营者违反本法第四十六条规定，采取集中交易方式进行交易，或者进行标准化合约交易的，依照有关法律、行政法规的规定处罚。

第七十六条 电子商务经营者违反本法规定，有下列行为之一的，由市场监督管理部门责令限期改正，可以处一万元以下的罚款，对其中的电子商务平台经营者，依照本法第八十一条第一款的规定处罚：

(一)未在首页显著位置公示营业执照信息、行政许可信息、属于不需要办理市场主体登记情形等信息，或者上述信息的链接标识的；

(二)未在首页显著位置持续公示终止电子商务的有关信息的；

(三)未明示用户信息查询、更正、删除以及用户注销的方式、程序， 或者对用户信息查询、更正、删除以及用户注销设置不合理条件的。

电子商务平台经营者对违反前款规定的平台内经营者未采取必要措施的，由市场监督管理部门责令限期改正，可以处二万元以上十万元以下的罚款。

第七十七条 电子商务经营者违反本法第十八条第一款规定提供搜索结果，或者违反本法第十九条规定搭售商品、服务的， 由市场监督管理部门责令限期改正，没收违法所得，可以并处五万元以上二十万元以下的罚款；情节严重的，并处二十万元以上五十万元以下的罚款。

第七十八条 电子商务经营者违反本法第二十一条规定，未向消费者明示押金退还的方式、程序， 对押金退还设置不合理条件，或者不及时退还押金的，由有关主管部门责令限期改正，可以处五万元以上二十万元以下的罚款；情节严重的，处二十万元以上五十万元以下的罚款。

第七十九条 电子商务经营者违反法律、行政法规有关个人信息保护的规定，或者不履行本法第三十条和有关法律、行政法规规定的网络安全保障义务的， 依照《中华人民共和国网络安全法》等法律、行政法规的规定处罚。

第八十条 电子商务平台经营者有下列行为之一的，由有关主管部门责令限期改正；逾期不改正的，处二万元以上十万元以下的罚款；情节严重的，责令停业整顿，并处十万元以上五十万元以下的罚款：

(一)不履行本法第二十七条规定的核验、登记义务的；

(二)不按照本法第二十八条规定向市场监督管理部门、税务部门报送有关信息的；

(三)不按照本法第二十九条规定对违法情形采取必要的处置措施，或者未向有关主管部门报告的；

(四)不履行本法第三十一条规定的商品和服务信息、交易信息保存义务的。

法律、行政法规对前款规定的违法行为的处罚另有规定的，依照其规定。

第八十一条 电子商务平台经营者违反本法规定，有下列行为之一的，由市场监督管理部门责令限期改正，可以处二万元以上十万元以下的罚款；情节严重的，处十万元以上五十万元以下的罚款：

(一)未在首页显著位置持续公示平台服务协议、交易规则信息或者上述信息的链接标识的；

(二)修改交易规则未在首页显著位置公开征求意见，未按照规定的时间提前公示修改内容，或者阻止平台内经营者退出的；

(三)未以显著方式区分标记自营业务和平台内经营者开展的业务的；

(四)未为消费者提供对平台内销售的商品或者提供的服务进行评价的途径，或者擅自删除消费者的评价的。

电子商务平台经营者违反本法第四十条规定，对竞价排名的商品或者服务未显著标明“广告”的，依照《中华人民共和国广告法》的规定处罚。

第八十二条 电子商务平台经营者违反本法第三十五条规定，对平台内经营者在平台内的交易、交易价格或者与其他经营者的交易等进行不合理限制或者附加不合理条件，或者向平台内经营者收取不合理费用的，由市场监督管理部门责令限期改正，可以处五万元以上五十万元以下的罚款；情节严重的，处五十万元以上二百万元以下的罚款。

第八十三条 电子商务平台经营者违反本法第三十八条规定，对平台内经营者侵害消费者合法权益行为未采取必要措施，或者对平台内经营者未尽到资质资格审核义务，或者对消费者未尽到安全保障义务的，由市场监督管理部门责令限期改正，可以处五万元以上五十万元以下的罚款；情节严重的，责令停业整顿，并处五十万元以上二百万元以下的罚款。

第八十四条 电子商务平台经营者违反本法第四十二条、第四十五条规定，对平台内经营者实施侵犯知识产权行为未依法采取必要措施的，由有关知识产权行政部门责令限期改正；逾期不改正的，处五万元以上五十万元以下的罚款；情节严重的，处五十万元以上二百万元以下的罚款。

第八十五条 电子商务经营者违反本法规定，销售的商品或者提供的服务不符合保障人身、财产安全的要求， 实施虚假或者引人误解的商业宣传等不正当竞争行为，滥用市场支配地位，或者实施侵犯知识产权、侵害消费者权益等行为的，依照有关法律的规定处罚。

第八十六条 电子商务经营者有本法规定的违法行为的，依照有关法律、行政法规的规定记入信用档案，并予以公示。

第八十七条 依法负有电子商务监督管理职责的部门的工作人员，玩忽职守、滥用职权、徇私舞弊， 或者泄露、出售或者非法向他人提供在履行职责中所知悉的个人信息、隐私和商业秘密的，依法追究法律责任。

第八十八条 违反本法规定，构成违反治安管理行为的，依法给予治安管理处罚；构成犯罪的，依法追究刑事责任。

第七章 附 则

第八十九条 本法自 2019 年 1 月 1 日起施行。

中华人民共和国密码法

中华人民共和国主席令第三十五号

《中华人民共和国密码法》已由中华人民共和国第十三届全国人民代表大会常务委员会第十四次会议于 2019 年 10 月 26 日通过，现予公布，自 2020 年 1 月 1 日起施行。

中华人民共和国主席 习近平

2019 年 10 月 26 日

中华人民共和国密码法

(2019 年 10 月 26 日第十三届全国人民代表大会常务委员会第十四次会议通过)

第一条 为了规范密码应用和管理，促进密码事业发展，保障网络与信息安全，维护国家安全和社会公共利益，保护公民、法人和其他组织的合法权益， 制定本法。

第二条 本法所称密码，是指采用特定变换的方法对信息等进行加密保护、安全认证的技术、产品和服务。

第三条 密码工作坚持总体国家安全观，遵循统一领导、分级负责，创新发展、服务大局，依法管理、保障安全的原则。

第四条 坚持中国共产党对密码工作的领导。中央密码工作领导机构对全国密码工作实行统一领导，制定国家密码工作重大方针政策，统筹协调国家密码重大事项和重要工作，推进国家密码法治建设。

第五条 国家密码管理部门负责管理全国的密码工作。县级以上地方各级密码管理部门负责管理本行政区域的密码工作。

国家机关和涉及密码工作的单位在其职责范围内负责本机关、本单位或者本系统的密码工作。

第六条 国家对密码实行分类管理。

密码分为核心密码、普通密码和商用密码。

第七条 核心密码、普通密码用于保护国家秘密信息，核心密码保护信息的最高密级为绝密级，普通密码保护信息的最高密级为机密级。

核心密码、普通密码属于国家秘密。密码管理部门依照本法和有关法律、行政法规、国家有关规定对核心密码、普通密码实行严格统一管理。

第八条 商用密码用于保护不属于国家秘密的信息。

公民、法人和其他组织可以依法使用商用密码保护网络与信息安全。

第九条 国家鼓励和支持密码科学技术研究和应用，依法保护密码领域的知识产权，促进密码科学技术进步和创新。

国家加强密码人才培养和队伍建设，对在密码工作中作出突出贡献的组织和个人，按照国家有关规定给予表彰和奖励。

第十条 国家采取多种形式加强密码安全教育，将密码安全教育纳入国民教育体系和公务员教育培训体系，增强公民、法人和其他组织的密码安全意识。

第十一条 县级以上人民政府应当将密码工作纳入本级国民经济和社会发展规划，所需经费列入本级财政预算。

第十二条 任何组织或者个人不得窃取他人加密保护的信息或者非法侵入他人的密码保障系统。

任何组织或者个人不得利用密码从事危害国家安全、社会公共利益、他人合法权益等违法犯罪活动。

第二章 核心密码、普通密码

第十三条 国家加强核心密码、普通密码的科学规划、管理和使用，加强制度建设，完善管理措施，增强密码安全保障能力。

第十四条 在有线、无线通信中传递的国家秘密信息，以及存储、处理国家秘密信息的信息系统，应当依照法律、行政法规和国家有关规定使用核心密码、普通密码进行加密保护、安全认证。

第十五条 从事核心密码、普通密码科研、生产、服务、检测、装备、使用和销毁等工作的机构(以下统称密码工作机构)应当按照法律、行政法规、国家有关规定以及核心密码、普通密码标准的要求， 建立健全安全管理制度，采取严格的保密措施和保密责任制，确保核心密码、普通密码的安全。

第十六条 密码管理部门依法对密码工作机构的核心密码、普通密码工作进行指导、监督和检查，密码工作机构应当配合。

第十七条 密码管理部门根据工作需要会同有关部门建立核心密码、普通密码的安全监测预警、安全风险评估、信息通报、重大事项会商和应急处置等协作机制，确保核心密码、普通密码安全管理的协同联动和有序高效。

密码工作机构发现核心密码、普通密码泄密或者影响核心密码、普通密码安全的重大问题、风险隐患的， 应当立即采取应对措施，并及时向保密行政管理部

门、密码管理部门报告， 由保密行政管理部门、密码管理部门会同有关部门组织开展调查、处置，并指导有关密码工作机构及时消除安全隐患。

第十八条 国家加强密码工作机构建设，保障其履行工作职责。

国家建立适应核心密码、普通密码工作需要的人员录用、选调、保密、考核、培训、待遇、奖惩、交流、退出等管理制度。

第十九条 密码管理部门因工作需要，按照国家有关规定，可以提请公安、交通运输、海关等部门对核心密码、普通密码有关物品和人员提供免检等便利，有关部门应当予以协助。

第二十条 密码管理部门和密码工作机构应当建立健全严格的监督和安全审查制度，对其工作人员遵守法律和纪律等情况进行监督，并依法采取必要措施，定期或者不定期组织开展安全审查。

第三章 商用密码

第二十一条 国家鼓励商用密码技术的研究开发、学术交流、成果转化和推广应用，健全统一、开放、竞争、有序的商用密码市场体系， 鼓励和促进商用密码产业发展。

各级人民政府及其有关部门应当遵循非歧视原则，依法平等对待包括外商投资企业在内的商用密码科研、生产、销售、服务、进出口等单位(以下统称商用密码从业单位)。国家鼓励在外商投资过程中基于自愿原则和商业规则开展商用密码技术合作。行政机关及其工作人员不得利用行政手段强制转让商用密码技术。

商用密码的科研、生产、销售、服务和进出口， 不得损害国家安全、社会公共利益或者他人合法权益。

第二十二条 国家建立和完善商用密码标准体系。

国务院标准化行政主管部门和国家密码管理部门依据各自职责，组织制定商用密码国家标准、行业标准。

国家支持社会团体、企业利用自主创新技术制定高于国家标准、行业标准相关技术要求的商用密码团体标准、企业标准。

第二十三条 国家推动参与商用密码国际标准化活动，参与制定商用密码国际标准，推进商用密码中国标准与国外标准之间的转化运用。

国家鼓励企业、社会团体和教育、科研机构等参与商用密码国际标准化活动。

第二十四条 商用密码从业单位开展商用密码活动，应当符合有关法律、行政法规、商用密码强制性国家标准以及该从业单位公开标准的技术要求。

国家鼓励商 用密码从业单位采用商用密码推荐性国家标准、行业标准，提升商用密码的防护能力，维护用户的合法权益。

第二十五条 国家推进商用密码检测认证体系建设，制定商用密码检测认证技术规范、规则， 鼓励商用密码从业单位自愿接受商用密码检测认证，提升市场竞争力。

商用密码检测、认证机构应当依法取得相关资质， 并依照法律、行政法规的规定和商用密码检测认证技术规范、规则开展商用密码检测认证。

商用密码检测、认证机构应当对其在商用密码检测认证中所知悉的国家秘密和商业秘密承担保密义务。

第二十六条 涉及国家安全、国计民生、社会公共利益的商用密码产品，应当依法列入网络关键设备和网络安全专用产品目录，由具备资格的机构检测认证合格后，方可销售或者提供。商用密码产品检测认证适用《中华人民共和国网络安全法》的有关规定，避免重复检测认证。

商用密码服务使用网络关键设备和网络安全专用产品的，应当经商用密码认证机构对该商用密码服务认证合格。

第二十七条 法律、行政法规和国家有关规定要求使用商用密码进行保护的关键信息基础设施，其运营者应当使用商用密码进行保护，自行或者委托商用密码检测机构开展商用密码应用安全性评估。商用密码应用安全性评估应当与关键信息基础设施安全检测评估、网络安全等级测评制度相衔接， 避免重复评估、测评。

关键信息基础设施的运营者采购涉及商用密码的网络产品和服务，可能影响国家安全的，应当按照《中华人民共和国网络安全法》的规定， 通过国家网信部门会同国家密码管理部门等有关部门组织的国家安全审查。

第二十八条 国务院商务主管部门、国家密码管理部门依法对涉及国家安全、社会公共利益且具有加密保护功能的商用密码实施进口许可，对涉及国家安全、社会公共利益或者中国承担国际义务的商用密码实施出口管制。商用密码进口许可清单和出口管制清单由国务院商务主管部门会同国家密码管理部门和海关总

署制定并公布。

大众消费类产品所采用的商用密码不实行进口许可和出口管制制度。

第二十九条 国家密码管理部门对采用商用密码技术从事电子政务电子认证服务的机构进行认定，会同有关部门负责政务活动中使用电子签名、数据电文的管理。

第三十条 商用密码领域的行业协会等组织依照法律、行政法规及其章程的规定，为商用密码从业单位提供信息、技术、培训等服务， 引导和督促商用密码从业单位依法开展商用密码活动，加强行业自律，推动行业诚信建设，促进行业健康发展。

第三十一条 密码管理部门和有关部门建立日常监管和随机抽查相结合的商用密码事中事后监管制度，建立统一的商用密码监督管理信息平台，推进事中事后监管与社会信用体系相衔接，强化商用密码从业单位自律和社会监督。

密码管理部门和有关部门及其工作人员不得要求商用密码从业单位和商用密码检测、认证机构向其披露源代码等密码相关专有信息， 并对其在履行职责中知悉的商业秘密和个人隐私严格保密，不得泄露或者非法向他人提供。

第四章 法律责任

第三十二条 违反本法第十二条规定，窃取他人加密保护的信息，非法侵入他人的密码保障系统，或者利用密码从事危害国家安全、社会公共利益、他人合法权益等违法活动的，由有关部门依照《中华人民共和国网络安全法》和其他有关法律、行政法规的规定追究法律责任。

第三十三条 违反本法第十四条规定，未按照要求使用核心密码、普通密码的，由密码管理部门责令改正或者停止违法行为，给予警告；情节严重的，由密码管理部门建议有关国家机关、单位对直接负责的主管人员和其他直接责任人员依法给予处分或者处理。

第三十四条 违反本法规定，发生核心密码、普通密码泄密案件的， 由保密行政管理部门、密码管理部门建议有关国家机关、单位对直接负责的主管人员和其他直接责任人员依法给予处分或者处理。

违反本法第十七条第二款规定，发现核心密码、普通密码泄密或者影响核心密码、普通密码安全的重大问题、风险隐患， 未立即采取应对措施，或者未及时

报告的，由保密行政管理部门、密码管理部门建议有关国家机关、单位对直接负责的主管人员和其他直接责任人员依法给予处分或者处理。

第三十五条 商用密码检测、认证机构违反本法第二十五条第二款、第三款规定开展商用密码检测认证的，由市场监督管理部门会同密码管理部门责令改正或者停止违法行为，给予警告，没收违法所得；违法所得三十万元以上的，可以并处违法所得一倍以上三倍以下罚款；没有违法所得或者违法所得不足三十万元的，可以并处十万元以上三十万元以下罚款；情节严重的，依法吊销相关资质。

第三十六条 违反本法第二十六条规定，销售或者提供未经检测认证或者检测认证不合格的商用密码产品，或者提供未经认证或者认证不合格的商用密码服务的，由市场监督管理部门会同密码管理部门责令改正或者停止违法行为，给予警告，没收违法产品和违法所得；违法所得十万元以上的，可以并处违法所得一倍以上三倍以下罚款；没有违法所得或者违法所得不足十万元的，可以并处三万元以上十万元以下罚款。

第三十七条 关键信息基础设施的运营者违反本法第二十七条第一款规定，未按照要求使用商用密码，或者未按照要求开展商用密码应用安全性评估的，由密码管理部门责令改正，给予警告；拒不改正或者导致危害网络安全等后果的，处十万元以上一百万元以下罚款，对直接负责的主管人员处一万元以上十万元以下罚款。

关键信息基础设施的运营者违反本法第二十七条第二款规定，使用未经安全审查或者安全审查未通过的产品或者服务的，由有关主管部门责令停止使用，处采购金额一倍以上十倍以下罚款；对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。

第三十八条 违反本法第二十八条实施进口许可、出口管制的规定，进出口商用密码的，由国务院商务主管部门或者海关依法予以处罚。

第三十九条 违反本法第二十九条规定，未经认定从事电子政务电子认证服务的，由密码管理部门责令改正或者停止违法行为，给予警告，没收违法产品和违法所得；违法所得三十万元以上的，可以并处违法所得一倍以上三倍以下罚款；没有违法所得或者违法所得不足三十万元的，可以并处十万元以上三十万元以下罚款。

第四十条 密码管理部门和有关部门、单位的工作人员在密码工作中滥用职权、玩忽职守、徇私舞弊， 或者泄露、非法向他人提供在履行职责中知悉的商业秘密和个人隐私的，依法给予处分。

第四十一条 违反本法规定，构成犯罪的，依法追究刑事责任；给他人造成损害的，依法承担民事责任。

第五章 附 则

第四十二条 国家密码管理部门依照法律、行政法规的规定，制定密码管理规章。

第四十三条 中国人民解放军和中国人民武装警察部队的密码工作管理办法，由中央军事委员会根据本法制定。

第四十四条 本法自 2020 年 1 月 1 日起施行。

中华人民共和国基本医疗卫生与健康促进法

中华人民共和国主席令第三十八号

《中华人民共和国基本医疗卫生与健康促进法》已由中华人民共和国第十三届全国人民代表大会常务委员会第十五次会议于 2019 年 12 月 28 日通过，现予公布，自 2020 年 6 月 1 日起施行。

中华人民共和国主席 习 近 平

2019 年 12 月 28 日

中华人民共和国基本医疗卫生与健康促进法

(2019 年 12 月 28 日第十三届全国人民代表大会常务委员会第十五次会议通过)

第一章 总 则

第一条 为了发展医疗卫生与健康事业，保障公民享有基本医疗卫生服务，提高公民健康水平，推进健康中国建设，根据宪法，制定本法。

第二条 从事医疗卫生、健康促进及其监督管理活动，适用本法。

第三条 医疗卫生与健康事业应当坚持以人民为中心，为人民健康服务。

医疗卫生事业应当坚持公益性原则。

第四条 国家和社会尊重、保护公民的健康权。

国家实施健康中国战略，普及健康生活，优化健康服务，完善健康保障，建设健康环境，发展健康产业，提升公民全生命周期健康水平。

国家建立健康教育制度，保障公民获得健康教育的权利，提高公民的健康素养。

第五条 公民依法享有从国家和社会获得基本医疗卫生服务的权利。

国家建立基本医疗卫生制度，建立健全医疗卫生服务体系，保护和实现公民获得基本医疗卫生服务的权利。

第六条 各级人民政府应当把人民健康放在优先发展的战略地位，将健康理念融入各项政策，坚持预防为主，完善健康促进工作体系，组织实施健康促进的规划和行动，推进全民健身，建立健康影响评估制度，将公民主要健康指标改善情况纳入政府目标责任考核。

全社会应当共同关心和支持医疗卫生与健康事业的发展。

第七条 国务院和地方各级人民政府领导医疗卫生与健康促进工作。

国务院卫生健康主管部门负责统筹协调全国医疗卫生与健康促进工作。国务院其他有关部门在各自职责范围内负责有关的医疗卫生与健康促进工作。

县级以上地方人民政府卫生健康主管部门负责统筹协调本行政区域医疗卫生与健康促进工作。县级以上地方人民政府其他有关部门在各自职责范围内负责有关的医疗卫生与健康促进工作。

第八条 国家加强医学基础科学研究，鼓励医学科学技术创新，支持临床医学发展，促进医学科技成果的转化和应用，推进医疗卫生与信息技术融合发展，推广医疗卫生适宜技术，提高医疗卫生服务质量。

国家发展医学教育，完善适应医疗卫生事业发展需要的医学教育体系，大力培养医疗卫生人才。

第九条 国家大力发展中医药事业，坚持中西医并重、传承与创新相结合，发挥中医药在医疗卫生与健康事业中的独特作用。

第十条 国家合理规划和配置医疗卫生资源，以基层为重点，采取多种措施优先支持县级以下医疗卫生机构发展，提高其医疗卫生服务能力。

第十一条 国家加大对医疗卫生与健康事业的财政投入，通过增加转移支付等方式重点扶持革命老区、民族地区、边疆地区和经济欠发达地区发展医疗卫生与健康事业。

第十二条 国家鼓励和支持公民、法人和其他组织通过依法举办机构和捐赠、

资助等方式，参与医疗卫生与健康事业，满足公民多样化、差异化、个性化健康需求。

公民、法人和其他组织捐赠财产用于医疗卫生与健康事业的， 依法享受税收优惠。

第十三条 对在医疗卫生与健康事业中做出突出贡献的组织和个人，按照国家规定给予表彰、奖励。

第十四条 国家鼓励和支持医疗卫生与健康促进领域的对外交流合作。

开展医疗卫生与健康促进对外交流合作活动，应当遵守法律、法规， 维护国家主权、安全和社会公共利益。

第二章 基本医疗卫生服务

第十五条 基本医疗卫生服务，是指维护人体健康所必需、与经济社会发展水平相适应、公民可公平获得的， 采用适宜药物、适宜技术、适宜设备提供的疾病预防、诊断、治疗、护理和康复等服务。

基本医疗卫生服务包括基本公共卫生服务和基本医疗服务。基本公共卫生服务由国家免费提供。

第十六条 国家采取措施，保障公民享有安全有效的基本公共卫生服务，控制影响健康的危险因素，提高疾病的预防控制水平。

国家基本公共卫生服务项目由国务院卫生健康主管部门会同国务院财政部门、中医药主管部门等共同确定。

省、自治区、直辖市人民政府可以在国家基本公共卫生服务项目基础上， 补充确定本行政区域的基本公共卫生服务项目，并报国务院卫生健康主管部门备案。

第十七条 国务院和省、自治区、直辖市人民政府可以将针对重点地区、重点疾病和特定人群的服务内容纳入基本公共卫生服务项目并组织实施。

县级以上地方人民政府针对本行政区域重大疾病和主要健康危险因素，开展专项防控工作。

第十八条 县级以上人民政府通过举办专业公共卫生机构、基层医疗卫生机构和医院，或者从其他医疗卫生机构购买服务的方式提供基本公共卫生服务。

第十九条 国家建立健全突发事件卫生应急体系，制定和完善应急预案，组织开展突发事件的医疗救治、卫生学调查处置和心理援助等卫生应急工作， 有效

控制和消除危害。

第二十条　国家建立传染病防控制度，制定传染病防治规划并组织实施，加强传染病监测预警，坚持预防为主、防治结合，联防联控、群防群控、源头防控、综合治理，阻断传播途径，保护易感人群，降低传染病的危害。

任何组织和个人应当接受、配合医疗卫生机构为预防、控制、消除传染病危害依法采取的调查、检验、采集样本、隔离治疗、医学观察等措施。

第二十一条　国家实行预防接种制度，加强免疫规划工作。居民有依法接种免疫规划疫苗的权利和义务。政府向居民免费提供免疫规划疫苗。

第二十二条　国家建立慢性非传染性疾病防控与管理制度，对慢性非传染性疾病及其致病危险因素开展监测、调查和综合防控干预， 及时发现高危人群，为患者和高危人群提供诊疗、早期干预、随访管理和健康教育等服务。

第二十三条　国家加强职业健康保护。县级以上人民政府应当制定职业病防治规划，建立健全职业健康工作机制，加强职业健康监督管理，提高职业病综合防治能力和水平。

用人单位应当控制职业病危害因素，采取工程技术、个体防护和健康管理等综合治理措施，改善工作环境和劳动条件。

第二十四条　国家发展妇幼保健事业，建立健全妇幼健康服务体系，为妇女、儿童提供保健及常见病防治服务，保障妇女、儿童健康。

国家采取措施，为公民提供婚前保健、孕产期保健等服务，促进生殖健康，预防出生缺陷。

第二十五条　国家发展老年人保健事业。国务院和省、自治区、直辖市人民政府应当将老年人健康管理和常见病预防等纳入基本公共卫生服务项目。

第二十六条　国家发展残疾预防和残疾人康复事业，完善残疾预防和残疾人康复及其保障体系，采取措施为残疾人提供基本康复服务。

县级以上人民政府应当优先开展残疾儿童康复工作，实行康复与教育相结合。

第二十七条　国家建立健全院前急救体系，为急危重症患者提供及时、规范、有效的急救服务。

卫生健康主管部门、红十字会等有关部门、组织应当积极开展急救培训， 普及急救知识，鼓励医疗卫生人员、经过急救培训的人员积极参与公共场所急救服

务。公共场所应当按照规定配备必要的急救设备、设施。

急救中心(站)不得以未付费为由拒绝或者拖延为急危重症患者提供急救服务。

第二十八条 国家发展精神卫生事业，建设完善精神卫生服务体系，维护和增进公民心理健康，预防、治疗精神障碍。

国家采取措施，加强心理健康服务体系和人才队伍建设，促进心理健康教育、心理评估、心理咨询与心理治疗服务的有效衔接， 设立为公众提供公益服务的心理援助热线，加强未成年人、残疾人和老年人等重点人群心理健康服务。

第二十九条 基本医疗服务主要由政府举办的医疗卫生机构提供。鼓励社会力量举办的医疗卫生机构提供基本医疗服务。

第三十条 国家推进基本医疗服务实行分级诊疗制度，引导非急诊患者首先到基层医疗卫生机构就诊，实行首诊负责制和转诊审核责任制，逐步建立基层首诊、双向转诊、急慢分治、上下联动的机制，并与基本医疗保险制度相衔接。

县级以上地方人民政府根据本行政区域医疗卫生需求，整合区域内政府举办的医疗卫生资源，因地制宜建立医疗联合体等协同联动的医疗服务合作机制。鼓励社会力量举办的医疗卫生机构参与医疗服务合作机制。

第三十一条 国家推进基层医疗卫生机构实行家庭医生签约服务，建立家庭医生服务团队，与居民签订协议，根据居民健康状况和医疗需求提供基本医疗卫生服务。

第三十二条 公民接受医疗卫生服务，对病情、诊疗方案、医疗风险、医疗费用等事项依法享有知情同意的权利。

需要实施手术、特殊检查、特殊治疗的， 医疗卫生人员应当及时向患者说明医疗风险、替代医疗方案等情况，并取得其同意；不能或者不宜向患者说明的，应当向患者的近亲属说明，并取得其同意。法律另有规定的，依照其规定。

开展药物、医疗器械临床试验和其他医学研究应当遵守医学伦理规范， 依法通过伦理审查，取得知情同意。

第三十三条 公民接受医疗卫生服务，应当受到尊重。医疗卫生机构、医疗卫生人员应当关心爱护、平等对待患者，尊重患者人格尊严，保护患者隐私。

公民接受医疗卫生服务，应当遵守诊疗制度和医疗卫生服务秩序，尊重医疗

卫生人员。

第三章 医疗卫生机构

第三十四条 国家建立健全由基层医疗卫生机构、医院、专业公共卫生机构等组成的城乡全覆盖、功能互补、连续协同的医疗卫生服务体系。

国家加强县级医院、乡镇卫生院、村卫生室、社区卫生服务中心(站)和专业公共卫生机构等的建设，建立健全农村医疗卫生服务网络和城市社区卫生服务网络。

第三十五条 基层医疗卫生机构主要提供预防、保健、健康教育、疾病管理，为居民建立健康档案，常见病、多发病的诊疗以及部分疾病的康复、护理， 接收医院转诊患者，向医院转诊超出自身服务能力的患者等基本医疗卫生服务。

医院主要提供疾病诊治，特别是急危重症和疑难病症的诊疗，突发事件医疗处置和救援以及健康教育等医疗卫生服务，并开展医学教育、医疗卫生人员培训、医学科学研究和对基层医疗卫生机构的业务指导等工作。

专业公共卫生机构主要提供传染病、慢性非传染性疾病、职业病、地方病等疾病预防控制和健康教育、妇幼保健、精神卫生、院前急救、采供血、食品安全风险监测评估、出生缺陷防治等公共卫生服务。

第三十六条 各级各类医疗卫生机构应当分工合作，为公民提供预防、保健、治疗、护理、康复、安宁疗护等全方位全周期的医疗卫生服务。

各级人民政府采取措施支持医疗卫生机构与养老机构、儿童福利机构、社区组织建立协作机制，为老年人、孤残儿童提供安全、便捷的医疗和健康服务。

第三十七条 县级以上人民政府应当制定并落实医疗卫生服务体系规划，科学配置医疗卫生资源，举办医疗卫生机构，为公民获得基本医疗卫生服务提供保障。

政府举办医疗卫生机构，应当考虑本行政区域人口、经济社会发展状况、医疗卫生资源、健康危险因素、发病率、患病率以及紧急救治需求等情况。

第三十八条 举办医疗机构，应当具备下列条件，按照国家有关规定办理审批或者备案手续：

(一)有符合规定的名称、组织机构和场所；

(二)有与其开展的业务相适应的经费、设施、设备和医疗卫生人员；

(三)有相应的规章制度;

(四)能够独立承担民事责任;

(五)法律、行政法规规定的其他条件。

医疗机构依法取得执业许可证。禁止伪造、变造、买卖、出租、出借医疗机构执业许可证。

各级各类医疗卫生机构的具体条件和配置应当符合国务院卫生健康主管部门制定的医疗卫生机构标准。

第三十九条 国家对医疗卫生机构实行分类管理。

医疗卫生服务体系坚持以非营利性医疗卫生机构为主体、营利性医疗卫生机构为补充。政府举办非营利性医疗卫生机构， 在基本医疗卫生事业中发挥主导作用，保障基本医疗卫生服务公平可及。

以政府资金、捐赠资产举办或者参与举办的医疗卫生机构不得设立为营利性医疗卫生机构。

医疗卫生机构不得对外出租、承包医疗科室。非营利性医疗卫生机构不得向出资人、举办者分配或者变相分配收益。

第四十条 政府举办的医疗卫生机构应当坚持公益性质，所有收支均纳入预算管理，按照医疗卫生服务体系规划合理设置并控制规模。

国家鼓励政府举办的医疗卫生机构与社会力量合作举办非营利性医疗卫生机构。

政府举办的医疗卫生机构不得与其他组织投资设立非独立法人资格的医疗卫生机构，不得与社会资本合作举办营利性医疗卫生机构。

第四十一条 国家采取多种措施，鼓励和引导社会力量依法举办医疗卫生机构，支持和规范社会力量举办的医疗卫生机构与政府举办的医疗卫生机构开展多种类型的医疗业务、学科建设、人才培养等合作。

社会力量举办的医疗卫生机构在基本医疗保险定点、重点专科建设、科研教学、等级评审、特定医疗技术准入、医疗卫生人员职称评定等方面享有与政府举办的医疗卫生机构同等的权利。

社会力量可以选择设立非营利性或者营利性医疗卫生机构。社会力量举办的非营利性医疗卫生机构按照规定享受与政府举办的医疗卫生机构同等的税收、财

政补助、用地、用水、用电、用气、用热等政策，并依法接受监督管理。

第四十二条 国家以建成的医疗卫生机构为基础，合理规划与设置国家医学中心和国家、省级区域性医疗中心， 诊治疑难重症，研究攻克重大医学难题，培养高层次医疗卫生人才。

第四十三条 医疗卫生机构应当遵守法律、法规、规章，建立健全内部质量管理和控制制度，对医疗卫生服务质量负责。

医疗卫生机构应当按照临床诊疗指南、临床技术操作规范和行业标准以及医学伦理规范等有关要求，合理进行检查、用药、诊疗， 加强医疗卫生安全风险防范，优化服务流程，持续改进医疗卫生服务质量。

第四十四条 国家对医疗卫生技术的临床应用进行分类管理，对技术难度大、医疗风险高，服务能力、人员专业技术水平要求较高的医疗卫生技术实行严格管理。

医疗卫生机构开展医疗卫生技术临床应用，应当与其功能任务相适应，遵循科学、安全、规范、有效、经济的原则，并符合伦理。

第四十五条 国家建立权责清晰、管理科学、治理完善、运行高效、监督有力的现代医院管理制度。

医院应当制定章程，建立和完善法人治理结构，提高医疗卫生服务能力和运行效率。

第四十六条 医疗卫生机构执业场所是提供医疗卫生服务的公共场所，任何组织或者个人不得扰乱其秩序。

第四十七条 国家完善医疗风险分担机制，鼓励医疗机构参加医疗责任保险或者建立医疗风险基金，鼓励患者参加医疗意外保险。

第四十八条 国家鼓励医疗卫生机构不断改进预防、保健、诊断、治疗、护理和康复的技术、设备与服务， 支持开发适合基层和边远地区应用的医疗卫生技术。

第四十九条 国家推进全民健康信息化，推动健康医疗大数据、人工智能等的应用发展，加快医疗卫生信息基础设施建设，制定健康医疗数据采集、存储、分析和应用的技术标准，运用信息技术促进优质医疗卫生资源的普及与共享。

县级以上人民政府及其有关部门应当采取措施，推进信息技术在医疗卫生领

域和医学教育中的应用，支持探索发展医疗卫生服务新模式、新业态。

国家采取措施，推进医疗卫生机构建立健全医疗卫生信息交流和信息安全制度，应用信息技术开展远程医疗服务，构建线上线下一体化医疗服务模式。

第五十条 发生自然灾害、事故灾难、公共卫生事件和社会安全事件等严重威胁人民群众生命健康的突发事件时，医疗卫生机构、医疗卫生人员应当服从政府部门的调遣，参与卫生应急处置和医疗救治。对致病、致残、死亡的参与人员，按照规定给予工伤或者抚恤、烈士褒扬等相关待遇。

第四章 医疗卫生人员

第五十一条 医疗卫生人员应当弘扬敬佑生命、救死扶伤、甘于奉献、大爱无疆的崇高职业精神，遵守行业规范，恪守医德，努力提高专业水平和服务质量。

医疗卫生行业组织、医疗卫生机构、医学院校应当加强对医疗卫生人员的医德医风教育。

第五十二条 国家制定医疗卫生人员培养规划，建立适应行业特点和社会需求的医疗卫生人员培养机制和供需平衡机制，完善医学院校教育、毕业后教育和继续教育体系，建立健全住院医师、专科医师规范化培训制度，建立规模适宜、结构合理、分布均衡的医疗卫生队伍。

国家加强全科医生的培养和使用。全科医生主要提供常见病、多发病的诊疗和转诊、预防、保健、康复，以及慢性病管理、健康管理等服务。

第五十三条 国家对医师、护士等医疗卫生人员依法实行执业注册制度。医疗卫生人员应当依法取得相应的职业资格。

第五十四条 医疗卫生人员应当遵循医学科学规律，遵守有关临床诊疗技术规范和各项操作规范以及医学伦理规范，使用适宜技术和药物，合理诊疗，因病施治，不得对患者实施过度医疗。

医疗卫生人员不得利用职务之便索要、非法收受财物或者牟取其他不正当利益。

第五十五条 国家建立健全符合医疗卫生行业特点的人事、薪酬、奖励制度，体现医疗卫生人员职业特点和技术劳动价值。

对从事传染病防治、放射医学和精神卫生工作以及其他在特殊岗位工作的医疗卫生人员，应当按照国家规定给予适当的津贴。津贴标准应当定期调整。

第五十六条 国家建立医疗卫生人员定期到基层和艰苦边远地区从事医疗卫生工作制度。

国家采取定向免费培养、对口支援、退休返聘等措施， 加强基层和艰苦边远地区医疗卫生队伍建设。

执业医师晋升为副高级技术职称的，应当有累计一年以上在县级以下或者对口支援的医疗卫生机构提供医疗卫生服务的经历。

对在基层和艰苦边远地区工作的医疗卫生人员，在薪酬津贴、职称评定、职业发展、教育培训和表彰奖励等方面实行优惠待遇。

国家加强乡村医疗卫生队伍建设，建立县乡村上下贯通的职业发展机制，完善对乡村医疗卫生人员的服务收入多渠道补助机制和养老政策。

第五十七条 全社会应当关心、尊重医疗卫生人员，维护良好安全的医疗卫生服务秩序，共同构建和谐医患关系。

医疗卫生人员的人身安全、人格尊严不受侵犯， 其合法权益受法律保护。禁止任何组织或者个人威胁、危害医疗卫生人员人身安全， 侵犯医疗卫生人员人格尊严。

国家采取措施，保障医疗卫生人员执业环境。

第五章 药品供应保障

第五十八条 国家完善药品供应保障制度，建立工作协调机制，保障药品的安全、有效、可及。

第五十九条 国家实施基本药物制度，遴选适当数量的基本药物品种，满足疾病防治基本用药需求。

国家公布基本药物目录，根据药品临床应用实践、药品标准变化、药品新上市情况等，对基本药物目录进行动态调整。

基本药物按照规定优先纳入基本医疗保险药品目录。

国家提高基本药物的供给能力，强化基本药物质量监管，确保基本药物公平可及、合理使用。

第六十条 国家建立健全以临床需求为导向的药品审评审批制度，支持临床急需药品、儿童用药品和防治罕见病、重大疾病等药品的研制、生产， 满足疾病防治需求。

第六十一条 国家建立健全药品研制、生产、流通、使用全过程追溯制度，加强药品管理，保证药品质量。

第六十二条 国家建立健全药品价格监测体系，开展成本价格调查，加强药品价格监督检查，依法查处价格垄断、价格欺诈、不正当竞争等违法行为， 维护药品价格秩序。

国家加强药品分类采购管理和指导。参加药品采购投标的投标人不得以低于成本的报价竞标，不得以欺诈、串通投标、滥用市场支配地位等方式竞标。

第六十三条 国家建立中央与地方两级医药储备，用于保障重大灾情、疫情及其他突发事件等应急需要。

第六十四条 国家建立健全药品供求监测体系，及时收集和汇总分析药品供求信息，定期公布药品生产、流通、使用等情况。

第六十五条 国家加强对医疗器械的管理，完善医疗器械的标准和规范，提高医疗器械的安全有效水平。

国务院卫生健康主管部门和省、自治区、直辖市人民政府卫生健康主管部门应当根据技术的先进性、适宜性和可及性， 编制大型医用设备配置规划，促进区域内医用设备合理配置、充分共享。

第六十六条 国家加强中药的保护与发展，充分体现中药的特色和优势，发挥其在预防、保健、医疗、康复中的作用。

第六章 健 康 促 进

第六十七条 各级人民政府应当加强健康教育工作及其专业人才培养，建立健康知识和技能核心信息发布制度，普及健康科学知识，向公众提供科学、准确的健康信息。

医疗卫生、教育、体育、宣传等机构、基层群众性自治组织和社会组织应当开展健康知识的宣传和普及。医疗卫生人员在提供医疗卫生服务时， 应当对患者开展健康教育。新闻媒体应当开展健康知识的公益宣传。健康知识的宣传应当科学、准确。

第六十八条 国家将健康教育纳入国民教育体系。学校应当利用多种形式实施健康教育，普及健康知识、科学健身知识、急救知识和技能， 提高学生主动防病的意识，培养学生良好的卫生习惯和健康的行为习惯，减少、改善学生近视、

肥胖等不良健康状况。

学校应当按照规定开设体育与健康课程，组织学生开展广播体操、眼保健操、体能锻炼等活动。

学校按照规定配备校医，建立和完善卫生室、保健室等。

县级以上人民政府教育主管部门应当按照规定将学生体质健康水平纳入学校考核体系。

第六十九条 公民是自己健康的第一责任人，树立和践行对自己健康负责的健康管理理念，主动学习健康知识，提高健康素养，加强健康管理。倡导家庭成员相互关爱，形成符合自身和家庭特点的健康生活方式。

公民应当尊重他人的健康权利和利益，不得损害他人健康和社会公共利益。

第七十条 国家组织居民健康状况调查和统计，开展体质监测，对健康绩效进行评估，并根据评估结果制定、完善与健康相关的法律、法规、政策和规划。

第七十一条 国家建立疾病和健康危险因素监测、调查和风险评估制度。县级以上人民政府及其有关部门针对影响健康的主要问题，组织开展健康危险因素研究，制定综合防治措施。

国家加强影响健康的环境问题预防和治理，组织开展环境质量对健康影响的研究，采取措施预防和控制与环境问题有关的疾病。

第七十二条 国家大力开展爱国卫生运动，鼓励和支持开展爱国卫生月等群众性卫生与健康活动，依靠和动员群众控制和消除健康危险因素，改善环境卫生状况，建设健康城市、健康村镇、健康社区。

第七十三条 国家建立科学、严格的食品、饮用水安全监督管理制度，提高安全水平。

第七十四条 国家建立营养状况监测制度，实施经济欠发达地区、重点人群营养干预计划，开展未成年人和老年人营养改善行动，倡导健康饮食习惯，减少不健康饮食引起的疾病风险。

第七十五条 国家发展全民健身事业，完善覆盖城乡的全民健身公共服务体系，加强公共体育设施建设，组织开展和支持全民健身活动，加强全民健身指导服务，普及科学健身知识和方法。

国家鼓励单位的体育场地设施向公众开放。

第七十六条 国家制定并实施未成年人、妇女、老年人、残疾人等的健康工作计划，加强重点人群健康服务。

国家推动长期护理保障工作，鼓励发展长期护理保险。

第七十七条 国家完善公共场所卫生管理制度。县级以上人民政府卫生健康等主管部门应当加强对公共场所的卫生监督。公共场所卫生监督信息应当依法向社会公开。

公共场所经营单位应当建立健全并严格实施卫生管理制度，保证其经营活动持续符合国家对公共场所的卫生要求。

第七十八条 国家采取措施，减少吸烟对公民健康的危害。

公共场所控制吸烟，强化监督执法。

烟草制品包装应当印制带有说明吸烟危害的警示。

禁止向未成年人出售烟酒。

第七十九条 用人单位应当为职工创造有益于健康的环境和条件，严格执行劳动安全卫生等相关规定，积极组织职工开展健身活动，保护职工健康。

国家鼓励用人单位开展职工健康指导工作。

国家提倡用人单位为职工定期开展健康检查。法律、法规对健康检查有规定的，依照其规定。

第七章 资 金 保 障

第八十条 各级人民政府应当切实履行发展医疗卫生与健康事业的职责，建立与经济社会发展、财政状况和健康指标相适应的医疗卫生与健康事业投入机制，将医疗卫生与健康促进经费纳入本级政府预算，按照规定主要用于保障基本医疗服务、公共卫生服务、基本医疗保障和政府举办的医疗卫生机构建设和运行发展。

第八十一条 县级以上人民政府通过预算、审计、监督执法、社会监督等方式，加强资金的监督管理。

第八十二条 基本医疗服务费用主要由基本医疗保险基金和个人支付。国家依法多渠道筹集基本医疗保险基金，逐步完善基本医疗保险可持续筹资和保障水平调整机制。

公民有依法参加基本医疗保险的权利和义务。用人单位和职工按照国家规定缴纳职工基本医疗保险费。城乡居民按照规定缴纳城乡居民基本医疗保险费。

第八十三条 国家建立以基本医疗保险为主体，商业健康保险、医疗救助、职工互助医疗和医疗慈善服务等为补充的、多层次的医疗保障体系。

国家鼓励发展商业健康保险，满足人民群众多样化健康保障需求。

国家完善医疗救助制度，保障符合条件的困难群众获得基本医疗服务。

第八十四条 国家建立健全基本医疗保险经办机构与协议定点医疗卫生机构之间的协商谈判机制，科学合理确定基本医疗保险基金支付标准和支付方式，引导医疗卫生机构合理诊疗，促进患者有序流动，提高基本医疗保险基金使用效益。

第八十五条 基本医疗保险基金支付范围由国务院医疗保障主管部门组织制定，并应当听取国务院卫生健康主管部门、中医药主管部门、药品监督管理部门、财政部门等的意见。

省、自治区、直辖市人民政府可以按照国家有关规定， 补充确定本行政区域基本医疗保险基金支付的具体项目和标准，并报国务院医疗保障主管部门备案。

国务院医疗保障主管部门应当对纳入支付范围的基本医疗保险药品目录、诊疗项目、医疗服务设施标准等组织开展循证医学和经济性评价， 并应当听取国务院卫生健康主管部门、中医药主管部门、药品监督管理部门、财政部门等有关方面的意见。评价结果应当作为调整基本医疗保险基金支付范围的依据。

第八章 监 督 管 理

第八十六条 国家建立健全机构自治、行业自律、政府监管、社会监督相结合的医疗卫生综合监督管理体系。

县级以上人民政府卫生健康主管部门对医疗卫生行业实行属地化、全行业监督管理。

第八十七条 县级以上人民政府医疗保障主管部门应当提高医疗保障监管能力和水平，对纳入基本医疗保险基金支付范围的医疗服务行为和医疗费用加强监督管理，确保基本医疗保险基金合理使用、安全可控。

第八十八条 县级以上人民政府应当组织卫生健康、医疗保障、药品监督管理、发展改革、财政等部门建立沟通协商机制， 加强制度衔接和工作配合，提高医疗卫生资源使用效率和保障水平。

第八十九条 县级以上人民政府应当定期向本级人民代表大会或者其常务委员会报告基本医疗卫生与健康促进工作，依法接受监督。

第九十条 县级以上人民政府有关部门未履行医疗卫生与健康促进工作相关职责的，本级人民政府或者上级人民政府有关部门应当对其主要负责人进行约谈。

地方人民政府未履行医疗卫生与健康促进工作相关职责的，上级人民政府应当对其主要负责人进行约谈。

被约谈的部门和地方人民政府应当立即采取措施，进行整改。

约谈情况和整改情况应当纳入有关部门和地方人民政府工作评议、考核记录。

第九十一条 县级以上地方人民政府卫生健康主管部门应当建立医疗卫生机构绩效评估制度，组织对医疗卫生机构的服务质量、医疗技术、药品和医用设备使用等情况进行评估。评估应当吸收行业组织和公众参与。评估结果应当以适当方式向社会公开，作为评价医疗卫生机构和卫生监管的重要依据。

第九十二条 国家保护公民个人健康信息，确保公民个人健康信息安全。任何组织或者个人不得非法收集、使用、加工、传输公民个人健康信息， 不得非法买卖、提供或者公开公民个人健康信息。

第九十三条 县级以上人民政府卫生健康主管部门、医疗保障主管部门应当建立医疗卫生机构、人员等信用记录制度， 纳入全国信用信息共享平台，按照国家规定实施联合惩戒。

第九十四条 县级以上地方人民政府卫生健康主管部门及其委托的卫生健康监督机构，依法开展本行政区域医疗卫生等行政执法工作。

第九十五条 县级以上人民政府卫生健康主管部门应当积极培育医疗卫生行业组织，发挥其在医疗卫生与健康促进工作中的作用，支持其参与行业管理规范、技术标准制定和医疗卫生评价、评估、评审等工作。

第九十六条 国家建立医疗纠纷预防和处理机制，妥善处理医疗纠纷，维护医疗秩序。

第九十七条 国家鼓励公民、法人和其他组织对医疗卫生与健康促进工作进行社会监督。

任何组织和个人对违反本法规定的行为，有权向县级以上人民政府卫生健康主管部门和其他有关部门投诉、举报。

第九章 法 律 责 任

第九十八条 违反本法规定，地方各级人民政府、县级以上人民政府卫生健

康主管部门和其他有关部门，滥用职权、玩忽职守、徇私舞弊的， 对直接负责的主管人员和其他直接责任人员依法给予处分。

第九十九条 违反本法规定，未取得医疗机构执业许可证擅自执业的，由县级以上人民政府卫生健康主管部门责令停止执业活动，没收违法所得和药品、医疗器械，并处违法所得五倍以上二十倍以下的罚款，违法所得不足一万元的，按一万元计算。

违反本法规定，伪造、变造、买卖、出租、出借医疗机构执业许可证的，由县级以上人民政府卫生健康主管部门责令改正，没收违法所得，并处违法所得五倍以上十五倍以下的罚款，违法所得不足一万元的，按一万元计算；情节严重的，吊销医疗机构执业许可证。

第一百条 违反本法规定，有下列行为之一的，由县级以上人民政府卫生健康主管部门责令改正，没收违法所得，并处违法所得二倍以上十倍以下的罚款，违法所得不足一万元的，按一万元计算；对直接负责的主管人员和其他直接责任人员依法给予处分：

(一)政府举办的医疗卫生机构与其他组织投资设立非独立法人资格的医疗卫生机构；

(二)医疗卫生机构对外出租、承包医疗科室；

(三)非营利性医疗卫生机构向出资人、举办者分配或者变相分配收益。

第一百零一条 违反本法规定，医疗卫生机构等的医疗信息安全制度、保障措施不健全，导致医疗信息泄露，或者医疗质量管理和医疗技术管理制度、安全措施不健全的， 由县级以上人民政府卫生健康等主管部门责令改正，给予警告，并处一万元以上五万元以下的罚款；情节严重的，可以责令停止相应执业活动，对直接负责的主管人员和其他直接责任人员依法追究法律责任。

第一百零二条 违反本法规定，医疗卫生人员有下列行为之一的，由县级以上人民政府卫生健康主管部门依照有关执业医师、护士管理和医疗纠纷预防处理等法律、行政法规的规定给予行政处罚：

(一)利用职务之便索要、非法收受财物或者牟取其他不正当利益；

(二)泄露公民个人健康信息；

(三)在开展医学研究或提供医疗卫生服务过程中未按照规定履行告知义务

或者违反医学伦理规范。

前款规定的人员属于政府举办的医疗卫生机构中的人员的，依法给予处分。

第一百零三条 违反本法规定，参加药品采购投标的投标人以低于成本的报价竞标，或者以欺诈、串通投标、滥用市场支配地位等方式竞标的， 由县级以上人民政府医疗保障主管部门责令改正，没收违法所得；中标的，中标无效，处中标项目金额千分之五以上千分之十以下的罚款，对法定代表人、主要负责人、直接负责的主管人员和其他责任人员处对单位罚款数额百分之五以上百分之十以下的罚款；情节严重的，取消其二年至五年内参加药品采购投标的资格并予以公告。

第一百零四条 违反本法规定，以欺诈、伪造证明材料或者其他手段骗取基本医疗保险待遇，或者基本医疗保险经办机构以及医疗机构、药品经营单位等以欺诈、伪造证明材料或者其他手段骗取基本医疗保险基金支出的， 由县级以上人民政府医疗保障主管部门依照有关社会保险的法律、行政法规规定给予行政处罚。

第一百零五条 违反本法规定，扰乱医疗卫生机构执业场所秩序，威胁、危害医疗卫生人员人身安全，侵犯医疗卫生人员人格尊严，非法收集、使用、加工、传输公民个人健康信息，非法买卖、提供或者公开公民个人健康信息等， 构成违反治安管理行为的，依法给予治安管理处罚。

第一百零六条 违反本法规定，构成犯罪的，依法追究刑事责任；造成人身、财产损害的，依法承担民事责任。

第十章 附 则

第一百零七条 本法中下列用语的含义：

(一)主要健康指标，是指人均预期寿命、孕产妇死亡率、婴儿死亡率、五岁以下儿童死亡率等。

(二)医疗卫生机构，是指基层医疗卫生机构、医院和专业公共卫生机构等。

(三)基层医疗卫生机构，是指乡镇卫生院、社区卫生服务中心(站)、村卫生室、医务室、门诊部和诊所等。

(四)专业公共卫生机构，是指疾病预防控制中心、专科疾病防治机构、健康教育机构、急救中心(站)和血站等。

(五)医疗卫生人员，是指执业医师、执业助理医师、注册护士、药师(士)、

检验技师(士)、影像技师(士)和乡村医生等卫生专业人员。

(六)基本药物，是指满足疾病防治基本用药需求，适应现阶段基本国情和保障能力，剂型适宜，价格合理，能够保障供应，可公平获得的药品。

第一百零八条 省、自治区、直辖市和设区的市、自治州可以结合实际，制定本地方发展医疗卫生与健康事业的具体办法。

第一百零九条 中国人民解放军和中国人民武装警察部队的医疗卫生与健康促进工作，由国务院和中央军事委员会依照本法制定管理办法。

第一百一十条 本法自 2020 年 6 月 1 日起施行。

中华人民共和国数据安全法

中华人民共和国主席令第八十四号

《中华人民共和国数据安全法》已由中华人民共和国第十三届全国人民代表大会常务委员会第二十九次会议于 2021 年 6 月 10 日通过，现予公布，自 2021 年 9 月 1 日起施行。

中华人民共和国主席 习近平

2021 年 6 月 10 日

中华人民共和国数据安全法

(2021 年 6 月 10 日第十三届全国人民代表大会常务委员会第二十九次会议通过)

第一章 总 则

第一条 为了规范数据处理活动，保障数据安全，促进数据开发利用，保护个人、组织的合法权益，维护国家主权、安全和发展利益，制定本法。

第二条 在中华人民共和国境内开展数据处理活动及其安全监管，适用本法。

在中华人民共和国境外开展数据处理活动，损害中华人民共和国国家安全、公共利益或者公民、组织合法权益的，依法追究法律责任。

第三条 本法所称数据，是指任何以电子或者其他方式对信息的记录。

数据处理，包括数据的收集、存储、使用、加工、传输、提供、公开等。

数据安全，是指通过采取必要措施，确保数据处于有效保护和合法利用的状态，以及具备保障持续安全状态的能力。

第四条 维护数据安全，应当坚持总体国家安全观，建立健全数据安全治理

体系，提高数据安全保障能力。

第五条 中央国家安全领导机构负责国家数据安全工作的决策和议事协调，研究制定、指导实施国家数据安全战略和有关重大方针政策， 统筹协调国家数据安全的重大事项和重要工作，建立国家数据安全工作协调机制。

第六条 各地区、各部门对本地区、本部门工作中收集和产生的数据及数据安全负责。

工业、电信、交通、金融、自然资源、卫生健康、教育、科技等主管部门承担本行业、本领域数据安全监管职责。

公安机关、国家安全机关等依照本法和有关法律、行政法规的规定， 在各自职责范围内承担数据安全监管职责。

国家网信部门依照本法和有关法律、行政法规的规定， 负责统筹协调网络数据安全和相关监管工作。

第七条 国家保护个人、组织与数据有关的权益，鼓励数据依法合理有效利用，保障数据依法有序自由流动，促进以数据为关键要素的数字经济发展。

第八条 开展数据处理活动，应当遵守法律、法规，尊重社会公德和伦理，遵守商业道德和职业道德，诚实守信，履行数据安全保护义务，承担社会责任，不得危害国家安全、公共利益，不得损害个人、组织的合法权益。

第九条 国家支持开展数据安全知识宣传普及，提高全社会的数据安全保护意识和水平，推动有关部门、行业组织、科研机构、企业、个人等共同参与数据安全保护工作，形成全社会共同维护数据安全和促进发展的良好环境。

第十条 相关行业组织按照章程，依法制定数据安全行为规范和团体标准，加强行业自律，指导会员加强数据安全保护，提高数据安全保护水平，促进行业健康发展。

第十一条 国家积极开展数据安全治理、数据开发利用等领域的国际交流与合作，参与数据安全相关国际规则和标准的制定，促进数据跨境安全、自由流动。

第十二条 任何个人、组织都有权对违反本法规定的行为向有关主管部门投诉、举报。收到投诉、举报的部门应当及时依法处理。

有关主管部门应当对投诉、举报人的相关信息予以保密， 保护投诉、举报人的合法权益。

第二章 数据安全与发展

第十三条 国家统筹发展和安全，坚持以数据开发利用和产业发展促进数据安全，以数据安全保障数据开发利用和产业发展。

第十四条 国家实施大数据战略，推进数据基础设施建设，鼓励和支持数据在各行业、各领域的创新应用。

省级以上人民政府应当将数字经济发展纳入本级国民经济和社会发展规划，并根据需要制定数字经济发展规划。

第十五条 国家支持开发利用数据提升公共服务的智能化水平。提供智能化公共服务，应当充分考虑老年人、残疾人的需求， 避免对老年人、残疾人的日常生活造成障碍。

第十六条 国家支持数据开发利用和数据安全技术研究，鼓励数据开发利用和数据安全等领域的技术推广和商业创新，培育、发展数据开发利用和数据安全产品、产业体系。

第十七条 国家推进数据开发利用技术和数据安全标准体系建设。国务院标准化行政主管部门和国务院有关部门根据各自的职责，组织制定并适时修订有关数据开发利用技术、产品和数据安全相关标准。国家支持企业、社会团体和教育、科研机构等参与标准制定。

第十八条 国家促进数据安全检测评估、认证等服务的发展，支持数据安全检测评估、认证等专业机构依法开展服务活动。

国家支持有关部门、行业组织、企业、教育和科研机构、有关专业机构等在数据安全风险评估、防范、处置等方面开展协作。

第十九条 国家建立健全数据交易管理制度，规范数据交易行为，培育数据交易市场。

第二十条 国家支持教育、科研机构和企业等开展数据开发利用技术和数据安全相关教育和培训，采取多种方式培养数据开发利用技术和数据安全专业人才，促进人才交流。

第三章 数据安全制度

第二十一条 国家建立数据分类分级保护制度，根据数据在经济社会发展中的重要程度，以及一旦遭到篡改、破坏、泄露或者非法获取、非法利用， 对国家

安全、公共利益或者个人、组织合法权益造成的危害程度， 对数据实行分类分级保护。国家数据安全工作协调机制统筹协调有关部门制定重要数据目录， 加强对重要数据的保护。

关系国家安全、国民经济命脉、重要民生、重大公共利益等数据属于国家核心数据，实行更加严格的管理制度。

各地区、各部门应当按照数据分类分级保护制度， 确定本地区、本部门以及相关行业、领域的重要数据具体目录，对列入目录的数据进行重点保护。

第二十二条 国家建立集中统一、高效权威的数据安全风险评估、报告、信息共享、监测预警机制。国家数据安全工作协调机制统筹协调有关部门加强数据安全风险信息的获取、分析、研判、预警工作。

第二十三条 国家建立数据安全应急处置机制。发生数据安全事件，有关主管部门应当依法启动应急预案，采取相应的应急处置措施，防止危害扩大，消除安全隐患，并及时向社会发布与公众有关的警示信息。

第二十四条 国家建立数据安全审查制度，对影响或者可能影响国家安全的数据处理活动进行国家安全审查。

依法作出的安全审查决定为最终决定。

第二十五条 国家对与维护国家安全和利益、履行国际义务相关的属于管制物项的数据依法实施出口管制。

第二十六条 任何国家或者地区在与数据和数据开发利用技术等有关的投资、贸易等方面对中华人民共和国采取歧视性的禁止、限制或者其他类似措施的， 中华人民共和国可以根据实际情况对该国家或者地区对等采取措施。

第四章 数据安全保护义务

第二十七条 开展数据处理活动应当依照法律、法规的规定，建立健全全流程数据安全管理制度，组织开展数据安全教育培训，采取相应的技术措施和其他必要措施，保障数据安全。利用互联网等信息网络开展数据处理活动， 应当在网络安全等级保护制度的基础上，履行上述数据安全保护义务。

重要数据的处理者应当明确数据安全负责人和管理机构，落实数据安全保护责任。

第二十八条 开展数据处理活动以及研究开发数据新技术，应当有利于促进

经济社会发展，增进人民福祉，符合社会公德和伦理。

第二十九条 开展数据处理活动应当加强风险监测，发现数据安全缺陷、漏洞等风险时，应当立即采取补救措施；发生数据安全事件时，应当立即采取处置措施，按照规定及时告知用户并向有关主管部门报告。

第三十条 重要数据的处理者应当按照规定对其数据处理活动定期开展风险评估，并向有关主管部门报送风险评估报告。

风险评估报告应当包括处理的重要数据的种类、数量， 开展数据处理活动的情况，面临的数据安全风险及其应对措施等。

第三十一条 关键信息基础设施的运营者在中华人民共和国境内运营中收集和产生的重要数据的出境安全管理，适用《中华人民共和国网络安全法》的规定；其他数据处理者在中华人民共和国境内运营中收集和产生的重要数据的出境安全管理办法，由国家网信部门会同国务院有关部门制定。

第三十二条 任何组织、个人收集数据，应当采取合法、正当的方式，不得窃取或者以其他非法方式获取数据。

法律、行政法规对收集、使用数据的目的、范围有规定的， 应当在法律、行政法规规定的目的和范围内收集、使用数据。

第三十三条 从事数据交易中介服务的机构提供服务，应当要求数据提供方说明数据来源，审核交易双方的身份，并留存审核、交易记录。

第三十四条 法律、行政法规规定提供数据处理相关服务应当取得行政许可的，服务提供者应当依法取得许可。

第三十五条 公安机关、国家安全机关因依法维护国家安全或者侦查犯罪的需要调取数据，应当按照国家有关规定，经过严格的批准手续，依法进行，有关组织、个人应当予以配合。

第三十六条 中华人民共和国主管机关根据有关法律和中华人民共和国缔结或者参加的国际条约、协定， 或者按照平等互惠原则，处理外国司法或者执法机构关于提供数据的请求。非经中华人民共和国主管机关批准， 境内的组织、个人不得向外国司法或者执法机构提供存储于中华人民共和国境内的数据。

第五章 政务数据安全与开放

第三十七条 国家大力推进电子政务建设，提高政务数据的科学性、准确性、

时效性，提升运用数据服务经济社会发展的能力。

第三十八条 国家机关为履行法定职责的需要收集、使用数据，应当在其履行法定职责的范围内依照法律、行政法规规定的条件和程序进行； 对在履行职责中知悉的个人隐私、个人信息、商业秘密、保密商务信息等数据应当依法予以保密，不得泄露或者非法向他人提供。

第三十九条 国家机关应当依照法律、行政法规的规定，建立健全数据安全管理制度，落实数据安全保护责任，保障政务数据安全。

第四十条 国家机关委托他人建设、维护电子政务系统，存储、加工政务数据，应当经过严格的批准程序，并应当监督受托方履行相应的数据安全保护义务。受托方应当依照法律、法规的规定和合同约定履行数据安全保护义务， 不得擅自留存、使用、泄露或者向他人提供政务数据。

第四十一条 国家机关应当遵循公正、公平、便民的原则，按照规定及时、准确地公开政务数据。依法不予公开的除外。

第四十二条 国家制定政务数据开放目录，构建统一规范、互联互通、安全可控的政务数据开放平台，推动政务数据开放利用。

第四十三条 法律、法规授权的具有管理公共事务职能的组织为履行法定职责开展数据处理活动，适用本章规定。

第六章 法律责任

第四十四条 有关主管部门在履行数据安全监管职责中，发现数据处理活动存在较大安全风险的，可以按照规定的权限和程序对有关组织、个人进行约谈，并要求有关组织、个人采取措施进行整改，消除隐患。

第四十五条 开展数据处理活动的组织、个人不履行本法第二十七条、第二十九条、第三十条规定的数据安全保护义务的， 由有关主管部门责令改正，给予警告，可以并处五万元以上五十万元以下罚款，对直接负责的主管人员和其他直接责任人员可以处一万元以上十万元以下罚款；拒不改正或者造成大量数据泄露等严重后果的，处五十万元以上二百万元以下罚款，并可以责令暂停相关业务、停业整顿、吊销相关业务许可证或者吊销营业执照， 对直接负责的主管人员和其他直接责任人员处五万元以上二十万元以下罚款。

违反国家核心数据管理制度，危害国家主权、安全和发展利益的， 由有关主

管部门处二百万元以上一千万元以下罚款，并根据情况责令暂停相关业务、停业整顿、吊销相关业务许可证或者吊销营业执照；构成犯罪的，依法追究刑事责任。

第四十六条 违反本法第三十一条规定，向境外提供重要数据的，由有关主管部门责令改正，给予警告，可以并处十万元以上一百万元以下罚款，对直接负责的主管人员和其他直接责任人员可以处一万元以上十万元以下罚款；情节严重的，处一百万元以上一千万元以下罚款，并可以责令暂停相关业务、停业整顿、吊销相关业务许可证或者吊销营业执照，对直接负责的主管人员和其他直接责任人员处十万元以上一百万元以下罚款。

第四十七条 从事数据交易中介服务的机构未履行本法第三十三条规定的义务的，由有关主管部门责令改正，没收违法所得，处违法所得一倍以上十倍以下罚款，没有违法所得或者违法所得不足十万元的，处十万元以上一百万元以下罚款，并可以责令暂停相关业务、停业整顿、吊销相关业务许可证或者吊销营业执照；对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。

第四十八条 违反本法第三十五条规定，拒不配合数据调取的，由有关主管部门责令改正，给予警告，并处五万元以上五十万元以下罚款，对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。

违反本法第三十六条规定，未经主管机关批准向外国司法或者执法机构提供数据的，由有关主管部门给予警告，可以并处十万元以上一百万元以下罚款，对直接负责的主管人员和其他直接责任人员可以处一万元以上十万元以下罚款；造成严重后果的，处一百万元以上五百万元以下罚款，并可以责令暂停相关业务、停业整顿、吊销相关业务许可证或者吊销营业执照， 对直接负责的主管人员和其他直接责任人员处五万元以上五十万元以下罚款。

第四十九条 国家机关不履行本法规定的数据安全保护义务的，对直接负责的主管人员和其他直接责任人员依法给予处分。

第五十条 履行数据安全监管职责的国家工作人员玩忽职守、滥用职权、徇私舞弊的，依法给予处分。

第五十一条 窃取或者以其他非法方式获取数据，开展数据处理活动排除、限制竞争，或者损害个人、组织合法权益的， 依照有关法律、行政法规的规定处罚。

第五十二条 违反本法规定，给他人造成损害的，依法承担民事责任。

违反本法规定，构成违反治安管理行为的，依法给予治安管理处罚；构成犯罪的，依法追究刑事责任。

第七章 附 则

第五十三条 开展涉及国家秘密的数据处理活动，适用《中华人民共和国保守国家秘密法》等法律、行政法规的规定。

在统计、档案工作中开展数据处理活动，开展涉及个人信息的数据处理活动，还应当遵守有关法律、行政法规的规定。

第五十四条 军事数据安全保护的办法，由中央军事委员会依据本法另行制定。

第五十五条 本法自 2021 年 9 月 1 日起施行。

中华人民共和国个人信息保护法

中华人民共和国主席令第九十一号

《中华人民共和国个人信息保护法》已由中华人民共和国第十三届全国人民代表大会常务委员会第三十次会议于 2021 年 8 月 20 日通过，现予公布，自 2021 年 11 月 1 日起施行。

中华人民共和国主席 习近平

2021 年 8 月 20 日

中华人民共和国个人信息保护法

(2021 年 8 月 20 日第十三届全国人民代表大会常务委员会第三十次会议通过)

第一章 总 则

第一条 为了保护个人信息权益，规范个人信息处理活动，促进个人信息合理利用，根据宪法，制定本法。

第二条 自然人的个人信息受法律保护，任何组织、个人不得侵害自然人的个人信息权益。

第三条 在中华人民共和国境内处理自然人个人信息的活动，适用本法。

在中华人民共和国境外处理中华人民共和国境内自然人个人信息的活动，有下列情形之一的，也适用本法：

(一)以向境内自然人提供产品或者服务为目的；

(二)分析、评估境内自然人的行为；

(三)法律、行政法规规定的其他情形。

第四条 个人信息是以电子或者其他方式记录的与已识别或者可识别的自然人有关的各种信息，不包括匿名化处理后的信息。

个人信息的处理包括个人信息的收集、存储、使用、加工、传输、提供、公开、删除等。

第五条 处理个人信息应当遵循合法、正当、必要和诚信原则，不得通过误导、欺诈、胁迫等方式处理个人信息。

第六条 处理个人信息应当具有明确、合理的目的，并应当与处理目的直接相关，采取对个人权益影响最小的方式。

收集个人信息，应当限于实现处理目的的最小范围，不得过度收集个人信息。

第七条 处理个人信息应当遵循公开、透明原则，公开个人信息处理规则，明示处理的目的、方式和范围。

第八条 处理个人信息应当保证个人信息的质量，避免因个人信息不准确、不完整对个人权益造成不利影响。

第九条 个人信息处理者应当对其个人信息处理活动负责，并采取必要措施保障所处理的个人信息的安全。

第十条 任何组织、个人不得非法收集、使用、加工、传输他人个人信息，不得非法买卖、提供或者公开他人个人信息； 不得从事危害国家安全、公共利益的个人信息处理活动。

第十一条 国家建立健全个人信息保护制度，预防和惩治侵害个人信息权益的行为，加强个人信息保护宣传教育，推动形成政府、企业、相关社会组织、公众共同参与个人信息保护的良好环境。

第十二条 国家积极参与个人信息保护国际规则的制定，促进个人信息保护方面的国际交流与合作，推动与其他国家、地区、国际组织之间的个人信息保护规则、标准等互认。

第二章 个人信息处理规则

第一节 一般规定

第十三条 符合下列情形之一的，个人信息处理者方可处理个人信息：

(一)取得个人的同意;

(二)为订立、履行个人作为一方当事人的合同所必需，或者按照依法制定的劳动规章制度和依法签订的集体合同实施人力资源管理所必需;

(三)为履行法定职责或者法定义务所必需;

(四)为应对突发公共卫生事件，或者紧急情况下为保护自然人的生命健康和财产安全所必需;

(五)为公共利益实施新闻报道、舆论监督等行为， 在合理的范围内处理个人信息;

(六)依照本法规定在合理的范围内处理个人自行公开或者其他已经合法公开的个人信息;

(七)法律、行政法规规定的其他情形。

依照本法其他有关规定，处理个人信息应当取得个人同意，但是有前款第二项至第七项规定情形的，不需取得个人同意。

第十四条 基于个人同意处理个人信息的，该同意应当由个人在充分知情的前提下自愿、明确作出。法律、行政法规规定处理个人信息应当取得个人单独同意或者书面同意的，从其规定。

个人信息的处理目的、处理方式和处理的个人信息种类发生变更的， 应当重新取得个人同意。

第十五条 基于个人同意处理个人信息的，个人有权撤回其同意。个人信息处理者应当提供便捷的撤回同意的方式。

个人撤回同意，不影响撤回前基于个人同意已进行的个人信息处理活动的效力。

第十六条 个人信息处理者不得以个人不同意处理其个人信息或者撤回同意为由，拒绝提供产品或者服务;处理个人信息属于提供产品或者服务所必需的除外。

第十七条 个人信息处理者在处理个人信息前，应当以显著方式、清晰易懂的语言真实、准确、完整地向个人告知下列事项:

(一)个人信息处理者的名称或者姓名和联系方式;

(二)个人信息的处理目的、处理方式，处理的个人信息种类、保存期限;

(三)个人行使本法规定权利的方式和程序;

(四)法律、行政法规规定应当告知的其他事项。

前款规定事项发生变更的，应当将变更部分告知个人。

个人信息处理者通过制定个人信息处理规则的方式告知第一款规定事项的，处理规则应当公开，并且便于查阅和保存。

第十八条 个人信息处理者处理个人信息，有法律、行政法规规定应当保密或者不需要告知的情形的，可以不向个人告知前条第一款规定的事项。

紧急情况下为保护自然人的生命健康和财产安全无法及时向个人告知的，个人信息处理者应当在紧急情况消除后及时告知。

第十九条 除法律、行政法规另有规定外，个人信息的保存期限应当为实现处理目的所必要的最短时间。

第二十条 两个以上的个人信息处理者共同决定个人信息的处理目的和处理方式的，应当约定各自的权利和义务。但是， 该约定不影响个人向其中任何一个个人信息处理者要求行使本法规定的权利。

个人信息处理者共同处理个人信息，侵害个人信息权益造成损害的，应当依法承担连带责任。

第二十一条 个人信息处理者委托处理个人信息的，应当与受托人约定委托处理的目的、期限、处理方式、个人信息的种类、保护措施以及双方的权利和义务等，并对受托人的个人信息处理活动进行监督。

受托人应当按照约定处理个人信息，不得超出约定的处理目的、处理方式等处理个人信息；委托合同不生效、无效、被撤销或者终止的， 受托人应当将个人信息返还个人信息处理者或者予以删除，不得保留。

未经个人信息处理者同意，受托人不得转委托他人处理个人信息。

第二十二条 个人信息处理者因合并、分立、解散、被宣告破产等原因需要转移个人信息的，应当向个人告知接收方的名称或者姓名和联系方式。接收方应当继续履行个人信息处理者的义务。接收方变更原先的处理目的、处理方式的，应当依照本法规定重新取得个人同意。

第二十三条 个人信息处理者向其他个人信息处理者提供其处理的个人信息的，应当向个人告知接收方的名称或者姓名、联系方式、处理目的、处理方式和

个人信息的种类，并取得个人的单独同意。接收方应当在上述处理目的、处理方式和个人信息的种类等范围内处理个人信息。接收方变更原先的处理目的、处理方式的，应当依照本法规定重新取得个人同意。

第二十四条 个人信息处理者利用个人信息进行自动化决策，应当保证决策的透明度和结果公平、公正， 不得对个人在交易价格等交易条件上实行不合理的差别待遇。

通过自动化决策方式向个人进行信息推送、商业营销， 应当同时提供不针对其个人特征的选项，或者向个人提供便捷的拒绝方式。

通过自动化决策方式作出对个人权益有重大影响的决定，个人有权要求个人信息处理者予以说明，并有权拒绝个人信息处理者仅通过自动化决策的方式作出决定。

第二十五条 个人信息处理者不得公开其处理的个人信息，取得个人单独同意的除外。

第二十六条 在公共场所安装图像采集、个人身份识别设备，应当为维护公共安全所必需，遵守国家有关规定，并设置显著的提示标识。所收集的个人图像、身份识别信息只能用于维护公共安全的目的，不得用于其他目的；取得个人单独同意的除外。

第二十七条 个人信息处理者可以在合理的范围内处理个人自行公开或者其他已经合法公开的个人信息；个人明确拒绝的除外。个人信息处理者处理已公开的个人信息，对个人权益有重大影响的，应当依照本法规定取得个人同意。

第二节 敏感个人信息的处理规则

第二十八条 敏感个人信息是一旦泄露或者非法使用，容易导致自然人的人格尊严受到侵害或者人身、财产安全受到危害的个人信息， 包括生物识别、宗教信仰、特定身份、医疗健康、金融账户、行踪轨迹等信息， 以及不满十四周岁未成年人的个人信息。

只有在具有特定的目的和充分的必要性，并采取严格保护措施的情形下，个人信息处理者方可处理敏感个人信息。

第二十九条 处理敏感个人信息应当取得个人的单独同意；法律、行政法规规定处理敏感个人信息应当取得书面同意的，从其规定。

第三十条 个人信息处理者处理敏感个人信息的，除本法第十七条第一款规定的事项外，还应当向个人告知处理敏感个人信息的必要性以及对个人权益的影响；依照本法规定可以不向个人告知的除外。

第三十一条 个人信息处理者处理不满十四周岁未成年人个人信息的，应当取得未成年人的父母或者其他监护人的同意。

个人信息处理者处理不满十四周岁未成年人个人信息的，应当制定专门的个人信息处理规则。

第三十二条 法律、行政法规对处理敏感个人信息规定应当取得相关行政许可或者作出其他限制的，从其规定。

第三节 国家机关处理个人信息的特别规定

第三十三条 国家机关处理个人信息的活动，适用本法；本节有特别规定的，适用本节规定。

第三十四条 国家机关为履行法定职责处理个人信息，应当依照法律、行政法规规定的权限、程序进行，不得超出履行法定职责所必需的范围和限度。

第三十五条 国家机关为履行法定职责处理个人信息，应当依照本法规定履行告知义务；有本法第十八条第一款规定的情形，或者告知将妨碍国家机关履行法定职责的除外。

第三十六条 国家机关处理的个人信息应当在中华人民共和国境内存储；确需向境外提供的，应当进行安全评估。安全评估可以要求有关部门提供支持与协助。

第三十七条 法律、法规授权的具有管理公共事务职能的组织为履行法定职责处理个人信息，适用本法关于国家机关处理个人信息的规定。

第三章 个人信息跨境提供的规则

第三十八条 个人信息处理者因业务等需要，确需向中华人民共和国境外提供个人信息的，应当具备下列条件之一：

(一)依照本法第四十条的规定通过国家网信部门组织的安全评估；

(二)按照国家网信部门的规定经专业机构进行个人信息保护认证；

(三)按照国家网信部门制定的标准合同与境外接收方订立合同，约定双方的权利和义务；

(四)法律、行政法规或者国家网信部门规定的其他条件。

中华人民共和国缔结或者参加的国际条约、协定对向中华人民共和国境外提供个人信息的条件等有规定的，可以按照其规定执行。

个人信息处理者应当采取必要措施，保障境外接收方处理个人信息的活动达到本法规定的个人信息保护标准。

第三十九条 个人信息处理者向中华人民共和国境外提供个人信息的，应当向个人告知境外接收方的名称或者姓名、联系方式、处理目的、处理方式、个人信息的种类以及个人向境外接收方行使本法规定权利的方式和程序等事项，并取得个人的单独同意。

第四十条 关键信息基础设施运营者和处理个人信息达到国家网信部门规定数量的个人信息处理者，应当将在中华人民共和国境内收集和产生的个人信息存储在境内。确需向境外提供的，应当通过国家网信部门组织的安全评估；法律、行政法规和国家网信部门规定可以不进行安全评估的，从其规定。

第四十一条 中华人民共和国主管机关根据有关法律和中华人民共和国缔结或者参加的国际条约、协定， 或者按照平等互惠原则，处理外国司法或者执法机构关于提供存储于境内个人信息的请求。非经中华人民共和国主管机关批准， 个人信息处理者不得向外国司法或者执法机构提供存储于中华人民共和国境内的个人信息。

第四十二条 境外的组织、个人从事侵害中华人民共和国公民的个人信息权益，或者危害中华人民共和国国家安全、公共利益的个人信息处理活动的， 国家网信部门可以将其列入限制或者禁止个人信息提供清单，予以公告，并采取限制或者禁止向其提供个人信息等措施。

第四十三条 任何国家或者地区在个人信息保护方面对中华人民共和国采取歧视性的禁止、限制或者其他类似措施的， 中华人民共和国可以根据实际情况对该国家或者地区对等采取措施。

第四章 个人在个人信息处理活动中的权利

第四十四条 个人对其个人信息的处理享有知情权、决定权，有权限制或者拒绝他人对其个人信息进行处理；法律、行政法规另有规定的除外。

第四十五条 个人有权向个人信息处理者查阅、复制其个人信息；有本法第

十八条第一款、第三十五条规定情形的除外。

个人请求查阅、复制其个人信息的，个人信息处理者应当及时提供。

个人请求将个人信息转移至其指定的个人信息处理者，符合国家网信部门规定条件的，个人信息处理者应当提供转移的途径。

第四十六条 个人发现其个人信息不准确或者不完整的，有权请求个人信息处理者更正、补充。

个人请求更正、补充其个人信息的， 个人信息处理者应当对其个人信息予以核实，并及时更正、补充。

第四十七条 有下列情形之一的，个人信息处理者应当主动删除个人信息；个人信息处理者未删除的，个人有权请求删除：

(一)处理目的已实现、无法实现或者为实现处理目的不再必要；

(二)个人信息处理者停止提供产品或者服务，或者保存期限已届满；

(三)个人撤回同意；

(四)个人信息处理者违反法律、行政法规或者违反约定处理个人信息；

(五)法律、行政法规规定的其他情形。

法律、行政法规规定的保存期限未届满， 或者删除个人信息从技术上难以实现的，个人信息处理者应当停止除存储和采取必要的安全保护措施之外的处理。

第四十八条 个人有权要求个人信息处理者对其个人信息处理规则进行解释说明。

第四十九条 自然人死亡的，其近亲属为了自身的合法、正当利益， 可以对死者的相关个人信息行使本章规定的查阅、复制、更正、删除等权利； 死者生前另有安排的除外。

第五十条 个人信息处理者应当建立便捷的个人行使权利的申请受理和处理机制。拒绝个人行使权利的请求的，应当说明理由。

个人信息处理者拒绝个人行使权利的请求的，个人可以依法向人民法院提起诉讼。

第五章 个人信息处理者的义务

第五十一条 个人信息处理者应当根据个人信息的处理目的、处理方式、个人信息的种类以及对个人权益的影响、可能存在的安全风险等， 采取下列措施确

保个人信息处理活动符合法律、行政法规的规定， 并防止未经授权的访问以及个人信息泄露、篡改、丢失：

(一)制定内部管理制度和操作规程；

(二)对个人信息实行分类管理；

(三)采取相应的加密、去标识化等安全技术措施；

(四)合理确定个人信息处理的操作权限，并定期对从业人员进行安全教育和培训；

(五)制定并组织实施个人信息安全事件应急预案；

(六)法律、行政法规规定的其他措施。

第五十二条 处理个人信息达到国家网信部门规定数量的个人信息处理者应当指定个人信息保护负责人，负责对个人信息处理活动以及采取的保护措施等进行监督。

个人信息处理者应当公开个人信息保护负责人的联系方式，并将个人信息保护负责人的姓名、联系方式等报送履行个人信息保护职责的部门。

第五十三条 本法第三条第二款规定的中华人民共和国境外的个人信息处理者，应当在中华人民共和国境内设立专门机构或者指定代表，负责处理个人信息保护相关事务，并将有关机构的名称或者代表的姓名、联系方式等报送履行个人信息保护职责的部门。

第五十四条 个人信息处理者应当定期对其处理个人信息遵守法律、行政法规的情况进行合规审计。

第五十五条 有下列情形之一的，个人信息处理者应当事前进行个人信息保护影响评估，并对处理情况进行记录：

(一)处理敏感个人信息；

(二)利用个人信息进行自动化决策；

(三)委托处理个人信息、向其他个人信息处理者提供个人信息、公开个人信息；

(四)向境外提供个人信息；

(五)其他对个人权益有重大影响的个人信息处理活动。

第五十六条 个人信息保护影响评估应当包括下列内容：

(一)个人信息的处理目的、处理方式等是否合法、正当、必要;

(二)对个人权益的影响及安全风险;

(三)所采取的保护措施是否合法、有效并与风险程度相适应。

个人信息保护影响评估报告和处理情况记录应当至少保存三年。

第五十七条 发生或者可能发生个人信息泄露、篡改、丢失的,个人信息处理者应当立即采取补救措施,并通知履行个人信息保护职责的部门和个人。通知应当包括下列事项:

(一)发生或者可能发生个人信息泄露、篡改、丢失的信息种类、原因和可能造成的危害;

(二)个人信息处理者采取的补救措施和个人可以采取的减轻危害的措施;

(三)个人信息处理者的联系方式。

个人信息处理者采取措施能够有效避免信息泄露、篡改、丢失造成危害的,个人信息处理者可以不通知个人;履行个人信息保护职责的部门认为可能造成危害的,有权要求个人信息处理者通知个人。

第五十八条 提供重要互联网平台服务、用户数量巨大、业务类型复杂的个人信息处理者,应当履行下列义务:

(一)按照国家规定建立健全个人信息保护合规制度体系,成立主要由外部成员组成的独立机构对个人信息保护情况进行监督;

(二)遵循公开、公平、公正的原则, 制定平台规则,明确平台内产品或者服务提供者处理个人信息的规范和保护个人信息的义务;

(三)对严重违反法律、行政法规处理个人信息的平台内的产品或者服务提供者,停止提供服务;

(四)定期发布个人信息保护社会责任报告,接受社会监督。

第五十九条 接受委托处理个人信息的受托人,应当依照本法和有关法律、行政法规的规定,采取必要措施保障所处理的个人信息的安全,并协助个人信息处理者履行本法规定的义务。

第六章 履行个人信息保护职责的部门

第六十条 国家网信部门负责统筹协调个人信息保护工作和相关监督管理工作。国务院有关部门依照本法和有关法律、行政法规的规定, 在各自职责范围内

负责个人信息保护和监督管理工作。

县级以上地方人民政府有关部门的个人信息保护和监督管理职责，按照国家有关规定确定。

前两款规定的部门统称为履行个人信息保护职责的部门。

第六十一条 履行个人信息保护职责的部门履行下列个人信息保护职责：

(一)开展个人信息保护宣传教育，指导、监督个人信息处理者开展个人信息保护工作；

(二)接受、处理与个人信息保护有关的投诉、举报；

(三)组织对应用程序等个人信息保护情况进行测评，并公布测评结果；

(四)调查、处理违法个人信息处理活动；

(五)法律、行政法规规定的其他职责。

第六十二条 国家网信部门统筹协调有关部门依据本法推进下列个人信息保护工作：

(一)制定个人信息保护具体规则、标准；

(二)针对小型个人信息处理者、处理敏感个人信息以及人脸识别、人工智能等新技术、新应用，制定专门的个人信息保护规则、标准；

(三)支持研究开发和推广应用安全、方便的电子身份认证技术， 推进网络身份认证公共服务建设；

(四)推进个人信息保护社会化服务体系建设，支持有关机构开展个人信息保护评估、认证服务；

(五)完善个人信息保护投诉、举报工作机制。

第六十三条 履行个人信息保护职责的部门履行个人信息保护职责，可以采取下列措施：

(一)询问有关当事人，调查与个人信息处理活动有关的情况；

(二)查阅、复制当事人与个人信息处理活动有关的合同、记录、账簿以及其他有关资料；

(三)实施现场检查，对涉嫌违法的个人信息处理活动进行调查；

(四)检查与个人信息处理活动有关的设备、物品； 对有证据证明是用于违法个人信息处理活动的设备、物品， 向本部门主要负责人书面报告并经批准，可以

查封或者扣押。

履行个人信息保护职责的部门依法履行职责，当事人应当予以协助、配合，不得拒绝、阻挠。

第六十四条 履行个人信息保护职责的部门在履行职责中，发现个人信息处理活动存在较大风险或者发生个人信息安全事件的，可以按照规定的权限和程序对该个人信息处理者的法定代表人或者主要负责人进行约谈，或者要求个人信息处理者委托专业机构对其个人信息处理活动进行合规审计。个人信息处理者应当按照要求采取措施，进行整改，消除隐患。

履行个人信息保护职责的部门在履行职责中，发现违法处理个人信息涉嫌犯罪的，应当及时移送公安机关依法处理。

第六十五条 任何组织、个人有权对违法个人信息处理活动向履行个人信息保护职责的部门进行投诉、举报。收到投诉、举报的部门应当依法及时处理， 并将处理结果告知投诉、举报人。

履行个人信息保护职责的部门应当公布接受投诉、举报的联系方式。

第七章 法律责任

第六十六条 违反本法规定处理个人信息，或者处理个人信息未履行本法规定的个人信息保护义务的，由履行个人信息保护职责的部门责令改正，给予警告，没收违法所得，对违法处理个人信息的应用程序，责令暂停或者终止提供服务；拒不改正的，并处一百万元以下罚款；对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。

有前款规定的违法行为，情节严重的，由省级以上履行个人信息保护职责的部门责令改正，没收违法所得，并处五千万元以下或者上一年度营业额百分之五以下罚款，并可以责令暂停相关业务或者停业整顿、通报有关主管部门吊销相关业务许可或者吊销营业执照；对直接负责的主管人员和其他直接责任人员处十万元以上一百万元以下罚款，并可以决定禁止其在一定期限内担任相关企业的董事、监事、高级管理人员和个人信息保护负责人。

第六十七条 有本法规定的违法行为的，依照有关法律、行政法规的规定记入信用档案，并予以公示。

第六十八条 国家机关不履行本法规定的个人信息保护义务的，由其上级机

关或者履行个人信息保护职责的部门责令改正；对直接负责的主管人员和其他直接责任人员依法给予处分。

履行个人信息保护职责的部门的工作人员玩忽职守、滥用职权、徇私舞弊，尚不构成犯罪的，依法给予处分。

第六十九条 处理个人信息侵害个人信息权益造成损害，个人信息处理者不能证明自己没有过错的，应当承担损害赔偿等侵权责任。

前款规定的损害赔偿责任按照个人因此受到的损失或者个人信息处理者因此获得的利益确定；个人因此受到的损失和个人信息处理者因此获得的利益难以确定的，根据实际情况确定赔偿数额。

第七十条 个人信息处理者违反本法规定处理个人信息，侵害众多个人的权益的，人民检察院、法律规定的消费者组织和由国家网信部门确定的组织可以依法向人民法院提起诉讼。

第七十一条 违反本法规定，构成违反治安管理行为的，依法给予治安管理处罚；构成犯罪的，依法追究刑事责任。

第八章 附 则

第七十二条 自然人因个人或者家庭事务处理个人信息的，不适用本法。

法律对各级人民政府及其有关部门组织实施的统计、档案管理活动中的个人信息处理有规定的，适用其规定。

第七十三条 本法下列用语的含义：

(一)个人信息处理者，是指在个人信息处理活动中自主决定处理目的、处理方式的组织、个人。

(二) 自动化决策，是指通过计算机程序自动分析、评估个人的行为习惯、兴趣爱好或者经济、健康、信用状况等，并进行决策的活动。

(三)去标识化，是指个人信息经过处理，使其在不借助额外信息的情况下无法识别特定自然人的过程。

(四)匿名化，是指个人信息经过处理无法识别特定自然人且不能复原的过程。

第七十四条 本法自 2021 年 11 月 1 日起施行。

中华人民共和国反电信网络诈骗法

(2022 年 9 月 2 日第十三届全国人民代表大会常务委员会第三十六次会议通过)

目 录

第一章 总 则

第一条 为了预防、遏制和惩治电信网络诈骗活动，加强反电信网络诈骗工作，保护公民和组织的合法权益，维护社会稳定和国家安全，根据宪法，制定本法。

第二条 本法所称电信网络诈骗，是指以非法占有为目的，利用电信网络技术手段，通过远程、非接触等方式，诈骗公私财物的行为。

第三条 打击治理在中华人民共和国境内实施的电信网络诈骗活动或者中华人民共和国公民在境外实施的电信网络诈骗活动，适用本法。

境外的组织、个人针对中华人民共和国境内实施电信网络诈骗活动的， 或者为他人针对境内实施电信网络诈骗活动提供产品、服务等帮助的， 依照本法有关规定处理和追究责任。

第四条 反电信网络诈骗工作坚持以人民为中心，统筹发展和安全；坚持系统观念、法治思维， 注重源头治理、综合治理；坚持齐抓共管、群防群治，全面落实打防管控各项措施，加强社会宣传教育防范；坚持精准防治，保障正常生产经营活动和群众生活便利。

第五条 反电信网络诈骗工作应当依法进行，维护公民和组织的合法权益。

有关部门和单位、个人应当对在反电信网络诈骗工作过程中知悉的国家秘密、商业秘密和个人隐私、个人信息予以保密。

第六条 国务院建立反电信网络诈骗工作机制，统筹协调打击治理工作。

地方各级人民政府组织领导本行政区域内反电信网络诈骗工作，确定反电信网络诈骗目标任务和工作机制，开展综合治理。

公安机关牵头负责反电信网络诈骗工作，金融、电信、网信、市场监管等有关部门依照职责履行监管主体责任，负责本行业领域反电信网络诈骗工作。

人民法院、人民检察院发挥审判、检察职能作用， 依法防范、惩治电信网络诈骗活动。

电信业务经营者、银行业金融机构、非银行支付机构、互联网服务提供者承担风险防控责任，建立反电信网络诈骗内部控制机制和安全责任制度，加强新业务涉诈风险安全评估。

第七条 有关部门、单位在反电信网络诈骗工作中应当密切协作，实现跨行业、跨地域协同配合、快速联动， 加强专业队伍建设，有效打击治理电信网络诈骗活动。

第八条 各级人民政府和有关部门应当加强反电信网络诈骗宣传，普及相关法律和知识，提高公众对各类电信网络诈骗方式的防骗意识和识骗能力。

教育行政、市场监管、民政等有关部门和村民委员会、居民委员会， 应当结合电信网络诈骗受害群体的分布等特征，加强对老年人、青少年等群体的宣传教育，增强反电信网络诈骗宣传教育的针对性、精准性， 开展反电信网络诈骗宣传教育进学校、进企业、进社区、进农村、进家庭等活动。

各单位应当加强内部防范电信网络诈骗工作，对工作人员开展防范电信网络诈骗教育；个人应当加强电信网络诈骗防范意识。单位、个人应当协助、配合有关部门依照本法规定开展反电信网络诈骗工作。

第二章 电信治理

第九条 电信业务经营者应当依法全面落实电话用户真实身份信息登记制度。

基础电信企业和移动通信转售企业应当承担对代理商落实电话用户实名制管理责任，在协议中明确代理商实名制登记的责任和有关违约处置措施。

第十条 办理电话卡不得超出国家有关规定限制的数量。

对经识别存在异常办卡情形的，电信业务经营者有权加强核查或者拒绝办卡。具体识别办法由国务院电信主管部门制定。

国务院电信主管部门组织建立电话用户开卡数量核验机制和风险信息共享机制，并为用户查询名下电话卡信息提供便捷渠道。

第十一条 电信业务经营者对监测识别的涉诈异常电话卡用户应当重新进行

实名核验，根据风险等级采取有区别的、相应的核验措施。对未按规定核验或者核验未通过的，电信业务经营者可以限制、暂停有关电话卡功能。

第十二条 电信业务经营者建立物联网卡用户风险评估制度，评估未通过的，不得向其销售物联网卡；严格登记物联网卡用户身份信息；采取有效技术措施限定物联网卡开通功能、使用场景和适用设备。

单位用户从电信业务经营者购买物联网卡再将载有物联网卡的设备销售给其他用户的，应当核验和登记用户身份信息，并将销量、存量及用户实名信息传送给号码归属的电信业务经营者。

电信业务经营者对物联网卡的使用建立监测预警机制。对存在异常使用情形的，应当采取暂停服务、重新核验身份和使用场景或者其他合同约定的处置措施。

第十三条 电信业务经营者应当规范真实主叫号码传送和电信线路出租，对改号电话进行封堵拦截和溯源核查。

电信业务经营者应当严格规范国际通信业务出入口局主叫号码传送，真实、准确向用户提示来电号码所属国家或者地区，对网内和网间虚假主叫、不规范主叫进行识别、拦截。

第十四条 任何单位和个人不得非法制造、买卖、提供或者使用下列设备、软件：

(一)电话卡批量插入设备；

(二)具有改变主叫号码、虚拟拨号、互联网电话违规接入公用电信网络等功能的设备、软件；

(三)批量账号、网络地址自动切换系统， 批量接收提供短信验证、语音验证的平台；

(四)其他用于实施电信网络诈骗等违法犯罪的设备、软件。

电信业务经营者、互联网服务提供者应当采取技术措施， 及时识别、阻断前款规定的非法设备、软件接入网络，并向公安机关和相关行业主管部门报告。

第三章 金融治理

第十五条 银行业金融机构、非银行支付机构为客户开立银行账户、支付账户及提供支付结算服务，和与客户业务关系存续期间，应当建立客户尽职调查制度，依法识别受益所有人，采取相应风险管理措施，防范银行账户、支付账户等

被用于电信网络诈骗活动。

第十六条 开立银行账户、支付账户不得超出国家有关规定限制的数量。

对经识别存在异常开户情形的，银行业金融机构、非银行支付机构有权加强核查或者拒绝开户。

中国人民银行、国务院银行业监督管理机构组织有关清算机构建立跨机构开户数量核验机制和风险信息共享机制，并为客户提供查询名下银行账户、支付账户的便捷渠道。银行业金融机构、非银行支付机构应当按照国家有关规定提供开户情况和有关风险信息。相关信息不得用于反电信网络诈骗以外的其他用途。

第十七条 银行业金融机构、非银行支付机构应当建立开立企业账户异常情形的风险防控机制。金融、电信、市场监管、税务等有关部门建立开立企业账户相关信息共享查询系统，提供联网核查服务。

市场主体登记机关应当依法对企业实名登记履行身份信息核验职责；依照规定对登记事项进行监督检查，对可能存在虚假登记、涉诈异常的企业重点监督检查，依法撤销登记的，依照前款的规定及时共享信息；为银行业金融机构、非银行支付机构进行客户尽职调查和依法识别受益所有人提供便利。

第十八条 银行业金融机构、非银行支付机构应当对银行账户、支付账户及支付结算服务加强监测，建立完善符合电信网络诈骗活动特征的异常账户和可疑交易监测机制。

中国人民银行统筹建立跨银行业金融机构、非银行支付机构的反洗钱统一监测系统，会同国务院公安部门完善与电信网络诈骗犯罪资金流转特点相适应的反洗钱可疑交易报告制度。

对监测识别的异常账户和可疑交易，银行业金融机构、非银行支付机构应当根据风险情况，采取核实交易情况、重新核验身份、延迟支付结算、限制或者中止有关业务等必要的防范措施。

银行业金融机构、非银行支付机构依照第一款规定开展异常账户和可疑交易监测时，可以收集异常客户互联网协议地址、网卡地址、支付受理终端信息等必要的交易信息、设备位置信息。上述信息未经客户授权， 不得用于反电信网络诈骗以外的其他用途。

第十九条 银行业金融机构、非银行支付机构应当按照国家有关规定，完整、

准确传输直接提供商品或者服务的商户名称、收付款客户名称及账号等交易信息，保证交易信息的真实、完整和支付全流程中的一致性。

第二十条 国务院公安部门会同有关部门建立完善电信网络诈骗涉案资金即时查询、紧急止付、快速冻结、及时解冻和资金返还制度， 明确有关条件、程序和救济措施。

公安机关依法决定采取上述措施的，银行业金融机构、非银行支付机构应当予以配合。

第四章 互联网治理

第二十一条 电信业务经营者、互联网服务提供者为用户提供下列服务，在与用户签订协议或者确认提供服务时，应当依法要求用户提供真实身份信息，用户不提供真实身份信息的，不得提供服务：

(一)提供互联网接入服务；

(二)提供网络代理等网络地址转换服务；

(三)提供互联网域名注册、服务器托管、空间租用、云服务、内容分发服务；

(四)提供信息、软件发布服务，或者提供即时通讯、网络交易、网络游戏、网络直播发布、广告推广服务。

第二十二条 互联网服务提供者对监测识别的涉诈异常账号应当重新核验，根据国家有关规定采取限制功能、暂停服务等处置措施。

互联网服务提供者应当根据公安机关、电信主管部门要求，对涉案电话卡、涉诈异常电话卡所关联注册的有关互联网账号进行核验，根据风险情况，采取限期改正、限制功能、暂停使用、关闭账号、禁止重新注册等处置措施。

第二十三条 设立移动互联网应用程序应当按照国家有关规定向电信主管部门办理许可或者备案手续。

为应用程序提供封装、分发服务的， 应当登记并核验应用程序开发运营者的真实身份信息，核验应用程序的功能、用途。

公安、电信、网信等部门和电信业务经营者、互联网服务提供者应当加强对分发平台以外途径下载传播的涉诈应用程序重点监测、及时处置。

第二十四条 提供域名解析、域名跳转、网址链接转换服务的，应当按照国家有关规定，核验域名注册、解析信息和互联网协议地址的真实性、准确性， 规

范域名跳转，记录并留存所提供相应服务的日志信息，支持实现对解析、跳转、转换记录的溯源。

第二十五条 任何单位和个人不得为他人实施电信网络诈骗活动提供下列支持或者帮助：

(一)出售、提供个人信息；

(二)帮助他人通过虚拟货币交易等方式洗钱；

(三)其他为电信网络诈骗活动提供支持或者帮助的行为。

电信业务经营者、互联网服务提供者应当依照国家有关规定， 履行合理注意义务，对利用下列业务从事涉诈支持、帮助活动进行监测识别和处置：

(一)提供互联网接入、服务器托管、网络存储、通讯传输、线路出租、域名解析等网络资源服务；

(二)提供信息发布或者搜索、广告推广、引流推广等网络推广服务；

(三)提供应用程序、网站等网络技术、产品的制作、维护服务；

(四)提供支付结算服务。

第二十六条 公安机关办理电信网络诈骗案件依法调取证据的，互联网服务提供者应当及时提供技术支持和协助。

互联网服务提供者依照本法规定对有关涉诈信息、活动进行监测时， 发现涉诈违法犯罪线索、风险信息的， 应当依照国家有关规定，根据涉诈风险类型、程度情况移送公安、金融、电信、网信等部门。有关部门应当建立完善反馈机制，将相关情况及时告知移送单位。

第五章 综合措施

第二十七条 公安机关应当建立完善打击治理电信网络诈骗工作机制，加强专门队伍和专业技术建设，各警种、各地公安机关应当密切配合， 依法有效惩处电信网络诈骗活动。

公安机关接到电信网络诈骗活动的报案或者发现电信网络诈骗活动，应当依照《中华人民共和国刑事诉讼法》的规定立案侦查。

第二十八条 金融、电信、网信部门依照职责对银行业金融机构、非银行支付机构、电信业务经营者、互联网服务提供者落实本法规定情况进行监督检查。有关监督检查活动应当依法规范开展。

第二十九条 个人信息处理者应当依照《中华人民共和国个人信息保护法》等法律规定，规范个人信息处理，加强个人信息保护，建立个人信息被用于电信网络诈骗的防范机制。

履行个人信息保护职责的部门、单位对可能被电信网络诈骗利用的物流信息、交易信息、贷款信息、医疗信息、婚介信息等实施重点保护。公安机关办理电信网络诈骗案件，应当同时查证犯罪所利用的个人信息来源，依法追究相关人员和单位责任。

第三十条 电信业务经营者、银行业金融机构、非银行支付机构、互联网服务提供者应当对从业人员和用户开展反电信网络诈骗宣传，在有关业务活动中对防范电信网络诈骗作出提示，对本领域新出现的电信网络诈骗手段及时向用户作出提醒，对非法买卖、出租、出借本人有关卡、账户、账号等被用于电信网络诈骗的法律责任作出警示。

新闻、广播、电视、文化、互联网信息服务等单位， 应当面向社会有针对性地开展反电信网络诈骗宣传教育。

任何单位和个人有权举报电信网络诈骗活动，有关部门应当依法及时处理，对提供有效信息的举报人依照规定给予奖励和保护。

第三十一条 任何单位和个人不得非法买卖、出租、出借电话卡、物联网卡、电信线路、短信端口、银行账户、支付账户、互联网账号等， 不得提供实名核验帮助；不得假冒他人身份或者虚构代理关系开立上述卡、账户、账号等。

对经设区的市级以上公安机关认定的实施前款行为的单位、个人和相关组织者，以及因从事电信网络诈骗活动或者关联犯罪受过刑事处罚的人员，可以按照国家有关规定记入信用记录，采取限制其有关卡、账户、账号等功能和停止非柜面业务、暂停新业务、限制入网等措施。对上述认定和措施有异议的， 可以提出申诉，有关部门应当建立健全申诉渠道、信用修复和救济制度。具体办法由国务院公安部门会同有关主管部门规定。

第三十二条 国家支持电信业务经营者、银行业金融机构、非银行支付机构、互联网服务提供者研究开发有关电信网络诈骗反制技术，用于监测识别、动态封堵和处置涉诈异常信息、活动。

国务院公安部门、金融管理部门、电信主管部门和国家网信部门等应当统筹

负责本行业领域反制技术措施建设，推进涉电信网络诈骗样本信息数据共享，加强涉诈用户信息交叉核验，建立有关涉诈异常信息、活动的监测识别、动态封堵和处置机制。

依据本法第十一条、第十二条、第十八条、第二十二条和前款规定， 对涉诈异常情形采取限制、暂停服务等处置措施的， 应当告知处置原因、救济渠道及需要提交的资料等事项，被处置对象可以向作出决定或者采取措施的部门、单位提出申诉。作出决定的部门、单位应当建立完善申诉渠道，及时受理申诉并核查，核查通过的，应当即时解除有关措施。

第三十三条 国家推进网络身份认证公共服务建设，支持个人、企业自愿使用，电信业务经营者、银行业金融机构、非银行支付机构、互联网服务提供者对存在涉诈异常的电话卡、银行账户、支付账户、互联网账号， 可以通过国家网络身份认证公共服务对用户身份重新进行核验。

第三十四条 公安机关应当会同金融、电信、网信部门组织银行业金融机构、非银行支付机构、电信业务经营者、互联网服务提供者等建立预警劝阻系统， 对预警发现的潜在被害人，根据情况及时采取相应劝阻措施。对电信网络诈骗案件应当加强追赃挽损，完善涉案资金处置制度，及时返还被害人的合法财产。对遭受重大生活困难的被害人，符合国家有关救助条件的，有关方面依照规定给予救助。

第三十五条 经国务院反电信网络诈骗工作机制决定或者批准，公安、金融、电信等部门对电信网络诈骗活动严重的特定地区，可以依照国家有关规定采取必要的临时风险防范措施。

第三十六条 对前往电信网络诈骗活动严重地区的人员，出境活动存在重大涉电信网络诈骗活动嫌疑的，移民管理机构可以决定不准其出境。

因从事电信网络诈骗活动受过刑事处罚的人员，设区的市级以上公安机关可以根据犯罪情况和预防再犯罪的需要，决定自处罚完毕之日起六个月至三年以内不准其出境，并通知移民管理机构执行。

第三十七条 国务院公安部门等会同外交部门加强国际执法司法合作，与有关国家、地区、国际组织建立有效合作机制， 通过开展国际警务合作等方式，提升在信息交流、调查取证、侦查抓捕、追赃挽损等方面的合作水平， 有效打击遏

制跨境电信网络诈骗活动。

第六章 法律责任

第三十八条 组织、策划、实施、参与电信网络诈骗活动或者为电信网络诈骗活动提供帮助，构成犯罪的，依法追究刑事责任。

前款行为尚不构成犯罪的，由公安机关处十日以上十五日以下拘留；没收违法所得，处违法所得一倍以上十倍以下罚款，没有违法所得或者违法所得不足一万元的，处十万元以下罚款。

第三十九条 电信业务经营者违反本法规定，有下列情形之一的，由有关主管部门责令改正，情节较轻的，给予警告、通报批评， 或者处五万元以上五十万元以下罚款；情节严重的，处五十万元以上五百万元以下罚款，并可以由有关主管部门责令暂停相关业务、停业整顿、吊销相关业务许可证或者吊销营业执照，对其直接负责的主管人员和其他直接责任人员，处一万元以上二十万元以下罚款：

(一)未落实国家有关规定确定的反电信网络诈骗内部控制机制的；

(二)未履行电话卡、物联网卡实名制登记职责的；

(三)未履行对电话卡、物联网卡的监测识别、监测预警和相关处置职责的；

(四)未对物联网卡用户进行风险评估，或者未限定物联网卡的开通功能、使用场景和适用设备的；

(五)未采取措施对改号电话、虚假主叫或者具有相应功能的非法设备进行监测处置的。

第四十条 银行业金融机构、非银行支付机构违反本法规定，有下列情形之一的，由有关主管部门责令改正，情节较轻的，给予警告、通报批评， 或者处五万元以上五十万元以下罚款；情节严重的，处五十万元以上五百万元以下罚款，并可以由有关主管部门责令停止新增业务、缩减业务类型或者业务范围、暂停相关业务、停业整顿、吊销相关业务许可证或者吊销营业执照， 对其直接负责的主管人员和其他直接责任人员，处一万元以上二十万元以下罚款：

(一)未落实国家有关规定确定的反电信网络诈骗内部控制机制的；

(二)未履行尽职调查义务和有关风险管理措施的；

(三)未履行对异常账户、可疑交易的风险监测和相关处置义务的；

(四)未按照规定完整、准确传输有关交易信息的。

第四十一条 电信业务经营者、互联网服务提供者违反本法规定，有下列情形之一的，由有关主管部门责令改正，情节较轻的，给予警告、通报批评， 或者处五万元以上五十万元以下罚款；情节严重的，处五十万元以上五百万元以下罚款，并可以由有关主管部门责令暂停相关业务、停业整顿、关闭网站或者应用程序、吊销相关业务许可证或者吊销营业执照， 对其直接负责的主管人员和其他直接责任人员，处一万元以上二十万元以下罚款：

(一)未落实国家有关规定确定的反电信网络诈骗内部控制机制的；

(二)未履行网络服务实名制职责，或者未对涉案、涉诈电话卡关联注册互联网账号进行核验的；

(三)未按照国家有关规定，核验域名注册、解析信息和互联网协议地址的真实性、准确性，规范域名跳转，或者记录并留存所提供相应服务的日志信息的；

(四)未登记核验移动互联网应用程序开发运营者的真实身份信息或者未核验应用程序的功能、用途，为其提供应用程序封装、分发服务的；

(五)未履行对涉诈互联网账号和应用程序，以及其他电信网络诈骗信息、活动的监测识别和处置义务的；

(六)拒不依法为查处电信网络诈骗犯罪提供技术支持和协助，或者未按规定移送有关违法犯罪线索、风险信息的。

第四十二条 违反本法第十四条、第二十五条第一款规定的，没收违法所得，由公安机关或者有关主管部门处违法所得一倍以上十倍以下罚款，没有违法所得或者违法所得不足五万元的，处五十万元以下罚款；情节严重的，由公安机关并处十五日以下拘留。

第四十三条 违反本法第二十五条第二款规定，由有关主管部门责令改正，情节较轻的，给予警告、通报批评， 或者处五万元以上五十万元以下罚款；情节严重的，处五十万元以上五百万元以下罚款，并可以由有关主管部门责令暂停相关业务、停业整顿、关闭网站或者应用程序， 对其直接负责的主管人员和其他直接责任人员，处一万元以上二十万元以下罚款。

第四十四条 违反本法第三十一条第一款规定的，没收违法所得，由公安机关处违法所得一倍以上十倍以下罚款，没有违法所得或者违法所得不足二万元的，处二十万元以下罚款；情节严重的，并处十五日以下拘留。

第四十五条 反电信网络诈骗工作有关部门、单位的工作人员滥用职权、玩忽职守、徇私舞弊， 或者有其他违反本法规定行为，构成犯罪的，依法追究刑事责任。

第四十六条 组织、策划、实施、参与电信网络诈骗活动或者为电信网络诈骗活动提供相关帮助的违法犯罪人员，除依法承担刑事责任、行政责任以外， 造成他人损害的，依照《中华人民共和国民法典》等法律的规定承担民事责任。

电信业务经营者、银行业金融机构、非银行支付机构、互联网服务提供者等违反本法规定，造成他人损害的，依照《中华人民共和国民法典》等法律的规定承担民事责任。

第四十七条 人民检察院在履行反电信网络诈骗职责中，对于侵害国家利益和社会公共利益的行为，可以依法向人民法院提起公益诉讼。

第四十八条 有关单位和个人对依照本法作出的行政处罚和行政强制措施决定不服的，可以依法申请行政复议或者提起行政诉讼。

第七章 附 则

第四十九条 反电信网络诈骗工作涉及的有关管理和责任制度，本法没有规定的，适用《中华人民共和国网络安全法》、《中华人民共和国个人信息保护法》、《中华人民共和国反洗钱法》等相关法律规定。

第五十条 本法自 2022 年 12 月 1 日起施行。

全国人民代表大会常务委员会关于维护互联网安全的决定

(2000 年 12 月 28 日第九届全国人民代表大会常务委员会第十九次会议通过 根据 2011 年 1 月 8 日《国务院关于废止和修改部分行政法规的决定》修订)

我国的互联网，在国家大力倡导和积极推动下，在经济建设和各项事业中得到日益广泛的应用，使人们的生产、工作、学习和生活方式已经开始并将继续发生深刻的变化，对于加快我国国民经济、科学技术的发展和社会服务信息化进程具有重要作用。同时， 如何保障互联网的运行安全和信息安全问题已经引起全社会的普遍关注。为了兴利除弊， 促进我国互联网的健康发展，维护国家安全和社会公共利益，保护个人、法人和其他组织的合法权益，特作如下决定：

一、为了保障互联网的运行安全， 对有下列行为之一，构成犯罪的，依照刑法有关规定追究刑事责任：

(一)侵入国家事务、国防建设、尖端科学技术领域的计算机信息系统;

(二)故意制作、传播计算机病毒等破坏性程序,攻击计算机系统及通信网络,致使计算机系统及通信网络遭受损害;

(三)违反国家规定,擅自中断计算机网络或者通信服务,造成计算机网络或者通信系统不能正常运行。

二、为了维护国家安全和社会稳定, 对有下列行为之一,构成犯罪的,依照刑法有关规定追究刑事责任:

(一)利用互联网造谣、诽谤或者发表、传播其他有害信息, 煽动颠覆国家政权、推翻社会主义制度,或者煽动分裂国家、破坏国家统一;

(二)通过互联网窃取、泄露国家秘密、情报或者军事秘密;

(三)利用互联网煽动民族仇恨、民族歧视,破坏民族团结;

(四)利用互联网组织邪教组织、联络邪教组织成员, 破坏国家法律、行政法规实施。

三、为了维护社会主义市场经济秩序和社会管理秩序,对有下列行为之一,构成犯罪的,依照刑法有关规定追究刑事责任:

(一)利用互联网销售伪劣产品或者对商品、服务作虚假宣传;

(二)利用互联网损害他人商业信誉和商品声誉;

(三)利用互联网侵犯他人知识产权;

(四)利用互联网编造并传播影响证券、期货交易或者其他扰乱金融秩序的虚假信息;

(五)在互联网上建立淫秽网站、网页, 提供淫秽站点链接服务,或者传播淫秽书刊、影片、音像、图片。

四、为了保护个人、法人和其他组织的人身、财产等合法权利, 对有下列行为之一,构成犯罪的,依照刑法有关规定追究刑事责任:

(一)利用互联网侮辱他人或者捏造事实诽谤他人;

(二)非法截获、篡改、删除他人电子邮件或者其他数据资料, 侵犯公民通信自由和通信秘密;

(三)利用互联网进行盗窃、诈骗、敲诈勒索。

五、利用互联网实施本决定第一条、第二条、第三条、第四条所列行为以外

的其他行为，构成犯罪的，依照刑法有关规定追究刑事责任。

六、利用互联网实施违法行为， 违反社会治安管理，尚不构成犯罪的，由公安机关依照《治安管理处罚法》予以处罚； 违反其他法律、行政法规， 尚不构成犯罪的，由有关行政管理部门依法给予行政处罚；对直接负责的主管人员和其他直接责任人员，依法给予行政处分或者纪律处分。

利用互联网侵犯他人合法权益，构成民事侵权的，依法承担民事责任。

七、各级人民政府及有关部门要采取积极措施， 在促进互联网的应用和网络技术的普及过程中，重视和支持对网络安全技术的研究和开发，增强网络的安全防护能力。有关主管部门要加强对互联网的运行安全和信息安全的宣传教育， 依法实施有效的监督管理，防范和制止利用互联网进行的各种违法活动，为互联网的健康发展创造良好的社会环境。从事互联网业务的单位要依法开展活动， 发现互联网上出现违法犯罪行为和有害信息时，要采取措施，停止传输有害信息，并及时向有关机关报告。任何单位和个人在利用互联网时， 都要遵纪守法，抵制各种违法犯罪行为和有害信息。人民法院、人民检察院、公安机关、国家安全机关要各司其职，密切配合，依法严厉打击利用互联网实施的各种犯罪活动。要动员全社会的力量，依靠全社会的共同努力，保障互联网的运行安全与信息安全，促进社会主义精神文明和物质文明建设。

全国人民代表大会常务委员会关于加强网络信息保护的决定

(2012 年 12 月 28 日第十一届全国人民代表大会常务委员会第三十次会议通过)

为了保护网络信息安全，保障公民、法人和其他组织的合法权益， 维护国家安全和社会公共利益，特作如下决定：

一、国家保护能够识别公民个人身份和涉及公民个人隐私的电子信息。

任何组织和个人不得窃取或者以其他非法方式获取公民个人电子信息，不得出售或者非法向他人提供公民个人电子信息。

二、网络服务提供者和其他企业事业单位在业务活动中收集、使用公民个人电子信息，应当遵循合法、正当、必要的原则，明示收集、使用信息的目的、方式和范围，并经被收集者同意，不得违反法律、法规的规定和双方的约定收集、使用信息。

网络服务提供者和其他企业事业单位收集、使用公民个人电子信息， 应当公

开其收集、使用规则。

三、网络服务提供者和其他企业事业单位及其工作人员对在业务活动中收集的公民个人电子信息必须严格保密，不得泄露、篡改、毁损， 不得出售或者非法向他人提供。

四、网络服务提供者和其他企业事业单位应当采取技术措施和其他必要措施，确保信息安全，防止在业务活动中收集的公民个人电子信息泄露、毁损、丢失。在发生或者可能发生信息泄露、毁损、丢失的情况时，应当立即采取补救措施。

五、网络服务提供者应当加强对其用户发布的信息的管理， 发现法律、法规禁止发布或者传输的信息的，应当立即停止传输该信息，采取消除等处置措施，保存有关记录，并向有关主管部门报告。

六、网络服务提供者为用户办理网站接入服务， 办理固定电话、移动电话等入网手续，或者为用户提供信息发布服务，应当在与用户签订协议或者确认提供服务时，要求用户提供真实身份信息。

七、任何组织和个人未经电子信息接收者同意或者请求， 或者电子信息接收者明确表示拒绝的，不得向其固定电话、移动电话或者个人电子邮箱发送商业性电子信息。

八、公民发现泄露个人身份、散布个人隐私等侵害其合法权益的网络信息，或者受到商业性电子信息侵扰的，有权要求网络服务提供者删除有关信息或者采取其他必要措施予以制止。

九、任何组织和个人对窃取或者以其他非法方式获取、出售或者非法向他人提供公民个人电子信息的违法犯罪行为以及其他网络信息违法犯罪行为，有权向有关主管部门举报、控告； 接到举报、控告的部门应当依法及时处理。被侵权人可以依法提起诉讼。

十、有关主管部门应当在各自职权范围内依法履行职责， 采取技术措施和其他必要措施，防范、制止和查处窃取或者以其他非法方式获取、出售或者非法向他人提供公民个人电子信息的违法犯罪行为以及其他网络信息违法犯罪行为。有关主管部门依法履行职责时，网络服务提供者应当予以配合，提供技术支持。

国家机关及其工作人员对在履行职责中知悉的公民个人电子信息应当予以保密，不得泄露、篡改、毁损，不得出售或者非法向他人提供。

十一、对有违反本决定行为的， 依法给予警告、罚款、没收违法所得、吊销许可证或者取消备案、关闭网站、禁止有关责任人员从事网络服务业务等处罚，记入社会信用档案并予以公布；构成违反治安管理行为的，依法给予治安管理处罚。构成犯罪的，依法追究刑事责任。侵害他人民事权益的，依法承担民事责任。

十二、本决定自公布之日起施行。

第二章 国务院

中华人民共和国计算机信息系统安全保护条例

（1994 年 2 月 18 日中华人民共和国国务院令第 147 号发布 根据 2011 年 1 月 8 日《国务院关于废止和修改部分行政法规的决定》修订）

第一章 总 则

第一条 为了保护计算机信息系统的安全，促进计算机的应用和发展，保障社会主义现代化建设的顺利进行，制定本条例。

第二条 本条例所称的计算机信息系统，是指由计算机及其相关的和配套的设备、设施(含网络)构成的，按照一定的应用目标和规则对信息进行采集、加工、存储、传输、检索等处理的人机系统。

第三条 计算机信息系统的安全保护，应当保障计算机及其相关的和配套的设备、设施(含网络)的安全，运行环境的安全，保障信息的安全，保障计算机功能的正常发挥，以维护计算机信息系统的安全运行。

第四条 计算机信息系统的安全保护工作，重点维护国家事务、经济建设、国防建设、尖端科学技术等重要领域的计算机信息系统的安全。

第五条 中华人民共和国境内的计算机信息系统的安全保护，适用本条例。

未联网的微型计算机的安全保护办法，另行制定。

第六条 公安部主管全国计算机信息系统安全保护工作。国家安全部、国家保密局和国务院其他有关部门，在国务院规定的职责范围内做好计算机信息系统安全保护的有关工作。

第七条 任何组织或个人，不得利用计算机信息系统从事危害国家利益、集体利益和公民合法利益的活动，不得危害计算机信息系统的安全。

第二章 安全保护制度

第八条 计算机信息系统的建设和应用，应当遵守法律、行政法规和国家其他有关规定。

第九条 计算机信息系统实行安全等级保护。安全等级的划分标准和安全等级保护的具体办法，由公安部会同有关部门制定。

第十条 计算机机房应当符合国家标准和国家有关规定。在计算机机房附近施工，不得危害计算机信息系统的安全。

第十一条 进行国际联网的计算机信息系统，由计算机信息系统的使用单位报省级以上人民政府公安机关备案。

第十二条 运输、携带、邮寄计算机信息媒体进出境的，应当如实向海关申报。

第十三条 计算机信息系统的使用单位应当建立健全安全管理制度，负责本单位计算机信息系统的安全保护工作。

第十四条 对计算机信息系统中发生的案件，有关使用单位应当在24小时内向当地县级以上人民政府公安机关报告。

第十五条 对计算机病毒和危害社会公共安全的其他有害数据的防治研究工作，由公安部归口管理。

第十六条 国家对计算机信息系统安全专用产品的销售实行许可证制度。具体办法由公安部会同有关部门制定。

第三章 安全监督

第十七条 公安机关对计算机信息系统保护工作行使下列监督职权：

(一)监督、检查、指导计算机信息系统安全保护工作；

(二)查处危害计算机信息系统安全的违法犯罪案件；

(三)履行计算机信息系统安全保护工作的其他监督职责。

第十八条 公安机关发现影响计算机信息系统安全的隐患时，应当及时通知使用单位采取安全保护措施。

第十九条 公安部在紧急情况下，可以就涉及计算机信息系统安全的特定事项发布专项通令。

第四章 法律责任

第二十条 违反本条例的规定，有下列行为之一的，由公安机关处以警告或

者停机整顿：

(一)违反计算机信息系统安全等级保护制度，危害计算机信息系统安全的；

(二)违反计算机信息系统国际联网备案制度的；

(三)不按照规定时间报告计算机信息系统中发生的案件的；

(四)接到公安机关要求改进安全状况的通知后，在限期内拒不改进的；

(五)有危害计算机信息系统安全的其他行为的。

第二十一条 计算机机房不符合国家标准和国家其他有关规定的，或者在计算机机房附近施工危害计算机信息系统安全的，由公安机关会同有关单位进行处理。

第二十二条 运输、携带、邮寄计算机信息媒体进出境，不如实向海关申报的，由海关依照《中华人民共和国海关法》和本条例以及其他有关法律、法规的规定处理。

第二十三条 故意输入计算机病毒以及其他有害数据危害计算机信息系统安全的，或者未经许可出售计算机信息系统安全专用产品的，由公安机关处

以警告或者对个人处以 5000 元以下的罚款、对单位处以 15000 元以下的罚款；有违法所得的，除予以没收外，可以处以违法所得 1 至 3 倍的罚款。

第二十四条 违反本条例的规定，构成违反治安管理行为的，依照《中华人民共和国治安管理处罚法》的有关规定处罚；构成犯罪的，依法追究刑事责任。

第二十五条 任何组织或者个人违反本条例的规定，给国家、集体或者他人财产造成损失的，应当依法承担民事责任。

第二十六条 当事人对公安机关依照本条例所作出的具体行政行为不服的，可以依法申请行政复议或者提起行政诉讼。

第二十七条 执行本条例的国家公务员利用职权，索取、收受贿赂或者有其他违法、失职行为， 构成犯罪的，依法追究刑事责任；尚不构成犯罪的，给予行政处分。

第五章 附 则

第二十八条 本条例下列用语的含义：

计算机病毒，是指编制或者在计算机程序中插入的破坏计算机功能或者毁坏数据，影响计算机使用，并能自我复制的一组计算机指令或者程序代码。

计算机信息系统安全专用产品，是指用于保护计算机信息系统安全的专用硬件和软件产品。

第二十九条 军队的计算机信息系统安全保护工作，按照军队的有关法规执行。

第三十条 公安部可以根据本条例制定实施办法。

第三十一条 本条例自发布之日起施行。

中华人民共和国计算机信息网络国际联网管理暂行规定

（1996 年 2 月 1 日中华人民共和国国务院令第 195 号发布 根据 1997 年 5 月 20 日《国务院关于修改〈中华人民共和国计算机信息网络国际联网管理暂行规定〉的决定》第一次修改 根据 2024 年年 3 月 10 日《国务院关于修改和废止部分行政法规的决定》第二次修改）

第一条 为了加强对计算机信息网络国际联网的管理，保障国际计算机信息交流的健康发展，制定本规定。

第二条 中华人民共和国境内的计算机信息网络进行国际联网，应当依照本规定办理。

第三条 本规定下列用语的含义是：

(一)计算机信息网络国际联网(以下简称国际联网)，是指中华人民共和国境内的计算机信息网络为实现信息的国际交流，同外国的计算机信息网络相联接。

(二)互联网络，是指直接进行国际联网的计算机信息网络；互联单位，是指负责互联网络运行的单位。

(三)接入网络，是指通过接入互联网络进行国际联网的计算机信息网络；接入单位，是指负责接入网络运行的单位。

第四条 国家对国际联网实行统筹规划、统一标准、分级管理、促进发展的原则。

第五条 国务院信息化工作领导小组(以下简称领导小组)，负责协调、解决有关国际联网工作中的重大问题。

领导小组办公室按照本规定制定具体管理办法，明确国际出入口信道提供单位、互联单位、接入单位和用户的权利、义务和责任，并负责对国际联网工

作的检查监督。

第六条 计算机信息网络直接进行国际联网，必须使用国家公用电信网提供的国际出入口信道。

任何单位和个人不得自行建立或者使用其他信道进行国际联网。

第七条 已经建立的互联网络，根据国务院有关规定调整后，分别由国务院电信主管部门、教育行政部门和中国科学院管理。

新建互联网络，必须报经国务院批准。

第八条 接入网络必须通过互联网络进行国际联网。

接入单位拟从事国际联网经营活动的，应当向有权受理从事国际联网经营活动申请的互联单位主管部门或者主管单位申请领取国际联网经营许可证；未取得国际联网经营许可证的，不得从事国际联网经营业务。

接入单位拟从事非经营活动的，应当报经有权受理从事非经营活动申请的互联单位主管部门或者主管单位审批；未经批准的，不得接入互联网络进行国际联网。

申请领取国际联网经营许可证或者办理审批手续时，应当提供其计算机信息网络的性质、应用范围和主机地址等资料。

国际联网经营许可证的格式，由领导小组统一制定。

第九条 从事国际联网经营活动的和从事非经营活动的接入单位都必须具备下列条件：

(一)是依法设立的企业法人或者事业法人；

(二)具有相应的计算机信息网络、装备以及相应的技术人员和管理人员；

(三)具有健全的安全保密管理制度和技术保护措施；

(四)符合法律和国务院规定的其他条件。

接入单位从事国际联网经营活动的，除必须具备本条前款规定条件外，还应当具备为用户提供长期服务的能力。

从事国际联网经营活动的接入单位的情况发生变化，不再符合本条第一款、第二款规定条件的，其国际联网经营许可证由发证机构予以吊销；从事非经营活动的接入单位的情况发生变化，不再符合本条第一款规定条件的，其国际联网资格由审批机构予以取消。

第十条 个人、法人和其他组织(以下统称用户)使用的计算机或者计算机信息网络，需要进行国际联网的，必须通过接入网络进行国际联网。

前款规定的计算机或者计算机信息网络，需要接入网络的，应当征得接入单位的同意，并办理登记手续。

第十一条 国际出入口信道提供单位、互联单位和接入单位，应当建立相应的网络管理中心，依照法律和国家有关规定加强对本单位及其用户的管理，做好网络信息安全管理工作，确保为用户提供良好、安全的服务。

第十二条 互联单位与接入单位，应当负责本单位及其用户有关国际联网的技术培训和管理教育工作。

第十三条 从事国际联网业务的单位和个人，应当遵守国家有关法律、行政法规，严格执行安全保密制度，不得利用国际联网从事危害国家安全、泄露国家秘密等违法犯罪活动，不得制作、查阅、复制和传播妨碍社会治安的信息和淫秽色情等信息。

第十四条 违反本规定第六条、第八条和第十条的规定的，由公安机关责令停止联网，给予警告，可以并处 15000 元以下的罚款；有违法所得的，没收违法所得。

第十五条 违反本规定，同时触犯其他有关法律、行政法规的，依照有关法律、行政法规的规定予以处罚；构成犯罪的，依法追究刑事责任。

第十六条 与台湾、香港、澳门地区的计算机信息网络的联网，参照本规定执行。

第十七条 本规定自发布之日起施行。

中华人民共和国计算机信息网络国际联网安全保护管理办法

(1997 年 12 月 11 日国务院批准 1997 年 12 月 16 日公安部令第 33 号发布 根据 2011 年 1 月 8 日国务院令第 588 号《国务院关于废止和修改部分行政法规的决定》修订)

第一章 总 则

第一条 为了加强对计算机信息网络国际联网的安全保护，维护公共秩序和社会稳定，根据《中华人民共和国计算机信息系统安全保护条例》、《中华人民共和国计算机信息网络国际联网管理暂行规定》和其他法律、行政法规的规

定，制定本办法。

第二条 中华人民共和国境内的计算机信息网络国际联网安全保护管理，适用本办法。

第三条 公安部计算机管理监察机构负责计算机信息网络国际联网的安全保护管理工作。

公安机关计算机管理监察机构应当保护计算机信息网络国际联网的公共安全，维护从事国际联网业务的单位和个人的合法权益和公众利益。

第四条 任何单位和个人不得利用国际联网危害国家安全、泄露国家秘密，不得侵犯国家的、社会的、集体的利益和公民的合法权益，不得从事违法犯罪活动。

第五条 任何单位和个人不得利用国际联网制作、复制、查阅和传播下列信息：

(一)煽动抗拒、破坏宪法和法律、行政法规实施的；

(二)煽动颠覆国家政权，推翻社会主义制度的；

(三)煽动分裂国家、破坏国家统一的；

(四)煽动民族仇恨、民族歧视，破坏民族团结的；

(五)捏造或者歪曲事实，散布谣言，扰乱社会秩序的；

(六)宣扬封建迷信、淫秽、色情、赌博、暴力、凶杀、恐怖，教唆犯罪的；

(七)公然侮辱他人或者捏造事实诽谤他人的；

(八)损害国家机关信誉的；

(九)其他违反宪法和法律、行政法规的。

第六条 任何单位和个人不得从事下列危害计算机信息网络安全的活动：

(一)未经允许，进入计算机信息网络或者使用计算机信息网络资源的；

(二)未经允许，对计算机信息网络功能进行删除、修改或者增加的；

(三)未经允许，对计算机信息网络中存储、处理或者传输的数据和应用程序进行删除、修改或者增加的；

(四)故意制作、传播计算机病毒等破坏性程序的；

(五)其他危害计算机信息网络安全的。

第七条 用户的通信自由和通信秘密受法律保护。任何单位和个人不得违反法律规定，利用国际联网侵犯用户的通信自由和通信秘密。

第二章 安全保护责任

第八条 从事国际联网业务的单位和个人应当接受公安机关的安全监督、检查和指导，如实向公安机关提供有关安全保护的信息、资料及数据文件，协助公安机关查处通过国际联网的计算机信息网络的违法犯罪行为。

第九条 国际出入口信道提供单位、互联单位的主管部门或者主管单位，应当依照法律和国家有关规定负责国际出入口信道、所属互联网络的安全保护管理工作。

第十条 互联单位、接入单位及使用计算机信息网络国际联网的法人和其他组织应当履行下列安全保护职责：

(一)负责本网络的安全保护管理工作，建立健全安全保护管理制度；

(二)落实安全保护技术措施，保障本网络的运行安全和信息安全；

(三)负责对本网络用户的安全教育和培训；

(四)对委托发布信息的单位和个人进行登记，并对所提供的信息内容按照本办法第五条进行审核；

(五)建立计算机信息网络电子公告系统的用户登记和信息管理制度；

(六)发现有本办法第四条、第五条、第六条、第七条所列情形之一的，应当保留有关原始记录，并在 24 小时内向当地公安机关报告；

(七)按照国家有关规定，删除本网络中含有本办法第五条内容的地址、目录或者关闭服务器。

第十一条 用户在接入单位办理入网手续时，应当填写用户备案表。备案表由公安部监制。

第十二条 互联单位、接入单位、使用计算机信息网络国际联网的法人和其他组织(包括跨省、自治区、直辖市联网的单位和所属的分支机构)，应当自网络正式联通之日起 30 日内，到所在地的省、自治区、直辖市人民政府公安机关指定的受理机关办理备案手续。

前款所列单位应当负责将接入本网络的接入单位和用户情况报当地公安机关备案，并及时报告本网络中接入单位和用户的变更情况。

第十三条 使用公用账号的注册者应当加强对公用账号的管理，建立账号使用登记制度。用户账号不得转借、转让。

第十四条 涉及国家事务、经济建设、国防建设、尖端科学技术等重要领域的单位办理备案手续时，应当出具其行政主管部门的审批证明。

前款所列单位的计算机信息网络与国际联网，应当采取相应的安全保护措施。

第三章 安全监督

第十五条 省、自治区、直辖市公安厅(局)，地(市)、县(市)公安局，应当有相应机构负责国际联网的安全保护管理工作。

第十六条 公安机关计算机管理监察机构应当掌握互联单位、接入单位和用户的备案情况，建立备案档案，进行备案统计，并按照国家有关规定逐级上报。

第十七条 公安机关计算机管理监察机构应当督促互联单位、接入单位及有关用户建立健全安全保护管理制度。监督、检查网络安全保护管理以及技术措施的落实情况。

公安机关计算机管理监察机构在组织安全检查时，有关单位应当派人参加。公安机关计算机管理监察机构对安全检查发现的问题，应当提出改进意见，作出详细记录，存档备查。

第十八条 公安机关计算机管理监察机构发现含有本办法第五条所列内容的地址、目录或者服务器时，应当通知有关单位关闭或者删除。

第十九条 公安机关计算机管理监察机构应当负责追踪和查处通过计算机信息网络的违法行为和针对计算机信息网络的犯罪案件，对违反本办法第四条、第七条规定的违法犯罪行为，应当按照国家有关规定移送有关部门或者司法机关处理。

第四章 法律责任

第二十条 违反法律、行政法规，有本办法第五条、第六条所列行为之一的，由公安机关给予警告，有违法所得的，没收违法所得，对个人可以并处5000元以下的罚款，对单位可以并处1.5万元以下的罚款；情节严重的，并可以给予6个月以内停止联网、停机整顿的处罚，必要时可以建议原发证、审批

机构吊销经营许可证或者取消联网资格；构成违反治安管理行为的，依照治安管理处罚法的规定处罚；构成犯罪的，依法追究刑事责任。

第二十一条 有下列行为之一的，由公安机关责令限期改正，给予警告，有违法所得的，没收违法所得；在规定的限期内未改正的，对单位的主管负责人员和其他直接责任人员可以并处 5000 元以下的罚款，对单位可以并处 1.5 万元以下的罚款；情节严重的，并可以给予 6 个月以内的停止联网、停机整顿的处罚，必要时可以建议原发证、审批机构吊销经营许可证或者取消联网资格。

(一)未建立安全保护管理制度的；

(二)未采取安全技术保护措施的；

(三)未对网络用户进行安全教育和培训的；

(四)未提供安全保护管理所需信息、资料及数据文件，或者所提供内容不真实的；

(五)对委托其发布的信息内容未进行审核或者对委托单位和个人未进行登记的；

(六)未建立电子公告系统的用户登记和信息管理制度的；

(七)未按照国家有关规定，删除网络地址、目录或者关闭服务器的；

(八)未建立公用账号使用登记制度的；

(九)转借、转让用户账号的。

第二十二条 违反本办法第四条、第七条规定的，依照有关法律、法规予以处罚。

第二十三条 违反本办法第十一条、第十二条规定，不履行备案职责的，由公安机关给予警告或者停机整顿不超过 6 个月的处罚。

第五章 附 则

第二十四条 与香港特别行政区和台湾、澳门地区联网的计算机信息网络的安全保护管理，参照本办法执行。

第二十五条 本办法自 1997 年 12 月 30 日起施行。

中华人民共和国电信条例

(2000 年 9 月 25 日中华人民共和国国务院令第 291 号公布 根据 2014 年 7 月 29 日《国务院关于修改部分行政法规的决定》第一次修订 根据 2016 年 2 月 6 日

《国务院关于修改部分行政法规的决定》第二次修订)

第一章 总 则

第一条 为了规范电信市场秩序，维护电信用户和电信业务经营者的合法权益，保障电信网络和信息的安全，促进电信业的健康发展，制定本条例。

第二条 在中华人民共和国境内从事电信活动或者与电信有关的活动，必须遵守本条例。

本条例所称电信，是指利用有线、无线的电磁系统或者光电系统， 传送、发射或者接收语音、文字、数据、图像以及其他任何形式信息的活动。

第三条 国务院信息产业主管部门依照本条例的规定对全国电信业实施监督管理。

省、自治区、直辖市电信管理机构在国务院信息产业主管部门的领导下， 依照本条例的规定对本行政区域内的电信业实施监督管理。

第四条 电信监督管理遵循政企分开、破除垄断、鼓励竞争、促进发展和公开、公平、公正的原则。

电信业务经营者应当依法经营，遵守商业道德，接受依法实施的监督检查。

第五条 电信业务经营者应当为电信用户提供迅速、准确、安全、方便和价格合理的电信服务。

第六条 电信网络和信息的安全受法律保护。任何组织或者个人不得利用电信网络从事危害国家安全、社会公共利益或者他人合法权益的活动。

第二章 电信市场

第一节 电信业务许可

第七条 国家对电信业务经营按照电信业务分类，实行许可制度。

经营电信业务，必须依照本条例的规定取得国务院信息产业主管部门或者省、自治区、直辖市电信管理机构颁发的电信业务经营许可证。

未取得电信业务经营许可证，任何组织或者个人不得从事电信业务经营活动。

第八条 电信业务分为基础电信业务和增值电信业务。

基础电信业务，是指提供公共网络基础设施、公共数据传送和基本话音通信服务的业务。增值电信业务， 是指利用公共网络基础设施提供的电信与信息服务的业务。

电信业务分类的具体划分在本条例所附的《电信业务分类目录》中列出。国务院信息产业主管部门根据实际情况，可以对目录所列电信业务分类项目作局部调整，重新公布。

第九条 经营基础电信业务，须经国务院信息产业主管部门审查批准，取得《基础电信业务经营许可证》。

经营增值电信业务，业务覆盖范围在两个以上省、自治区、直辖市的， 须经国务院信息产业主管部门审查批准，取得《跨地区增值电信业务经营许可证》；业务覆盖范围在一个省、自治区、直辖市行政区域内的， 须经省、自治区、直辖市电信管理机构审查批准，取得《增值电信业务经营许可证》。

运用新技术试办《电信业务分类目录》未列出的新型电信业务的，应当向省、自治区、直辖市电信管理机构备案。

第十条 经营基础电信业务，应当具备下列条件：

(一)经营者为依法设立的专门从事基础电信业务的公司，且公司中国有股权或者股份不少于 51%；

(二)有可行性研究报告和组网技术方案；

(三)有与从事经营活动相适应的资金和专业人员；

(四)有从事经营活动的场地及相应的资源；

(五)有为用户提供长期服务的信誉或者能力；

(六)国家规定的其他条件。

第十一条 申请经营基础电信业务，应当向国务院信息产业主管部门提出申请，并提交本条例第十条规定的相关文件。国务院信息产业主管部门应当自受理申请之日起 180 日内审查完毕，作出批准或者不予批准的决定。予以批准的， 颁发《基础电信业务经营许可证》；不予批准的，应当书面通知申请人并说明理由。

第十二条 国务院信息产业主管部门审查经营基础电信业务的申请时，应当考虑国家安全、电信网络安全、电信资源可持续利用、环境保护和电信市场的竞争状况等因素。

颁发《基础电信业务经营许可证》，应当按照国家有关规定采用招标方式。

第十三条 经营增值电信业务，应当具备下列条件：

(一)经营者为依法设立的公司；

(二)有与开展经营活动相适应的资金和专业人员;

(三)有为用户提供长期服务的信誉或者能力;

(四)国家规定的其他条件。

第十四条 申请经营增值电信业务,应当根据本条例第九条第二款的规定,向国务院信息产业主管部门或者省、自治区、直辖市电信管理机构提出申请, 并提交本条例第十三条规定的相关文件。申请经营的增值电信业务, 按照国家有关规定须经有关主管部门审批的,还应当提交有关主管部门审核同意的文件。国务院信息产业主管部门或者省、自治区、直辖市电信管理机构应当自收到申请之日起 60 日内审查完毕,作出批准或者不予批准的决定。予以批准的,颁发《跨地区增值电信业务经营许可证》或者《增值电信业务经营许可证》;不予批准的,应当书面通知申请人并说明理由。

第十五条 电信业务经营者在经营过程中,变更经营主体、业务范围或者停止经营的,应当提前 90 日向原颁发许可证的机关提出申请,并办理相应手续;停止经营的,还应当按照国家有关规定做好善后工作。

第十六条 专用电信网运营单位在所在地区经营电信业务的,应当依照本条例规定的条件和程序提出申请,经批准,取得电信业务经营许可证。

第二节 电信网间互联

第十七条 电信网之间应当按照技术可行、经济合理、公平公正、相互配合的原则,实现互联互通。

主导的电信业务经营者不得拒绝其他电信业务经营者和专用网运营单位提出的互联互通要求。

前款所称主导的电信业务经营者,是指控制必要的基础电信设施并且在电信业务市场中占有较大份额,能够对其他电信业务经营者进入电信业务市场构成实质性影响的经营者。

主导的电信业务经营者由国务院信息产业主管部门确定。

第十八条 主导的电信业务经营者应当按照非歧视和透明化的原则,制定包括网间互联的程序、时限、非捆绑网络元素目录等内容的互联规程。互联规程应当报国务院信息产业主管部门审查同意。该互联规程对主导的电信业务经营者的互联互通活动具有约束力。

第十九条 公用电信网之间、公用电信网与专用电信网之间的网间互联，由网间互联双方按照国务院信息产业主管部门的网间互联管理规定进行互联协商，并订立网间互联协议。

第二十条 网间互联双方经协商未能达成网间互联协议的，自一方提出互联要求之日起 60 日内，任何一方均可以按照网间互联覆盖范围向国务院信息产业主管部门或者省、自治区、直辖市电信管理机构申请协调； 收到申请的机关应当依照本条例第十七条第一款规定的原则进行协调，促使网间互联双方达成协议；自网间互联一方或者双方申请协调之日起 45 日内经协调仍不能达成协议的，由协调机关随机邀请电信技术专家和其他有关方面专家进行公开论证并提出网间互联方案。协调机关应当根据专家论证结论和提出的网间互联方案作出决定， 强制实现互联互通。

第二十一条 网间互联双方必须在协议约定或者决定规定的时限内实现互联互通，遵守网间互联协议和国务院信息产业主管部门的相关规定，保障网间通信畅通，任何一方不得擅自中断互联互通。网间互联遇有通信技术障碍的， 双方应当立即采取有效措施予以消除。网间互联双方在互联互通中发生争议的， 依照本条例第二十条规定的程序和办法处理。

网间互联的通信质量应当符合国家有关标准。主导的电信业务经营者向其他电信业务经营者提供网间互联，服务质量不得低于本网内的同类业务及向其子公司或者分支机构提供的同类业务质量。

第二十二条 网间互联的费用结算与分摊应当执行国家有关规定，不得在规定标准之外加收费用。

网间互联的技术标准、费用结算办法和具体管理规定， 由国务院信息产业主管部门制定。

第三节 电信资费

第二十三条 电信资费实行市场调节价。电信业务经营者应当统筹考虑生产经营成本、电信市场供求状况等因素，合理确定电信业务资费标准。

第二十四条 国家依法加强对电信业务经营者资费行为的监管，建立健全监管规则，维护消费者合法权益。

第二十五条 电信业务经营者应当根据国务院信息产业主管部门和省、自治

区、直辖市电信管理机构的要求， 提供准确、完备的业务成本数据及其他有关资料。

第四节 电信资源

第二十六条 国家对电信资源统一规划、集中管理、合理分配，实行有偿使用制度。

前款所称电信资源，是指无线电频率、卫星轨道位置、电信网码号等用于实现电信功能且有限的资源。

第二十七条 电信业务经营者占有、使用电信资源，应当缴纳电信资源费。具体收费办法由国务院信息产业主管部门会同国务院财政部门、价格主管部门制定，报国务院批准后公布施行。

第二十八条 电信资源的分配，应当考虑电信资源规划、用途和预期服务能力。

分配电信资源，可以采取指配的方式，也可以采用拍卖的方式。

取得电信资源使用权的，应当在规定的时限内启用所分配的资源，并达到规定的最低使用规模。未经国务院信息产业主管部门或者省、自治区、直辖市电信管理机构批准，不得擅自使用、转让、出租电信资源或者改变电信资源的用途。

第二十九条 电信资源使用者依法取得电信网码号资源后，主导的电信业务经营者和其他有关单位有义务采取必要的技术措施，配合电信资源使用者实现其电信网码号资源的功能。

法律、行政法规对电信资源管理另有特别规定的，从其规定。

第三章 电信服务

第三十条 电信业务经营者应当按照国家规定的电信服务标准向电信用户提供服务。电信业务经营者提供服务的种类、范围、资费标准和时限， 应当向社会公布，并报省、自治区、直辖市电信管理机构备案。

电信用户有权自主选择使用依法开办的各类电信业务。

第三十一条 电信用户申请安装、移装电信终端设备的，电信业务经营者应当在其公布的时限内保证装机开通；由于电信业务经营者的原因逾期未能装机开通的，应当每日按照收取的安装费、移装费或者其他费用数额 1%的比例，向电信用户支付违约金。

第三十二条 电信用户申告电信服务障碍的，电信业务经营者应当自接到申告之日起，城镇 48 小时、农村 72 小时内修复或者调通；不能按期修复或者调通的，应当及时通知电信用户，并免收障碍期间的月租费用。但是， 属于电信终端设备的原因造成电信服务障碍的除外。

第三十三条 电信业务经营者应当为电信用户交费和查询提供方便。电信用户要求提供国内长途通信、国际通信、移动通信和信息服务等收费清单的， 电信业务经营者应当免费提供。

电信用户出现异常的巨额电信费用时，电信业务经营者一经发现，应当尽可能迅速告知电信用户，并采取相应的措施。

前款所称巨额电信费用，是指突然出现超过电信用户此前 3 个月平均电信费用 5 倍以上的费用。

第三十四条 电信用户应当按照约定的时间和方式及时、足额地向电信业务经营者交纳电信费用；电信用户逾期不交纳电信费用的，电信业务经营者有权要求补交电信费用，并可以按照所欠费用每日加收 3‰的违约金。

对超过收费约定期限 30 日仍不交纳电信费用的电信用户，电信业务经营者可以暂停向其提供电信服务。电信用户在电信业务经营者暂停服务 60 日内仍未补交电信费用和违约金的，电信业务经营者可以终止提供服务，并可以依法追缴欠费和违约金。

经营移动电信业务的经营者可以与电信用户约定交纳电信费用的期限、方式，不受前款规定期限的限制。

电信业务经营者应当在迟延交纳电信费用的电信用户补足电信费用、违约金后的 48 小时内，恢复暂停的电信服务。

第三十五条 电信业务经营者因工程施工、网络建设等原因，影响或者可能影响正常电信服务的，必须按照规定的时限及时告知用户，并向省、自治区、直辖市电信管理机构报告。

因前款原因中断电信服务的，电信业务经营者应当相应减免用户在电信服务中断期间的相关费用。

出现本条第一款规定的情形，电信业务经营者未及时告知用户的，应当赔偿由此给用户造成的损失。

第三十六条 经营本地电话业务和移动电话业务的电信业务经营者，应当免费向用户提供火警、匪警、医疗急救、交通事故报警等公益性电信服务并保障通信线路畅通。

第三十七条 电信业务经营者应当及时为需要通过中继线接入其电信网的集团用户，提供平等、合理的接入服务。

未经批准，电信业务经营者不得擅自中断接入服务。

第三十八条 电信业务经营者应当建立健全内部服务质量管理制度，并可以制定并公布施行高于国家规定的电信服务标准的企业标准。

电信业务经营者应当采取各种形式广泛听取电信用户意见，接受社会监督，不断提高电信服务质量。

第三十九条 电信业务经营者提供的电信服务达不到国家规定的电信服务标准或者其公布的企业标准的，或者电信用户对交纳电信费用持有异议的，电信用户有权要求电信业务经营者予以解决；电信业务经营者拒不解决或者电信用户对解决结果不满意的，电信用户有权向国务院信息产业主管部门或者省、自治区、直辖市电信管理机构或者其他有关部门申诉。收到申诉的机关必须对申诉及时处理，并自收到申诉之日起 30 日内向申诉者作出答复。

电信用户对交纳本地电话费用有异议的，电信业务经营者还应当应电信用户的要求免费提供本地电话收费依据，并有义务采取必要措施协助电信用户查找原因。

第四十条 电信业务经营者在电信服务中，不得有下列行为：

(一)以任何方式限定电信用户使用其指定的业务；

(二)限定电信用户购买其指定的电信终端设备或者拒绝电信用户使用自备的已经取得入网许可的电信终端设备；

(三)无正当理由拒绝、拖延或者中止对电信用户的电信服务；

(四)对电信用户不履行公开作出的承诺或者作容易引起误解的虚假宣传；

(五)以不正当手段刁难电信用户或者对投诉的电信用户打击报复。

第四十一条 电信业务经营者在电信业务经营活动中，不得有下列行为：

(一)以任何方式限制电信用户选择其他电信业务经营者依法开办的电信服务；

(二)对其经营的不同业务进行不合理的交叉补贴;

(三)以排挤竞争对手为目的，低于成本提供电信业务或者服务，进行不正当竞争。

第四十二条 国务院信息产业主管部门或者省、自治区、直辖市电信管理机构应当依据职权对电信业务经营者的电信服务质量和经营活动进行监督检查，并向社会公布监督抽查结果。

第四十三条 电信业务经营者必须按照国家有关规定履行相应的电信普遍服务义务。

国务院信息产业主管部门可以采取指定的或者招标的方式确定电信业务经营者具体承担电信普遍服务的义务。

电信普遍服务成本补偿管理办法，由国务院信息产业主管部门会同国务院财政部门、价格主管部门制定，报国务院批准后公布施行。

第四章 电信建设

第一节 电信设施建设

第四十四条 公用电信网、专用电信网、广播电视传输网的建设应当接受国务院信息产业主管部门的统筹规划和行业管理。

属于全国性信息网络工程或者国家规定限额以上建设项目的公用电信网、专用电信网、广播电视传输网建设， 在按照国家基本建设项目审批程序报批前，应当征得国务院信息产业主管部门同意。

基础电信建设项目应当纳入地方各级人民政府城市建设总体规划和村镇、集镇建设总体规划。

第四十五条 城市建设和村镇、集镇建设应当配套设置电信设施。建筑物内的电信管线和配线设施以及建设项目用地范围内的电信管道，应当纳入建设项目的设计文件，并随建设项目同时施工与验收。所需经费应当纳入建设项目概算。

有关单位或者部门规划、建设道路、桥梁、隧道或者地下铁道等，应当事先通知省、自治区、直辖市电信管理机构和电信业务经营者， 协商预留电信管线等事宜。

第四十六条 基础电信业务经营者可以在民用建筑物上附挂电信线路或者设置小型天线、移动通信基站等公用电信设施， 但是应当事先通知建筑物产权人或

者使用人，并按照省、自治区、直辖市人民政府规定的标准向该建筑物的产权人或者其他权利人支付使用费。

第四十七条 建设地下、水底等隐蔽电信设施和高空电信设施，应当按照国家有关规定设置标志。

基础电信业务经营者建设海底电信缆线，应当征得国务院信息产业主管部门同意，并征求有关部门意见后，依法办理有关手续。海底电信缆线由国务院有关部门在海图上标出。

第四十八条 任何单位或者个人不得擅自改动或者迁移他人的电信线路及其他电信设施；遇有特殊情况必须改动或者迁移的，应当征得该电信设施产权人同意，由提出改动或者迁移要求的单位或者个人承担改动或者迁移所需费用，并赔偿由此造成的经济损失。

第四十九条 从事施工、生产、种植树木等活动，不得危及电信线路或者其他电信设施的安全或者妨碍线路畅通；可能危及电信安全时，应当事先通知有关电信业务经营者，并由从事该活动的单位或者个人负责采取必要的安全防护措施。

违反前款规定，损害电信线路或者其他电信设施或者妨碍线路畅通的，应当恢复原状或者予以修复，并赔偿由此造成的经济损失。

第五十条 从事电信线路建设，应当与已建的电信线路保持必要的安全距离；难以避开或者必须穿越，或者需要使用已建电信管道的，应当与已建电信线路的产权人协商，并签订协议；经协商不能达成协议的，根据不同情况，由国务院信息产业主管部门或者省、自治区、直辖市电信管理机构协调解决。

第五十一条 任何组织或者个人不得阻止或者妨碍基础电信业务经营者依法从事电信设施建设和向电信用户提供公共电信服务；但是，国家规定禁止或者限制进入的区域除外。

第五十二条 执行特殊通信、应急通信和抢修、抢险任务的电信车辆，经公安交通管理机关批准，在保障交通安全畅通的前提下可以不受各种禁止机动车通行标志的限制。

第二节 电信设备进网

第五十三条 国家对电信终端设备、无线电通信设备和涉及网间互联的设备实行进网许可制度。

接入公用电信网的电信终端设备、无线电通信设备和涉及网间互联的设备，必须符合国家规定的标准并取得进网许可证。

实行进网许可制度的电信设备目录，由国务院信息产业主管部门会同国务院产品质量监督部门制定并公布施行。

第五十四条 办理电信设备进网许可证的，应当向国务院信息产业主管部门提出申请，并附送经国务院产品质量监督部门认可的电信设备检测机构出具的检测报告或者认证机构出具的产品质量认证证书。

国务院信息产业主管部门应当自收到电信设备进网许可申请之日起 60 日内，对申请及电信设备检测报告或者产品质量认证证书审查完毕。经审查合格的， 颁发进网许可证；经审查不合格的，应当书面答复并说明理由。

第五十五条 电信设备生产企业必须保证获得进网许可的电信设备的质量稳定、可靠，不得降低产品质量和性能。

电信设备生产企业应当在其生产的获得进网许可的电信设备上粘贴进网许可标志。

国务院产品质量监督部门应当会同国务院信息产业主管部门对获得进网许可证的电信设备进行质量跟踪和监督抽查，公布抽查结果。

第五章 电信安全

第五十六条 任何组织或者个人不得利用电信网络制作、复制、发布、传播含有下列内容的信息：

(一)反对宪法所确定的基本原则的；

(二)危害国家安全，泄露国家秘密，颠覆国家政权，破坏国家统一的；

(三)损害国家荣誉和利益的；

(四)煽动民族仇恨、民族歧视，破坏民族团结的；

(五)破坏国家宗教政策，宣扬邪教和封建迷信的；

(六)散布谣言，扰乱社会秩序，破坏社会稳定的；

(七)散布淫秽、色情、赌博、暴力、凶杀、恐怖或者教唆犯罪的；

(八)侮辱或者诽谤他人，侵害他人合法权益的；

(九)含有法律、行政法规禁止的其他内容的。

第五十七条 任何组织或者个人不得有下列危害电信网络安全和信息安全的

行为：

(一)对电信网的功能或者存储、处理、传输的数据和应用程序进行删除或者修改；

(二)利用电信网从事窃取或者破坏他人信息、损害他人合法权益的活动；

(三)故意制作、复制、传播计算机病毒或者以其他方式攻击他人电信网络等电信设施；

(四)危害电信网络安全和信息安全的其他行为。

第五十八条 任何组织或者个人不得有下列扰乱电信市场秩序的行为：

(一)采取租用电信国际专线、私设转接设备或者其他方法， 擅自经营国际或者香港特别行政区、澳门特别行政区和台湾地区电信业务；

(二)盗接他人电信线路，复制他人电信码号，使用明知是盗接、复制的电信设施或者码号；

(三)伪造、变造电话卡及其他各种电信服务有价凭证；

(四)以虚假、冒用的身份证件办理入网手续并使用移动电话。

第五十九条 电信业务经营者应当按照国家有关电信安全的规定，建立健全内部安全保障制度，实行安全保障责任制。

第六十条 电信业务经营者在电信网络的设计、建设和运行中，应当做到与国家安全和电信网络安全的需求同步规划，同步建设，同步运行。

第六十一条 在公共信息服务中，电信业务经营者发现电信网络中传输的信息明显属于本条例第五十六条所列内容的，应当立即停止传输，保存有关记录，并向国家有关机关报告。

第六十二条 使用电信网络传输信息的内容及其后果由电信用户负责。

电信用户使用电信网络传输的信息属于国家秘密信息的，必须依照保守国家秘密法的规定采取保密措施。

第六十三条 在发生重大自然灾害等紧急情况下，经国务院批准，国务院信息产业主管部门可以调用各种电信设施，确保重要通信畅通。

第六十四条 在中华人民共和国境内从事国际通信业务，必须通过国务院信息产业主管部门批准设立的国际通信出入口局进行。

我国内地与香港特别行政区、澳门特别行政区和台湾地区之间的通信， 参照

前款规定办理。

第六十五条 电信用户依法使用电信的自由和通信秘密受法律保护。除因国家安全或者追查刑事犯罪的需要，由公安机关、国家安全机关或者人民检察院依照法律规定的程序对电信内容进行检查外，任何组织或者个人不得以任何理由对电信内容进行检查。

电信业务经营者及其工作人员不得擅自向他人提供电信用户使用电信网络所传输信息的内容。

第六章 罚则

第六十六条 违反本条例第五十六条、第五十七条的规定，构成犯罪的，依法追究刑事责任；尚不构成犯罪的，由公安机关、国家安全机关依照有关法律、行政法规的规定予以处罚。

第六十七条 有本条例第五十八条第(二)、(三)、(四)项所列行为之一，扰乱电信市场秩序，构成犯罪的，依法追究刑事责任；尚不构成犯罪的，由国务院信息产业主管部门或者省、自治区、直辖市电信管理机构依据职权责令改正， 没收违法所得，处违法所得 3 倍以上 5 倍以下罚款；没有违法所得或者违法所得不足 1 万元的，处 1 万元以上 10 万元以下罚款。

第六十八条 违反本条例的规定，伪造、冒用、转让电信业务经营许可证、电信设备进网许可证或者编造在电信设备上标注的进网许可证编号的，由国务院信息产业主管部门或者省、自治区、直辖市电信管理机构依据职权没收违法所得，处违法所得 3 倍以上 5 倍以下罚款；没有违法所得或者违法所得不足 1 万元的，处 1 万元以上 10 万元以下罚款。

第六十九条 违反本条例规定，有下列行为之一的，由国务院信息产业主管部门或者省、自治区、直辖市电信管理机构依据职权责令改正，没收违法所得，处违法所得 3 倍以上 5 倍以下罚款；没有违法所得或者违法所得不足 5 万元的，处 10 万元以上 100 万元以下罚款；情节严重的，责令停业整顿：

(一)违反本条例第七条第三款的规定或者有本条例第五十八条第(一)项所列行为，擅自经营电信业务的，或者超范围经营电信业务的；

(二)未通过国务院信息产业主管部门批准，设立国际通信出入口进行国际通信的；

(三)擅自使用、转让、出租电信资源或者改变电信资源用途的;

(四)擅自中断网间互联互通或者接入服务的;

(五)拒不履行普遍服务义务的。

第七十条 违反本条例的规定,有下列行为之一的,由国务院信息产业主管部门或者省、自治区、直辖市电信管理机构依据职权责令改正,没收违法所得,处违法所得 1 倍以上 3 倍以下罚款;没有违法所得或者违法所得不足 1 万元的,处 1 万元以上 10 万元以下罚款;情节严重的,责令停业整顿:

(一)在电信网间互联中违反规定加收费用的;

(二)遇有网间通信技术障碍,不采取有效措施予以消除的;

(三)擅自向他人提供电信用户使用电信网络所传输信息的内容的;

(四)拒不按照规定缴纳电信资源使用费的。

第七十一条 违反本条例第四十一条的规定,在电信业务经营活动中进行不正当竞争的,由国务院信息产业主管部门或者省、自治区、直辖市电信管理机构依据职权责令改正,处 10 万元以上 100 万元以下罚款;情节严重的,责令停业整顿。

第七十二条 违反本条例的规定,有下列行为之一的, 由国务院信息产业主管部门或者省、自治区、直辖市电信管理机构依据职权责令改正, 处 5 万元以上 50 万元以下罚款;情节严重的,责令停业整顿:

(一)拒绝其他电信业务经营者提出的互联互通要求的;

(二)拒不执行国务院信息产业主管部门或者省、自治区、直辖市电信管理机构依法作出的互联互通决定的;

(三)向其他电信业务经营者提供网间互联的服务质量低于本网及其子公司或者分支机构的。

第七十三条 违反本条例第三十三条第一款、第三十九条第二款的规定,电信业务经营者拒绝免费为电信用户提供国内长途通信、国际通信、移动通信和信息服务等收费清单,或者电信用户对交纳本地电话费用有异议并提出要求时,拒绝为电信用户免费提供本地电话收费依据的,由省、自治区、直辖市电信管理机构责令改正,并向电信用户赔礼道歉;拒不改正并赔礼道歉的,处以警告,并处 5000 元以上 5 万元以下的罚款。

第七十四条 违反本条例第四十条的规定，由省、自治区、直辖市电信管理机构责令改正，并向电信用户赔礼道歉，赔偿电信用户损失；拒不改正并赔礼道歉、赔偿损失的， 处以警告，并处 1 万元以上 10 万元以下的罚款；情节严重的，责令停业整顿。

第七十五条 违反本条例的规定，有下列行为之一的， 由省、自治区、直辖市电信管理机构责令改正，处 1 万元以上 10 万元以下的罚款：

(一)销售未取得进网许可的电信终端设备的；

(二)非法阻止或者妨碍电信业务经营者向电信用户提供公共电信服务的；

(三)擅自改动或者迁移他人的电信线路及其他电信设施的。

第七十六条 违反本条例的规定，获得电信设备进网许可证后降低产品质量和性能的，由产品质量监督部门依照有关法律、行政法规的规定予以处罚。

第七十七条 有本条例第五十六条、第五十七条和第五十八条所列禁止行为之一，情节严重的，由原发证机关吊销电信业务经营许可证。

国务院信息产业主管部门或者省、自治区、直辖市电信管理机构吊销电信业务经营许可证后，应当通知企业登记机关。

第七十八条 国务院信息产业主管部门或者省、自治区、直辖市电信管理机构工作人员玩忽职守、滥用职权、徇私舞弊，构成犯罪的，依法追究刑事责任；尚不构成犯罪的，依法给予行政处分。

第七章 附 则

第七十九条 外国的组织或者个人在中华人民共和国境内投资与经营电信业务和香港特别行政区、澳门特别行政区与台湾地区的组织或者个人在内地投资与经营电信业务的具体办法，由国务院另行制定。

第八十条 本条例自公布之日起施行。

附

电信业务分类目录

一、基础电信业务

(一)固定网络国内长途及本地电话业务；

(二)移动网络电话和数据业务；

(三)卫星通信及卫星移动通信业务；

(四)互联网及其他公共数据传送业务;

(五)带宽、波长、光纤、光缆、管道及其他网络元素出租、出售业务;

(六)网络承载、接入及网络外包等业务;

(七)国际通信基础设施、国际电信业务;

(八)无线寻呼业务;

(九)转售的基础电信业务。

第(八)、(九)项业务比照增值电信业务管理。

二、增值电信业务

(一)电子邮件;

(二)语音信箱;

(三)在线信息库存储和检索;

(四)电子数据交换;

(五)在线数据处理与交易处理;

(六)增值传真;

(七)互联网接入服务;

(八)互联网信息服务;

(九)可视电话会议服务。

地图管理条例

(2015 年 11 月 11 日国务院第 111 次常务会议通过 2015 年 11 月 26 日中华人民共和国国务院令第 664 号公布 自 2016 年 1 月 1 日起施行)

第一章 总 则

第一条 为了加强地图管理，维护国家主权、安全和利益，促进地理信息产业健康发展，为经济建设、社会发展和人民生活服务， 根据《中华人民共和国测绘法》，制定本条例。

第二条 在中华人民共和国境内从事向社会公开的地图的编制、审核、出版和互联网地图服务以及监督检查活动，应当遵守本条例。

第三条 地图工作应当遵循维护国家主权、保障地理信息安全、方便群众生活的原则。

地图的编制、审核、出版和互联网地图服务应当遵守有关保密法律、法规的

规定。

第四条 国务院测绘地理信息行政主管部门负责全国地图工作的统一监督管理。国务院其他有关部门按照国务院规定的职责分工，负责有关的地图工作。

县级以上地方人民政府负责管理测绘地理信息工作的行政部门（以下称测绘地理信息行政主管部门）负责本行政区域地图工作的统一监督管理。县级以上地方人民政府其他有关部门按照本级人民政府规定的职责分工，负责有关的地图工作。

第五条 各级人民政府及其有关部门、新闻媒体应当加强国家版图宣传教育，增强公民的国家版图意识。

国家版图意识教育应当纳入中小学教学内容。

公民、法人和其他组织应当使用正确表示国家版图的地图。

第六条 国家鼓励编制和出版符合标准和规定的各类地图产品，支持地理信息科学技术创新和产业发展，加快地理信息产业结构调整和优化升级，促进地理信息深层次应用。

县级以上人民政府应当建立健全政府部门间地理信息资源共建共享机制。

县级以上人民政府测绘地理信息行政主管部门应当采取有效措施，及时获取、处理、更新基础地理信息数据， 通过地理信息公共服务平台向社会提供地理信息公共服务，实现地理信息数据开放共享。

第二章 地图编制

第七条 从事地图编制活动的单位应当依法取得相应的测绘资质证书，并在资质等级许可的范围内开展地图编制工作。

第八条 编制地图，应当执行国家有关地图编制标准，遵守国家有关地图内容表示的规定。

地图上不得表示下列内容：

（一）危害国家统一、主权和领土完整的；

（二）危害国家安全、损害国家荣誉和利益的；

（三）属于国家秘密的；

（四）影响民族团结、侵害民族风俗习惯的；

（五）法律、法规规定不得表示的其他内容。

第九条 编制地图，应当选用最新的地图资料并及时补充或者更新，正确反映各要素的地理位置、形态、名称及相互关系，且内容符合地图使用目的。

编制涉及中华人民共和国国界的世界地图、全国地图， 应当完整表示中华人民共和国疆域。

第十条 在地图上绘制中华人民共和国国界、中国历史疆界、世界各国间边界、世界各国间历史疆界，应当遵守下列规定：

(一)中华人民共和国国界，按照中国国界线画法标准样图绘制；

(二)中国历史疆界，依据有关历史资料，按照实际历史疆界绘制；

(三)世界各国间边界，按照世界各国国界线画法参考样图绘制；

(四)世界各国间历史疆界，依据有关历史资料，按照实际历史疆界绘制。

中国国界线画法标准样图、世界各国国界线画法参考样图， 由外交部和国务院测绘地理信息行政主管部门拟订，报国务院批准后公布。

第十一条 在地图上绘制我国县级以上行政区域界线或者范围，应当符合行政区域界线标准画法图、国务院批准公布的特别行政区行政区域图和国家其他有关规定。

行政区域界线标准画法图由国务院民政部门和国务院测绘地理信息行政主管部门拟订，报国务院批准后公布。

第十二条 在地图上表示重要地理信息数据，应当使用依法公布的重要地理信息数据。

第十三条 利用涉及国家秘密的测绘成果编制地图的，应当依法使用经国务院测绘地理信息行政主管部门或者省、自治区、直辖市人民政府测绘地理信息行政主管部门进行保密技术处理的测绘成果。

第十四条 县级以上人民政府测绘地理信息行政主管部门应当向社会公布公益性地图，供无偿使用。

县级以上人民政府测绘地理信息行政主管部门应当及时组织收集与地图内容相关的行政区划、地名、交通、水系、植被、公共设施、居民点等的变更情况，用于定期更新公益性地图。有关部门和单位应当及时提供相关更新资料。

第三章 地图审核

第十五条 国家实行地图审核制度。

向社会公开的地图，应当报送有审核权的测绘地理信息行政主管部门审核。但是，景区图、街区图、地铁线路图等内容简单的地图除外。

地图审核不得收取费用。

第十六条 出版地图的，由出版单位送审；展示或者登载不属于出版物的地图的，由展示者或者登载者送审；进口不属于出版物的地图或者附着地图图形的产品的，由进口者送审；进口属于出版物的地图，依照《出版管理条例》的有关规定执行；出口不属于出版物的地图或者附着地图图形的产品的，由出口者送审；生产附着地图图形的产品的，由生产者送审。

送审应当提交以下材料：

(一)地图审核申请表；

(二)需要审核的地图样图或者样品；

(三)地图编制单位的测绘资质证书。

进口不属于出版物的地图和附着地图图形的产品的，仅需提交前款第一项、第二项规定的材料。利用涉及国家秘密的测绘成果编制地图的， 还应当提交保密技术处理证明。

第十七条 国务院测绘地理信息行政主管部门负责下列地图的审核：

(一)全国地图以及主要表现地为两个以上省、自治区、直辖市行政区域的地图；

(二)香港特别行政区地图、澳门特别行政区地图以及台湾地区地图；

(三)世界地图以及主要表现地为国外的地图；

(四)历史地图。

第十八条 省、自治区、直辖市人民政府测绘地理信息行政主管部门负责审核主要表现地在本行政区域范围内的地图。其中， 主要表现地在设区的市行政区域范围内不涉及国界线的地图，由设区的市级人民政府测绘地理信息行政主管部门负责审核。

第十九条 有审核权的测绘地理信息行政主管部门应当自受理地图审核申请之日起 20 个工作日内，作出审核决定。

时事宣传地图、时效性要求较高的图书和报刊等插附地图的， 应当自受理地图审核申请之日起 7 个工作日内，作出审核决定。

应急保障等特殊情况需要使用地图的，应当即送即审。

第二十条 涉及专业内容的地图，应当依照国务院测绘地理信息行政主管部门会同有关部门制定的审核依据进行审核。没有明确审核依据的， 由有审核权的测绘地理信息行政主管部门征求有关部门的意见，有关部门应当自收到征求意见材料之日起 20 个工作日内提出意见。征求意见时间不计算在地图审核的期限内。

世界地图、历史地图、时事宣传地图没有明确审核依据的， 由国务院测绘地理信息行政主管部门商外交部进行审核。

第二十一条 送审地图符合下列规定的，由有审核权的测绘地理信息行政主管部门核发地图审核批准文件，并注明审图号：

(一)符合国家有关地图编制标准，完整表示中华人民共和国疆域；

(二)国界、边界、历史疆界、行政区域界线或者范围、重要地理信息数据、地名等符合国家有关地图内容表示的规定；

(三)不含有地图上不得表示的内容。

地图审核批准文件和审图号应当在有审核权的测绘地理信息行政主管部门网站或者其他新闻媒体上及时公告。

第二十二条 经审核批准的地图，应当在地图或者附着地图图形的产品的适当位置显著标注审图号。其中，属于出版物的，应当在版权页标注审图号。

第二十三条 全国性中小学教学地图， 由国务院教育行政部门会同国务院测绘地理信息行政主管部门、外交部组织审定； 地方性中小学教学地图，由省、自治区、直辖市人民政府教育行政部门会同省、自治区、直辖市人民政府测绘地理信息行政主管部门组织审定。

第二十四条 任何单位和个人不得出版、展示、登载、销售、进口、出口不符合国家有关标准和规定的地图，不得携带、寄递不符合国家有关标准和规定的地图进出境。

进口、出口地图的，应当向海关提交地图审核批准文件和审图号。

第二十五条 经审核批准的地图，送审者应当按照有关规定向有审核权的测绘地理信息行政主管部门免费送交样本。

第四章 地图出版

第二十六条 县级以上人民政府出版行政主管部门应当加强对地图出版活动

的监督管理，依法对地图出版违法行为进行查处。

第二十七条 出版单位从事地图出版活动的，应当具有国务院出版行政主管部门审核批准的地图出版业务范围，并依照《出版管理条例》的有关规定办理审批手续。

第二十八条 出版单位根据需要，可以在出版物中插附经审核批准的地图。

第二十九条 任何出版单位不得出版未经审定的中小学教学地图。

第三十条 出版单位出版地图，应当按照国家有关规定向国家图书馆、中国版本图书馆和国务院出版行政主管部门免费送交样本。

第三十一条 地图著作权的保护，依照有关著作权法律、法规的规定执行。

第五章 互联网地图服务

第三十二条 国家鼓励和支持互联网地图服务单位开展地理信息开发利用和增值服务。

县级以上人民政府应当加强对互联网地图服务行业的政策扶持和监督管理。

第三十三条 互联网地图服务单位向公众提供地理位置定位、地理信息上传标注和地图数据库开发等服务的，应当依法取得相应的测绘资质证书。

互联网地图服务单位从事互联网地图出版活动的，应当经国务院出版行政主管部门依法审核批准。

第三十四条 互联网地图服务单位应当将存放地图数据的服务器设在中华人民共和国境内，并制定互联网地图数据安全管理制度和保障措施。

县级以上人民政府测绘地理信息行政主管部门应当会同有关部门加强对互联网地图数据安全的监督管理。

第三十五条 互联网地图服务单位收集、使用用户个人信息的，应当明示收集、使用信息的目的、方式和范围，并经用户同意。

互联网地图服务单位需要收集、使用用户个人信息的， 应当公开收集、使用规则，不得泄露、篡改、出售或者非法向他人提供用户的个人信息。

互联网地图服务单位应当采取技术措施和其他必要措施，防止用户的个人信息泄露、丢失。

第三十六条 互联网地图服务单位用于提供服务的地图数据库及其他数据库不得存储、记录含有按照国家有关规定在地图上不得表示的内容。互联网地图服

务单位发现其网站传输的地图信息含有不得表示的内容的，应当立即停止传输，保存有关记录，并向县级以上人民政府测绘地理信息行政主管部门、出版行政主管部门、网络安全和信息化主管部门等有关部门报告。

第三十七条 任何单位和个人不得通过互联网上传标注含有按照国家有关规定在地图上不得表示的内容。

第三十八条 互联网地图服务单位应当使用经依法审核批准的地图，加强对互联网地图新增内容的核查校对，并按照国家有关规定向国务院测绘地理信息行政主管部门或者省、自治区、直辖市测绘地理信息行政主管部门备案。

第三十九条 互联网地图服务单位对在工作中获取的涉及国家秘密、商业秘密的信息，应当保密。

第四十条 互联网地图服务单位应当加强行业自律，推进行业信用体系建设，提高服务水平。

第四十一条 从事互联网地图服务活动，适用本章的规定；本章没有规定的，适用本条例其他有关规定。

第六章 监督检查

第四十二条 县级以上人民政府及其有关部门应当依法加强对地图编制、出版、展示、登载、生产、销售、进口、出口等活动的监督检查。

第四十三条 县级以上人民政府测绘地理信息行政主管部门、出版行政主管部门和其他有关部门依法进行监督检查时，有权采取下列措施：

(一)进入涉嫌地图违法行为的场所实施现场检查；

(二)查阅、复制有关合同、票据、账簿等资料；

(三)查封、扣押涉嫌违法的地图、附着地图图形的产品以及用于实施地图违法行为的设备、工具、原材料等。

第四十四条 国务院测绘地理信息行政主管部门、国务院出版行政主管部门应当建立健全地图监督管理信息系统，实现信息资源共享，方便公众查询。

第四十五条 县级以上人民政府测绘地理信息行政主管部门应当根据国家有关标准和技术规范，加强地图质量监督管理。

地图编制、出版、展示、登载、生产、销售、进口、出口单位应当建立健全地图质量责任制度，采取有效措施，保证地图质量。

第四十六条 任何单位和个人对地图违法行为有权进行举报。

接到举报的人民政府或者有关部门应当及时依法调查处理，并为举报人保密。

第七章 法律责任

第四十七条 县级以上人民政府及其有关部门违反本条例规定，有下列行为之一的，由主管机关或者监察机关责令改正；情节严重的，对直接负责的主管人员和其他直接责任人员依法给予处分；直接负责的主管人员和其他直接责任人员的行为构成犯罪的，依法追究刑事责任：

(一)不依法作出行政许可决定或者办理批准文件的；

(二)发现违法行为或者接到对违法行为的举报不予查处的；

(三)其他未依照本条例规定履行职责的行为。

第四十八条 违反本条例规定，未取得测绘资质证书或者超越测绘资质等级许可的范围从事地图编制活动或者互联网地图服务活动的，依照《中华人民共和国测绘法》的有关规定进行处罚。

第四十九条 违反本条例规定，应当送审而未送审的，责令改正，给予警告，没收违法地图或者附着地图图形的产品，可以处 10 万元以下的罚款；有违法所得的，没收违法所得；构成犯罪的，依法追究刑事责任。

第五十条 违反本条例规定，不需要送审的地图不符合国家有关标准和规定的，责令改正，给予警告，没收违法地图或者附着地图图形的产品，可以处 10 万元以下的罚款；有违法所得的，没收违法所得；情节严重的， 可以向社会通报；构成犯罪的，依法追究刑事责任。

第五十一条 违反本条例规定，经审核不符合国家有关标准和规定的地图未按照审核要求修改即向社会公开的，责令改正，给予警告，没收违法地图或者附着地图图形的产品，可以处 10 万元以下的罚款；有违法所得的，没收违法所得；情节严重的，责令停业整顿，降低资质等级或者吊销测绘资质证书，可以向社会通报；构成犯罪的，依法追究刑事责任。

第五十二条 违反本条例规定，弄虚作假、伪造申请材料骗取地图审核批准文件，或者伪造、冒用地图审核批准文件和审图号的， 责令停止违法行为，给予警告，没收违法地图和附着地图图形的产品，并处 10 万元以上 20 万元以下的罚款；有违法所得的，没收违法所得；情节严重的，责令停业整顿，降低资质等级

或者吊销测绘资质证书；构成犯罪的，依法追究刑事责任。

第五十三条 违反本条例规定，未在地图的适当位置显著标注审图号，或者未按照有关规定送交样本的，责令改正，给予警告；情节严重的，责令停业整顿，降低资质等级或者吊销测绘资质证书。

第五十四条 违反本条例规定，互联网地图服务单位使用未经依法审核批准的地图提供服务，或者未对互联网地图新增内容进行核查校对的，责令改正，给予警告，可以处 20 万元以下的罚款；有违法所得的，没收违法所得；情节严重的，责令停业整顿，降低资质等级或者吊销测绘资质证书；构成犯罪的，依法追究刑事责任。

第五十五条 违反本条例规定，通过互联网上传标注了含有按照国家有关规定在地图上不得表示的内容的，责令改正，给予警告，可以处 10 万元以下的罚款；构成犯罪的，依法追究刑事责任。

第五十六条 本条例规定的降低资质等级、吊销测绘资质证书的行政处罚，由颁发资质证书的部门决定；其他行政处罚由县级以上人民政府测绘地理信息行政主管部门决定。

第八章 附 则

第五十七条 军队单位编制的地图的管理以及海图的管理，按照国务院、中央军事委员会的规定执行。

第五十八条 本条例自 2016 年 1 月 1 日起施行。国务院 1995 年 7 月 10 日发布的《中华人民共和国地图编制出版管理条例》同时废止。

中华人民共和国人类遗传资源管理条例

（2019 年 3 月 20 日国务院第 41 次常务会议通过 2019 年 5 月 28 日中华人民共和国国务院令第 717 号公布 自 2019 年 7 月 1 日起施行 根据 2024 年年 3 月 10 日《国务院关于修改和废止部分行政法规的决定》修改）

第一章 总 则

第一条 为了有效保护和合理利用我国人类遗传资源，维护公众健康、国家安全和社会公共利益，制定本条例。

第二条 本条例所称人类遗传资源包括人类遗传资源材料和人类遗传资源信息。

人类遗传资源材料是指含有人体基因组、基因等遗传物质的器官、组织、细胞等遗传材料。

人类遗传资源信息是指利用人类遗传资源材料产生的数据等信息资料。

第三条 采集、保藏、利用、对外提供我国人类遗传资源，应当遵守本条例。

为临床诊疗、采供血服务、查处违法犯罪、兴奋剂检测和殡葬等活动需要，采集、保藏器官、组织、细胞等人体物质及开展相关活动，依照相关法律、行政法规规定执行。

第四条 国务院卫生健康主管部门负责全国人类遗传资源管理工作；国务院其他有关部门在各自的职责范围内，负责有关人类遗传资源管理工作。

省、自治区、直辖市人民政府人类遗传资源主管部门负责本行政区域人类遗传资源管理工作；省、自治区、直辖市人民政府其他有关部门在各自的职责范围内，负责本行政区域有关人类遗传资源管理工作。

第五条 国家加强对我国人类遗传资源的保护，开展人类遗传资源调查，对重要遗传家系和特定地区人类遗传资源实行申报登记制度。

国务院卫生健康主管部门负责组织我国人类遗传资源调查，制定重要遗传家系和特定地区人类遗传资源申报登记具体办法。

第六条 国家支持合理利用人类遗传资源开展科学研究、发展生物医药产业、提高诊疗技术，提高我国生物安全保障能力，提升人民健康保障水平。

第七条 外国组织、个人及其设立或者实际控制的机构不得在我国境内采集、保藏我国人类遗传资源，不得向境外提供我国人类遗传资源。

第八条 采集、保藏、利用、对外提供我国人类遗传资源，不得危害我国公众健康、国家安全和社会公共利益。

第九条 采集、保藏、利用、对外提供我国人类遗传资源，应当符合伦理原则，并按照国家有关规定进行伦理审查。

采集、保藏、利用、对外提供我国人类遗传资源，应当尊重人类遗传资源提供者的隐私权，取得其事先知情同意，并保护其合法权益。

采集、保藏、利用、对外提供我国人类遗传资源，应当遵守国务院卫生健康主管部门制定的技术规范。

第十条 禁止买卖人类遗传资源。

为科学研究依法提供或者使用人类遗传资源并支付或者收取合理成本费用，不视为买卖。

第二章 采集和保藏

第十一条 采集我国重要遗传家系、特定地区人类遗传资源或者采集国务院卫生健康主管部门规定种类、数量的人类遗传资源的， 应当符合下列条件，并经国务院卫生健康主管部门批准：

(一)具有法人资格；

(二)采集目的明确、合法；

(三)采集方案合理；

(四)通过伦理审查；

(五)具有负责人类遗传资源管理的部门和管理制度；

(六)具有与采集活动相适应的场所、设施、设备和人员。

第十二条 采集我国人类遗传资源，应当事先告知人类遗传资源提供者采集目的、采集用途、对健康可能产生的影响、个人隐私保护措施及其享有的自愿参与和随时无条件退出的权利，征得人类遗传资源提供者书面同意。

在告知人类遗传资源提供者前款规定的信息时，必须全面、完整、真实、准确，不得隐瞒、误导、欺骗。

第十三条 国家加强人类遗传资源保藏工作，加快标准化、规范化的人类遗传资源保藏基础平台和人类遗传资源大数据建设，为开展相关研究开发活动提供支撑。

国家鼓励科研机构、高等学校、医疗机构、企业根据自身条件和相关研究开发活动需要开展人类遗传资源保藏工作，并为其他单位开展相关研究开发活动提供便利。

第十四条 保藏我国人类遗传资源、为科学研究提供基础平台的，应当符合下列条件，并经国务院卫生健康主管部门批准：

(一)具有法人资格；

(二)保藏目的明确、合法；

(三)保藏方案合理；

(四)拟保藏的人类遗传资源来源合法；

(五)通过伦理审查;

(六)具有负责人类遗传资源管理的部门和保藏管理制度;

(七)具有符合国家人类遗传资源保藏技术规范和要求的场所、设施、设备和人员。

第十五条 保藏单位应当对所保藏的人类遗传资源加强管理和监测，采取安全措施，制定应急预案，确保保藏、使用安全。

保藏单位应当完整记录人类遗传资源保藏情况，妥善保存人类遗传资源的来源信息和使用信息，确保人类遗传资源的合法使用。

保藏单位应当就本单位保藏人类遗传资源情况向国务院卫生健康主管部门提交年度报告。

第十六条 国家人类遗传资源保藏基础平台和数据库应当依照国家有关规定向有关科研机构、高等学校、医疗机构、企业开放。

为公众健康、国家安全和社会公共利益需要， 国家可以依法使用保藏单位保藏的人类遗传资源。

第三章 利用和对外提供

第十七条 国务院卫生健康主管部门和省、自治区、直辖市人民政府人类遗传资源主管部门应当会同本级人民政府有关部门对利用人类遗传资源开展科学研究、发展生物医药产业统筹规划， 合理布局，加强创新体系建设，促进生物科技和产业创新、协调发展。

第十八条 科研机构、高等学校、医疗机构、企业利用人类遗传资源开展研究开发活动，对其研究开发活动以及成果的产业化依照法律、行政法规和国家有关规定予以支持。

第十九条 国家鼓励科研机构、高等学校、医疗机构、企业根据自身条件和相关研究开发活动需要，利用我国人类遗传资源开展国际合作科学研究，提升相关研究开发能力和水平。

第二十条 利用我国人类遗传资源开展生物技术研究开发活动或者开展临床试验的，应当遵守有关生物技术研究、临床应用管理法律、行政法规和国家有关规定。

第二十一条 外国组织及外国组织、个人设立或者实际控制的机构(以下称外

方单位)需要利用我国人类遗传资源开展科学研究活动的，应当遵守我国法律、行政法规和国家有关规定，并采取与我国科研机构、高等学校、医疗机构、企业(以下称中方单位)合作的方式进行。

第二十二条 利用我国人类遗传资源开展国际合作科学研究的，应当符合下列条件，并由合作双方共同提出申请，经国务院卫生健康主管部门批准：

(一)对我国公众健康、国家安全和社会公共利益没有危害；

(二)合作双方为具有法人资格的中方单位、外方单位， 并具有开展相关工作的基础和能力；

(三)合作研究目的和内容明确、合法，期限合理；

(四)合作研究方案合理；

(五)拟使用的人类遗传资源来源合法，种类、数量与研究内容相符；

(六)通过合作双方各自所在国(地区)的伦理审查；

(七)研究成果归属明确，有合理明确的利益分配方案。

为获得相关药品和医疗器械在我国上市许可，在临床机构利用我国人类遗传资源开展国际合作临床试验、不涉及人类遗传资源材料出境的， 不需要审批。但是，合作双方在开展临床试验前应当将拟使用的人类遗传资源种类、数量及其用途向国务院卫生健康主管部门备案。国务院卫生健康主管部门和省、自治区、直辖市人民政府人类遗传资源主管部门加强对备案事项的监管。

第二十三条 在利用我国人类遗传资源开展国际合作科学研究过程中，合作方、研究目的、研究内容、合作期限等重大事项发生变更的， 应当办理变更审批手续。

第二十四条 利用我国人类遗传资源开展国际合作科学研究，应当保证中方单位及其研究人员在合作期间全过程、实质性地参与研究， 研究过程中的所有记录以及数据信息等完全向中方单位开放并向中方单位提供备份。

利用我国人类遗传资源开展国际合作科学研究，产生的成果申请专利的，应当由合作双方共同提出申请，专利权归合作双方共有。研究产生的其他科技成果，其使用权、转让权和利益分享办法由合作双方通过合作协议约定； 协议没有约定的，合作双方都有使用的权利，但向第三方转让须经合作双方同意，所获利益按合作双方贡献大小分享。

第二十五条 利用我国人类遗传资源开展国际合作科学研究，合作双方应当按照平等互利、诚实信用、共同参与、共享成果的原则， 依法签订合作协议，并依照本条例第二十四条的规定对相关事项作出明确、具体的约定。

第二十六条 利用我国人类遗传资源开展国际合作科学研究，合作双方应当在国际合作活动结束后 6 个月内共同向国务院卫生健康主管部门提交合作研究情况报告。

第二十七条 利用我国人类遗传资源开展国际合作科学研究，或者因其他特殊情况确需将我国人类遗传资源材料运送、邮寄、携带出境的，应当符合下列条件，并取得国务院卫生健康主管部门出具的人类遗传资源材料出境证明：

(一)对我国公众健康、国家安全和社会公共利益没有危害；

(二)具有法人资格；

(三)有明确的境外合作方和合理的出境用途；

(四)人类遗传资源材料采集合法或者来自合法的保藏单位；

(五)通过伦理审查。

利用我国人类遗传资源开展国际合作科学研究，需要将我国人类遗传资源材料运送、邮寄、携带出境的，可以单独提出申请，也可以在开展国际合作科学研究申请中列明出境计划一并提出申请，由国务院卫生健康主管部门合并审批。

将我国人类遗传资源材料运送、邮寄、携带出境的，凭人类遗传资源材料出境证明办理海关手续。

第二十八条 将人类遗传资源信息向外国组织、个人及其设立或者实际控制的机构提供或者开放使用，不得危害我国公众健康、国家安全和社会公共利益；可能影响我国公众健康、国家安全和社会公共利益的， 应当通过国务院卫生健康主管部门组织的安全审查。

将人类遗传资源信息向外国组织、个人及其设立或者实际控制的机构提供或者开放使用的，应当向国务院卫生健康主管部门备案并提交信息备份。

利用我国人类遗传资源开展国际合作科学研究产生的人类遗传资源信息，合作双方可以使用。

第四章 服务和监督

第二十九条 国务院卫生健康主管部门应当加强电子政务建设，方便申请人

利用互联网办理审批、备案等事项。

第三十条 国务院卫生健康主管部门应当制定并及时发布有关采集、保藏、利用、对外提供我国人类遗传资源的审批指南和示范文本，加强对申请人办理有关审批、备案等事项的指导。

第三十一条 国务院卫生健康主管部门应当聘请生物技术、医药、卫生、伦理、法律等方面的专家组成专家评审委员会，对依照本条例规定提出的采集、保藏我国人类遗传资源，开展国际合作科学研究以及将我国人类遗传资源材料运送、邮寄、携带出境的申请进行技术评审。评审意见作为作出审批决定的参考依据。

第三十二条 国务院卫生健康主管部门应当自受理依照本条例规定提出的采集、保藏我国人类遗传资源，开展国际合作科学研究以及将我国人类遗传资源材料运送、邮寄、携带出境申请之日起 20 个工作日内，作出批准或者不予批准的决定；不予批准的，应当说明理由。因特殊原因无法在规定期限内作出审批决定的，经国务院卫生健康主管部门负责人批准，可以延长 10 个工作日。

第三十三条 国务院卫生健康主管部门和省、自治区、直辖市人民政府人类遗传资源主管部门应当加强对采集、保藏、利用、对外提供人类遗传资源活动各环节的监督检查，发现违反本条例规定的，及时依法予以处理并向社会公布检查、处理结果。

第三十四条 国务院卫生健康主管部门和省、自治区、直辖市人民政府人类遗传资源主管部门进行监督检查，可以采取下列措施：

(一)进入现场检查；

(二)询问相关人员；

(三)查阅、复制有关资料；

(四)查封、扣押有关人类遗传资源。

第三十五条 任何单位和个人对违反本条例规定的行为，有权向国务院卫生健康主管部门和省、自治区、直辖市人民政府人类遗传资源主管部门投诉、举报。

国务院卫生健康主管部门和省、自治区、直辖市人民政府人类遗传资源主管部门应当公布投诉、举报电话和电子邮件地址，接受相关投诉、举报。对查证属实的，给予举报人奖励。

第五章 法律责任

第三十六条 违反本条例规定，有下列情形之一的，由国务院卫生健康主管部门责令停止违法行为，没收违法采集、保藏的人类遗传资源和违法所得，处 50 万元以上 500 万元以下罚款，违法所得在 100 万元以上的，处违法所得 5 倍以上 10 倍以下罚款：

(一)未经批准，采集我国重要遗传家系、特定地区人类遗传资源， 或者采集国务院卫生健康主管部门规定种类、数量的人类遗传资源；

(二)未经批准，保藏我国人类遗传资源；

(三)未经批准，利用我国人类遗传资源开展国际合作科学研究；

(四)未通过安全审查，将可能影响我国公众健康、国家安全和社会公共利益的人类遗传资源信息向外国组织、个人及其设立或者实际控制的机构提供或者开放使用；

(五)开展国际合作临床试验前未将拟使用的人类遗传资源种类、数量及其用途向国务院卫生健康主管部门备案。

第三十七条 提供虚假材料或者采取其他欺骗手段取得行政许可的， 由国务院卫生健康主管部门撤销已经取得的行政许可，处 50 万元以上 500 万元以下罚款，5 年内不受理相关责任人及单位提出的许可申请。

第三十八条 违反本条例规定，未经批准将我国人类遗传资源材料运送、邮寄、携带出境的， 由海关依照法律、行政法规的规定处罚。人类遗传资源主管部门应当配合海关开展鉴定等执法协助工作。海关应当将依法没收的人类遗传资源材料移送省、自治区、直辖市人民政府人类遗传资源主管部门进行处理。

第三十九条 违反本条例规定，有下列情形之一的，由省、自治区、直辖市人民政府人类遗传资源主管部门责令停止开展相关活动，没收违法采集、保藏的人类遗传资源和违法所得，处 50 万元以上 100 万元以下罚款，违法所得在 100 万元以上的，处违法所得 5 倍以上 10 倍以下罚款：

(一)采集、保藏、利用、对外提供我国人类遗传资源未通过伦理审查；

(二)采集我国人类遗传资源未经人类遗传资源提供者事先知情同意，或者采取隐瞒、误导、欺骗等手段取得人类遗传资源提供者同意；

(三)采集、保藏、利用、对外提供我国人类遗传资源违反相关技术规范；

(四)将人类遗传资源信息向外国组织、个人及其设立或者实际控制的机构提

供或者开放使用，未向国务院卫生健康主管部门备案或者提交信息备份。

第四十条 违反本条例规定，有下列情形之一的，由国务院卫生健康主管部门责令改正，给予警告，可以处 50 万元以下罚款：

(一)保藏我国人类遗传资源过程中未完整记录并妥善保存人类遗传资源的来源信息和使用信息；

(二)保藏我国人类遗传资源未提交年度报告；

(三)开展国际合作科学研究未及时提交合作研究情况报告。

第四十一条 外国组织、个人及其设立或者实际控制的机构违反本条例规定，在我国境内采集、保藏我国人类遗传资源，利用我国人类遗传资源开展科学研究，或者向境外提供我国人类遗传资源的，由国务院卫生健康主管部门责令停止违法行为，没收违法采集、保藏的人类遗传资源和违法所得，处 100 万元以上 1000 万元以下罚款，违法所得在 100 万元以上的，处违法所得 5 倍以上 10 倍以下罚款。

第四十二条 违反本条例规定，买卖人类遗传资源的， 由国务院卫生健康主管部门责令停止违法行为，没收违法采集、保藏的人类遗传资源和违法所得， 处 100 万元以上 1000 万元以下罚款，违法所得在 100 万元以上的，处违法所得 5 倍以上 10 倍以下罚款。

第四十三条 对有本条例第三十六条、第三十九条、第四十一条、第四十二条规定违法行为的单位，情节严重的，由国务院卫生健康主管部门或者省、自治区、直辖市人民政府人类遗传资源主管部门依据职责禁止其 1 至 5 年内从事采集、保藏、利用、对外提供我国人类遗传资源的活动；情节特别严重的，永久禁止其从事采集、保藏、利用、对外提供我国人类遗传资源的活动。

对有本条例第三十六条至第三十九条、第四十一条、第四十二条规定违法行为的单位的法定代表人、主要负责人、直接负责的主管人员以及其他责任人员，依法给予处分，并由国务院卫生健康主管部门或者省、自治区、直辖市人民政府人类遗传资源主管部门依据职责没收其违法所得，处 50 万元以下罚款；情节严重的，禁止其 1 至 5 年内从事采集、保藏、利用、对外提供我国人类遗传资源的活动；情节特别严重的，永久禁止其从事采集、保藏、利用、对外提供我国人类遗传资源的活动。

单位和个人有本条例规定违法行为的，记入信用记录，并依照有关法律、行政法规的规定向社会公示。

第四十四条 违反本条例规定，侵害他人合法权益的，依法承担民事责任；构成犯罪的，依法追究刑事责任。

第四十五条 国务院卫生健康主管部门和省、自治区、直辖市人民政府人类遗传资源主管部门的工作人员违反本条例规定，不履行职责或者滥用职权、玩忽职守、徇私舞弊的，依法给予处分；构成犯罪的，依法追究刑事责任。

第六章 附 则

第四十六条 人类遗传资源相关信息属于国家秘密的，应当依照《中华人民共和国保守国家秘密法》和国家其他有关保密规定实施保密管理。

第四十七条 本条例自 2019 年 7 月 1 日起施行。

互联网信息服务管理办法

（2000 年 9 月 25 日中华人民共和国国务院令第 292 号公布 根据 2011 年 1 月 8 日《国务院关于废止和修改部分行政法规的决定》修订）

第一条 为了规范互联网信息服务活动，促进互联网信息服务健康有序发展，制定本办法。

第二条 在中华人民共和国境内从事互联网信息服务活动，必须遵守本办法。

本办法所称互联网信息服务，是指通过互联网向上网用户提供信息的服务活动。

第三条 互联网信息服务分为经营性和非经营性两类。

经营性互联网信息服务，是指通过互联网向上网用户有偿提供信息或者网页制作等服务活动。

非经营性互联网信息服务，是指通过互联网向上网用户无偿提供具有公开性、共享性信息的服务活动。

第四条 国家对经营性互联网信息服务实行许可制度；对非经营性互联网信息服务实行备案制度。

未取得许可或者未履行备案手续的，不得从事互联网信息服务。

第五条 从事新闻、出版、教育、医疗保健、药品和医疗器械等互联网信息服务，依照法律、行政法规以及国家有关规定须经有关主管部门审核同意的， 在

申请经营许可或者履行备案手续前，应当依法经有关主管部门审核同意。

第六条 从事经营性互联网信息服务，除应当符合《中华人民共和国电信条例》规定的要求外，还应当具备下列条件：

(一)有业务发展计划及相关技术方案；

(二)有健全的网络与信息安全保障措施，包括网站安全保障措施、信息安全保密管理制度、用户信息安全管理制度；

(三)服务项目属于本办法第五条规定范围的，已取得有关主管部门同意的文件。

第七条 从事经营性互联网信息服务，应当向省、自治区、直辖市电信管理机构或者国务院信息产业主管部门申请办理互联网信息服务增值电信业务经营许可证(以下简称经营许可证)。

省、自治区、直辖市电信管理机构或者国务院信息产业主管部门应当自收到申请之日起 60 日内审查完毕，作出批准或者不予批准的决定。予以批准的，颁发经营许可证；不予批准的，应当书面通知申请人并说明理由。

申请人取得经营许可证后，应当持经营许可证向企业登记机关办理登记手续。

第八条 从事非经营性互联网信息服务，应当向省、自治区、直辖市电信管理机构或者国务院信息产业主管部门办理备案手续。办理备案时， 应当提交下列材料：

(一)主办单位和网站负责人的基本情况；

(二)网站网址和服务项目；

(三)服务项目属于本办法第五条规定范围的，已取得有关主管部门的同意文件。

省、自治区、直辖市电信管理机构对备案材料齐全的，应当予以备案并编号。

第九条 从事互联网信息服务，拟开办电子公告服务的，应当在申请经营性互联网信息服务许可或者办理非经营性互联网信息服务备案时，按照国家有关规定提出专项申请或者专项备案。

第十条 省、自治区、直辖市电信管理机构和国务院信息产业主管部门应当公布取得经营许可证或者已履行备案手续的互联网信息服务提供者名单。

第十一条 互联网信息服务提供者应当按照经许可或者备案的项目提供服务，

不得超出经许可或者备案的项目提供服务。

非经营性互联网信息服务提供者不得从事有偿服务。

互联网信息服务提供者变更服务项目、网站网址等事项的，应当提前 30 日向原审核、发证或者备案机关办理变更手续。

第十二条 互联网信息服务提供者应当在其网站主页的显著位置标明其经营许可证编号或者备案编号。

第十三条 互联网信息服务提供者应当向上网用户提供良好的服务，并保证所提供的信息内容合法。

第十四条 从事新闻、出版以及电子公告等服务项目的互联网信息服务提供者，应当记录提供的信息内容及其发布时间、互联网地址或者域名； 互联网接入服务提供者应当记录上网用户的上网时间、用户账号、互联网地址或者域名、主叫电话号码等信息。

互联网信息服务提供者和互联网接入服务提供者的记录备份应当保存 60 日，并在国家有关机关依法查询时，予以提供。

第十五条 互联网信息服务提供者不得制作、复制、发布、传播含有下列内容的信息：

(一)反对宪法所确定的基本原则的；

(二)危害国家安全，泄露国家秘密，颠覆国家政权，破坏国家统一的；

(三)损害国家荣誉和利益的；

(四)煽动民族仇恨、民族歧视，破坏民族团结的；

(五)破坏国家宗教政策，宣扬邪教和封建迷信的；

(六)散布谣言，扰乱社会秩序，破坏社会稳定的；

(七)散布淫秽、色情、赌博、暴力、凶杀、恐怖或者教唆犯罪的；

(八)侮辱或者诽谤他人，侵害他人合法权益的；

(九)含有法律、行政法规禁止的其他内容的。

第十六条 互联网信息服务提供者发现其网站传输的信息明显属于本办法第十五条所列内容之一的，应当立即停止传输，保存有关记录，并向国家有关机关报告。

第十七条 经营性互联网信息服务提供者申请在境内境外上市或者同外商合

资、合作， 应当事先经国务院信息产业主管部门审查同意；其中，外商投资的比例应当符合有关法律、行政法规的规定。

第十八条 国务院信息产业主管部门和省、自治区、直辖市电信管理机构，依法对互联网信息服务实施监督管理。

新闻、出版、教育、卫生、药品监督管理、工商行政管理和公安、国家安全等有关主管部门，在各自职责范围内依法对互联网信息内容实施监督管理。

第十九条 违反本办法的规定，未取得经营许可证，擅自从事经营性互联网信息服务，或者超出许可的项目提供服务的，由省、自治区、直辖市电信管理机构责令限期改正，有违法所得的，没收违法所得，处违法所得 3 倍以上 5 倍以下的罚款；没有违法所得或者违法所得不足 5 万元的，处 10 万元以上 100 万元以下的罚款；情节严重的，责令关闭网站。

违反本办法的规定，未履行备案手续，擅自从事非经营性互联网信息服务，或者超出备案的项目提供服务的，由省、自治区、直辖市电信管理机构责令限期改正；拒不改正的，责令关闭网站。

第二十条 制作、复制、发布、传播本办法第十五条所列内容之一的信息，构成犯罪的，依法追究刑事责任；尚不构成犯罪的，由公安机关、国家安全机关依照《中华人民共和国治安管理处罚法》、《计算机信息网络国际联网安全保护管理办法》等有关法律、行政法规的规定予以处罚； 对经营性互联网信息服务提供者，并由发证机关责令停业整顿直至吊销经营许可证，通知企业登记机关；对非经营性互联网信息服务提供者，并由备案机关责令暂时关闭网站直至关闭网站。

第二十一条 未履行本办法第十四条规定的义务的，由省、自治区、直辖市电信管理机构责令改正；情节严重的，责令停业整顿或者暂时关闭网站。

第二十二条 违反本办法的规定，未在其网站主页上标明其经营许可证编号或者备案编号的，由省、自治区、直辖市电信管理机构责令改正，处 5000 元以上 5 万元以下的罚款。

第二十三条 违反本办法第十六条规定的义务的，由省、自治区、直辖市电信管理机构责令改正；情节严重的，对经营性互联网信息服务提供者，并由发证机关吊销经营许可证，对非经营性互联网信息服务提供者，并由备案机关责令关闭网站。

第二十四条 互联网信息服务提供者在其业务活动中，违反其他法律、法规的，由新闻、出版、教育、卫生、药品监督管理和工商行政管理等有关主管部门依照有关法律、法规的规定处罚。

第二十五条 电信管理机构和其他有关主管部门及其工作人员，玩忽职守、滥用职权、徇私舞弊， 疏于对互联网信息服务的监督管理，造成严重后果，构成犯罪的，依法追究刑事责任；尚不构成犯罪的，对直接负责的主管人员和其他直接责任人员依法给予降级、撤职直至开除的行政处分。

第二十六条 在本办法公布前从事互联网信息服务的，应当自本办法公布之日起 60 日内依照本办法的有关规定补办有关手续。

第二十七条 本办法自公布之日起施行。

计算机软件保护条例

(2001 年 12 月 20 日中华人民共和国国务院令第 339 号公布 根据 2011 年 1 月 8 日《国务院关于废止和修改部分行政法规的决定》第一次修订 根据 2013 年 1 月 30 日《国务院关于修改〈计算机软件保护条例〉的决定》第二次修订)

第一章 总 则

第一条 为了保护计算机软件著作权人的权益，调整计算机软件在开发、传播和使用中发生的利益关系，鼓励计算机软件的开发与应用，促进软件产业和国民经济信息化的发展，根据《中华人民共和国著作权法》，制定本条例。

第二条 本条例所称计算机软件(以下简称软件)，是指计算机程序及其有关文档。

第三条 本条例下列用语的含义：

(一)计算机程序，是指为了得到某种结果而可以由计算机等具有信息处理能力的装置执行的代码化指令序列，或者可以被自动转换成代码化指令序列的符号化指令序列或者符号化语句序列。同一计算机程序的源程序和目标程序为同一作品。

(二)文档，是指用来描述程序的内容、组成、设计、功能规格、开发情况、测试结果及使用方法的文字资料和图表等，如程序设计说明书、流程图、用户手册等。

(三)软件开发者，是指实际组织开发、直接进行开发， 并对开发完成的软件

承担责任的法人或者其他组织；或者依靠自己具有的条件独立完成软件开发，并对软件承担责任的自然人。

(四)软件著作权人，是指依照本条例的规定，对软件享有著作权的自然人、法人或者其他组织。

第四条 受本条例保护的软件必须由开发者独立开发，并已固定在某种有形物体上。

第五条 中国公民、法人或者其他组织对其所开发的软件，不论是否发表，依照本条例享有著作权。

外国人、无国籍人的软件首先在中国境内发行的，依照本条例享有著作权。

外国人、无国籍人的软件， 依照其开发者所属国或者经常居住地国同中国签订的协议或者依照中国参加的国际条约享有的著作权，受本条例保护。

第六条 本条例对软件著作权的保护不延及开发软件所用的思想、处理过程、操作方法或者数学概念等。

第七条 软件著作权人可以向国务院著作权行政管理部门认定的软件登记机构办理登记。软件登记机构发放的登记证明文件是登记事项的初步证明。

办理软件登记应当缴纳费用。软件登记的收费标准由国务院著作权行政管理部门会同国务院价格主管部门规定。

第二章 软件著作权

第八条 软件著作权人享有下列各项权利：

(一)发表权，即决定软件是否公之于众的权利；

(二)署名权，即表明开发者身份，在软件上署名的权利；

(三)修改权，即对软件进行增补、删节，或者改变指令、语句顺序的权利；

(四)复制权，即将软件制作一份或者多份的权利；

(五)发行权，即以出售或者赠与方式向公众提供软件的原件或者复制件的权利；

(六)出租权，即有偿许可他人临时使用软件的权利，但是软件不是出租的主要标的的除外；

(七)信息网络传播权，即以有线或者无线方式向公众提供软件，使公众可以在其个人选定的时间和地点获得软件的权利；

(八)翻译权，即将原软件从一种自然语言文字转换成另一种自然语言文字的权利；

(九)应当由软件著作权人享有的其他权利。

软件著作权人可以许可他人行使其软件著作权，并有权获得报酬。

软件著作权人可以全部或者部分转让其软件著作权，并有权获得报酬。

第九条 软件著作权属于软件开发者，本条例另有规定的除外。

如无相反证明，在软件上署名的自然人、法人或者其他组织为开发者。

第十条 由两个以上的自然人、法人或者其他组织合作开发的软件，其著作权的归属由合作开发者签订书面合同约定。无书面合同或者合同未作明确

约定，合作开发的软件可以分割使用的，开发者对各自开发的部分可以单独享有著作权；但是，行使著作权时，不得扩展到合作开发的软件整体的著作权。合作开发

的软件不能分割使用的，其著作权由各合作开发者共同享有，通过协商一致行使；不能协商一致，又无正当理由的，任何一方不得阻止他方行使除转让权以外的其他

权利，但是所得收益应当合理分配给所有合作开发者。

第十一条 接受他人委托开发的软件，其著作权的归属由委托人与受托人签订书面合同约定；无书面合同或者合同未作明确约定的，其著作权由受托人享有。

第十二条 由国家机关下达任务开发的软件，著作权的归属与行使由项目任务书或者合同规定；项目任务书或者合同中未作明确规定的，软件著作权由接受任务的法人或者其他组织享有。

第十三条 自然人在法人或者其他组织中任职期间所开发的软件有下列情形之一的，该软件著作权由该法人或者其他组织享有，该法人或者其他组织可以对开发软件的自然人进行奖励：

(一)针对本职工作中明确指定的开发目标所开发的软件；

(二)开发的软件是从事本职工作活动所预见的结果或者自然的结果；

(三)主要使用了法人或者其他组织的资金、专用设备、未公开的专门信息等物质技术条件所开发并由法人或者其他组织承担责任的软件。

第十四条 软件著作权自软件开发完成之日起产生。

自然人的软件著作权，保护期为自然人终生及其死亡后 50 年，截止于自然人死亡后第 50 年的 12 月 31 日；软件是合作开发的，截止于最后死亡的自然人死亡后第 50 年的 12 月 31 日。

法人或者其他组织的软件著作权，保护期为 50 年，截止于软件首次发表后第 50 年的 12 月 31 日，但软件自开发完成之日起 50 年内未发表的，本条例不再保护。

第十五条 软件著作权属于自然人的，该自然人死亡后，在软件著作权的保护期内，软件著作权的继承人可以依照《中华人民共和国继承法》的有关规定，继承本条例第八条规定的除署名权以外的其他权利。

软件著作权属于法人或者其他组织的，法人或者其他组织变更、终止后， 其著作权在本条例规定的保护期内由承受其权利义务的法人或者其他组织享有；没有承受其权利义务的法人或者其他组织的，由国家享有。

第十六条 软件的合法复制品所有人享有下列权利：

(一)根据使用的需要把该软件装入计算机等具有信息处理能力的装置内；

(二)为了防止复制品损坏而制作备份复制品。这些备份复制品不得通过任何方式提供给他人使用，并在所有人丧失该合法复制品的所有权时，负责将备份复制品销毁；

(三)为了把该软件用于实际的计算机应用环境或者改进其功能、性能而进行必要的修改；但是，除合同另有约定外，未经该软件著作权人许可，不得向任何第三方提供修改后的软件。

第十七条 为了学习和研究软件内含的设计思想和原理，通过安装、显示、传输或者存储软件等方式使用软件的，可以不经软件著作权人许可，不向其支付报酬。

第三章 软件著作权的许可使用和转让

第十八条 许可他人行使软件著作权的，应当订立许可使用合同。

许可使用合同中软件著作权人未明确许可的权利，被许可人不得行使。

第十九条 许可他人专有行使软件著作权的，当事人应当订立书面合同。

没有订立书面合同或者合同中未明确约定为专有许可的，被许可行使的权利应当视为非专有权利。

第二十条 转让软件著作权的，当事人应当订立书面合同。

第二十一条 订立许可他人专有行使软件著作权的许可合同，或者订立转让软件著作权合同，可以向国务院著作权行政管理部门认定的软件登记机构登记。

第二十二条 中国公民、法人或者其他组织向外国人许可或者转让软件著作权的，应当遵守《中华人民共和国技术进出口管理条例》的有关规定。

第四章 法律责任

第二十三条 除《中华人民共和国著作权法》或者本条例另有规定外，有下列侵权行为的，应当根据情况，承担停止侵害、消除影响、赔礼道歉、赔偿损失等民事责任：

(一)未经软件著作权人许可，发表或者登记其软件的；

(二)将他人软件作为自己的软件发表或者登记的；

(三)未经合作者许可，将与他人合作开发的软件作为自己单独完成的软件发表或者登记的；

(四)在他人软件上署名或者更改他人软件上的署名的；

(五)未经软件著作权人许可，修改、翻译其软件的；

(六)其他侵犯软件著作权的行为。

第二十四条 除《中华人民共和国著作权法》、本条例或者其他法律、行政法规另有规定外，未经软件著作权人许可，有下列侵权行为的，应当根据情况，承担停止侵害、消除影响、赔礼道歉、赔偿损失等民事责任； 同时损害社会公共利益的，由著作权行政管理部门责令停止侵权行为，没收违法所得，没收、销毁侵权复制品，可以并处罚款；情节严重的，著作权行政管理部门并可以没收主要用于制作侵权复制品的材料、工具、设备等； 触犯刑律的，依照刑法关于侵犯著作权罪、销售侵权复制品罪的规定，依法追究刑事责任：

(一)复制或者部分复制著作权人的软件的；

(二)向公众发行、出租、通过信息网络传播著作权人的软件的；

(三)故意避开或者破坏著作权人为保护其软件著作权而采取的技术措施的；

(四)故意删除或者改变软件权利管理电子信息的；

(五)转让或者许可他人行使著作权人的软件著作权的。

有前款第一项或者第二项行为的，可以并处每件 100 元或者货值金额 1 倍以

上5倍以下的罚款；有前款第三项、第四项或者第五项行为的，可以并处 20 万元以下的罚款。

第二十五条 侵犯软件著作权的赔偿数额，依照《中华人民共和国著作权法》第四十九条的规定确定。

第二十六条 软件著作权人有证据证明他人正在实施或者即将实施侵犯其权利的行为，如不及时制止，将会使其合法权益受到难以弥补的损害的，可以依照《中华人民共和国著作权法》第五十条的规定， 在提起诉讼前向人民法院申请采取责令停止有关行为和财产保全的措施。

第二十七条 为了制止侵权行为，在证据可能灭失或者以后难以取得的情况下，软件著作权人可以依照《中华人民共和国著作权法》第五十一条的规定，在提起诉讼前向人民法院申请保全证据。

第二十八条 软件复制品的出版者、制作者不能证明其出版、制作有合法授权的，或者软件复制品的发行者、出租者不能证明其发行、出租的复制品有合法来源的，应当承担法律责任。

第二十九条 软件开发者开发的软件， 由于可供选用的表达方式有限而与已经存在的软件相似的，不构成对已经存在的软件的著作权的侵犯。

第三十条 软件的复制品持有人不知道也没有合理理由应当知道该软件是侵权复制品的，不承担赔偿责任；但是，应当停止使用、销毁该侵权复制

品。如果停止使用并销毁该侵权复制品将给复制品使用人造成重大损失的，复制品使用人可以在向软件著作权人支付合理费用后继续使用。

第三十一条 软件著作权侵权纠纷可以调解。

软件著作权合同纠纷可以依据合同中的仲裁条款或者事后达成的书面仲裁协议，向仲裁机构申请仲裁。

当事人没有在合同中订立仲裁条款，事后又没有书面仲裁协议的，可以直接向人民法院提起诉讼。

第五章 附 则

第三十二条 本条例施行前发生的侵权行为，依照侵权行为发生时的国家有关规定处理。

第三十三条 本条例自 2002 年 1 月 1 日起施行。1991 年 6 月 4 日国务院发

布的《计算机软件保护条例》同时废止。

征信业管理条例

中华人民共和国国务院令第 631 号

《征信业管理条例》已经 2012 年 12 月 26 日国务院第 228 次常务会议通过，现予公布，自 2013 年 3 月 15 日起施行。

总理 温家宝

2013 年 1 月 21 日

征信业管理条例

第一章 总 则

第一条 为了规范征信活动，保护当事人合法权益，引导、促进征信业健康发展，推进社会信用体系建设，制定本条例。

第二条 在中国境内从事征信业务及相关活动，适用本条例。

本条例所称征信业务，是指对企业、事业单位等组织(以下统称企业)的信用信息和个人的信用信息进行采集、整理、保存、加工， 并向信息使用者提供的活动。

国家设立的金融信用信息基础数据库进行信息的采集、整理、保存、加工和提供，适用本条例第五章规定。

国家机关以及法律、法规授权的具有管理公共事务职能的组织依照法律、行政法规和国务院的规定，为履行职责进行的企业和个人信息的采集、整理、保存、加工和公布，不适用本条例。

第三条 从事征信业务及相关活动，应当遵守法律法规，诚实守信，不得危害国家秘密，不得侵犯商业秘密和个人隐私。

第四条 中国人民银行(以下称国务院征信业监督管理部门)及其派出机构依法对征信业进行监督管理。

县级以上地方人民政府和国务院有关部门依法推进本地区、本行业的社会信用体系建设，培育征信市场，推动征信业发展。

第二章 征 信 机 构

第五条 本条例所称征信机构，是指依法设立，主要经营征信业务的机构。

第六条 设立经营个人征信业务的征信机构，应当符合《中华人民共和国公

司法》规定的公司设立条件和下列条件，并经国务院征信业监督管理部门批准：

(一)主要股东信誉良好，最近 3 年无重大违法违规记录；

(二)注册资本不少于人民币 5000 万元；

(三)有符合国务院征信业监督管理部门规定的保障信息安全的设施、设备和制度、措施；

(四)拟任董事、监事和高级管理人员符合本条例第八条规定的任职条件；

(五)国务院征信业监督管理部门规定的其他审慎性条件。

第七条 申请设立经营个人征信业务的征信机构，应当向国务院征信业监督管理部门提交申请书和证明其符合本条例第六条规定条件的材料。

国务院征信业监督管理部门应当依法进行审查，自受理申请之日起 60 日内作出批准或者不予批准的决定。决定批准的， 颁发个人征信业务经营许可证；不予批准的，应当书面说明理由。

经批准设立的经营个人征信业务的征信机构，凭个人征信业务经营许可证向公司登记机关办理登记。

未经国务院征信业监督管理部门批准，任何单位和个人不得经营个人征信业务。

第八条 经营个人征信业务的征信机构的董事、监事和高级管理人员，应当熟悉与征信业务相关的法律法规，具有履行职责所需的征信业从业经验和管理能力，最近 3 年无重大违法违规记录，并取得国务院征信业监督管理部门核准的任职资格。

第九条 经营个人征信业务的征信机构设立分支机构、合并或者分立、变更注册资本、变更出资额占公司资本总额 5%以上或者持股占公司股份 5%以上的股东的，应当经国务院征信业监督管理部门批准。

经营个人征信业务的征信机构变更名称的，应当向国务院征信业监督管理部门办理备案。

第十条 设立经营企业征信业务的征信机构，应当符合《中华人民共和国公司法》规定的设立条件，并自公司登记机关准予登记之日起 30 日内向所在地的国务院征信业监督管理部门派出机构办理备案，并提供下列材料：

(一)营业执照；

(二)股权结构、组织机构说明;

(三)业务范围、业务规则、业务系统的基本情况;

(四)信息安全和风险防范措施。

备案事项发生变更的，应当自变更之日起 30 日内向原备案机构办理变更备案。

第十一条 征信机构应当按照国务院征信业监督管理部门的规定，报告上一年度开展征信业务的情况。

国务院征信业监督管理部门应当向社会公告经营个人征信业务和企业征信业务的征信机构名单，并及时更新。

第十二条 征信机构解散或者被依法宣告破产的，应当向国务院征信业监督管理部门报告，并按照下列方式处理信息数据库:

(一)与其他征信机构约定并经国务院征信业监督管理部门同意，转让给其他征信机构;

(二)不能依照前项规定转让的，移交给国务院征信业监督管理部门指定的征信机构;

(三)不能依照前两项规定转让、移交的， 在国务院征信业监督管理部门的监督下销毁。

经营个人征信业务的征信机构解散或者被依法宣告破产的，还应当在国务院征信业监督管理部门指定的媒体上公告，并将个人征信业务经营许可证交国务院征信业监督管理部门注销。

第三章 征信业务规则

第十三条 采集个人信息应当经信息主体本人同意，未经本人同意不得采集。但是，依照法律、行政法规规定公开的信息除外。

企业的董事、监事、高级管理人员与其履行职务相关的信息， 不作为个人信息。

第十四条 禁止征信机构采集个人的宗教信仰、基因、指纹、血型、疾病和病史信息以及法律、行政法规规定禁止采集的其他个人信息。

征信机构不得采集个人的收入、存款、有价证券、商业保险、不动产的信息和纳税数额信息。但是， 征信机构明确告知信息主体提供该信息可能产生的不利

后果，并取得其书面同意的除外。

第十五条 信息提供者向征信机构提供个人不良信息，应当事先告知信息主体本人。但是，依照法律、行政法规规定公开的不良信息除外。

第十六条 征信机构对个人不良信息的保存期限，自不良行为或者事件终止之日起为 5 年；超过 5 年的，应当予以删除。

在不良信息保存期限内，信息主体可以对不良信息作出说明，征信机构应当予以记载。

第十七条 信息主体可以向征信机构查询自身信息。个人信息主体有权每年两次免费获取本人的信用报告。

第十八条 向征信机构查询个人信息的，应当取得信息主体本人的书面同意并约定用途。但是，法律规定可以不经同意查询的除外。

征信机构不得违反前款规定提供个人信息。

第十九条 征信机构或者信息提供者、信息使用者采用格式合同条款取得个人信息主体同意的，应当在合同中作出足以引起信息主体注意的提示，并按照信息主体的要求作出明确说明。

第二十条 信息使用者应当按照与个人信息主体约定的用途使用个人信息，不得用作约定以外的用途，不得未经个人信息主体同意向第三方提供。

第二十一条 征信机构可以通过信息主体、企业交易对方、行业协会提供信息，政府有关部门依法已公开的信息，人民法院依法公布的判决、裁定等渠道，采集企业信息。

征信机构不得采集法律、行政法规禁止采集的企业信息。

第二十二条 征信机构应当按照国务院征信业监督管理部门的规定，建立健全和严格执行保障信息安全的规章制度，并采取有效技术措施保障信息安全。

经营个人征信业务的征信机构应当对其工作人员查询个人信息的权限和程序作出明确规定，对工作人员查询个人信息的情况进行登记，如实记载查询工作人员的姓名，查询的时间、内容及用途。工作人员不得违反规定的权限和程序查询信息，不得泄露工作中获取的信息。

第二十三条 征信机构应当采取合理措施，保障其提供信息的准确性。

征信机构提供的信息供信息使用者参考。

第二十四条 征信机构在中国境内采集的信息的整理、保存和加工，应当在中国境内进行。

征信机构向境外组织或者个人提供信息，应当遵守法律、行政法规和国务院征信业监督管理部门的有关规定。

第四章 异议和投诉

第二十五条 信息主体认为征信机构采集、保存、提供的信息存在错误、遗漏的，有权向征信机构或者信息提供者提出异议，要求更正。

征信机构或者信息提供者收到异议，应当按照国务院征信业监督管理部门的规定对相关信息作出存在异议的标注，自收到异议之日起 20 日内进行核查和处理，并将结果书面答复异议人。

经核查，确认相关信息确有错误、遗漏的， 信息提供者、征信机构应当予以更正；确认不存在错误、遗漏的， 应当取消异议标注；经核查仍不能确认的，对核查情况和异议内容应当予以记载。

第二十六条 信息主体认为征信机构或者信息提供者、信息使用者侵害其合法权益的，可以向所在地的国务院征信业监督管理部门派出机构投诉。

受理投诉的机构应当及时进行核查和处理，自受理之日起 30 日内书面答复投诉人。

信息主体认为征信机构或者信息提供者、信息使用者侵害其合法权益的， 可以直接向人民法院起诉。

第五章 金融信用信息基础数据库

第二十七条 国家设立金融信用信息基础数据库，为防范金融风险、促进金融业发展提供相关信息服务。

金融信用信息基础数据库由专业运行机构建设、运行和维护。该运行机构不以营利为目的，由国务院征信业监督管理部门监督管理。

第二十八条 金融信用信息基础数据库接收从事信贷业务的机构按照规定提供的信贷信息。

金融信用信息基础数据库为信息主体和取得信息主体本人书面同意的信息使用者提供查询服务。国家机关可以依法查询金融信用信息基础数据库的信息。

第二十九条 从事信贷业务的机构应当按照规定向金融信用信息基础数据库

提供信贷信息。

从事信贷业务的机构向金融信用信息基础数据库或者其他主体提供信贷信息，应当事先取得信息主体的书面同意，并适用本条例关于信息提供者的规定。

第三十条 不从事信贷业务的金融机构向金融信用信息基础数据库提供、查询信用信息以及金融信用信息基础数据库接收其提供的信用信息的具体办法，由国务院征信业监督管理部门会同国务院有关金融监督管理机构依法制定。

第三十一条 金融信用信息基础数据库运行机构可以按照补偿成本原则收取查询服务费用，收费标准由国务院价格主管部门规定。

第三十二条 本条例第十四条、第十六条、第十七条、第十八条、第二十二条、第二十三条、第二十四条、第二十五条、第二十六条适用于金融信用信息基础数据库运行机构。

第六章 监 督 管 理

第三十三条 国务院征信业监督管理部门及其派出机构依照法律、行政法规和国务院的规定，履行对征信业和金融信用信息基础数据库运行机构的监督管理职责，可以采取下列监督检查措施：

(一)进入征信机构、金融信用信息基础数据库运行机构进行现场检查， 对向金融信用信息基础数据库提供或者查询信息的机构遵守本条例有关规定的情况进行检查；

(二)询问当事人和与被调查事件有关的单位和个人，要求其对与被调查事件有关的事项作出说明；

(三)查阅、复制与被调查事件有关的文件、资料， 对可能被转移、销毁、隐匿或者篡改的文件、资料予以封存；

(四)检查相关信息系统。

进行现场检查或者调查的人员不得少于 2 人，并应当出示合法证件和检查、调查通知书。

被检查、调查的单位和个人应当配合，如实提供有关文件、资料，不得隐瞒、拒绝和阻碍。

第三十四条 经营个人征信业务的征信机构、金融信用信息基础数据库、向金融信用信息基础数据库提供或者查询信息的机构发生重大信息泄露等事件的，

国务院征信业监督管理部门可以采取临时接管相关信息系统等必要措施，避免损害扩大。

第三十五条 国务院征信业监督管理部门及其派出机构的工作人员对在工作中知悉的国家秘密和信息主体的信息，应当依法保密。

第七章 法 律 责 任

第三十六条 未经国务院征信业监督管理部门批准，擅自设立经营个人征信业务的征信机构或者从事个人征信业务活动的，由国务院征信业监督管理部门予以取缔，没收违法所得，并处 5 万元以上 50 万元以下的罚款；构成犯罪的，依法追究刑事责任。

第三十七条 经营个人征信业务的征信机构违反本条例第九条规定的，由国务院征信业监督管理部门责令限期改正，对单位处 2 万元以上 20 万元以下的罚款；对直接负责的主管人员和其他直接责任人员给予警告，处 1 万元以下的罚款。

经营企业征信业务的征信机构未按照本条例第十条规定办理备案的，由其所在地的国务院征信业监督管理部门派出机构责令限期改正；逾期不改正的，依照前款规定处罚。

第三十八条 征信机构、金融信用信息基础数据库运行机构违反本条例规定，有下列行为之一的，由国务院征信业监督管理部门或者其派出机构责令限期改正，对单位处 5 万元以上 50 万元以下的罚款；对直接负责的主管人员和其他直接责任人员处 1 万元以上 10 万元以下的罚款；有违法所得的，没收违法所得。给信息主体造成损失的，依法承担民事责任；构成犯罪的，依法追究刑事责任：

(一)窃取或者以其他方式非法获取信息；

(二)采集禁止采集的个人信息或者未经同意采集个人信息；

(三)违法提供或者出售信息；

(四)因过失泄露信息；

(五)逾期不删除个人不良信息；

(六)未按照规定对异议信息进行核查和处理；

(七)拒绝、阻碍国务院征信业监督管理部门或者其派出机构检查、调查或者不如实提供有关文件、资料；

(八)违反征信业务规则，侵害信息主体合法权益的其他行为。

经营个人征信业务的征信机构有前款所列行为之一，情节严重或者造成严重后果的，由国务院征信业监督管理部门吊销其个人征信业务经营许可证。

第三十九条 征信机构违反本条例规定，未按照规定报告其上一年度开展征信业务情况的，由国务院征信业监督管理部门或者其派出机构责令限期改正；逾期不改正的，对单位处 2 万元以上 10 万元以下的罚款；对直接负责的主管人员和其他直接责任人员给予警告，处 1 万元以下的罚款。

第四十条 向金融信用信息基础数据库提供或者查询信息的机构违反本条例规定，有下列行为之一的，由国务院征信业监督管理部门或者其派出机构责令限期改正，对单位处 5 万元以上 50 万元以下的罚款；对直接负责的主管人员和其他直接责任人员处 1 万元以上 10 万元以下的罚款；有违法所得的，没收违法所得。给信息主体造成损失的， 依法承担民事责任；构成犯罪的，依法追究刑事责任：

(一)违法提供或者出售信息；

(二)因过失泄露信息；

(三)未经同意查询个人信息或者企业的信贷信息；

(四)未按照规定处理异议或者对确有错误、遗漏的信息不予更正；

(五)拒绝、阻碍国务院征信业监督管理部门或者其派出机构检查、调查或者不如实提供有关文件、资料。

第四十一条 信息提供者违反本条例规定，向征信机构、金融信用信息基础数据库提供非依法公开的个人不良信息，未事先告知信息主体本人，情节严重或者造成严重后果的，由国务院征信业监督管理部门或者其派出机构对单位处 2 万元以上 20 万元以下的罚款；对个人处 1 万元以上 5 万元以下的罚款。

第四十二条 信息使用者违反本条例规定，未按照与个人信息主体约定的用途使用个人信息或者未经个人信息主体同意向第三方提供个人信息，情节严重或者造成严重后果的，由国务院征信业监督管理部门或者其派出机构对单位处 2 万元以上 20 万元以下的罚款；对个人处 1 万元以上 5 万元以下的罚款；有违法所得的，没收违法所得。给信息主体造成损失的，依法承担民事责任；构成犯罪的，依法追究刑事责任。

第四十三条 国务院征信业监督管理部门及其派出机构的工作人员滥用职权、玩忽职守、徇私舞弊， 不依法履行监督管理职责，或者泄露国家秘密、信息主体信息的，依法给予处分。给信息主体造成损失的， 依法承担民事责任；构成犯罪的，依法追究刑事责任。

第八章 附 则

第四十四条 本条例下列用语的含义：

(一)信息提供者，是指向征信机构提供信息的单位和个人，以及向金融信用信息基础数据库提供信息的单位。

(二)信息使用者，是指从征信机构和金融信用信息基础数据库获取信息的单位和个人。

(三)不良信息，是指对信息主体信用状况构成负面影响的下列信息：信息主体在借贷、赊购、担保、租赁、保险、使用信用卡等活动中未按照合同履行义务的信息，对信息主体的行政处罚信息，人民法院判决或者裁定信息主体履行义务以及强制执行的信息，以及国务院征信业监督管理部门规定的其他不良信息。

第四十五条 外商投资征信机构的设立条件， 由国务院征信业监督管理部门会同国务院有关部门制定，报国务院批准。

境外征信机构在境内经营征信业务，应当经国务院征信业监督管理部门批准。

第四十六条 本条例施行前已经经营个人征信业务的机构，应当自本条例施行之日起 6 个月内，依照本条例的规定申请个人征信业务经营许可证。

本条例施行前已经经营企业征信业务的机构，应当自本条例施行之日起 3 个月内，依照本条例的规定办理备案。

第四十七条 本条例自 2013 年 3 月 15 日起施行。

信息网络传播权保护条例

(2006 年 5 月 18 日中华人民共和国国务院令第 468 号公布 根据 2013 年 1 月 30 日《国务院关于修改〈信息网络传播权保护条例〉的决定》修订)

第一条 为保护著作权人、表演者、录音录像制作者(以下统称权利人)的信息网络传播权，鼓励有益于社会主义精神文明、物质文明建设的作品的创作和传播，根据《中华人民共和国著作权法》(以下简称著作权法)，制定本条例。

第二条 权利人享有的信息网络传播权受著作权法和本条例保护。除法律、

行政法规另有规定的外，任何组织或者个人将他人的作品、表演、录音录像制品通过信息网络向公众提供，应当取得权利人许可，并支付报酬。

第三条 依法禁止提供的作品、表演、录音录像制品，不受本条例保护。

权利人行使信息网络传播权，不得违反宪法和法律、行政法规，不得损害公共利益。

第四条 为了保护信息网络传播权，权利人可以采取技术措施。

任何组织或者个人不得故意避开或者破坏技术措施，不得故意制造、进口或者向公众提供主要用于避开或者破坏技术措施的装置或者部件，不得故意为他人避开或者破坏技术措施提供技术服务。但是，法律、行政法规规定可以避开的除外。

第五条 未经权利人许可，任何组织或者个人不得进行下列行为：

(一)故意删除或者改变通过信息网络向公众提供的作品、表演、录音录像制品的权利管理电子信息，但由于技术上的原因无法避免删除或者改变的除外；

(二)通过信息网络向公众提供明知或者应知未经权利人许可被删除或者改变权利管理电子信息的作品、表演、录音录像制品。

第六条 通过信息网络提供他人作品，属于下列情形的，可以不经著作权人许可，不向其支付报酬：

(一)为介绍、评论某一作品或者说明某一问题，在向公众提供的作品中适当引用已经发表的作品；

(二)为报道时事新闻，在向公众提供的作品中不可避免地再现或者引用已经发表的作品；

(三)为学校课堂教学或者科学研究，向少数教学、科研人员提供少量已经发表的作品；

(四)国家机关为执行公务，在合理范围内向公众提供已经发表的作品；

(五)将中国公民、法人或者其他组织已经发表的、以汉语言文字创作的作品翻译成的少数民族语言文字作品，向中国境内少数民族提供；

(六)不以营利为目的，以盲人能够感知的独特方式向盲人提供已经发表的文字作品；

(七)向公众提供在信息网络上已经发表的关于政治、经济问题的时事性文章;

(八)向公众提供在公众集会上发表的讲话。

第七条 图书馆、档案馆、纪念馆、博物馆、美术馆等可以不经著作权人许可，通过信息网络向本馆馆舍内服务对象提供本馆收藏的合法出版的数字作品和依法为陈列或者保存版本的需要以数字化形式复制的作品，不向其支付报酬，但不得直接或者间接获得经济利益。当事人另有约定的除外。

前款规定的为陈列或者保存版本需要以数字化形式复制的作品，应当是已经损毁或者濒临损毁、丢失或者失窃，或者其存储格式已经过时，并且在市场上无法购买或者只能以明显高于标定的价格购买的作品。

第八条 为通过信息网络实施九年制义务教育或者国家教育规划，可以不经著作权人许可，使用其已经发表作品的片断或者短小的文字作品、音乐作品或者单幅的美术作品、摄影作品制作课件，由制作课件或者依法取得课件的远程教育机构通过信息网络向注册学生提供，但应当向著作权人支付报酬。

第九条 为扶助贫困，通过信息网络向农村地区的公众免费提供中国公民、法人或者其他组织已经发表的种植养殖、防病治病、防灾减灾等与扶助贫困有关的作品和适应基本文化需求的作品，网络服务提供者应当在提供前公告拟提供的作品及其作者、拟支付报酬的标准。自公告之日起 30 日内，著作权人不同意提供的，网络服务提供者不得提供其作品；自公告之日起满 30 日，著作权人没有异议的，网络服务提供者可以提供其作品，并按照公告的标准向著作权人支付报酬。网络服务提供者提供著作权人的作品后，著作权人不同意提供的，网络服务提供者应当立即删除著作权人的作品，并按照公告的标准向著作权人支付提供作品期间的报酬。

依照前款规定提供作品的，不得直接或者间接获得经济利益。

第十条 依照本条例规定不经著作权人许可、通过信息网络向公众提供其作品的，还应当遵守下列规定:

(一)除本条例第六条第一项至第六项、第七条规定的情形外，不得提供作者事先声明不许提供的作品;

(二)指明作品的名称和作者的姓名(名称);

(三)依照本条例规定支付报酬;

(四)采取技术措施,防止本条例第七条、第八条、第九条规定的服务对象以外的其他人获得著作权人的作品,并防止本条例第七条规定的服务对象的复制行为对著作权人利益造成实质性损害;

(五)不得侵犯著作权人依法享有的其他权利。

第十一条 通过信息网络提供他人表演、录音录像制品的,应当遵守本条例第六条至第十条的规定。

第十二条 属于下列情形的,可以避开技术措施,但不得向他人提供避开技术措施的技术、装置或者部件,不得侵犯权利人依法享有的其他权利:

(一)为学校课堂教学或者科学研究,通过信息网络向少数教学、科研人员提供已经发表的作品、表演、录音录像制品,而该作品、表演、录音录像制品只能通过信息网络获取;

(二)不以营利为目的,通过信息网络以盲人能够感知的独特方式向盲人提供已经发表的文字作品,而该作品只能通过信息网络获取;

(三)国家机关依照行政、司法程序执行公务;

(四)在信息网络上对计算机及其系统或者网络的安全性能进行测试。

第十三条 著作权行政管理部门为了查处侵犯信息网络传播权的行为,可以要求网络服务提供者提供涉嫌侵权的服务对象的姓名(名称)、联系方式、网络地址等资料。

第十四条 对提供信息存储空间或者提供搜索、链接服务的网络服务提供者,权利人认为其服务所涉及的作品、表演、录音录像制品,侵犯自己的信息网络传播权或者被删除、改变了自己的权利管理电子信息的,可以向该网络服务提供者提交书面通知,要求网络服务提供者删除该作品、表演、录音录像制品,或者断开与该作品、表演、录音录像制品的链接。通知书应当包含下列内容:

(一)权利人的姓名(名称)、联系方式和地址;

(二)要求删除或者断开链接的侵权作品、表演、录音录像制品的名称和网络地址;

(三)构成侵权的初步证明材料。

权利人应当对通知书的真实性负责。

第十五条 网络服务提供者接到权利人的通知书后，应当立即删除涉嫌侵权的作品、表演、录音录像制品，或者断开与涉嫌侵权的作品、表演、录音录像制品的链接，并同时将通知书转送提供作品、表演、录音录像制品的服务对象；服务对象网络地址不明、无法转送的，应当将通知书的内容同时在信息网络上公告。

第十六条 服务对象接到网络服务提供者转送的通知书后，认为其提供的作品、表演、录音录像制品未侵犯他人权利的，可以向网络服务提供者提交书面说明，要求恢复被删除的作品、表演、录音录像制品，或者恢复与被断开的作品、表演、录音录像制品的链接。书面说明应当包含下列内容：

(一)服务对象的姓名(名称)、联系方式和地址；

(二)要求恢复的作品、表演、录音录像制品的名称和网络地址；

(三)不构成侵权的初步证明材料。

服务对象应当对书面说明的真实性负责。

第十七条 网络服务提供者接到服务对象的书面说明后，应当立即恢复被删除的作品、表演、录音录像制品，或者可以恢复与被断开的作品、表演、录音录像制品的链接，同时将服务对象的书面说明转送权利人。权利人不得再通知网络服务提供者删除该作品、表演、录音录像制品，或者断开与该作品、表演、录音录像制品的链接。

第十八条 违反本条例规定，有下列侵权行为之一的，根据情况承担停止侵害、消除影响、赔礼道歉、赔偿损失等民事责任；同时损害公共利益的，可以由著作权行政管理部门责令停止侵权行为，没收违法所得，非法经营额 5 万元以上的，可处非法经营额 1 倍以上 5 倍以下的罚款；没有非法经营额或者非法经营额 5 万元以下的，根据情节轻重，可处 25 万元以下的罚款；情节严重的，著作权行政管理部门可以没收主要用于提供网络服务的计算机等设备；构成犯罪的，依法追究刑事责任：

(一)通过信息网络擅自向公众提供他人的作品、表演、录音录像制品的；

(二)故意避开或者破坏技术措施的；

(三)故意删除或者改变通过信息网络向公众提供的作品、表演、录音录像

制品的权利管理电子信息，或者通过信息网络向公众提供明知或者应知未经权利人许可而被删除或者改变权利管理电子信息的作品、表演、录音录像制品的；

(四)为扶助贫困通过信息网络向农村地区提供作品、表演、录音录像制品超过规定范围，或者未按照公告的标准支付报酬，或者在权利人不同意提供其作品、表演、录音录像制品后未立即删除的；

(五)通过信息网络提供他人的作品、表演、录音录像制品，未指明作品、表演、录音录像制品的名称或者作者、表演者、录音录像制作者的姓名(名称)，或者未支付报酬，或者未依照本条例规定采取技术措施防止服务对象以外的其他人获得他人的作品、表演、录音录像制品，或者未防止服务对象的复制行为对权利人利益造成实质性损害的。

第十九条 违反本条例规定，有下列行为之一的，由著作权行政管理部门予以警告，没收违法所得，没收主要用于避开、破坏技术措施的装置或者部件；情节严重的，可以没收主要用于提供网络服务的计算机等设备；非法经营额 5 万元以上的，可处非法经营额 1 倍以上 5 倍以下的罚款；没有非法经营额或者非法经营额 5 万元以下的，根据情节轻重，可处 25 万元以下的罚款；构成犯罪的，依法追究刑事责任：

(一)故意制造、进口或者向他人提供主要用于避开、破坏技术措施的装置或者部件，或者故意为他人避开或者破坏技术措施提供技术服务的；

(二)通过信息网络提供他人的作品、表演、录音录像制品，获得经济利益的；

(三)为扶助贫困通过信息网络向农村地区提供作品、表演、录音录像制品，未在提供前公告作品、表演、录音录像制品的名称和作者、表演者、录音录像制作者的姓名(名称)以及报酬标准的。

第二十条 网络服务提供者根据服务对象的指令提供网络自动接入服务，或者对服务对象提供的作品、表演、录音录像制品提供自动传输服务，并具备下列条件的，不承担赔偿责任：

(一)未选择并且未改变所传输的作品、表演、录音录像制品；

(二)向指定的服务对象提供该作品、表演、录音录像制品，并防止指定的

服务对象以外的其他人获得。

第二十一条 网络服务提供者为提高网络传输效率，自动存储从其他网络服务提供者获得的作品、表演、录音录像制品，根据技术安排自动向服务对象提供，并具备下列条件的，不承担赔偿责任：

(一)未改变自动存储的作品、表演、录音录像制品；

(二)不影响提供作品、表演、录音录像制品的原网络服务提供者掌握服务对象获取该作品、表演、录音录像制品的情况；

(三)在原网络服务提供者修改、删除或者屏蔽该作品、表演、录音录像制品时，根据技术安排自动予以修改、删除或者屏蔽。

第二十二条 网络服务提供者为服务对象提供信息存储空间，供服务对象通过信息网络向公众提供作品、表演、录音录像制品，并具备下列条件的，不承担赔偿责任：

(一)明确标示该信息存储空间是为服务对象所提供，并公开网络服务提供者的名称、联系人、网络地址；

(二)未改变服务对象所提供的作品、表演、录音录像制品；

(三)不知道也没有合理的理由应当知道服务对象提供的作品、表演、录音录像制品侵权；

(四)未从服务对象提供作品、表演、录音录像制品中直接获得经济利益；

(五)在接到权利人的通知书后，根据本条例规定删除权利人认为侵权的作品、表演、录音录像制品。

第二十三条 网络服务提供者为服务对象提供搜索或者链接服务，在接到权利人的通知书后，根据本条例规定断开与侵权的作品、表演、录音录像制品的链接的，不承担赔偿责任；但是，明知或者应知所链接的作品、表演、录音录像制品侵权的，应当承担共同侵权责任。

第二十四条 因权利人的通知导致网络服务提供者错误删除作品、表演、录音录像制品，或者错误断开与作品、表演、录音录像制品的链接，给服务对象造成损失的，权利人应当承担赔偿责任。

第二十五条 网络服务提供者无正当理由拒绝提供或者拖延提供涉嫌侵权的服务对象的姓名(名称)、联系方式、网络地址等资料的，由著作权行政管理部

门予以警告；情节严重的，没收主要用于提供网络服务的计算机等设备。

第二十六条 本条例下列用语的含义：

信息网络传播权，是指以有线或者无线方式向公众提供作品、表演或者录音录像制品，使公众可以在其个人选定的时间和地点获得作品、表演或者录音录像制品的权利。

技术措施，是指用于防止、限制未经权利人许可浏览、欣赏作品、表演、录音录像制品的或者通过信息网络向公众提供作品、表演、录音录像制品的有效技术、装置或者部件。

权利管理电子信息，是指说明作品及其作者、表演及其表演者、录音录像制品及其制作者的信息，作品、表演、录音录像制品权利人的信息和使用条件的信息，以及表示上述信息的数字或者代码。

第二十七条 本条例自 2006 年 7 月 1 日起施行。

关键信息基础设施安全保护条例

中华人民共和国国务院令第 745 号

《关键信息基础设施安全保护条例》已经 2021 年 4 月 27 日国务院第 133 次常务会议通过，现予公布，自 2021 年 9 月 1 日起施行。

总理 李克强

2021 年 7 月 30 日

关键信息基础设施安全保护条例

第一章 总 则

第一条 为了保障关键信息基础设施安全，维护网络安全，根据《中华人民共和国网络安全法》，制定本条例。

第二条 本条例所称关键信息基础设施，是指公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务、国防科技工业等重要行业和领域的，以及其他一旦遭到破坏、丧失功能或者数据泄露， 可能严重危害国家安全、国计民生、公共利益的重要网络设施、信息系统等。

第三条 在国家网信部门统筹协调下，国务院公安部门负责指导监督关键信息基础设施安全保护工作。国务院电信主管部门和其他有关部门依照本条例和有关法律、行政法规的规定， 在各自职责范围内负责关键信息基础设施安全保护和

监督管理工作。

省级人民政府有关部门依据各自职责对关键信息基础设施实施安全保护和监督管理。

第四条 关键信息基础设施安全保护坚持综合协调、分工负责、依法保护，强化和落实关键信息基础设施运营者(以下简称运营者)主体责任，充分发挥政府及社会各方面的作用，共同保护关键信息基础设施安全。

第五条 国家对关键信息基础设施实行重点保护，采取措施，监测、防御、处置来源于中华人民共和国境内外的网络安全风险和威胁，保护关键信息基础设施免受攻击、侵入、干扰和破坏， 依法惩治危害关键信息基础设施安全的违法犯罪活动。

任何个人和组织不得实施非法侵入、干扰、破坏关键信息基础设施的活动，不得危害关键信息基础设施安全。

第六条 运营者依照本条例和有关法律、行政法规的规定以及国家标准的强制性要求，在网络安全等级保护的基础上，采取技术保护措施和其他必要措施，应对网络安全事件，防范网络攻击和违法犯罪活动，保障关键信息基础设施安全稳定运行，维护数据的完整性、保密性和可用性。

第七条 对在关键信息基础设施安全保护工作中取得显著成绩或者作出突出贡献的单位和个人，按照国家有关规定给予表彰。

第二章 关键信息基础设施认定

第八条 本条例第二条涉及的重要行业和领域的主管部门、监督管理部门是负责关键信息基础设施安全保护工作的部门(以下简称保护工作部门)。

第九条 保护工作部门结合本行业、本领域实际，制定关键信息基础设施认定规则，并报国务院公安部门备案。

制定认定规则应当主要考虑下列因素：

(一)网络设施、信息系统等对于本行业、本领域关键核心业务的重要程度；

(二)网络设施、信息系统等一旦遭到破坏、丧失功能或者数据泄露可能带来的危害程度；

(三)对其他行业和领域的关联性影响。

第十条 保护工作部门根据认定规则负责组织认定本行业、本领域的关键信

息基础设施，及时将认定结果通知运营者，并通报国务院公安部门。

第十一条 关键信息基础设施发生较大变化，可能影响其认定结果的，运营者应当及时将相关情况报告保护工作部门。保护工作部门自收到报告之日起 3 个月内完成重新认定，将认定结果通知运营者，并通报国务院公安部门。

第三章 运营者责任义务

第十二条 安全保护措施应当与关键信息基础设施同步规划、同步建设、同步使用。

第十三条 运营者应当建立健全网络安全保护制度和责任制，保障人力、财力、物力投入。运营者的主要负责人对关键信息基础设施安全保护负总责， 领导关键信息基础设施安全保护和重大网络安全事件处置工作，组织研究解决重大网络安全问题。

第十四条 运营者应当设置专门安全管理机构，并对专门安全管理机构负责人和关键岗位人员进行安全背景审查。审查时， 公安机关、国家安全机关应当予以协助。

第十五条 专门安全管理机构具体负责本单位的关键信息基础设施安全保护工作，履行下列职责：

(一)建立健全网络安全管理、评价考核制度， 拟订关键信息基础设施安全保护计划；

(二)组织推动网络安全防护能力建设，开展网络安全监测、检测和风险评估；

(三)按照国家及行业网络安全事件应急预案，制定本单位应急预案，定期开展应急演练，处置网络安全事件；

(四)认定网络安全关键岗位，组织开展网络安全工作考核，提出奖励和惩处建议；

(五)组织网络安全教育、培训；

(六)履行个人信息和数据安全保护责任，建立健全个人信息和数据安全保护制度；

(七)对关键信息基础设施设计、建设、运行、维护等服务实施安全管理；

(八)按照规定报告网络安全事件和重要事项。

第十六条 运营者应当保障专门安全管理机构的运行经费、配备相应的人员，

开展与网络安全和信息化有关的决策应当有专门安全管理机构人员参与。

第十七条 运营者应当自行或者委托网络安全服务机构对关键信息基础设施每年至少进行一次网络安全检测和风险评估，对发现的安全问题及时整改，并按照保护工作部门要求报送情况。

第十八条 关键信息基础设施发生重大网络安全事件或者发现重大网络安全威胁时，运营者应当按照有关规定向保护工作部门、公安机关报告。

发生关键信息基础设施整体中断运行或者主要功能故障、国家基础信息以及其他重要数据泄露、较大规模个人信息泄露、造成较大经济损失、违法信息较大范围传播等特别重大网络安全事件或者发现特别重大网络安全威胁时，保护工作部门应当在收到报告后，及时向国家网信部门、国务院公安部门报告。

第十九条 运营者应当优先采购安全可信的网络产品和服务；采购网络产品和服务可能影响国家安全的，应当按照国家网络安全规定通过安全审查。

第二十条 运营者采购网络产品和服务，应当按照国家有关规定与网络产品和服务提供者签订安全保密协议，明确提供者的技术支持和安全保密义务与责任，并对义务与责任履行情况进行监督。

第二十一条 运营者发生合并、分立、解散等情况，应当及时报告保护工作部门，并按照保护工作部门的要求对关键信息基础设施进行处置，确保安全。

第四章 保障和促进

第二十二条 保护工作部门应当制定本行业、本领域关键信息基础设施安全规划，明确保护目标、基本要求、工作任务、具体措施。

第二十三条 国家网信部门统筹协调有关部门建立网络安全信息共享机制，及时汇总、研判、共享、发布网络安全威胁、漏洞、事件等信息， 促进有关部门、保护工作部门、运营者以及网络安全服务机构等之间的网络安全信息共享。

第二十四条 保护工作部门应当建立健全本行业、本领域的关键信息基础设施网络安全监测预警制度，及时掌握本行业、本领域关键信息基础设施运行状况、安全态势，预警通报网络安全威胁和隐患，指导做好安全防范工作。

第二十五条 保护工作部门应当按照国家网络安全事件应急预案的要求，建立健全本行业、本领域的网络安全事件应急预案， 定期组织应急演练；指导运营者做好网络安全事件应对处置，并根据需要组织提供技术支持与协助。

第二十六条 保护工作部门应当定期组织开展本行业、本领域关键信息基础设施网络安全检查检测，指导监督运营者及时整改安全隐患、完善安全措施。

第二十七条 国家网信部门统筹协调国务院公安部门、保护工作部门对关键信息基础设施进行网络安全检查检测，提出改进措施。

有关部门在开展关键信息基础设施网络安全检查时，应当加强协同配合、信息沟通，避免不必要的检查和交叉重复检查。检查工作不得收取费用， 不得要求被检查单位购买指定品牌或者指定生产、销售单位的产品和服务。

第二十八条 运营者对保护工作部门开展的关键信息基础设施网络安全检查检测工作，以及公安、国家安全、保密行政管理、密码管理等有关部门依法开展的关键信息基础设施网络安全检查工作应当予以配合。

第二十九条 在关键信息基础设施安全保护工作中，国家网信部门和国务院电信主管部门、国务院公安部门等应当根据保护工作部门的需要， 及时提供技术支持和协助。

第三十条 网信部门、公安机关、保护工作部门等有关部门，网络安全服务机构及其工作人员对于在关键信息基础设施安全保护工作中获取的信息，只能用于维护网络安全，并严格按照有关法律、行政法规的要求确保信息安全， 不得泄露、出售或者非法向他人提供。

第三十一条 未经国家网信部门、国务院公安部门批准或者保护工作部门、运营者授权，任何个人和组织不得对关键信息基础设施实施漏洞探测、渗透性测试等可能影响或者危害关键信息基础设施安全的活动。对基础电信网络实施漏洞探测、渗透性测试等活动，应当事先向国务院电信主管部门报告。

第三十二条 国家采取措施，优先保障能源、电信等关键信息基础设施安全运行。

能源、电信行业应当采取措施， 为其他行业和领域的关键信息基础设施安全运行提供重点保障。

第三十三条 公安机关、国家安全机关依据各自职责依法加强关键信息基础设施安全保卫，防范打击针对和利用关键信息基础设施实施的违法犯罪活动。

第三十四条 国家制定和完善关键信息基础设施安全标准，指导、规范关键信息基础设施安全保护工作。

第三十五条 国家采取措施，鼓励网络安全专门人才从事关键信息基础设施安全保护工作；将运营者安全管理人员、安全技术人员培训纳入国家继续教育体系。

第三十六条 国家支持关键信息基础设施安全防护技术创新和产业发展，组织力量实施关键信息基础设施安全技术攻关。

第三十七条 国家加强网络安全服务机构建设和管理，制定管理要求并加强监督指导，不断提升服务机构能力水平，充分发挥其在关键信息基础设施安全保护中的作用。

第三十八条 国家加强网络安全军民融合，军地协同保护关键信息基础设施安全。

第五章 法律责任

第三十九条 运营者有下列情形之一的，由有关主管部门依据职责责令改正，给予警告；拒不改正或者导致危害网络安全等后果的，处 10 万元以上 100 万元以下罚款，对直接负责的主管人员处 1 万元以上 10 万元以下罚款：

(一)在关键信息基础设施发生较大变化，可能影响其认定结果时未及时将相关情况报告保护工作部门的；

(二)安全保护措施未与关键信息基础设施同步规划、同步建设、同步使用的；

(三)未建立健全网络安全保护制度和责任制的；

(四)未设置专门安全管理机构的；

(五)未对专门安全管理机构负责人和关键岗位人员进行安全背景审查的；

(六)开展与网络安全和信息化有关的决策没有专门安全管理机构人员参与的；

(七)专门安全管理机构未履行本条例第十五条规定的职责的；

(八)未对关键信息基础设施每年至少进行一次网络安全检测和风险评估，未对发现的安全问题及时整改，或者未按照保护工作部门要求报送情况的；

(九)采购网络产品和服务，未按照国家有关规定与网络产品和服务提供者签订安全保密协议的；

(十)发生合并、分立、解散等情况， 未及时报告保护工作部门，或者未按照保护工作部门的要求对关键信息基础设施进行处置的。

第四十条 运营者在关键信息基础设施发生重大网络安全事件或者发现重大网络安全威胁时，未按照有关规定向保护工作部门、公安机关报告的， 由保护工作部门、公安机关依据职责责令改正， 给予警告；拒不改正或者导致危害网络安全等后果的，处 10 万元以上 100 万元以下罚款，对直接负责的主管人员处 1 万元以上 10 万元以下罚款。

第四十一条 运营者采购可能影响国家安全的网络产品和服务，未按照国家网络安全规定进行安全审查的，由国家网信部门等有关主管部门依据职责责令改正，处采购金额 1 倍以上 10 倍以下罚款，对直接负责的主管人员和其他直接责任人员处 1 万元以上 10 万元以下罚款。

第四十二条 运营者对保护工作部门开展的关键信息基础设施网络安全检查检测工作，以及公安、国家安全、保密行政管理、密码管理等有关部门依法开展的关键信息基础设施网络安全检查工作不予配合的，由有关主管部门责令改正；拒不改正的，处 5 万元以上 50 万元以下罚款，对直接负责的主管人员和其他直接责任人员处 1 万元以上 10 万元以下罚款；情节严重的，依法追究相应法律责任。

第四十三条 实施非法侵入、干扰、破坏关键信息基础设施，危害其安全的活动尚不构成犯罪的，依照《中华人民共和国网络安全法》有关规定， 由公安机关没收违法所得，处 5 日以下拘留，可以并处 5 万元以上 50 万元以下罚款；情节较重的，处 5 日以上 15 日以下拘留，可以并处 10 万元以上 100 万元以下罚款。

单位有前款行为的，由公安机关没收违法所得，处 10 万元以上 100 万元以下罚款，并对直接负责的主管人员和其他直接责任人员依照前款规定处罚。

违反本条例第五条第二款和第三十一条规定，受到治安管理处罚的人员，5 年内不得从事网络安全管理和网络运营关键岗位的工作；受到刑事处罚的人员，终身不得从事网络安全管理和网络运营关键岗位的工作。

第四十四条 网信部门、公安机关、保护工作部门和其他有关部门及其工作人员未履行关键信息基础设施安全保护和监督管理职责或者玩忽职守、滥用职权、徇私舞弊的，依法对直接负责的主管人员和其他直接责任人员给予处分。

第四十五条 公安机关、保护工作部门和其他有关部门在开展关键信息基础

设施网络安全检查工作中收取费用，或者要求被检查单位购买指定品牌或者指定生产、销售单位的产品和服务的， 由其上级机关责令改正，退还收取的费用；情节严重的，依法对直接负责的主管人员和其他直接责任人员给予处分。

第四十六条 网信部门、公安机关、保护工作部门等有关部门、网络安全服务机构及其工作人员将在关键信息基础设施安全保护工作中获取的信息用于其他用途，或者泄露、出售、非法向他人提供的， 依法对直接负责的主管人员和其他直接责任人员给予处分。

第四十七条 关键信息基础设施发生重大和特别重大网络安全事件，经调查确定为责任事故的，除应当查明运营者责任并依法予以追究外，还应查明相关网络安全服务机构及有关部门的责任，对有失职、渎职及其他违法行为的， 依法追究责任。

第四十八条 电子政务关键信息基础设施的运营者不履行本条例规定的网络安全保护义务的，依照《中华人民共和国网络安全法》有关规定予以处理。

第四十九条 违反本条例规定，给他人造成损害的，依法承担民事责任。

违反本条例规定，构成违反治安管理行为的，依法给予治安管理处罚；构成犯罪的，依法追究刑事责任。

第六章 附 则

第五十条 存储、处理涉及国家秘密信息的关键信息基础设施的安全保护，还应当遵守保密法律、行政法规的规定。

关键信息基础设施中的密码使用和管理，还应当遵守相关法律、行政法规的规定。

第五十一条 本条例自 2021 年 9 月 1 日起施行。

商用密码管理条例

中华人民共和国国务院令第 760 号

《商用密码管理条例》已经 2023 年 4 月 14 日国务院第 4 次常务会议修订通过，现予公布，自 2023 年 7 月 1 日起施行。

总理 李强

2023 年 4 月 27 日

商用密码管理条例

（1999 年 10 月 7 日中华人民共和国国务院令第 273 号发布 2023 年 4 月 27 日中华人民共和国国务院令第 760 号修订）

第一章 总 则

第一条 为了规范商用密码应用和管理，鼓励和促进商用密码产业发展，保障网络与信息安全，维护国家安全和社会公共利益，保护公民、法人和其他组织的合法权益，根据《中华人民共和国密码法》等法律，制定本条例。

第二条 在中华人民共和国境内的商用密码科研、生产、销售、服务、检测、认证、进出口、应用等活动及监督管理，适用本条例。

本条例所称商用密码，是指采用特定变换的方法对不属于国家秘密的信息等进行加密保护、安全认证的技术、产品和服务。

第三条 坚持中国共产党对商用密码工作的领导，贯彻落实总体国家安全观。国家密码管理部门负责管理全国的商用密码工作。县级以上地方各级密码管理部门负责管理本行政区域的商用密码工作。

网信、商务、海关、市场监督管理等有关部门在各自职责范围内负责商用密码有关管理工作。

第四条 国家加强商用密码人才培养，建立健全商用密码人才发展体制机制和人才评价制度，鼓励和支持密码相关学科和专业建设，规范商用密码社会化培训，促进商用密码人才交流。

第五条 各级人民政府及其有关部门应当采取多种形式加强商用密码宣传教育，增强公民、法人和其他组织的密码安全意识。

第六条 商用密码领域的学会、行业协会等社会组织依照法律、行政法规及其章程的规定，开展学术交流、政策研究、公共服务等活动， 加强学术和行业自律，推动诚信建设，促进行业健康发展。

密码管理部门应当加强对商用密码领域社会组织的指导和支持。

第二章 科技创新与标准化

第七条 国家建立健全商用密码科学技术创新促进机制，支持商用密码科学技术自主创新，对作出突出贡献的组织和个人按照国家有关规定予以表彰和奖励。

国家依法保护商用密码领域的知识产权。从事商用密码活动， 应当增强知识产权意识，提高运用、保护和管理知识产权的能力。

国家鼓励在外商投资过程中基于自愿原则和商业规则开展商用密码技术合作。行政机关及其工作人员不得利用行政手段强制转让商用密码技术。

第八条 国家鼓励和支持商用密码科学技术成果转化和产业化应用，建立和完善商用密码科学技术成果信息汇交、发布和应用情况反馈机制。

第九条 国家密码管理部门组织对法律、行政法规和国家有关规定要求使用商用密码进行保护的网络与信息系统所使用的密码算法、密码协议、密钥管理机制等商用密码技术进行审查鉴定。

第十条 国务院标准化行政主管部门和国家密码管理部门依据各自职责，组织制定商用密码国家标准、行业标准， 对商用密码团体标准的制定进行规范、引导和监督。国家密码管理部门依据职责， 建立商用密码标准实施信息反馈和评估机制，对商用密码标准实施进行监督检查。

国家推动参与商用密码国际标准化活动，参与制定商用密码国际标准，推进商用密码中国标准与国外标准之间的转化运用，鼓励企业、社会团体和教育、科研机构等参与商用密码国际标准化活动。

其他领域的标准涉及商用密码的，应当与商用密码国家标准、行业标准保持协调。

第十一条 从事商用密码活动，应当符合有关法律、行政法规、商用密码强制性国家标准，以及自我声明公开标准的技术要求。

国家鼓励在商用密码活动中采用商用密码推荐性国家标准、行业标准， 提升商用密码的防护能力，维护用户的合法权益。

第三章 检测认证

第十二条 国家推进商用密码检测认证体系建设，鼓励在商用密码活动中自愿接受商用密码检测认证。

第十三条 从事商用密码产品检测、网络与信息系统商用密码应用安全性评估等商用密码检测活动，向社会出具具有证明作用的数据、结果的机构， 应当经国家密码管理部门认定，依法取得商用密码检测机构资质。

第十四条 取得商用密码检测机构资质，应当符合下列条件：

(一)具有法人资格；

(二)具有与从事商用密码检测活动相适应的资金、场所、设备设施、专业人

员和专业能力；

(三)具有保证商用密码检测活动有效运行的管理体系。

第十五条 申请商用密码检测机构资质，应当向国家密码管理部门提出书面申请，并提交符合本条例第十四条规定条件的材料。

国家密码管理部门应当自受理申请之日起20个工作日内，对申请进行审查，并依法作出是否准予认定的决定。

需要对申请人进行技术评审的，技术评审所需时间不计算在本条规定的期限内。国家密码管理部门应当将所需时间书面告知申请人。

第十六条 商用密码检测机构应当按照法律、行政法规和商用密码检测技术规范、规则， 在批准范围内独立、公正、科学、诚信地开展商用密码检测，对出具的检测数据、结果负责，并定期向国家密码管理部门报送检测实施情况。

商用密码检测技术规范、规则由国家密码管理部门制定并公布。

第十七条 国务院市场监督管理部门会同国家密码管理部门建立国家统一推行的商用密码认证制度，实行商用密码产品、服务、管理体系认证， 制定并公布认证目录和技术规范、规则。

第十八条 从事商用密码认证活动的机构，应当依法取得商用密码认证机构资质。

申请商用密码认证机构资质，应当向国务院市场监督管理部门提出书面申请。申请人除应当符合法律、行政法规和国家有关规定要求的认证机构基本条件外，还应当具有与从事商用密码认证活动相适应的检测、检查等技术能力。

国务院市场监督管理部门在审查商用密码认证机构资质申请时，应当征求国家密码管理部门的意见。

第十九条 商用密码认证机构应当按照法律、行政法规和商用密码认证技术规范、规则， 在批准范围内独立、公正、科学、诚信地开展商用密码认证，对出具的认证结论负责。

商用密码认证机构应当对其认证的商用密码产品、服务、管理体系实施有效的跟踪调查，以保证通过认证的商用密码产品、服务、管理体系持续符合认证要求。

第二十条 涉及国家安全、国计民生、社会公共利益的商用密码产品，应当

依法列入网络关键设备和网络安全专用产品目录，由具备资格的商用密码检测、认证机构检测认证合格后，方可销售或者提供。

第二十一条 商用密码服务使用网络关键设备和网络安全专用产品的，应当经商用密码认证机构对该商用密码服务认证合格。

第四章 电子认证

第二十二条 采用商用密码技术提供电子认证服务，应当具有与使用密码相适应的场所、设备设施、专业人员、专业能力和管理体系， 依法取得国家密码管理部门同意使用密码的证明文件。

第二十三条 电子认证服务机构应当按照法律、行政法规和电子认证服务密码使用技术规范、规则， 使用密码提供电子认证服务，保证其电子认证服务密码使用持续符合要求。

电子认证服务密码使用技术规范、规则由国家密码管理部门制定并公布。

第二十四条 采用商用密码技术从事电子政务电子认证服务的机构，应当经国家密码管理部门认定，依法取得电子政务电子认证服务机构资质。

第二十五条 取得电子政务电子认证服务机构资质，应当符合下列条件：

(一)具有企业法人或者事业单位法人资格；

(二)具有与从事电子政务电子认证服务活动及其使用密码相适应的资金、场所、设备设施和专业人员；

(三)具有为政务活动提供长期电子政务电子认证服务的能力；

(四)具有保证电子政务电子认证服务活动及其使用密码安全运行的管理体系。

第二十六条 申请电子政务电子认证服务机构资质，应当向国家密码管理部门提出书面申请，并提交符合本条例第二十五条规定条件的材料。

国家密码管理部门应当自受理申请之日起 20 个工作日内，对申请进行审查，并依法作出是否准予认定的决定。

需要对申请人进行技术评审的，技术评审所需时间不计算在本条规定的期限内。国家密码管理部门应当将所需时间书面告知申请人。

第二十七条 外商投资电子政务电子认证服务，影响或者可能影响国家安全的，应当依法进行外商投资安全审查。

第二十八条 电子政务电子认证服务机构应当按照法律、行政法规和电子政务电子认证服务技术规范、规则， 在批准范围内提供电子政务电子认证服务，并定期向主要办事机构所在地省、自治区、直辖市密码管理部门报送服务实施情况。

电子政务电子认证服务技术规范、规则由国家密码管理部门制定并公布。

第二十九条 国家建立统一的电子认证信任机制。国家密码管理部门负责电子认证信任源的规划和管理，会同有关部门推动电子认证服务互信互认。

第三十条 密码管理部门会同有关部门负责政务活动中使用电子签名、数据电文的管理。

政务活动中电子签名、电子印章、电子证照等涉及的电子认证服务， 应当由依法设立的电子政务电子认证服务机构提供。

第五章 进出口

第三十一条 涉及国家安全、社会公共利益且具有加密保护功能的商用密码，列入商用密码进口许可清单，实施进口许可。涉及国家安全、社会公共利益或者中国承担国际义务的商用密码，列入商用密码出口管制清单，实施出口管制。

商用密码进口许可清单和商用密码出口管制清单由国务院商务主管部门会同国家密码管理部门和海关总署制定并公布。

大众消费类产品所采用的商用密码不实行进口许可和出口管制制度。

第三十二条 进口商用密码进口许可清单中的商用密码或者出口商用密码出口管制清单中的商用密码，应当向国务院商务主管部门申请领取进出口许可证。

商用密码的过境、转运、通运、再出口， 在境外与综合保税区等海关特殊监管区域之间进出，或者在境外与出口监管仓库、保税物流中心等保税监管场所之间进出的，适用前款规定。

第三十三条 进口商用密码进口许可清单中的商用密码或者出口商用密码出口管制清单中的商用密码时，应当向海关交验进出口许可证，并按照国家有关规定办理报关手续。

进出口经营者未向海关交验进出口许可证，海关有证据表明进出口产品可能属于商用密码进口许可清单或者出口管制清单范围的，应当向进出口经营者提出质疑；海关可以向国务院商务主管部门提出组织鉴别，并根据国务院商务主管部门会同国家密码管理部门作出的鉴别结论依法处置。在鉴别或者质疑期间， 海关

对进出口产品不予放行。

第三十四条 申请商用密码进出口许可，应当向国务院商务主管部门提出书面申请，并提交下列材料：

(一)申请人的法定代表人、主要经营管理人以及经办人的身份证明；

(二)合同或者协议的副本；

(三)商用密码的技术说明；

(四)最终用户和最终用途证明；

(五)国务院商务主管部门规定提交的其他文件。

国务院商务主管部门应当自受理申请之日起 45 个工作日内，会同国家密码管理部门对申请进行审查，并依法作出是否准予许可的决定。

对国家安全、社会公共利益或者外交政策有重大影响的商用密码出口， 由国务院商务主管部门会同国家密码管理部门等有关部门报国务院批准。报国务院批准的，不受前款规定时限的限制。

第六章 应用促进

第三十五条 国家鼓励公民、法人和其他组织依法使用商用密码保护网络与信息安全，鼓励使用经检测认证合格的商用密码。

任何组织或者个人不得窃取他人加密保护的信息或者非法侵入他人的商用密码保障系统，不得利用商用密码从事危害国家安全、社会公共利益、他人合法权益等违法犯罪活动。

第三十六条 国家支持网络产品和服务使用商用密码提升安全性，支持并规范商用密码在信息领域新技术、新业态、新模式中的应用。

第三十七条 国家建立商用密码应用促进协调机制，加强对商用密码应用的统筹指导。国家机关和涉及商用密码工作的单位在其职责范围内负责本机关、本单位或者本系统的商用密码应用和安全保障工作。

密码管理部门会同有关部门加强商用密码应用信息收集、风险评估、信息通报和重大事项会商，并加强与网络安全监测预警和信息通报的衔接。

第三十八条 法律、行政法规和国家有关规定要求使用商用密码进行保护的关键信息基础设施，其运营者应当使用商用密码进行保护，制定商用密码应用方案，配备必要的资金和专业人员，同步规划、同步建设、同步运行商用密码保障

系统，自行或者委托商用密码检测机构开展商用密码应用安全性评估。

前款所列关键信息基础设施通过商用密码应用安全性评估方可投入运行，运行后每年至少进行一次评估，评估情况按照国家有关规定报送国家密码管理部门或者关键信息基础设施所在地省、自治区、直辖市密码管理部门备案。

第三十九条 法律、行政法规和国家有关规定要求使用商用密码进行保护的关键信息基础设施，使用的商用密码产品、服务应当经检测认证合格， 使用的密码算法、密码协议、密钥管理机制等商用密码技术应当通过国家密码管理部门审查鉴定。

第四十条 关键信息基础设施的运营者采购涉及商用密码的网络产品和服务，可能影响国家安全的，应当依法通过国家网信部门会同国家密码管理部门等有关部门组织的国家安全审查。

第四十一条 网络运营者应当按照国家网络安全等级保护制度要求，使用商用密码保护网络安全。国家密码管理部门根据网络的安全保护等级， 确定商用密码的使用、管理和应用安全性评估要求，制定网络安全等级保护密码标准规范。

第四十二条 商用密码应用安全性评估、关键信息基础设施安全检测评估、网络安全等级测评应当加强衔接，避免重复评估、测评。

第七章 监督管理

第四十三条 密码管理部门依法组织对商用密码活动进行监督检查，对国家机关和涉及商用密码工作的单位的商用密码相关工作进行指导和监督。

第四十四条 密码管理部门和有关部门建立商用密码监督管理协作机制，加强商用密码监督、检查、指导等工作的协调配合。

第四十五条 密码管理部门和有关部门依法开展商用密码监督检查，可以行使下列职权：

(一)进入商用密码活动场所实施现场检查；

(二)向当事人的法定代表人、主要负责人和其他有关人员调查、了解有关情况；

(三)查阅、复制有关合同、票据、账簿以及其他有关资料。

第四十六条 密码管理部门和有关部门推进商用密码监督管理与社会信用体系相衔接，依法建立推行商用密码经营主体信用记录、信用分级分类监管、失信

惩戒以及信用修复等机制。

第四十七条 商用密码检测、认证机构和电子政务电子认证服务机构及其工作人员，应当对其在商用密码活动中所知悉的国家秘密和商业秘密承担保密义务。

密码管理部门和有关部门及其工作人员不得要求商用密码科研、生产、销售、服务、进出口等单位和商用密码检测、认证机构向其披露源代码等密码相关专有信息，并对其在履行职责中知悉的商业秘密和个人隐私严格保密，不得泄露或者非法向他人提供。

第四十八条 密码管理部门和有关部门依法开展商用密码监督管理，相关单位和人员应当予以配合，任何单位和个人不得非法干预和阻挠。

第四十九条 任何单位或者个人有权向密码管理部门和有关部门举报违反本条例的行为。密码管理部门和有关部门接到举报， 应当及时核实、处理， 并为举报人保密。

第八章 法律责任

第五十条 违反本条例规定，未经认定向社会开展商用密码检测活动，或者未经认定从事电子政务电子认证服务的，由密码管理部门责令改正或者停止违法行为，给予警告，没收违法产品和违法所得；违法所得 30 万元以上的，可以并处违法所得 1 倍以上 3 倍以下罚款；没有违法所得或者违法所得不足 30 万元的，可以并处 10 万元以上 30 万元以下罚款。

违反本条例规定，未经批准从事商用密码认证活动的，由市场监督管理部门会同密码管理部门依照前款规定予以处罚。

第五十一条 商用密码检测机构开展商用密码检测，有下列情形之一的，由密码管理部门责令改正或者停止违法行为，给予警告，没收违法所得；违法所得 30 万元以上的，可以并处违法所得 1 倍以上 3 倍以下罚款；没有违法所得或者违法所得不足 30 万元的，可以并处 10 万元以上 30 万元以下罚款；情节严重的，依法吊销商用密码检测机构资质：

(一)超出批准范围；

(二)存在影响检测独立、公正、诚信的行为；

(三)出具的检测数据、结果虚假或者失实；

(四)拒不报送或者不如实报送实施情况；

(五)未履行保密义务;

(六)其他违反法律、行政法规和商用密码检测技术规范、规则开展商用密码检测的情形。

第五十二条 商用密码认证机构开展商用密码认证，有下列情形之一的，由市场监督管理部门会同密码管理部门责令改正或者停止违法行为，给予警告，没收违法所得；违法所得 30 万元以上的，可以并处违法所得 1 倍以上 3 倍以下罚款；没有违法所得或者违法所得不足 30 万元的，可以并处 10 万元以上 30 万元以下罚款；情节严重的，依法吊销商用密码认证机构资质：

(一)超出批准范围;

(二)存在影响认证独立、公正、诚信的行为;

(三)出具的认证结论虚假或者失实;

(四)未对其认证的商用密码产品、服务、管理体系实施有效的跟踪调查;

(五)未履行保密义务;

(六)其他违反法律、行政法规和商用密码认证技术规范、规则开展商用密码认证的情形。

第五十三条 违反本条例第二十条、第二十一条规定，销售或者提供未经检测认证或者检测认证不合格的商用密码产品，或者提供未经认证或者认证不合格的商用密码服务的，由市场监督管理部门会同密码管理部门责令改正或者停止违法行为，给予警告，没收违法产品和违法所得；违法所得 10 万元以上的，可以并处违法所得 1 倍以上 3 倍以下罚款；没有违法所得或者违法所得不足 10 万元的，可以并处 3 万元以上 10 万元以下罚款。

第五十四条 电子认证服务机构违反法律、行政法规和电子认证服务密码使用技术规范、规则使用密码的， 由密码管理部门责令改正或者停止违法行为，给予警告，没收违法所得；违法所得 30 万元以上的，可以并处违法所得 1 倍以上 3 倍以下罚款；没有违法所得或者违法所得不足 30 万元的，可以并处 10 万元以上 30 万元以下罚款；情节严重的，依法吊销电子认证服务使用密码的证明文件。

第五十五条 电子政务电子认证服务机构开展电子政务电子认证服务，有下列情形之一的，由密码管理部门责令改正或者停止违法行为，给予警告，没收违法所得；违法所得 30 万元以上的，可以并处违法所得 1 倍以上 3 倍以下罚款；

没有违法所得或者违法所得不足 30 万元的，可以并处 10 万元以上 30 万元以下罚款；情节严重的，责令停业整顿，直至吊销电子政务电子认证服务机构资质：

(一)超出批准范围；

(二)拒不报送或者不如实报送实施情况；

(三)未履行保密义务；

(四)其他违反法律、行政法规和电子政务电子认证服务技术规范、规则提供电子政务电子认证服务的情形。

第五十六条 电子签名人或者电子签名依赖方因依据电子政务电子认证服务机构提供的电子签名认证服务在政务活动中遭受损失，电子政务电子认证服务机构不能证明自己无过错的，承担赔偿责任。

第五十七条 政务活动中电子签名、电子印章、电子证照等涉及的电子认证服务，违反本条例第三十条规定，未由依法设立的电子政务电子认证服务机构提供的，由密码管理部门责令改正，给予警告；拒不改正或者有其他严重情节的，由密码管理部门建议有关国家机关、单位对直接负责的主管人员和其他直接责任人员依法给予处分或者处理。有关国家机关、单位应当将处分或者处理情况书面告知密码管理部门。

第五十八条 违反本条例规定进出口商用密码的，由国务院商务主管部门或者海关依法予以处罚。

第五十九条 窃取他人加密保护的信息，非法侵入他人的商用密码保障系统，或者利用商用密码从事危害国家安全、社会公共利益、他人合法权益等违法活动的，由有关部门依照《中华人民共和国网络安全法》和其他有关法律、行政法规的规定追究法律责任。

第六十条 关键信息基础设施的运营者违反本条例第三十八条、第三十九条规定，未按照要求使用商用密码，或者未按照要求开展商用密码应用安全性评估的，由密码管理部门责令改正，给予警告；拒不改正或者有其他严重情节的，处 10 万元以上 100 万元以下罚款，对直接负责的主管人员处 1 万元以上 10 万元以下罚款。

第六十一条 关键信息基础设施的运营者违反本条例第四十条规定，使用未经安全审查或者安全审查未通过的涉及商用密码的网络产品或者服务的，由有关

主管部门责令停止使用，处采购金额 1 倍以上 10 倍以下罚款；对直接负责的主管人员和其他直接责任人员处 1 万元以上 10 万元以下罚款。

第六十二条 网络运营者违反本条例第四十一条规定，未按照国家网络安全等级保护制度要求使用商用密码保护网络安全的，由密码管理部门责令改正，给予警告；拒不改正或者导致危害网络安全等后果的，处 1 万元以上 10 万元以下罚款，对直接负责的主管人员处 5000 元以上 5 万元以下罚款。

第六十三条 无正当理由拒不接受、不配合或者干预、阻挠密码管理部门、有关部门的商用密码监督管理的，由密码管理部门、有关部门责令改正， 给予警告；拒不改正或者有其他严重情节的，处 5 万元以上 50 万元以下罚款，对直接负责的主管人员和其他直接责任人员处 1 万元以上 10 万元以下罚款；情节特别严重的，责令停业整顿，直至吊销商用密码许可证件。

第六十四条 国家机关有本条例第六十条、第六十一条、第六十二条、第六十三条所列违法情形的，由密码管理部门、有关部门责令改正， 给予警告；拒不改正或者有其他严重情节的，由密码管理部门、有关部门建议有关国家机关对直接负责的主管人员和其他直接责任人员依法给予处分或者处理。有关国家机关应当将处分或者处理情况书面告知密码管理部门、有关部门。

第六十五条 密码管理部门和有关部门的工作人员在商用密码工作中滥用职权、玩忽职守、徇私舞弊， 或者泄露、非法向他人提供在履行职责中知悉的商业秘密、个人隐私、举报人信息的，依法给予处分。

第六十六条 违反本条例规定，构成犯罪的，依法追究刑事责任；给他人造成损害的，依法承担民事责任。

第九章 附 则

第六十七条 本条例自 2023 年 7 月 1 日起施行。

未成年人网络保护条例

中华人民共和国国务院令 第 766 号

《未成年人网络保护条例》已经 2023 年 9 月 20 日国务院第 15 次常务会议通过，现予公布，自 2024 年 1 月 1 日起施行。

总理 李强

2023 年 10 月 16 日

未成年人网络保护条例

第一章 总 则

第一条 为了营造有利于未成年人身心健康的网络环境，保障未成年人合法权益，根据《中华人民共和国未成年人保护法》、《中华人民共和国网络安全法》、《中华人民共和国个人信息保护法》等法律，制定本条例。

第二条 未成年人网络保护工作应当坚持中国共产党的领导，坚持以社会主义核心价值观为引领，坚持最有利于未成年人的原则，适应未成年人身心健康发展和网络空间的规律和特点，实行社会共治。

第三条 国家网信部门负责统筹协调未成年人网络保护工作，并依据职责做好未成年人网络保护工作。

国家新闻出版、电影部门和国务院教育、电信、公安、民政、文化和旅游、卫生健康、市场监督管理、广播电视等有关部门依据各自职责做好未成年人网络保护工作。

县级以上地方人民政府及其有关部门依据各自职责做好未成年人网络保护工作。

第四条 共产主义青年团、妇女联合会、工会、残疾人联合会、关心下一代工作委员会、青年联合会、学生联合会、少年先锋队以及其他人民团体、有关社会组织、基层群众性自治组织， 协助有关部门做好未成年人网络保护工作，维护未成年人合法权益。

第五条 学校、家庭应当教育引导未成年人参加有益身心健康的活动，科学、文明、安全、合理使用网络，预防和干预未成年人沉迷网络。

第六条 网络产品和服务提供者、个人信息处理者、智能终端产品制造者和销售者应当遵守法律、行政法规和国家有关规定，尊重社会公德，遵守商业道德，诚实信用，履行未成年人网络保护义务，承担社会责任。

第七条 网络产品和服务提供者、个人信息处理者、智能终端产品制造者和销售者应当接受政府和社会的监督，配合有关部门依法实施涉及未成年人网络保护工作的监督检查，建立便捷、合理、有效的投诉、举报渠道， 通过显著方式公布投诉、举报途径和方法，及时受理并处理公众投诉、举报。

第八条 任何组织和个人发现违反本条例规定的，可以向网信、新闻出版、

电影、教育、电信、公安、民政、文化和旅游、卫生健康、市场监督管理、广播电视等有关部门投诉、举报。收到投诉、举报的部门应当及时依法作出处理； 不属于本部门职责的，应当及时移送有权处理的部门。

第九条 网络相关行业组织应当加强行业自律，制定未成年人网络保护相关行业规范，指导会员履行未成年人网络保护义务，加强对未成年人的网络保护。

第十条 新闻媒体应当通过新闻报道、专题栏目（节目）、公益广告等方式，开展未成年人网络保护法律法规、政策措施、典型案例和有关知识的宣传， 对侵犯未成年人合法权益的行为进行舆论监督，引导全社会共同参与未成年人网络保护。

第十一条 国家鼓励和支持在未成年人网络保护领域加强科学研究和人才培养，开展国际交流与合作。

第十二条 对在未成年人网络保护工作中作出突出贡献的组织和个人，按照国家有关规定给予表彰和奖励。

第二章 网络素养促进

第十三条 国务院教育部门应当将网络素养教育纳入学校素质教育内容，并会同国家网信部门制定未成年人网络素养测评指标。

教育部门应当指导、支持学校开展未成年人网络素养教育， 围绕网络道德意识形成、网络法治观念培养、网络使用能力建设、人身财产安全保护等， 培育未成年人网络安全意识、文明素养、行为习惯和防护技能。

第十四条 县级以上人民政府应当科学规划、合理布局，促进公益性上网服务均衡协调发展，加强提供公益性上网服务的公共文化设施建设，改善未成年人上网条件。

县级以上地方人民政府应当通过为中小学校配备具有相应专业能力的指导教师、政府购买服务或者鼓励中小学校自行采购相关服务等方式， 为学生提供优质的网络素养教育课程。

第十五条 学校、社区、图书馆、文化馆、青少年宫等场所为未成年人提供互联网上网服务设施的，应当通过安排专业人员、招募志愿者等方式， 以及安装未成年人网络保护软件或者采取其他安全保护技术措施，为未成年人提供上网指导和安全、健康的上网环境。

第十六条 学校应当将提高学生网络素养等内容纳入教育教学活动，并合理使用网络开展教学活动，建立健全学生在校期间上网的管理制度，依法规范管理未成年学生带入学校的智能终端产品，帮助学生养成良好上网习惯，培养学生网络安全和网络法治意识，增强学生对网络信息的获取和分析判断能力。

第十七条 未成年人的监护人应当加强家庭家教家风建设，提高自身网络素养，规范自身使用网络的行为，加强对未成年人使用网络行为的教育、示范、引导和监督。

第十八条 国家鼓励和支持研发、生产和使用专门以未成年人为服务对象、适应未成年人身心健康发展规律和特点的网络保护软件、智能终端产品和未成年人模式、未成年人专区等网络技术、产品、服务， 加强网络无障碍环境建设和改造，促进未成年人开阔眼界、陶冶情操、提高素质。

第十九条 未成年人网络保护软件、专门供未成年人使用的智能终端产品应当具有有效识别违法信息和可能影响未成年人身心健康的信息、保护未成年人个人信息权益、预防未成年人沉迷网络、便于监护人履行监护职责等功能。

国家网信部门会同国务院有关部门根据未成年人网络保护工作的需要，明确未成年人网络保护软件、专门供未成年人使用的智能终端产品的相关技术标准或者要求，指导监督网络相关行业组织按照有关技术标准和要求对未成年人网络保护软件、专门供未成年人使用的智能终端产品的使用效果进行评估。

智能终端产品制造者应当在产品出厂前安装未成年人网络保护软件，或者采用显著方式告知用户安装渠道和方法。智能终端产品销售者在产品销售前应当采用显著方式告知用户安装未成年人网络保护软件的情况以及安装渠道和方法。

未成年人的监护人应当合理使用并指导未成年人使用网络保护软件、智能终端产品等，创造良好的网络使用家庭环境。

第二十条 未成年人用户数量巨大或者对未成年人群体具有显著影响的网络平台服务提供者，应当履行下列义务：

(一)在网络平台服务的设计、研发、运营等阶段， 充分考虑未成年人身心健康发展特点，定期开展未成年人网络保护影响评估；

(二)提供未成年人模式或者未成年人专区等，便利未成年人获取有益身心健康的平台内产品或者服务；

(三)按照国家规定建立健全未成年人网络保护合规制度体系，成立主要由外部成员组成的独立机构，对未成年人网络保护情况进行监督；

(四)遵循公开、公平、公正的原则， 制定专门的平台规则，明确平台内产品或者服务提供者的未成年人网络保护义务，并以显著方式提示未成年人用户依法享有的网络保护权利和遭受网络侵害的救济途径；

(五)对违反法律、行政法规严重侵害未成年人身心健康或者侵犯未成年人其他合法权益的平台内产品或者服务提供者，停止提供服务；

(六)每年发布专门的未成年人网络保护社会责任报告，并接受社会监督。

前款所称的未成年人用户数量巨大或者对未成年人群体具有显著影响的网络平台服务提供者的具体认定办法，由国家网信部门会同有关部门另行制定。

第三章 网络信息内容规范

第二十一条 国家鼓励和支持制作、复制、发布、传播弘扬社会主义核心价值观和社会主义先进文化、革命文化、中华优秀传统文化， 铸牢中华民族共同体意识，培养未成年人家国情怀和良好品德，引导未成年人养成良好生活习惯和行为习惯等的网络信息，营造有利于未成年人健康成长的清朗网络空间和良好网络生态。

第二十二条 任何组织和个人不得制作、复制、发布、传播含有宣扬淫秽、色情、暴力、邪教、迷信、赌博、引诱自残自杀、恐怖主义、分裂主义、极端主义等危害未成年人身心健康内容的网络信息。

任何组织和个人不得制作、复制、发布、传播或者持有有关未成年人的淫秽色情网络信息。

第二十三条 网络产品和服务中含有可能引发或者诱导未成年人模仿不安全行为、实施违反社会公德行为、产生极端情绪、养成不良嗜好等可能影响未成年人身心健康的信息的，制作、复制、发布、传播该信息的组织和个人应当在信息展示前予以显著提示。

国家网信部门会同国家新闻出版、电影部门和国务院教育、电信、公安、文化和旅游、广播电视等部门， 在前款规定基础上确定可能影响未成年人身心健康的信息的具体种类、范围、判断标准和提示办法。

第二十四条 任何组织和个人不得在专门以未成年人为服务对象的网络产品

和服务中制作、复制、发布、传播本条例第二十三条第一款规定的可能影响未成年人身心健康的信息。

网络产品和服务提供者不得在首页首屏、弹窗、热搜等处于产品或者服务醒目位置、易引起用户关注的重点环节呈现本条例第二十三条第一款规定的可能影响未成年人身心健康的信息。

网络产品和服务提供者不得通过自动化决策方式向未成年人进行商业营销。

第二十五条 任何组织和个人不得向未成年人发送、推送或者诱骗、强迫未成年人接触含有危害或者可能影响未成年人身心健康内容的网络信息。

第二十六条 任何组织和个人不得通过网络以文字、图片、音视频等形式，对未成年人实施侮辱、诽谤、威胁或者恶意损害形象等网络欺凌行为。

网络产品和服务提供者应当建立健全网络欺凌行为的预警预防、识别监测和处置机制，设置便利未成年人及其监护人保存遭受网络欺凌记录、行使通知权利的功能、渠道， 提供便利未成年人设置屏蔽陌生用户、本人发布信息可见范围、禁止转载或者评论本人发布信息、禁止向本人发送信息等网络欺凌信息防护选项。

网络产品和服务提供者应当建立健全网络欺凌信息特征库，优化相关算法模型，采用人工智能、大数据等技术手段和人工审核相结合的方式加强对网络欺凌信息的识别监测。

第二十七条 任何组织和个人不得通过网络以文字、图片、音视频等形式，组织、教唆、胁迫、引诱、欺骗、帮助未成年人实施违法犯罪行为。

第二十八条 以未成年人为服务对象的在线教育网络产品和服务提供者，应当按照法律、行政法规和国家有关规定， 根据不同年龄阶段未成年人身心发展特点和认知能力提供相应的产品和服务。

第二十九条 网络产品和服务提供者应当加强对用户发布信息的管理，采取有效措施防止制作、复制、发布、传播违反本条例第二十二条、第二十四条、第二十五条、第二十六条第一款、第二十七条规定的信息， 发现违反上述条款规定的信息的，应当立即停止传输相关信息，采取删除、屏蔽、断开链接等处置措施，防止信息扩散，保存有关记录，向网信、公安等部门报告，并对制作、复制、发布、传播上述信息的用户采取警示、限制功能、暂停服务、关闭账号等处置措施。

网络产品和服务提供者发现用户发布、传播本条例第二十三条第一款规定的

信息未予显著提示的，应当作出提示或者通知用户予以提示；未作出提示的，不得传输该信息。

第三十条　国家网信、新闻出版、电影部门和国务院教育、电信、公安、文化和旅游、广播电视等部门发现违反本条例第二十二条、第二十四条、第二十五条、第二十六条第一款、第二十七条规定的信息的， 或者发现本条例第二十三条第一款规定的信息未予显著提示的，应当要求网络产品和服务提供者按照本条例第二十九条的规定予以处理；对来源于境外的上述信息，应当依法通知有关机构采取技术措施和其他必要措施阻断传播。

第四章 个人信息网络保护

第三十一条　网络服务提供者为未成年人提供信息发布、即时通讯等服务的，应当依法要求未成年人或者其监护人提供未成年人真实身份信息。未成年人或者其监护人不提供未成年人真实身份信息的，网络服务提供者不得为未成年人提供相关服务。

网络直播服务提供者应当建立网络直播发布者真实身份信息动态核验机制，不得向不符合法律规定情形的未成年人用户提供网络直播发布服务。

第三十二条 个人信息处理者应当严格遵守国家网信部门和有关部门关于网络产品和服务必要个人信息范围的规定，不得强制要求未成年人或者其监护人同意非必要的个人信息处理行为，不得因为未成年人或者其监护人不同意处理未成年人非必要个人信息或者撤回同意，拒绝未成年人使用其基本功能服务。

第三十三条 未成年人的监护人应当教育引导未成年人增强个人信息保护意识和能力、掌握个人信息范围、了解个人信息安全风险， 指导未成年人行使其在个人信息处理活动中的查阅、复制、更正、补充、删除等权利， 保护未成年人个人信息权益。

第三十四条 未成年人或者其监护人依法请求查阅、复制、更正、补充、删除未成年人个人信息的，个人信息处理者应当遵守以下规定：

(一)提供便捷的支持未成年人或者其监护人查阅未成年人个人信息种类、数量等的方法和途径，不得对未成年人或者其监护人的合理请求进行限制；

(二)提供便捷的支持未成年人或者其监护人复制、更正、补充、删除未成年人个人信息的功能，不得设置不合理条件；

(三)及时受理并处理未成年人或者其监护人查阅、复制、更正、补充、删除未成年人个人信息的申请，拒绝未成年人或者其监护人行使权利的请求的，应当书面告知申请人并说明理由。

对未成年人或者其监护人依法提出的转移未成年人个人信息的请求，符合国家网信部门规定条件的，个人信息处理者应当提供转移的途径。

第三十五条 发生或者可能发生未成年人个人信息泄露、篡改、丢失的，个人信息处理者应当立即启动个人信息安全事件应急预案，采取补救措施，及时向网信等部门报告，并按照国家有关规定将事件情况以邮件、信函、电话、信息推送等方式告知受影响的未成年人及其监护人。

个人信息处理者难以逐一告知的，应当采取合理、有效的方式及时发布相关警示信息，法律、行政法规另有规定的除外。

第三十六条 个人信息处理者对其工作人员应当以最小授权为原则，严格设定信息访问权限，控制未成年人个人信息知悉范围。工作人员访问未成年人个人信息的，应当经过相关负责人或者其授权的管理人员审批，记录访问情况，并采取技术措施，避免违法处理未成年人个人信息。

第三十七条 个人信息处理者应当自行或者委托专业机构每年对其处理未成年人个人信息遵守法律、行政法规的情况进行合规审计， 并将审计情况及时报告网信等部门。

第三十八条 网络服务提供者发现未成年人私密信息或者未成年人通过网络发布的个人信息中涉及私密信息的，应当及时提示，并采取停止传输等必要保护措施，防止信息扩散。

网络服务提供者通过未成年人私密信息发现未成年人可能遭受侵害的，应当立即采取必要措施保存有关记录，并向公安机关报告。

第五章 网络沉迷防治

第三十九条 对未成年人沉迷网络进行预防和干预，应当遵守法律、行政法规和国家有关规定。

教育、卫生健康、市场监督管理等部门依据各自职责对从事未成年人沉迷网络预防和干预活动的机构实施监督管理。

第四十条 学校应当加强对教师的指导和培训，提高教师对未成年学生沉迷

网络的早期识别和干预能力。对于有沉迷网络倾向的未成年学生，学校应当及时告知其监护人，共同对未成年学生进行教育和引导，帮助其恢复正常的学习生活。

第四十一条 未成年人的监护人应当指导未成年人安全合理使用网络，关注未成年人上网情况以及相关生理状况、心理状况、行为习惯，防范未成年人接触危害或者可能影响其身心健康的网络信息，合理安排未成年人使用网络的时间，预防和干预未成年人沉迷网络。

第四十二条 网络产品和服务提供者应当建立健全防沉迷制度，不得向未成年人提供诱导其沉迷的产品和服务，及时修改可能造成未成年人沉迷的内容、功能和规则，并每年向社会公布防沉迷工作情况，接受社会监督。

第四十三条 网络游戏、网络直播、网络音视频、网络社交等网络服务提供者应当针对不同年龄阶段未成年人使用其服务的特点，坚持融合、友好、实用、有效的原则，设置未成年人模式，在使用时段、时长、功能和内容等方面按照国家有关规定和标准提供相应的服务，并以醒目便捷的方式为监护人履行监护职责提供时间管理、权限管理、消费管理等功能。

第四十四条 网络游戏、网络直播、网络音视频、网络社交等网络服务提供者应当采取措施，合理限制不同年龄阶段未成年人在使用其服务中的单次消费数额和单日累计消费数额，不得向未成年人提供与其民事行为能力不符的付费服务。

第四十五条 网络游戏、网络直播、网络音视频、网络社交等网络服务提供者应当采取措施，防范和抵制流量至上等不良价值倾向，不得设置以应援集资、投票打榜、刷量控评等为主题的网络社区、群组、话题，不得诱导未成年人参与应援集资、投票打榜、刷量控评等网络活动，并预防和制止其用户诱导未成年人实施上述行为。

第四十六条 网络游戏服务提供者应当通过统一的未成年人网络游戏电子身份认证系统等必要手段验证未成年人用户真实身份信息。

网络产品和服务提供者不得为未成年人提供游戏账号租售服务。

第四十七条 网络游戏服务提供者应当建立、完善预防未成年人沉迷网络的游戏规则，避免未成年人接触可能影响其身心健康的游戏内容或者游戏功能。

网络游戏服务提供者应当落实适龄提示要求，根据不同年龄阶段未成年人身心发展特点和认知能力，通过评估游戏产品的类型、内容与功能等要素，对游戏

产品进行分类，明确游戏产品适合的未成年人用户年龄阶段，并在用户下载、注册、登录界面等位置予以显著提示。

第四十八条 新闻出版、教育、卫生健康、文化和旅游、广播电视、网信等部门应当定期开展预防未成年人沉迷网络的宣传教育，监督检查网络产品和服务提供者履行预防未成年人沉迷网络义务的情况，指导家庭、学校、社会组织互相配合，采取科学、合理的方式对未成年人沉迷网络进行预防和干预。

国家新闻出版部门牵头组织开展未成年人沉迷网络游戏防治工作，会同有关部门制定关于向未成年人提供网络游戏服务的时段、时长、消费上限等管理规定。

卫生健康、教育等部门依据各自职责指导有关医疗卫生机构、高等学校等，开展未成年人沉迷网络所致精神障碍和心理行为问题的基础研究和筛查评估、诊断、预防、干预等应用研究。

第四十九条 严禁任何组织和个人以虐待、胁迫等侵害未成年人身心健康的方式干预未成年人沉迷网络、侵犯未成年人合法权益。

第六章 法律责任

第五十条 地方各级人民政府和县级以上有关部门违反本条例规定，不履行未成年人网络保护职责的，由其上级机关责令改正；拒不改正或者情节严重的，对负有责任的领导人员和直接责任人员依法给予处分。

第五十一条 学校、社区、图书馆、文化馆、青少年宫等违反本条例规定，不履行未成年人网络保护职责的，由教育、文化和旅游等部门依据各自职责责令改正；拒不改正或者情节严重的，对负有责任的领导人员和直接责任人员依法给予处分。

第五十二条 未成年人的监护人不履行本条例规定的监护职责或者侵犯未成年人合法权益的，由未成年人居住地的居民委员会、村民委员会、妇女联合会，监护人所在单位，中小学校、幼儿园等有关密切接触未成年人的单位依法予以批评教育、劝诫制止、督促其接受家庭教育指导等。

第五十三条 违反本条例第七条、第十九条第三款、第三十八条第二款规定的，由网信、新闻出版、电影、教育、电信、公安、民政、文化和旅游、市场监督管理、广播电视等部门依据各自职责责令改正； 拒不改正或者情节严重的，处 5 万元以上 50 万元以下罚款，对直接负责的主管人员和其他直接责任人员处 1

万元以上 10 万元以下罚款。

第五十四条 违反本条例第二十条第一款规定的，由网信、新闻出版、电信、公安、文化和旅游、广播电视等部门依据各自职责责令改正， 给予警告，没收违法所得；拒不改正的，并处 100 万元以下罚款，对直接负责的主管人员和其他直接责任人员处 1 万元以上 10 万元以下罚款。

违反本条例第二十条第一款第一项和第五项规定，情节严重的，由省级以上网信、新闻出版、电信、公安、文化和旅游、广播电视等部门依据各自职责责令改正，没收违法所得，并处 5000 万元以下或者上一年度营业额百分之五以下罚款，并可以责令暂停相关业务或者停业整顿、通报有关部门依法吊销相关业务许可证或者吊销营业执照；对直接负责的主管人员和其他直接责任人员处 10 万元以上 100 万元以下罚款，并可以决定禁止其在一定期限内担任相关企业的董事、监事、高级管理人员和未成年人保护负责人。

第五十五条 违反本条例第二十四条、第二十五条规定的，由网信、新闻出版、电影、电信、公安、文化和旅游、市场监督管理、广播电视等部门依据各自职责责令限期改正，给予警告，没收违法所得，可以并处 10 万元以下罚款；拒不改正或者情节严重的，责令暂停相关业务、停产停业或者吊销相关业务许可证、吊销营业执照，违法所得 100 万元以上的，并处违法所得 1 倍以上 10 倍以下罚款，没有违法所得或者违法所得不足 100 万元的，并处 10 万元以上 100 万元以下罚款。

第五十六条 违反本条例第二十六条第二款和第三款、第二十八条、第二十九条第一款、第三十一条第二款、第三十六条、第三十八条第一款、第四十二条至第四十五条、第四十六条第二款、第四十七条规定的， 由网信、新闻出版、电影、教育、电信、公安、文化和旅游、广播电视等部门依据各自职责责令改正，给予警告，没收违法所得，违法所得 100 万元以上的，并处违法所得 1 倍以上 10 倍以下罚款，没有违法所得或者违法所得不足 100 万元的，并处 10 万元以上 100 万元以下罚款，对直接负责的主管人员和其他直接责任人员处 1 万元以上 10 万元以下罚款；拒不改正或者情节严重的，并可以责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照。

第五十七条 网络产品和服务提供者违反本条例规定，受到关闭网站、吊销

相关业务许可证或者吊销营业执照处罚的，5 年内不得重新申请相关许可，其直接负责的主管人员和其他直接责任人员 5 年内不得从事同类网络产品和服务业务。

第五十八条 违反本条例规定，侵犯未成年人合法权益，给未成年人造成损害的，依法承担民事责任；构成违反治安管理行为的，依法给予治安管理处罚；构成犯罪的，依法追究刑事责任。

第七章 附 则

第五十九条 本条例所称智能终端产品，是指可以接入网络、具有操作系统、能够由用户自行安装应用软件的手机、计算机等网络终端产品。

第六十条 本条例自 2024 年 1 月 1 日起施行。

国务院办公厅关于印发科学数据管理办法的通知

国办发〔2018〕17 号

各省、自治区、直辖市人民政府，国务院各部委、各直属机构：

《科学数据管理办法》已经国务院同意，现印发给你们，请认真贯彻执行。

国务院办公厅

2018 年 3 月 17 日

科学数据管理办法

第一章 总 则

第一条 为进一步加强和规范科学数据管理，保障科学数据安全，提高开放共享水平，更好支撑国家科技创新、经济社会发展和国家安全， 根据《中华人民共和国科学技术进步法》、《中华人民共和国促进科技成果转化法》和《政务信息资源共享管理暂行办法》等规定，制定本办法。

第二条 本办法所称科学数据主要包括在自然科学、工程技术科学等领域，通过基础研究、应用研究、试验开发等产生的数据， 以及通过观测监测、考察调查、检验检测等方式取得并用于科学研究活动的原始数据及其衍生数据。

第三条 政府预算资金支持开展的科学数据采集生产、加工整理、开放共享和管理使用等活动适用本办法。

任何单位和个人在中华人民共和国境内从事科学数据相关活动，符合本办法规定情形的，按照本办法执行。

第四条 科学数据管理遵循分级管理、安全可控、充分利用的原则，明确责任主体，加强能力建设，促进开放共享。

第五条 任何单位和个人从事科学数据采集生产、使用、管理活动应当遵守国家有关法律法规及部门规章，不得利用科学数据从事危害国家安全、社会公共利益和他人合法权益的活动。

第二章 职 责

第六条 科学数据管理工作实行国家统筹、各部门与各地区分工负责的体制。

第七条 国务院科学技术行政部门牵头负责全国科学数据的宏观管理与综合协调，主要职责是：

(一)组织研究制定国家科学数据管理政策和标准规范；

(二)协调推动科学数据规范管理、开放共享及评价考核工作；

(三)统筹推进国家科学数据中心建设和发展；

(四)负责国家科学数据网络管理平台建设和数据维护。

第八条 国务院相关部门、省级人民政府相关部门(以下统称主管部门)在科学数据管理方面的主要职责是：

(一)负责建立健全本部门(本地区)科学数据管理政策和规章制度，宣传贯彻落实国家科学数据管理政策；

(二)指导所属法人单位加强和规范科学数据管理；

(三)按照国家有关规定做好或者授权有关单位做好科学数据定密工作；

(四)统筹规划和建设本部门(本地区)科学数据中心，推动科学数据开放共享；

(五)建立完善有效的激励机制，组织开展本部门(本地区)所属法人单位科学数据工作的评价考核。

第九条 有关科研院所、高等院校和企业等法人单位(以下统称法人单位)是科学数据管理的责任主体，主要职责是：

(一)贯彻落实国家和部门(地方)科学数据管理政策，建立健全本单位科学数据相关管理制度；

(二)按照有关标准规范进行科学数据采集生产、加工整理和长期保存， 确保数据质量；

(三)按照有关规定做好科学数据保密和安全管理工作；

(四)建立科学数据管理系统，公布科学数据开放目录并及时更新，积极开展科学数据共享服务；

(五)负责科学数据管理运行所需软硬件设施等条件、资金和人员保障。

第十条 科学数据中心是促进科学数据开放共享的重要载体，由主管部门委托有条件的法人单位建立，主要职责是：

(一)承担相关领域科学数据的整合汇交工作；

(二)负责科学数据的分级分类、加工整理和分析挖掘；

(三)保障科学数据安全，依法依规推动科学数据开放共享；

(四)加强国内外科学数据方面交流与合作。

第三章 采集、汇交与保存

第十一条 法人单位及科学数据生产者要按照相关标准规范组织开展科学数据采集生产和加工整理，形成便于使用的数据库或数据集。

法人单位应建立科学数据质量控制体系，保证数据的准确性和可用性。

第十二条 主管部门应建立科学数据汇交制度，在国家统一政务网络和数据共享交换平台的基础上开展本部门(本地区)的科学数据汇交工作。

第十三条 政府预算资金资助的各级科技计划(专项、基金等)项目所形成的科学数据，应由项目牵头单位汇交到相关科学数据中心。接收数据的科学数据中心应出具汇交凭证。

各级科技计划(专项、基金等)管理部门应建立先汇交科学数据、再验收科技计划(专项、基金等)项目的机制；项目/课题验收后产生的科学数据也应进行汇交。

第十四条 主管部门和法人单位应建立健全国内外学术论文数据汇交的管理制度。

利用政府预算资金资助形成的科学数据撰写并在国外学术期刊发表论文时需对外提交相应科学数据的，论文作者应在论文发表前将科学数据上交至所在单位统一管理。

第十五条 社会资金资助形成的涉及国家秘密、国家安全和社会公共利益的科学数据必须按照有关规定予以汇交。

鼓励社会资金资助形成的其他科学数据向相关科学数据中心汇交。

第十六条 法人单位应建立科学数据保存制度，配备数据存储、管理、服务和安全等必要设施，保障科学数据完整性和安全性。

第十七条 法人单位应加强科学数据人才队伍建设，在岗位设置、绩效收入、职称评定等方面建立激励机制。

第十八条 国务院科学技术行政部门应加强统筹布局，在条件好、资源优势明显的科学数据中心基础上，优化整合形成国家科学数据中心。

第四章 共享与利用

第十九条 政府预算资金资助形成的科学数据应当按照开放为常态、不开放为例外的原则，由主管部门组织编制科学数据资源目录，有关目录和数据应及时接入国家数据共享交换平台，面向社会和相关部门开放共享，畅通科学数据军民共享渠道。国家法律法规有特殊规定的除外。

第二十条 法人单位要对科学数据进行分级分类，明确科学数据的密级和保密期限、开放条件、开放对象和审核程序等， 按要求公布科学数据开放目录，通过在线下载、离线共享或定制服务等方式向社会开放共享。

第二十一条 法人单位应根据需求，对科学数据进行分析挖掘，形成有价值的科学数据产品，开展增值服务。鼓励社会组织和企业开展市场化增值服务。

第二十二条 主管部门和法人单位应积极推动科学数据出版和传播工作，支持科研人员整理发表产权清晰、准确完整、共享价值高的科学数据。

第二十三条 科学数据使用者应遵守知识产权相关规定，在论文发表、专利申请、专著出版等工作中注明所使用和参考引用的科学数据。

第二十四条 对于政府决策、公共安全、国防建设、环境保护、防灾减灾、公益性科学研究等需要使用科学数据的，法人单位应当无偿提供；确需收费的，应按照规定程序和非营利原则制定合理的收费标准，向社会公布并接受监督。

对于因经营性活动需要使用科学数据的，当事人双方应当签订有偿服务合同，明确双方的权利和义务。

国家法律法规有特殊规定的，遵从其规定。

第五章 保密与安全

第二十五条 涉及国家秘密、国家安全、社会公共利益、商业秘密和个人隐私的科学数据，不得对外开放共享；确需对外开放的，要对利用目的、用户资质、

保密条件等进行审查，并严格控制知悉范围。

第二十六条 涉及国家秘密的科学数据的采集生产、加工整理、管理和使用，按照国家有关保密规定执行。主管部门和法人单位应建立健全涉及国家秘密的科学数据管理与使用制度，对制作、审核、登记、拷贝、传输、销毁等环节进行严格管理。

对外交往与合作中需要提供涉及国家秘密的科学数据的，法人单位应明确提出利用数据的类别、范围及用途， 按照保密管理规定程序报主管部门批准。经主管部门批准后，法人单位按规定办理相关手续并与用户签订保密协议。

第二十七条 主管部门和法人单位应加强科学数据全生命周期安全管理，制定科学数据安全保护措施；加强数据下载的认证、授权等防护管理， 防止数据被恶意使用。

对于需对外公布的科学数据开放目录或需对外提供的科学数据，主管部门和法人单位应建立相应的安全保密审查制度。

第二十八条 法人单位和科学数据中心应按照国家网络安全管理规定，建立网络安全保障体系，采用安全可靠的产品和服务，完善数据管控、属性管理、身份识别、行为追溯、黑名单等管理措施，健全防篡改、防泄露、防攻击、防病毒等安全防护体系。

第二十九条 科学数据中心应建立应急管理和容灾备份机制，按照要求建立应急管理系统，对重要的科学数据进行异地备份。

第六章 附 则

第三十条 主管部门和法人单位应建立完善科学数据管理和开放共享工作评价考核制度。

第三十一条 对于伪造数据、侵犯知识产权、不按规定汇交数据等行为，主管部门可视情节轻重对相关单位和责任人给予责令整改、通报批评、处分等处理或依法给予行政处罚。

对违反国家有关法律法规的单位和个人，依法追究相应责任。

第三十二条 主管部门可参照本办法，制定具体实施细则。涉及国防领域的科学数据管理制度，由有关部门另行规定。

第三十三条 本办法自印发之日起施行。

国务院办公厅关于促进“互联网+医疗健康”发展的意见

国办发〔2018〕26 号

各省、自治区、直辖市人民政府，国务院各部委、各直属机构：

为深入贯彻落实习近平新时代中国特色社会主义思想和党的十九大精神，推进实施健康中国战略，提升医疗卫生现代化管理水平，优化资源配置，创新服务模式，提高服务效率，降低服务成本，满足人民群众日益增长的医疗卫生健康需求，根据《“健康中国 2030”规划纲要》和《国务院关于积极推进“互联网+”行动的指导意见》（国发〔2015〕40 号），经国务院同意，现就促进“互联网+医疗健康”发展提出以下意见。

一、健全“互联网+医疗健康”服务体系

(一)发展“互联网+”医疗服务。

1.鼓励医疗机构应用互联网等信息技术拓展医疗服务空间和内容，构建覆盖诊前、诊中、诊后的线上线下一体化医疗服务模式。

允许依托医疗机构发展互联网医院。医疗机构可以使用互联网医院作为第二名称，在实体医院基础上，运用互联网技术提供安全适宜的医疗服务，允许在线开展部分常见病、慢性病复诊。医师掌握患者病历资料后，允许在线开具部分常见病、慢性病处方。

支持医疗卫生机构、符合条件的第三方机构搭建互联网信息平台，开展远程医疗、健康咨询、健康管理服务，促进医院、医务人员、患者之间的有效沟通。（国家卫生健康委员会、国家发展改革委负责。排在第一位的部门为牵头部门，下同）

2.医疗联合体要积极运用互联网技术，加快实现医疗资源上下贯通、信息互通共享、业务高效协同，便捷开展预约诊疗、双向转诊、远程医疗等服务，推进“基层检查、上级诊断”，推动构建有序的分级诊疗格局。

鼓励医疗联合体内上级医疗机构借助人工智能等技术手段，面向基层提供远程会诊、远程心电诊断、远程影像诊断等服务，促进医疗联合体内医疗机构间检查检验结果实时查阅、互认共享。推进远程医疗服务覆盖全国所有医疗联合体和县级医院，并逐步向社区卫生服务机构、乡镇卫生院和村卫生室延伸，提升基层医疗服务能力和效率。（国家卫生健康委员会、国家发展改革委、财政

部、国家中医药局负责）

（二）创新“互联网+”公共卫生服务。

1.推动居民电子健康档案在线查询和规范使用。以高血压、糖尿病等为重点，加强老年慢性病在线服务管理。以纳入国家免疫规划的儿童为重点服务对象，整合现有预防接种信息平台，优化预防接种服务。鼓励利用可穿戴设备获取生命体征数据，为孕产妇提供健康监测与管理。加强对严重精神障碍患者的信息管理、随访评估和分类干预。（国家卫生健康委员会负责）

2.鼓励医疗卫生机构与互联网企业合作，加强区域医疗卫生信息资源整合，探索运用人群流动、气候变化等大数据技术分析手段，预测疾病流行趋势，加强对传染病等疾病的智能监测，提高重大疾病防控和突发公共卫生事件应对能力。（国家卫生健康委员会负责）

（三）优化“互联网+”家庭医生签约服务。

1.加快家庭医生签约服务智能化信息平台建设与应用，加强上级医院对基层的技术支持，探索线上考核评价和激励机制，提高家庭医生团队服务能力，提升签约服务质量和效率，增强群众对家庭医生的信任度。（国家卫生健康委员会、国家发展改革委、财政部、国家中医药局负责）

2.鼓励开展网上签约服务，为签约居民在线提供健康咨询、预约转诊、慢性病随访、健康管理、延伸处方等服务，推进家庭医生服务模式转变，改善群众签约服务感受。（国家卫生健康委员会负责）

（四）完善“互联网+”药品供应保障服务。

1.对线上开具的常见病、慢性病处方，经药师审核后，医疗机构、药品经营企业可委托符合条件的第三方机构配送。探索医疗卫生机构处方信息与药品零售消费信息互联互通、实时共享，促进药品网络销售和医疗物流配送等规范发展。（国家卫生健康委员会、国家市场监督管理总局、国家药品监督管理局负责）

2.依托全民健康信息平台，加强基于互联网的短缺药品多源信息采集和供应业务协同应用，提升基本药物目录、鼓励仿制的药品目录的遴选等能力。（国家卫生健康委员会、工业和信息化部、国家市场监督管理总局、国家药品监督管理局负责）

(五)推进“互联网+”医疗保障结算服务。

1.加快医疗保障信息系统对接整合，实现医疗保障数据与相关部门数据联通共享，逐步拓展在线支付功能，推进“一站式”结算，为参保人员提供更加便利的服务。(国家医疗保障局、人力资源社会保障部、国家卫生健康委员会等负责)

2.继续扩大联网定点医疗机构范围，逐步将更多基层医疗机构纳入异地就医直接结算。进一步做好外出务工人员和广大“双创”人员跨省异地住院费用直接结算。(国家医疗保障局负责)

3.大力推行医保智能审核和实时监控，将临床路径、合理用药、支付政策等规则嵌入医院信息系统，严格医疗行为和费用监管。(国家医疗保障局负责)

(六)加强“互联网+”医学教育和科普服务。

1.鼓励建立医疗健康教育培训云平台，提供多样化的医学在线课程和医学教育。构建网络化、数字化、个性化、终身化的医学教育培训体系，鼓励医疗工作者开展疑难杂症及重大疾病病例探讨交流，提升业务素质。(国家卫生健康委员会、教育部、人力资源社会保障部负责)

2.实施“继续医学教育+适宜技术推广”行动，围绕健康扶贫需求，重点针对基层和贫困地区，通过远程教育手段，推广普及实用型适宜技术。(国家卫生健康委员会、人力资源社会保障部、国家中医药局负责)

3.建立网络科普平台，利用互联网提供健康科普知识精准教育，普及健康生活方式，提高居民自我健康管理能力和健康素养。(国家卫生健康委员会、中国科协负责)

(七)推进“互联网+”人工智能应用服务。

1.研发基于人工智能的临床诊疗决策支持系统，开展智能医学影像识别、病理分型和多学科会诊以及多种医疗健康场景下的智能语音技术应用，提高医疗服务效率。支持中医辨证论治智能辅助系统应用，提升基层中医诊疗服务能力。开展基于人工智能技术、医疗健康智能设备的移动医疗示范，实现个人健康实时监测与评估、疾病预警、慢病筛查、主动干预。(国家发展改革委、科技部、工业和信息化部、国家卫生健康委员会、国家中医药局按职责分工负责)

2.加强临床、科研数据整合共享和应用，支持研发医疗健康相关的人工智

能技术、医用机器人、大型医疗设备、应急救援医疗设备、生物三维打印技术和可穿戴设备等。顺应工业互联网创新发展趋势，提升医疗健康设备的数字化、智能化制造水平，促进产业升级。(国家发展改革委、工业和信息化部、科技部、国家卫生健康委员会等按职责分工负责)

二、完善“互联网+医疗健康”支撑体系

(八)加快实现医疗健康信息互通共享。

1.各地区、各有关部门要协调推进统一权威、互联互通的全民健康信息平台建设，逐步实现与国家数据共享交换平台的对接联通，强化人口、公共卫生、医疗服务、医疗保障、药品供应、综合管理等数据采集，畅通部门、区域、行业之间的数据共享通道，促进全民健康信息共享应用。(国家发展改革委、工业和信息化部、公安部、人力资源社会保障部、国家卫生健康委员会、国家市场监督管理总局、国家医疗保障局、各省级人民政府负责)

2.加快建设基础资源信息数据库，完善全员人口、电子健康档案、电子病历等数据库。大力提升医疗机构信息化应用水平，二级以上医院要健全医院信息平台功能，整合院内各类系统资源，提升医院管理效率。三级医院要在2020年前实现院内医疗服务信息互通共享，有条件的医院要尽快实现。(国家卫生健康委员会负责)

3.健全基于互联网、大数据技术的分级诊疗信息系统，推动各级各类医院逐步实现电子健康档案、电子病历、检验检查结果的共享，以及在不同层级医疗卫生机构间的授权使用。支持老少边穷地区基层医疗卫生机构信息化软硬件建设。(国家卫生健康委员会、国家发展改革委、财政部负责)

(九)健全“互联网+医疗健康”标准体系。

1.健全统一规范的全国医疗健康数据资源目录与标准体系。加强“互联网+医疗健康”标准的规范管理，制订医疗服务、数据安全、个人信息保护、信息共享等基础标准，全面推开病案首页书写规范、疾病分类与代码、手术操作分类与代码、医学名词术语“四统一”。(国家卫生健康委员会、国家市场监督管理总局负责)

2.加快应用全国医院信息化建设标准和规范，强化省统筹区域平台和医院信息平台功能指引、数据标准的推广应用，统一数据接口，为信息互通共享提

供支撑。(国家卫生健康委员会、国家市场监督管理总局负责)

(十)提高医院管理和便民服务水平。

1.围绕群众日益增长的需求，利用信息技术，优化服务流程，提升服务效能，提高医疗服务供给与需求匹配度。到2020年，二级以上医院普遍提供分时段预约诊疗、智能导医分诊、候诊提醒、检验检查结果查询、诊间结算、移动支付等线上服务。有条件的医疗卫生机构可以开展移动护理、生命体征在线监测、智能医学影像识别、家庭监测等服务。(国家卫生健康委员会、国家中医药局负责)

2.支持医学检验机构、医疗卫生机构联合互联网企业，发展疾病预防、检验检测等医疗健康服务。推进院前急救车载监护系统与区域或医院信息平台连接，做好患者信息规范共享、远程急救指导和院内急救准备等工作，提高急救效能。推广“智慧中药房”，提高中药饮片、成方制剂等药事服务水平。(国家卫生健康委员会、工业和信息化部、国家中医药局负责)

(十一)提升医疗机构基础设施保障能力。

1.提升“互联网+医疗健康”服务保障水平，推进医疗卫生服务体系建设，科学布局，合理配置，实施区域中心医院医疗检测设备配置保障工程，国家对中西部等地区的贫困地区予以适当支持。加快基层医疗卫生机构标准化建设，提高基层装备保障能力。(国家卫生健康委员会、国家发展改革委、财政部负责)

2.重点支持高速宽带网络普遍覆盖城乡各级医疗机构，深入开展电信普遍服务试点，推动光纤宽带网络向农村医疗机构延伸。推动电信企业加快宽带网络演进升级步伐，部署大容量光纤宽带网络，提供高速率网络接入。完善移动宽带网络覆盖，支撑开展急救车载远程诊疗。(工业和信息化部、国家卫生健康委员会按职责分工负责)

3.面向远程医疗、医疗信息共享等需求，鼓励电信企业向医疗机构提供优质互联网专线、虚拟专用网(VPN)等网络接入服务，推进远程医疗专网建设，保障医疗相关数据传输服务质量。支持各医疗机构选择使用高速率高可靠的网络接入服务。(工业和信息化部、国家卫生健康委员会按职责分工负责)

(十二)及时制订完善相关配套政策。

1.适应“互联网+医疗健康”发展，进一步完善医保支付政策。逐步将符合条件的互联网诊疗服务纳入医保支付范围，建立费用分担机制，方便群众就近就医，促进优质医疗资源有效利用。健全互联网诊疗收费政策，加强使用管理，促进形成合理的利益分配机制，支持互联网医疗服务可持续发展。(国家医疗保障局负责)

2.完善医师多点执业政策，鼓励执业医师开展“互联网+医疗健康”服务。(国家卫生健康委员会负责)

三、加强行业监管和安全保障

(十三)强化医疗质量监管。

1.出台规范互联网诊疗行为的管理办法，明确监管底线，健全相关机构准入标准，最大限度减少准入限制，加强事中事后监管，确保医疗健康服务质量和安全。推进网络可信体系建设，加快建设全国统一标识的医疗卫生人员和医疗卫生机构可信医学数字身份、电子实名认证、数据访问控制信息系统，创新监管机制，提升监管能力。建立医疗责任分担机制，推行在线知情同意告知，防范和化解医疗风险。(国家卫生健康委员会、国家网信办、工业和信息化部、公安部负责)

2.互联网医疗健康服务平台等第三方机构应当确保提供服务人员的资质符合有关规定要求，并对所提供的服务承担责任。“互联网+医疗健康”服务产生的数据应当全程留痕，可查询、可追溯，满足行业监管需求。(国家卫生健康委员会、国家网信办、工业和信息化部、公安部、国家市场监督管理总局负责)

(十四)保障数据信息安全。

1.研究制定健康医疗大数据确权、开放、流通、交易和产权保护的法规。严格执行信息安全和健康医疗数据保密规定，建立完善个人隐私信息保护制度，严格管理患者信息、用户资料、基因数据等，对非法买卖、泄露信息行为依法依规予以惩处。(国家卫生健康委员会、国家网信办、工业和信息化部、公安部负责)

2.加强医疗卫生机构、互联网医疗健康服务平台、智能医疗设备以及关键信息基础设施、数据应用服务的信息防护，定期开展信息安全隐患排查、监测和预警。患者信息等敏感数据应当存储在境内，确需向境外提供的，应当依照

有关规定进行安全评估。(国家卫生健康委员会、国家网信办、工业和信息化部负责)

各地区、各有关部门要结合工作实际，及时出台配套政策措施，确保各项部署落到实处。中西部地区、农村贫困地区、偏远边疆地区要因地制宜，积极发展“互联网+医疗健康”，引入优质医疗资源，提高医疗健康服务的可及性。国家卫生健康委员会要会同有关部门按照任务分工，加强工作指导和督促检查，重要情况及时报告国务院。

国务院办公厅

2018 年 4 月 25 日

国务院办公厅印发关于切实解决老年人运用智能技术困难实施方案的通知

国办发〔2020〕45 号

各省、自治区、直辖市人民政府，国务院各部委、各直属机构：

《关于切实解决老年人运用智能技术困难的实施方案》已经国务院同意，现印发给你们，请结合实际认真贯彻落实。

各地区、各部门要落实主体责任， 加强工作统筹，建立工作台账，明确时间表和路线图，聚焦涉及老年人的高频事项和服务场景，坚持传统服务方式与智能化服务创新并行，切实解决老年人在运用智能技术方面遇到的突出困难，确保各项工作做实做细、落实到位， 为老年人提供更周全、更贴心、更直接的便利化服务。

国务院办公厅

2020 年 11 月 15 日

关于切实解决老年人运用智能技术困难的实施方案

随着我国互联网、大数据、人工智能等信息技术快速发展， 智能化服务得到广泛应用，深刻改变了生产生活方式，提高了社会治理和服务效能。但同时， 我国老龄人口数量快速增长，不少老年人不会上网、不会使用智能手机，在出行、就医、消费等日常生活中遇到不便， 无法充分享受智能化服务带来的便利，老年人面临的“数字鸿沟”问题日益凸显。为进一步推动解决老年人在运用智能技术方面遇到的困难，让老年人更好共享信息化发展成果，制定本实施方案。

一、总体要求

(一)指导思想。

以习近平新时代中国特色社会主义思想为指导，全面贯彻党的十九大和十九届二中、三中、四中、五中全会精神， 认真落实党中央、国务院决策部署，坚持以人民为中心的发展思想，满足人民日益增长的美好生活需要，持续推动充分兼顾老年人需要的智慧社会建设，坚持传统服务方式与智能化服务创新并行，切实解决老年人在运用智能技术方面遇到的困难。要适应统筹推进疫情防控和经济社会发展工作要求，聚焦老年人日常生活涉及的高频事项，做实做细为老年人服务的各项工作，增进包括老年人在内的全体人民福祉，让老年人在信息化发展中有更多获得感、幸福感、安全感。

(二)基本原则。

——坚持传统服务与智能创新相结合。在各类日常生活场景中， 必须保留老年人熟悉的传统服务方式，充分保障在运用智能技术方面遇到困难的老年人的基本需求；紧贴老年人需求特点，加强技术创新，提供更多智能化适老产品和服务，促进智能技术有效推广应用，让老年人能用、会用、敢用、想用。坚持“两条腿”走路，使智能化管理适应老年人，并不断改进传统服务方式，为老年人提供更周全、更贴心、更直接的便利化服务。

——坚持普遍适用与分类推进相结合。强化问题导向和需求导向， 针对老年人在运用智能技术方面遇到的突出共性问题，采取普遍适用的政策措施；对不同年龄段、不同教育背景、不同生活环境和习惯的老年人， 分类梳理问题，采取有针对性、差异化的解决方案。

——坚持线上服务与线下渠道相结合。线上服务更加突出人性化， 充分考虑老年人习惯，便利老年人使用；线下渠道进一步优化流程、简化手续， 不断改善老年人服务体验，与线上服务融合发展、互为补充，有效发挥兜底保障作用。

——坚持解决突出问题与形成长效机制相结合。围绕老年人出行、就医等高频事项和服务场景，抓紧解决目前最突出、最紧迫的问题， 切实保障老年人基本服务需要；在此基础上，逐步总结积累经验，不断提升智能化服务水平，完善服务保障措施，建立长效机制，有效解决老年人面临的“数字鸿沟”问题。

(三)工作目标。

在政策引导和全社会的共同努力下，有效解决老年人在运用智能技术方面遇

到的困难，让广大老年人更好地适应并融入智慧社会。到 2020 年底前，集中力量推动各项传统服务兜底保障到位，抓紧出台实施一批解决老年人运用智能技术最迫切问题的有效措施，切实满足老年人基本生活需要。到 2021 年底前，围绕老年人出行、就医、消费、文娱、办事等高频事项和服务场景， 推动老年人享受智能化服务更加普遍，传统服务方式更加完善。到 2022 年底前，老年人享受智能化服务水平显著提升、便捷性不断提高， 线上线下服务更加高效协同，解决老年人面临的“数字鸿沟”问题的长效机制基本建立。

二、重点任务

(一)做好突发事件应急响应状态下对老年人的服务保障。

1.完善“健康码”管理，便利老年人通行。在新冠肺炎疫情低风险地区， 除机场、铁路车站、长途客运站、码头和出入境口岸等特殊场所外， 一般不用查验“健康码”。对需查验“健康码”的情形，通过技术手段将疫情防控相关信息自动整合到“健康码”，简化操作以适合老年人使用，优化代办代查等服务，继续推行“健康码”全国互通互认，便利老年人跨省通行。各地不得将“健康码”作为人员通行的唯一凭证，对老年人等群体可采取凭有效身份证件登记、持纸质证明通行、出示“通信行程卡”作为辅助行程证明等替代措施。有条件的地区和场所要为不使用智能手机的老年人设立“无健康码通道”，做好服务引导和健康核验。在充分保障个人信息安全前提下，推进“健康码”与身份证、社保卡、老年卡、市民卡等互相关联， 逐步实现“刷卡”或“刷脸”通行。对因“健康码”管理不当造成恶劣影响的，根据有关规定追究相关单位负责人的责任。(国家卫生健康委、国务院办公厅、工业和信息化部牵头， 相关部门及各地区按职责分工负责)

2.保障居家老年人基本服务需要。在常态化疫情防控下， 为有效解决老年人无法使用智能技术获取线上服务的困难，组织、引导、便利城乡社区组织、机构和各类社会力量进社区、进家庭， 建设改造一批社区便民消费服务中心、老年服务站等设施，为居家老年人特别是高龄、空巢、失能、留守等重点群体， 提供生活用品代购、餐饮外卖、家政预约、代收代缴、挂号取药、上门巡诊、精神慰藉等服务，满足基本生活需求。(商务部、民政部、住房城乡建设部、国家卫生健康委等相关部门按职责分工负责)

3.在突发事件处置中做好帮助老年人应对工作。在自然灾害、事故灾难、公共卫生事件、社会安全事件等突发事件处置中， 需采取必要智能化管理和服务措施的，要在应急预案中统筹考虑老年人需要，提供突发事件风险提醒、紧急避难场所提示、“一键呼叫”应急救援、受灾人群转移安置、救灾物资分配发放等线上线下相结合的应急救援和保障服务，切实解决在应急处置状态下老年人遇到的困难。(应急部、公安部、国家卫生健康委等相关部门及各地区按职责分工负责)

(二)便利老年人日常交通出行。

4.优化老年人打车出行服务。保持巡游出租车扬召服务， 对电召服务要提高电话接线率。引导网约车平台公司优化约车软件， 增设“一键叫车”功能，鼓励提供电召服务，对老年人订单优先派车。鼓励有条件的地区在医院、居民集中居住区、重要商业区等场所设置出租车候客点、临时停靠点， 依托信息化技术提供便捷叫车服务。(交通运输部及各地区按职责分工负责)

5.便利老年人乘坐公共交通。铁路、公路、水运、民航客运等公共交通在推行移动支付、电子客票、扫码乘车的同时， 保留使用现金、纸质票据、凭证、证件等乘车的方式。推进交通一卡通全国互通与便捷应用，支持具备条件的社保卡增加交通出行功能，鼓励有条件的地区推行老年人凭身份证、社保卡、老年卡等证件乘坐城市公共交通。(交通运输部、人力资源社会保障部、人民银行、国家铁路局、中国民航局、中国国家铁路集团有限公司及各地区按职责分工负责)

6.提高客运场站人工服务质量。进一步优化铁路、公路、水运、民航客运场站及轨道交通站点等窗口服务，方便老年人现场购票、打印票证等。高速公路服务区、收费站等服务窗口要为老年人提供咨询、指引等便利化服务和帮助。(交通运输部、国家铁路局、中国民航局、中国国家铁路集团有限公司及各地区按职责分工负责)

(三)便利老年人日常就医。

7.提供多渠道挂号等就诊服务。医疗机构、相关企业要完善电话、网络、现场等多种预约挂号方式，畅通家人、亲友、家庭签约医生等代老年人预约挂号的渠道。医疗机构应提供一定比例的现场号源，保留挂号、缴费、打印检验报告等人工服务窗口，配备导医、志愿者、社会工作者等人员， 为老年人提供就医指导服务。(国家卫生健康委负责)

8.优化老年人网上办理就医服务。简化网上办理就医服务流程，为老年人提供语音引导、人工咨询等服务，逐步实现网上就医服务与医疗机构自助挂号、取号叫号、缴费、打印检验报告、取药等智能终端设备的信息联通，促进线上线下服务结合。推动通过身份证、社保卡、医保电子凭证等多介质办理就医服务，鼓励在就医场景中应用人脸识别等技术。(国家卫生健康委、公安部、人力资源社会保障部、国家医保局等相关部门按职责分工负责)

9.完善老年人日常健康管理服务。搭建社区、家庭健康服务平台，由家庭签约医生、家人和有关市场主体等共同帮助老年人获得健康监测、咨询指导、药品配送等服务，满足居家老年人的健康需求。推进“互联网+医疗健康”，提供老年人常见病、慢性病复诊以及随访管理等服务。(国家卫生健康委负责)

(四)便利老年人日常消费。

10.保留传统金融服务方式。任何单位和个人不得以格式条款、通知、声明、告示等方式拒收现金。要改善服务人员的面对面服务，零售、餐饮、商场、公园等老年人高频消费场所，水电气费等基本公共服务费用、行政事业性费用缴纳，应支持现金和银行卡支付。强化支付市场监管，加大对拒收现金、拒绝银行卡支付等歧视行为的整改整治力度。采用无人销售方式经营的场所应以适当方式满足消费者现金支付需求，提供现金支付渠道或转换手段。(人民银行、国家发展改革委、市场监管总局、银保监会等相关部门按职责分工负责)

11.提升网络消费便利化水平。完善金融科技标准规则体系，推动金融机构、非银行支付机构、网络购物平台等优化用户注册、银行卡绑定和支付流程，打造大字版、语音版、民族语言版、简洁版等适老手机银行APP，提升手机银行产品的易用性和安全性，便利老年人进行网上购物、订餐、家政、生活缴费等日常消费。平台企业要提供技术措施，保障老年人网上支付安全。(人民银行、国家发展改革委、市场监管总局、银保监会、证监会等相关部门按职责分工负责)

(五)便利老年人文体活动。

12.提高文体场所服务适老化程度。需要提前预约的公园、体育健身场馆、旅游景区、文化馆、图书馆、博物馆、美术馆等场所，应保留人工窗口和电话专线，为老年人保留一定数量的线下免预约进入或购票名额。同时，在老年人进入文体场馆和旅游景区、获取电子讲解、参与全民健身赛事活动、使用智能健身器

械等方面，提供必要的信息引导、人工帮扶等服务。（文化和旅游部、住房城乡建设部、体育总局及各地区按职责分工负责）

13.丰富老年人参加文体活动的智能化渠道。引导公共文化体育机构、文体和旅游类企业提供更多适老化智能产品和服务，同时开展丰富的传统文体活动。针对广场舞、群众歌咏等方面的普遍文化需求， 开发设计适老智能应用，为老年人社交娱乐提供便利。探索通过虚拟现实、增强现实等技术， 帮助老年人便捷享受在线游览、观赛观展、体感健身等智能化服务。（文化和旅游部、体育总局及各地区按职责分工负责）

（六）便利老年人办事服务。

14.优化“互联网+政务服务”应用。依托全国一体化政务服务平台，进一步推进政务数据共享，优化政务服务，实现社会保险待遇资格认证、津贴补贴领取等老年人高频服务事项便捷办理，让老年人办事少跑腿。各级政务服务平台应具备授权代理、亲友代办等功能， 方便不使用或不会操作智能手机的老年人网上办事。（国务院办公厅牵头，相关部门及各地区按职责分工负责）

15.设置必要的线下办事渠道。医疗、社保、民政、金融、电信、邮政、信访、出入境、生活缴费等高频服务事项，应保留线下办理渠道，并向基层延伸，为老年人提供便捷服务。实体办事大厅和社区综合服务设施应合理布局， 配备引导人员，设置现场接待窗口，优先接待老年人，推广“一站式”服务，进一步改善老年人办事体验。（相关部门及各地区按职责分工负责）

（七）便利老年人使用智能化产品和服务应用。

16.扩大适老化智能终端产品供给。推动手机等智能终端产品适老化改造，使其具备大屏幕、大字体、大音量、大电池容量、操作简单等更多方便老年人使用的特点。积极开发智能辅具、智能家居和健康监测、养老照护等智能化终端产品。发布智慧健康养老产品及服务推广目录， 开展应用试点示范，按照适老化要求推动智能终端持续优化升级。建设智慧健康养老终端设备的标准及检测公共服务平台，提升适老产品设计、研发、检测、认证能力。（工业和信息化部、国家发展改革委、民政部、国家卫生健康委、市场监管总局等相关部门按职责分工负责）

17.推进互联网应用适老化改造。组织开展互联网网站、移动互联网应用改

造专项行动，重点推动与老年人日常生活密切相关的政务服务、社区服务、新闻媒体、社交通讯、生活购物、金融服务等互联网网站、移动互联网应用适老化改造，使其更便于老年人获取信息和服务。优化界面交互、内容朗读、操作提示、语音辅助等功能，鼓励企业提供相关应用的“关怀模式”、“长辈模式”，将无障碍改造纳入日常更新维护。(工业和信息化部、民政部、人民银行、银保监会、证监会等相关部门按职责分工负责)

18.为老年人提供更优质的电信服务。持续开展电信普遍服务试点，推进行政村移动网络深度覆盖，加强偏远地区养老服务机构、老年活动中心等宽带网络覆盖。开展精准降费， 引导基础电信企业为老年人提供更大力度的资费优惠，合理降低使用手机、宽带网络等服务费用，推出更多老年人用得起的电信服务。(工业和信息化部、财政部、国务院国资委等相关部门按职责分工负责)

19.加强应用培训。针对老年人在日常生活中的应用困难，组织行业培训机构和专家开展专题培训，提高老年人对智能化应用的操作能力。鼓励亲友、村(居)委会、老年协会、志愿者等为老年人运用智能化产品提供相应帮助。引导厂商针对老年人常用的产品功能，设计制作专门的简易使用手册和视频教程。(教育部、民政部、人力资源社会保障部、国家卫生健康委、市场监管总局、银保监会、证监会等相关部门按职责分工负责)

20.开展老年人智能技术教育。将加强老年人运用智能技术能力列为老年教育的重点内容，通过体验学习、尝试应用、经验交流、互助帮扶等， 引导老年人了解新事物、体验新科技， 积极融入智慧社会。推动各类教育机构针对老年人研发全媒体课程体系，通过老年大学(学校)、养老服务机构、社区教育机构等， 采取线上线下相结合的方式，帮助老年人提高运用智能技术的能力和水平。(教育部、民政部、国家卫生健康委等相关部门按职责分工负责)

三、保障措施

(一)健全工作机制。建立国家发展改革委、国家卫生健康委牵头， 国务院各有关部门参加的部际联席会议机制，明确责任分工，加强统筹推进。各地区要建立相应的协调推进机制，细化措施，确保任务落实到位。各地区、各部门要加强工作协同和信息共享，形成统筹推进、分工负责、上下联动的工作格局， 加快建立解决老年人面临“数字鸿沟”问题的长效机制。(国家发展改革委、国家卫生

健康委牵头，相关部门及各地区按职责分工负责)

(二)完善法规规范。加快推动制修订涉及现金支付、消费者权益保护、防止诈骗、无障碍改造等相关法律法规和部门规章， 切实保障老年人使用智能技术过程中的各项合法权益。各地区要围绕出行、就医、消费、办事等老年人日常生活需求，推动相关地方性法规制修订工作。加快推进相关智能产品与服务标准规范制修订工作，进一步明确有关适老化的内容。(司法部、人民银行、市场监管总局牵头，相关部门及各地区按职责分工负责)

(三)加强督促落实。各地区、各部门要明确时间表、路线图，建立工作台账，强化工作落实，及时跟踪分析涉及本地区、本部门的相关政策措施实施进展及成效，确保各项工作措施做实做细、落实到位。要定期组织开展第三方评估， 对各地区公共服务适老化程度进行评价，相关结果纳入积极应对人口老龄化综合评估。(国家发展改革委、国家卫生健康委牵头，相关部门及各地区按职责分工负责)

(四)保障信息安全。规范智能化产品和服务中的个人信息收集、使用等活动，综合运用多种安全防护手段和风险控制措施，加强技术监测和监督检查，及时曝光并处置违法违规获取个人信息等行为。实施常态化综合监管， 加强与媒体等社会力量合作，充分依托各类举报投诉热线，严厉打击电信网络诈骗等违法行为，切实保障老年人安全使用智能化产品、享受智能化服务。(中央网信办、工业和信息化部、公安部等相关部门按职责分工负责)

(五)开展普及宣传。将促进老年人融入智慧社会作为人口老龄化国情教育重点，加强正面宣传和舆论监督，弘扬尊重和关爱老年人的社会风尚。开展智慧助老行动，将解决老年人运用智能技术困难相关工作，纳入老年友好城市、老年友好社区、老年宜居环境等建设中统筹推进。对各地区有益做法、典型案例及时进行宣传报道，组织开展经验交流。(中央宣传部、中央网信办、国家发展改革委、住房城乡建设部、国家卫生健康委等相关部门按职责分工负责)

关于印发《国务院未成年人保护工作领导小组关于加强未成年人保护工作的意见》的通知

国未保组〔2021〕1 号

各省、自治区、直辖市未成年人保护工作领导小组(委员会)，新疆生产建设兵团未成年人保护工作领导小组，国务院未成年人保护工作领导小组各成员单位：

《国务院未成年人保护工作领导小组关于加强未成年人保护工作的意见》已商中央编办同意，并经国务院未成年人保护工作领导小组第一次全体会议审议通过，现予印发，请认真贯彻落实。

国务院未成年人保护工作领导小组

2021 年 6 月 6 日

国务院未成年人保护工作领导小组关于加强未成年人保护工作的意见

未成年人保护工作关系国家未来和民族振兴。党中央始终高度重视未成年人工作，关心未成年人成长。习近平总书记多次指出， 少年儿童是祖国的未来，是中华民族的希望，强调培养好少年儿童是一项战略任务，事关长远。为深入学习贯彻习近平总书记重要指示批示精神，贯彻落实党中央、国务院关于加强未成年人保护工作决策部署，推动《中华人民共和国未成年人保护法》等法律法规落地落细，现就加强未成年人保护工作提出如下意见：

一、总体要求

(一)指导思想。

以习近平新时代中国特色社会主义思想为指导，深入学习贯彻习近平总书记关于未成年人保护工作重要指示批示精神，全面贯彻落实党的十九大、十九届二中、三中、四中、五中全会精神和党中央、国务院关于未成年人保护工作决策部署，立足新发展阶段、贯彻新发展理念、构建新发展格局， 以满足人民日益增长的美好生活需要为根本目的，进一步加强组织领导、完善运行机制、强化制度建设、健全服务体系，切实保护未成年人身心健康、保障未成年人合法权益。

(二)基本原则。

——坚持党对未成年人保护工作的领导。把党的领导贯穿未成年人保护工作全过程各方面，紧紧围绕统筹推进“五位一体”总体布局和协调推进“四个全面”战略布局，坚持思想道德教育和权益维护保障相融合，大力培育和践行社会主义核心价值观，培养有理想、有道德、有文化、有纪律的社会主义建设者和接班人，培养担当民族复兴大任的时代新人。

——坚持最有利于未成年人的原则。以依法保障未成年人平等享有生存权、发展权、受保护权和参与权等权利， 促进未成年人全面健康成长作为出发点和落脚点，在制定法律法规、政策规划和配置公共资源等方面优先考虑未成年人的利

益和需求，在处理未成年人事务中始终把未成年人权益和全面健康成长放在首位，确保未成年人依法得到特殊、优先保护。

——坚持系统谋划统筹推进。加强全局谋划、统筹布局、整体推进， 有效发挥各级未成年人保护工作协调机制统筹协调、督促指导作用， 着力补短板、强弱项，强化顶层设计、部门协作。坚持未成年人保护工作的政治性、群众性、时代性、协同性， 积极推动各方力量参与未成年人保护工作，构建家庭保护、学校保护、社会保护、网络保护、政府保护、司法保护“六位一体”的新时代未成年人保护工作格局。

(三)总体目标。

到 2025 年，上下衔接贯通、部门协调联动的未成年人保护工作体制机制基本形成，制度体系逐步健全，与未成年人保护法相衔接的法律法规体系不断完善，工作力量有效加强，侵害未成年人合法权益案件发生率明显下降，全社会关心关注未成年人健康成长的氛围显著增强。到 2035 年，与我国经济社会发展相适应、与人口发展战略相匹配的未成年人保护工作体系全面建立，加强未成年人保护工作成为各部门、各行业和社会各界的行动自觉， 成为全面建成社会主义现代化国家的显著标志之一，未成年人的生存权、发展权、受保护权、参与权等权利得到更加充分保障。

二、重点任务

(一)强化家庭监护责任。

1.加强家庭监护指导帮助。巩固和强化家庭监护主体责任， 加大宣传培训和健康教育力度，指导未成年人的父母或者其他监护人依法履行监护职责，抚养、教育和保护未成年人。推动构建家庭教育指导服务体系， 加强社区家长学校、家庭教育指导服务站点建设，为未成年人的父母或其他监护人、被委托人每年提供不少于一次公益性家庭教育指导服务。婚姻登记机关办理离婚登记及人民法院审理家事案件时涉及未成年子女的，要对当事人进行未成年人保护相关家庭教育指导。

2.完善家庭监护支持政策。全面落实产假等生育类假期制度和哺乳时间相关规定，鼓励有条件的地区探索开展育儿假试点。加强家庭照护支持指导， 增强家庭科学育儿能力。有条件的地区， 探索对依法收养孤儿和残疾儿童、非生父母履

行监护权的家庭在水电气等公共服务方面给予优惠。地方政府在配租公租房时，对符合当地住房保障条件且有未成年子女的家庭，可根据其未成年子女数量在户型选择方面给予适当照顾。推进儿童福利机构拓展集养、治、教、康和专业社会工作服务于一体的社会服务功能，探索向社会残疾儿童提供服务。

3.推进家庭监护监督工作。指导村(居)民委员会等相关组织对未成年人的父母或者其他监护人履行监护情况开展监督。村(居)民委员会等相关组织发现未成年人的父母或者其他监护人拒绝或者怠于履行监护责任时，要予以劝阻、制止或者批评教育，督促其履行监护职责；情节严重导致未成年人处于危困状态或造成严重后果的，要及时采取保护措施并向相关部门报告。

4.依法处置监护人侵害未成年人权益行为。公安机关接到报告或者公安机关、人民检察院、人民法院在办理案件过程中发现未成年人的父母或者其他监护人存在不依法履行监护职责或者侵犯未成年人合法权益的，应当予以训诫，并可以责令其接受家庭教育指导。对监护人严重损害未成年人身心健康及合法权益， 或者不履行监护职责致未成年人处于危困状态等监护侵害行为，依法督促、支持起诉。加强宣传引导和警示教育，及时向社会公布监护人侵害未成年人权益行为处置情况案例。

(二)加强学校保护工作。

5.加强未成年人思想道德教育。指导学校深入开展共产主义、中国特色社会主义和中国梦学习宣传教育，坚持立德树人，培育和践行社会主义核心价值观，引导广大未成年人听党话、跟党走， 养成良好思想品德和行为习惯。指导学校加强新修订的《中华人民共和国未成年人保护法》等法律法规宣传教育， 深入开展未成年人法治教育，提升学生法治意识。深化团教协作， 强化少先队实践育人作用，加强未成年人思想道德引领。

6.健全学校保护制度。制定《未成年人学校保护规定》，整合、完善学校保护制度体系。完善校园安全风险防控体系和依法处理机制， 加强校园周边综合治理。提高学生安全意识和自我防护能力，开展反欺凌、交通安全、应急避险自救、防范针对未成年人的犯罪行为等安全教育。积极发展公共交通和专用校车， 解决学生上下学乘车难问题，使用校车的学校要加强校车安全管理和使用。强化校园食品安全管理，严格落实校长(园长)集中用餐陪餐、家长代表陪餐、用餐信息公

开等制度。严厉打击涉及学校和学生安全的违法犯罪行为。推动落实义务教育学校课后服务全覆盖，与当地正常下班时间相衔接，解决家长接学生困难问题。

7.有效防范学生欺凌。进一步完善考评机制，将学生欺凌防治工作纳入责任督学挂牌督导范围、作为教育质量评价和工作考评重要内容。建立健全学生欺凌报告制度，制定学生欺凌防治工作责任清单，压实岗位责任。指导学校定期全面排查，及时发现苗头迹象或隐患点，做好疏导化解工作。完善校规校纪， 健全教育惩戒工作机制，依法依规处置欺凌事件。

8.创新学校保护工作机制。建立学校保护工作评估制度， 评估结果纳入学校管理水平评价和校长考评考核范围。严格落实教职员工准入查询性侵违法犯罪信息制度。充分发挥“法治副校长”、“法治辅导员”作用，常态化开展“法治进校园”、组织模拟法庭、以案释法、开设法治网课等多样化法治教育和法治实践活动，教育引导未成年人遵纪守法。依托中小学校、社区建设少年警校， 加强对未成年人的法治教育、安全教育。引入专业力量参与学生管理服务，有条件的地方，可通过建立学校社会工作站、设立社会工作岗位、政府购买服务等方式， 推进学校社会工作发展。

(三)加大社会保护力度。

9.有效落实强制报告制度。指导国家机关、村(居)民委员会、密切接触未成年人的单位、组织及其工作人员有效履行侵害未成年人事件强制报告义务， 提升识别、发现和报告意识与能力。建立强制报告线索的受理、调查、处置和反馈制度。加强强制报告法律法规和政策措施的宣传培训和教育引导工作。依法依规对未履行报告义务的组织和个人予以惩处。

10.切实发挥群团组织作用。共青团组织要大力推动实施中长期青年发展规划，依托“青年之家”、“12355 青少年服务台”、“青少年维权岗”等阵地有效维护青少年发展权益。妇联组织要加强对未成年人的父母或其他监护人、被委托人的家庭教育指导，依托“儿童之家”等活动场所，为未成年人保护工作提供支持。残联组织要加强残疾未成年人权益保障，落实残疾儿童康复救助制度，指导有条件的地方，扩大残疾儿童康复救助年龄范围，放宽对救助对象家庭经济条件的限制。工会组织要积极开展职工未成年子女关爱服务，推动用人单位母婴设施建设。关心下一代工作委员会等单位、组织要在职责范围内协助相关部门做好未成年人

保护工作。

11.积极指导村(居)民委员会履行法定职责。指导村(居)民委员会落实专人专岗负责未成年人保护工作的法定要求，每个村(社区)至少设立一名儿童主任，优先由村(居)民委员会女性委员或村(社区)妇联主席兼任，儿童数量较多的村(社区)要增设补充儿童主任。推进村(社区)少先队组织建设。持续推进“儿童之家”建设。鼓励村(居)民委员会设立下属的未成年人保护委员会。指导村(居)民委员会落实强制报告和家庭监护监督职责，提升发现报告能力。加强村(社区)未成年人活动场所和设施建设，推进村(社区)党群服务中心、文化活动室等服务设施向未成年人开放。指导村(居)民委员会组织开展未成年人保护相关政策宣讲、知识培训活动。

12.加强未成年人保护领域社会组织建设。培育和发展未成年人保护领域社会组织，到 2025 年，实现未成年人保护专业性社会组织县(市、区、旗)全覆盖。大力发展未成年人保护领域专业社会工作和志愿服务，充分发挥社会工作者在未成年人保护工作中资源链接、能力建设、心理干预、权益保护、法律服务、社会调查、社会观护、教育矫治、社区矫正、收养评估等专业优势， 积极引导志愿者参与未成年人保护工作。健全未成年人保护领域慈善行为导向机制， 依托全国儿童福利信息系统、全国慈善信息公开平台等加强数据共享和供需对接， 引导公益慈善组织提供个性化、差异化、有针对性的服务。

(四)完善网络保护工作。

13.完善未成年人网络保护法规政策体系。加快推动出台未成年人网络保护条例，完善配套政策，净化未成年人网络环境，保障未成年人网络空间安全，保护未成年人合法网络权益，构建网络环境保护长效机制。推动制定未成年人网络保护行业规范和行为准则。加强涉未成年人网课平台和教育移动互联网应用程序规范管理，完善未成年人网课平台备案管理制度。

14.加强未成年人个人信息网络保护。指导监督网络运营者有效履行未成年人个人信息网络保护的平台责任，严格依照法律规定和用户协议收集和使用未成年人个人信息。指导网络运营者对未成年人及其监护人提出的更正、删除未成年人网上个人信息的诉求，依法依规予以配合。严厉打击通过网络以文字、图片、音视频等形式对未成年人实施侮辱、诽谤、猥亵或恶意损害形象等网络欺凌行为，

指导网络运营者及时配合制止网络欺凌行为并防止信息扩散。

15.加强防止未成年人网络沉迷工作。规范网络游戏、网络直播和网络短视频等服务，有效遏制未成年人网络沉迷、过度消费等行为。加强前置审查， 严格网络游戏审批管理。严格实行网络游戏用户账号实名注册制度， 推动建立统一的未成年人网络游戏电子身份认证系统。有效控制未成年人使用网络游戏时段、时长，规定时间内不得以任何形式为未成年人提供游戏服务。严格规范向未成年人提供付费服务。加强中小学生手机管理，推进未成年学生在校专心学习。

(五)强化政府保护职能。

16.有效落实政府监护职责。加强政府监护体制机制建设，提高长期监护专业化服务水平，建立健全临时监护工作制度。建立监护评估制度， 建立健全由民政部门指定监护人和终止临时监护情形时监护人的监护能力评估工作规范，科学评判其履行监护职责的能力和条件，推动监护评估规范化专业化。完善因突发事件影响造成监护缺失未成年人救助保护制度措施。进一步健全孤儿保障制度，建立基本生活保障标准动态调整机制。

17.加强困境未成年人关爱服务。加强困境未成年人分类保障，分类实施困境未成年人保障政策。将符合条件的未成年人纳入最低生活保障、特困人员救助供养等社会救助范围，加强对困难家庭的重病、重残未成年人生活保障工作。合理确定事实无人抚养儿童生活补助标准，对符合条件的事实无人抚养儿童按规定落实医疗救助政策。结合实施乡村振兴战略深化农村留守儿童关爱服务， 完善义务教育控辍保学工作机制。进一步落实家庭经济困难儿童教育资助政策和义务教育阶段“两免一补”政策。

18.建设高质量教育体系。坚持教育公益性原则，推进基本公共教育服务均等化，推动义务教育优质均衡发展和城乡一体化。保障农业转移人口随迁子女平等享有基本公共教育服务。完善普惠性学前教育和特殊教育、专门教育保障机制，鼓励高中阶段学校多样化发展。办好每所学校， 关心每名学生成长，坚决克服唯分数、唯升学倾向。规范校外培训，切实减轻中小学生过重校外培训负担。

19.加强未成年人健康综合保障。完善医疗卫生和医疗保障制度，确保未成年人享有基本医疗、卫生保健服务。加强儿童早期发展服务， 推动建立医疗机构对儿童视力、听力、肢体、智力残疾和儿童孤独症早期筛查、诊断、干预和政府

康复救助衔接机制，深入开展重点地区儿童营养改善等项目。做好未成年人基本医疗保障工作，统筹基本医疗保险、大病保险、医疗救助三重制度， 实施综合保障。鼓励有条件的地方研究将基本的治疗性康复辅助器具逐步纳入基本医疗保险支付范围。加强未成年人心理健康教育和服务。重视未成年人早期视力保护， 加强综合防控儿童近视工作，及时预防和控制近视的发生与发展。加强中小学生睡眠管理工作，保证中小学生享有充足睡眠时间。切实加强未成年人肥胖防控工作。

20.推进婴幼儿照护服务。发展普惠托育服务体系，加大对社区婴幼儿照护服务支持力度。遵循婴幼儿发展规律， 完善有关政策法规体系和标准规范，促进婴幼儿照护服务专业化、规范化建设。加强托育机构监督管理，做好卫生保健、备案登记等工作，积极构建综合监管体系。加快培养婴幼儿照护服务专业人才，大力开展职业培训，增强从业人员法治意识。切实强化和落实各方面责任， 确保婴幼儿安全和健康。

21.加强和创新未成年人成长社会环境治理。构建未成年人成长社会环境治理联合执法机制，加大执法力度。落实未成年人入住旅馆、宾馆、酒店的核查与报告制度。加大对营业性歌舞娱乐场所、酒吧、互联网上网服务营业场所违规接待未成年人行为的处罚力度。落实密切接触未成年人行业违法犯罪信息准入查询制度。严格禁止向未成年人销售烟(含电子烟)、酒、彩票或者兑付彩票奖金。依法依规及时清理中小学校、幼儿园、托育机构周边设置的营业性娱乐场所、酒吧、互联网上网服务营业场所及烟(含电子烟)、酒、彩票销售网点。对部分儿童用品依法实施强制性产品认证管理，保障未成年人健康安全。加大互联网上涉及未成年人的重点应用服务的整治和查处力度，加强监管，督促企业切实落实针对未成年人保护的各项措施。督促中小学校、幼儿园、婴幼儿照护服务机构、线下教育培训机构、游乐园等未成年人集中活动场所落实安全主体责任。推进未成年人文身治理工作。做好未满十六周岁辍学学生劝返复学工作。加大对未成年人违法婚姻的治理力度，防止未成年人早婚早育现象。

(六)落实司法保护职责。

22.依法妥善办理涉未成年人案件。坚持“教育、感化、挽救”方针和“教育为主、惩罚为辅”原则，严格落实未成年人刑事案件特别程序，依法惩戒和精准帮教相结合，促进未成年人顺利回归社会。办理未成年人遭受性侵害或者暴力

伤害案件，施行“一站式取证”保护机制。对于性侵害未成年人犯罪，公安、检察部门积极主动沟通，询问被害人同步录音录像全覆盖。对涉案未成年人实施必要的心理干预、经济救助、法律援助、转学安置等保护措施， 积极引导专业社会工作者参与相关保护工作。

23.加强少年法庭建设。深化涉未成年人案件综合审判改革，将与未成年人权益保护和犯罪预防关系密切的涉及未成年人的刑事、民事及行政诉讼案件纳入少年法庭收案范围。审理涉及未成年人的案件， 从有利于未成年人健康成长的角度出发，推行社会调查、社会观护、心理疏导、司法救助、诉讼教育引导等制度，依法给予未成年人特殊、优先保护。加强未成年人法律援助，积极开展司法救助，及时帮扶司法过程中陷入困境的未成年人，充分体现司法的人文关怀。

24.深化未成年人检察法律监督。依法对涉及未成年人的诉讼活动、未成年人重新犯罪预防工作等开展法律监督。及时对未尽到未成年人教育、管理、救助、看护等保护职责的有关单位提出建议。进一步加强涉及未成年人刑事、民事、行政、公益诉讼检察业务统一集中办理工作。开展未成年人刑事案件羁押必要性审查，对涉及未成年人刑事案件立案、侦查和审判活动， 以及涉及未成年人民事诉讼、行政诉讼和执行活动进行监督。开展未成年人监管及未成年人社区矫正活动监督。加大对侵犯未成年人合法权益案件督促、支持相关组织和个人代为提起诉讼的力度，涉及公共利益的依法提起公益诉讼。推动未成年人司法保护协作机制和社会支持体系建设。

25.严厉打击涉未成年人违法犯罪行为。依法严惩利用未成年人实施黑恶势力犯罪，对拉拢、胁迫未成年人参加有组织犯罪的， 从严追诉、从重量刑。加强未成年人毒品预防教育，引导未成年人从小认清毒品危害，自觉抵制毒品。依法严厉惩治引诱、纵容未成年人从事吸贩毒活动的违法犯罪分子。落实《中国反对拐卖人口行动计划(2021-2030 年)》，预防和惩治拐卖未成年人犯罪行为。预防和打击使用童工违法行为。依法查处生产、销售用于未成年人的假冒伪劣食品、药品、玩具、用具和相关设施设备违法犯罪行为。

三、保障措施

(一)加强组织领导。强化党委领导、政府负责、民政牵头、部门协同、社会参与的未成年人保护工作格局。推动各地党委和政府将未成年人保护工作纳入国

民经济和社会发展规划及工作绩效评价。依法将未成年人保护工作纳入乡镇(街道)、村(社区)职责范围。将未成年人保护工作开展情况作为平安建设考核重要内容，落实落细文明城市、文明村镇、文明单位、文明家庭和文明校园创建中未成年人保护相关要求。制定实施《中国儿童发展纲要(2021-2030 年)》。按有关规定组织开展未成年人保护工作表彰奖励，对有突出表现的给予表彰。

(二)加大工作保障。加强未成年人服务设施建设， 建立和改善适合未成年人的活动场所和设施，支持公益性未成年人活动场所和设施的建设和运行。加强未成年人救助保护机构等场所服务设施设备建设。将未成年人保护工作相关经费纳入本级预算。将未成年人关爱服务纳入政府购买服务指导性目录， 通过政府购买服务等方式引导社会工作专业服务机构、公益慈善类社会组织为留守儿童、困境儿童等特殊儿童群体提供专业服务。加强民政部本级和地方各级政府用于社会福利事业的彩票公益金对未成年人保护工作的支持。加强未成年人保护科学研究和人才培养。

(三)充实工作力量。充实基层未成年人保护工作力量， 实现未成年人保护工作一线有机构负责、有专人办事、有经费保障。指导各地根据需要， 通过整合相关编制资源、盘活编制存量、推动机构转型等方式加强未成年人救助保护机构建设，承担好需依法临时监护的未成年人收留、抚养等相关工作。指导乡镇(街道)设立未成年人保护工作站，及时办理未成年人保护相关事务。加强儿童督导员、儿童主任专业化建设，鼓励其考取社会工作职业资格。加强未成年人审判组织建设和审判专业化、队伍职业化建设。各级人民法院、人民检察院根据实际需要明确相应机构或者指定人员负责未成年人审判、检察工作。指导基层公安派出所加强未成年人保护工作，根据实际明确相关人员负责未成年人保护工作。

(四)深入宣传引导。深入开展未成年人保护工作和《中华人民共和国未成年人保护法》等法律法规的宣传教育， 中央和地方有关新闻媒体可设置专栏，基层单位要充分利用所属网站、新媒体、宣传栏等平台， 开展全方位、多角度、立体式宣传活动，贯彻落实《新时代爱国主义教育实施纲要》、《新时代公民道德建设实施纲要》，营造全社会关心支持未成年人保护工作的良好氛围。进一步规范新闻媒体对涉及未成年人相关热点事件的宣传报道，传播社会正能量。

(五)强化监督检查。加强对未成年人保护工作的监督检查， 建立健全业务指

导、督促检查和重大事项通报制度。各级未成年人保护工作协调机制设立专兼职相结合的未成年人权益督查专员，负责牵头对各地各部门开展未成年人保护工作情况进行督促检查，对存在的突出问题以及侵害未成年人权益的恶性案件、重大事件进行跟踪指导、挂牌督办、限时整改。

第三章 工业和信息化部

非经营性互联网信息服务备案管理办法

(2005 年 2 月 8 日中华人民共和国信息产业部令第 33 号公布，自 2005 年 3 月 20 日起施行。根据 2024 年 1 月 18 日中华人民共和国工业和信息化部令第 68 号公布的《工业和信息化部关于修改部分规章的决定》修订)

第一条 为规范非经营性互联网信息服务备案及备案管理，促进互联网信息服务业的健康发展，根据《互联网信息服务管理办法》、《中华人民共和国电信条例》及其他相关法律、行政法规的规定，制定本办法。

第二条 在中华人民共和国境内提供非经营性互联网信息服务，履行备案手续，实施备案管理，适用本办法。

第三条 中华人民共和国工业和信息化部(以下简称“工业和信息化部”)对全国非经营性互联网信息服务备案管理工作进行监督指导，省、自治区、直辖市通信管理局(以下简称“省通信管理局”)具体实施非经营性互联网信息服务的备案管理工作。

拟从事非经营性互联网信息服务的，应当向其住所所在地省通信管理局履行备案手续。

第四条 省通信管理局在备案管理中应当遵循公开、公平、公正的原则，提供便民、优质、高效的服务。

非经营性互联网信息服务提供者从事非经营性互联网信息服务时，应当遵守国家的有关规定，接受有关部门依法实施的监督管理。

第五条 在中华人民共和国境内提供非经营性互联网信息服务，应当依法履行备案手续。

未经备案，不得在中华人民共和国境内从事非经营性互联网信息服务。

本办法所称在中华人民共和国境内提供非经营性互联网信息服务，是指在中

华人民共和国境内的组织或个人利用通过互联网域名访问的网站或者利用仅能通过互联网 IP 地址访问的网站，提供非经营性互联网信息服务。

第六条 省通信管理局通过工业和信息化部备案管理系统，采用网上备案方式进行备案管理。

第七条 拟从事非经营性互联网信息服务的，应当通过工业和信息化部备案管理系统如实填报《非经营性互联网信息服务备案登记表》(以下简称“《备案登记表》”，格式见本办法附录)，履行备案手续。

工业和信息化部根据实际情况，对《备案登记表》进行调整和公布。

第八条 拟通过接入经营性互联网络从事非经营性互联网信息服务的，可以委托因特网接入服务业务经营者、因特网数据中心业务经营者和以其他方式为其网站提供接入服务的电信业务经营者代为履行备案、备案变更、备案注销等手续。

第九条 拟通过接入中国教育和科研计算机网、中国科学技术网、中国国际经济贸易互联网、中国长城互联网等公益性互联网络从事非经营性互联网信息服务的，可以由为其网站提供互联网接入服务的公益性互联网络单位代为履行备案、备案变更、备案注销等手续。

第十条 因特网接入服务业务经营者、因特网数据中心业务经营者以及以其他方式为网站提供接入服务的电信业务经营者和公益性互联网络单位(以下统称“互联网接入服务提供者”)不得在已知或应知拟从事非经营性互联网信息服务的组织或者个人的备案信息不真实的情况下，为其代为履行备案、备案变更、备案注销等手续。

第十一条 拟从事新闻、出版、教育、医疗保健、药品和医疗器械、文化、广播电影电视节目等互联网信息服务，根据法律、行政法规以及国家有关规定应经有关主管部门审核同意的，在履行备案手续时，还应向其住所所在地省通信管理局提交相关主管部门审核同意的文件。

拟从事电子公告服务的，在履行备案手续时，还应当向其住所所在地省通信管理局提交电子公告服务专项备案材料。

第十二条 省通信管理局在收到备案人提交的备案材料后，材料齐全的，应当在二十个工作日内予以备案，向其发放备案编号，并通过工业和信息化部备案管理系统向社会公布有关备案信息；材料不齐全的，不予备案，在二十个工作日内

通知备案人并说明理由。

第十三条 非经营性互联网信息服务提供者应当在其网站开通时在主页底部的中央位置标明其备案编号，并在备案编号下方按要求链接工业和信息化部备案管理系统网址，供公众查询核对。

第十四条 非经营性互联网信息服务提供者在备案有效期内需要变更其《备案登记表》中填报的信息的，应当提前三十日登陆工业和信息化部备案系统向原备案机关履行备案变更手续。

第十五条 非经营性互联网信息服务提供者在备案有效期内需要终止提供服务的，应当在服务终止之日登陆工业和信息化部备案系统向原备案机关履行备案注销手续。

第十六条 非经营性互联网信息服务提供者应当保证所提供的信息内容合法。

本办法所称非经营性互联网信息服务提供者提供的信息内容，是指互联网信息服务提供者的网站的互联网域名或 IP 地址下所包括的信息内容。

第十七条 省通信管理局应当建立信誉管理、社会监督、情况调查等管理机制，对非经营性互联网信息服务活动实施监督管理。

第十八条 互联网接入服务提供者不得为未经备案的组织或者个人从事非经营性互联网信息服务提供互联网接入服务。

对被省通信管理局处以暂时关闭网站或关闭网站处罚的非经营性互联网信息服务提供者或者非法从事非经营性互联网信息服务的组织或者个人，互联网接入服务提供者应立即暂停或终止向其提供互联网接入服务。

第十九条 互联网接入服务提供者应当记录其接入的非经营性互联网信息服务提供者的备案信息。

互联网接入服务提供者应当依照国家有关规定做好用户信息动态管理、记录留存、有害信息报告等网络信息安全管理工作，根据工业和信息化部和省通信管理局的要求对所接入用户进行监督。

第二十条 省通信管理局依法对非经营性互联网信息服务备案实行年度审核。

省通信管理局通过工业和信息化部备案管理系统，采用网上方式进行年度审核。

第二十一条 非经营性互联网信息服务提供者应当在每年规定时间登陆工业

和信息化部备案管理系统，履行年度审核手续。

第二十二条 违反本办法第五条的规定，未履行备案手续提供非经营性互联网信息服务的，由住所所在地省通信管理局责令限期改正，并处一万元罚款；拒不改正的，关闭网站。

超出备案的项目提供服务的，由住所所在地省通信管理局责令限期改正，并处五千元以上一万元以下罚款；拒不改正的，关闭网站并注销备案。

第二十三条 违反本办法第七条第一款的规定，填报虚假备案信息的，由住所所在地省通信管理局关闭网站并注销备案。

第二十四条 违反本办法第十条、第十八条、第十九条的规定的，由违法行为发生地省通信管理局责令改正，并处一万元罚款。

第二十五条 违反本办法第十三条的规定，未在其备案编号下方链接工业和信息化部备案管理系统网址的，由住所所在地省通信管理局责令限期改正；逾期不改正的，处五千元以上一万元以下罚款。

第二十六条 违反本办法第十四条、第十五条的规定，未在规定时间履行备案变更手续，或未依法履行备案注销手续的，由住所所在地省通信管理局责令限期改正，并处一万元罚款。

第二十七条 非经营性信息服务提供者违反国家有关法律规定，依法应暂停或终止服务的，省通信管理局可根据法律、行政法规授权的同级机关的书面认定意见，暂时关闭网站，或关闭网站并注销备案。

第二十八条 在年度审核时，非经营性互联网信息服务提供者有下列情况之一的，由其住所所在地的省通信管理局通过工业和信息化部备案系统等媒体通告责令其限期改正；拒不改正的，关闭网站并注销备案：

(一)未在规定时间登陆备案网站提交年度审核信息的；

(二)新闻、教育、公安、安全、文化、广播电影电视、出版、保密等国家部门依法对各自主管的专项内容提出年度审核否决意见的。

第二十九条 本办法自 2005 年 3 月 20 日起施行。

附录：非经性互联网信息服务备案登记表.pdf

规范互联网信息服务市场秩序若干规定

中华人民共和国工业和信息化部令第 20 号

《规范互联网信息服务市场秩序若干规定》已经 2011 年 12 月 7 日中华人民共和国工业和信息化部第 22 次部务会议审议通过，现予公布，自 2012 年 3 月 15 日起施行。

部长：苗圩

二〇一一年十二月二十九日

规范互联网信息服务市场秩序若干规定

第一条 为了规范互联网信息服务市场秩序，保护互联网信息服务提供者和用户的合法权益，促进互联网行业的健康发展，根据《中华人民共和国电信条例》、《互联网信息服务管理办法》等法律、行政法规的规定，制定本规定。

第二条 在中华人民共和国境内从事互联网信息服务及与互联网信息服务有关的活动，应当遵守本规定。

第三条 工业和信息化部和各省、自治区、直辖市通信管理局(以下统称“电信管理机构”)依法对互联网信息服务活动实施监督管理。

第四条 互联网信息服务提供者应当遵循平等、自愿、公平、诚信的原则提供服务。

第五条 互联网信息服务提供者不得实施下列侵犯其他互联网信息服务提供者合法权益的行为：

(一)恶意干扰用户终端上其他互联网信息服务提供者的服务，或者恶意干扰与互联网信息服务相关的软件等产品(“与互联网信息服务相关的软件等产品”以下简称“产品”)的下载、安装、运行和升级；

(二)捏造、散布虚假事实损害其他互联网信息服务提供者的合法权益， 或者诋毁其他互联网信息服务提供者的服务或者产品；

(三)恶意对其他互联网信息服务提供者的服务或者产品实施不兼容；

(四)欺骗、误导或者强迫用户使用或者不使用其他互联网信息服务提供者的服务或者产品；

(五)恶意修改或者欺骗、误导、强迫用户修改其他互联网信息服务提供者的服务或者产品参数；

(六)其他违反国家法律规定，侵犯其他互联网信息服务提供者合法权益的行为。

第六条 对互联网信息服务提供者的服务或者产品进行评测，应当客观公正。

评测方公开或者向用户提供评测结果的，应当同时提供评测实施者、评测方法、数据来源、用户原始评价、评测手段和评测环境等与评测活动相关的信息。评测结果应当真实准确，与评测活动相关的信息应当完整全面。被评测的服务或者产品与评测方的服务或者产品相同或者功能类似的，评测结果中不得含有评测方的主观评价。

被评测方对评测结果有异议的，可以自行或者委托第三方就评测结果进行再评测，评测方应当予以配合。

评测方不得利用评测结果，欺骗、误导、强迫用户对被评测方的服务或者产品作出处置。

本规定所称评测，是指提供平台供用户评价，或者以其他方式对互联网信息服务或者产品的性能等进行评价和测试。

第七条 互联网信息服务提供者不得实施下列侵犯用户合法权益的行为：

(一)无正当理由拒绝、拖延或者中止向用户提供互联网信息服务或者产品；

(二)无正当理由限定用户使用或者不使用其指定的互联网信息服务或者产品；

(三)以欺骗、误导或者强迫等方式向用户提供互联网信息服务或者产品；

(四)提供的互联网信息服务或者产品与其向用户所作的宣传或者承诺不符；

(五)擅自改变服务协议或者业务规程，降低服务质量或者加重用户责任；

(六)与其他互联网信息服务提供者的服务或者产品不兼容时，未主动向用户提示和说明；

(七)未经提示并由用户主动选择同意，修改用户浏览器配置或者其他设置；

(八)其他违反国家法律规定，侵犯用户合法权益的行为。

第八条 互联网信息服务提供者在用户终端上进行软件下载、安装、运行、升级、卸载等操作的， 应当提供明确、完整的软件功能等信息， 并事先征得用户同意。

互联网信息服务提供者不得实施下列行为：

(一)欺骗、误导或者强迫用户下载、安装、运行、升级、卸载软件；

(二)未提供与软件安装方式同等或者更便捷的卸载方式；

(三)在未受其他软件影响和人为破坏的情况下，未经用户主动选择同意，软件卸载后有可执行代码或者其他不必要的文件驻留在用户终端。

第九条 互联网信息服务终端软件捆绑其他软件的，应当以显著的方式提示用户，由用户主动选择是否安装或者使用，并提供独立的卸载或者关闭方式，不得附加不合理条件。

第十条 互联网信息服务提供者在用户终端弹出广告或者其他与终端软件功能无关的信息窗口的，应当以显著的方式向用户提供关闭或者退出窗口的功能标识。

第十一条 未经用户同意，互联网信息服务提供者不得收集与用户相关、能够单独或者与其他信息结合识别用户的信息(以下简称“用户个人信息”)，不得将用户个人信息提供给他人，但是法律、行政法规另有规定的除外。

互联网信息服务提供者经用户同意收集用户个人信息的，应当明确告知用户收集和处理用户个人信息的方式、内容和用途， 不得收集其提供服务所必需以外的信息，不得将用户个人信息用于其提供服务之外的目的。

第十二条 互联网信息服务提供者应当妥善保管用户个人信息；保管的用户个人信息泄露或者可能泄露时，应当立即采取补救措施；造成或者可能造成严重后果的，应当立即向准予其互联网信息服务许可或者备案的电信管理机构报告，并配合相关部门进行的调查处理。

第十三条 互联网信息服务提供者应当加强系统安全防护，依法维护用户上载信息的安全，保障用户对上载信息的使用、修改和删除。

互联网信息服务提供者不得有下列行为：

(一)无正当理由擅自修改或者删除用户上载信息；

(二)未经用户同意，向他人提供用户上载信息，但是法律、行政法规另有规定的除外；

(三)擅自或者假借用户名义转移用户上载信息，或者欺骗、误导、强迫用户转移其上载信息；

(四)其他危害用户上载信息安全的行为。

第十四条 互联网信息服务提供者应当以显著的方式公布有效联系方式，接受用户及其他互联网信息服务提供者的投诉，并自接到投诉之日起十五日内作出

答复。

第十五条 互联网信息服务提供者认为其他互联网信息服务提供者实施违反本规定的行为，侵犯其合法权益并对用户权益造成或者可能造成重大影响的，应当立即向准予该其他互联网信息服务提供者互联网信息服务许可或者备案的电信管理机构报告。

电信管理机构应当对报告或者发现的可能违反本规定的行为的影响进行评估；影响特别重大的，相关省、自治区、直辖市通信管理局应当向工业和信息化部报告。电信管理机构在依据本规定作出处理决定前，可以要求互联网信息服务提供者暂停有关行为，互联网信息服务提供者应当执行。

第十六条 互联网信息服务提供者违反本规定第五条、第七条或者第十三条的规定，由电信管理机构依据职权责令改正，处以警告，可以并处一万元以上三万元以下的罚款，向社会公告；其中，《中华人民共和国电信条例》或者《互联网信息服务管理办法》规定法律责任的，依照其规定处理。

第十七条 评测方违反本规定第六条的规定的，由电信管理机构依据职权处以警告，可以并处一万元以上三万元以下的罚款，向社会公告。

第十八条 互联网信息服务提供者违反本规定第八条、第九条、第十条、第十一条、第十二条或者第十四条的规定的，由电信管理机构依据职权处以警告，可以并处一万元以上三万元以下的罚款，向社会公告。

第十九条 互联网信息服务提供者违反本规定第十五条规定，不执行电信管理机构暂停有关行为的要求的，由电信管理机构依据职权处以警告，向社会公告。

第二十条 互联网信息服务提供者违反其他法律、行政法规规定的，依照其规定处理。

第二十一条 本规定自 2012 年 3 月 15 日起施行。

电信和互联网用户个人信息保护规定

(2013 年 6 月 28 日中华人民共和国工业和信息化部第 2 次部务会议审议通过 2013 年 7 月 16 日中华人民共和国工业和信息化部第 24 号令公布 自 2013 年 9 月 1 日起施行)

第一章 总 则

第一条 为了保护电信和互联网用户的合法权益，维护网络信息安全，根据

《全国人民代表大会常务委员会关于加强网络信息保护的决定》、《中华人民共和国电信条例》和《互联网信息服务管理办法》等法律、行政法规，制定本规定。

第二条 在中华人民共和国境内提供电信服务和互联网信息服务过程中收集、使用用户个人信息的活动，适用本规定。

第三条 工业和信息化部和各省、自治区、直辖市通信管理局(以下统称电信管理机构)依法对电信和互联网用户个人信息保护工作实施监督管理。

第四条 本规定所称用户个人信息，是指电信业务经营者和互联网信息服务提供者在提供服务的过程中收集的用户姓名、出生日期、身份证件号码、住址、电话号码、账号和密码等能够单独或者与其他信息结合识别用户的信息以及用户使用服务的时间、地点等信息。

第五条 电信业务经营者、互联网信息服务提供者在提供服务的过程中收集、使用用户个人信息，应当遵循合法、正当、必要的原则。

第六条 电信业务经营者、互联网信息服务提供者对其在提供服务过程中收集、使用的用户个人信息的安全负责。

第七条 国家鼓励电信和互联网行业开展用户个人信息保护自律工作。

第二章 信息收集和使用规范

第八条 电信业务经营者、互联网信息服务提供者应当制定用户个人信息收集、使用规则，并在其经营或者服务场所、网站等予以公布。

第九条 未经用户同意，电信业务经营者、互联网信息服务提供者不得收集、使用用户个人信息。

电信业务经营者、互联网信息服务提供者收集、使用用户个人信息的，应当明确告知用户收集、使用信息的目的、方式和范围，查询、更正信息的渠道以及拒绝提供信息的后果等事项。

电信业务经营者、互联网信息服务提供者不得收集其提供服务所必需以外的用户个人信息或者将信息用于提供服务之外的目的，不得以欺骗、误导或者强迫等方式或者违反法律、行政法规以及双方的约定收集、使用信息。

电信业务经营者、互联网信息服务提供者在用户终止使用电信服务或者互联网信息服务后，应当停止对用户个人信息的收集和使用，并为用户提供注销

号码或者账号的服务。

法律、行政法规对本条第一款至第四款规定的情形另有规定的，从其规定。

第十条 电信业务经营者、互联网信息服务提供者及其工作人员对在提供服务过程中收集、使用的用户个人信息应当严格保密，不得泄露、篡改或者毁损，不得出售或者非法向他人提供。

第十一条 电信业务经营者、互联网信息服务提供者委托他人代理市场销售和技术服务等直接面向用户的服务性工作，涉及收集、使用用户个人信息的，应当对代理人的用户个人信息保护工作进行监督和管理，不得委托不符合本规定有关用户个人信息保护要求的代理人代办相关服务。

第十二条 电信业务经营者、互联网信息服务提供者应当建立用户投诉处理机制，公布有效的联系方式，接受与用户个人信息保护有关的投诉，并自接到投诉之日起十五日内答复投诉人。

第三章 安全保障措施

第十三条 电信业务经营者、互联网信息服务提供者应当采取以下措施防止用户个人信息泄露、毁损、篡改或者丢失：

(一)确定各部门、岗位和分支机构的用户个人信息安全管理责任；

(二)建立用户个人信息收集、使用及其相关活动的工作流程和安全管理制度；

(三)对工作人员及代理人实行权限管理，对批量导出、复制、销毁信息实行审查，并采取防泄密措施；

(四)妥善保管记录用户个人信息的纸介质、光介质、电磁介质等载体，并采取相应的安全储存措施；

(五)对储存用户个人信息的信息系统实行接入审查，并采取防入侵、防病毒等措施；

(六)记录对用户个人信息进行操作的人员、时间、地点、事项等信息；

(七)按照电信管理机构的规定开展通信网络安全防护工作；

(八)电信管理机构规定的其他必要措施。

第十四条 电信业务经营者、互联网信息服务提供者保管的用户个人信息发

生或者可能发生泄露、毁损、丢失的，应当立即采取补救措施；造成或者可能造成严重后果的，应当立即向准予其许可或者备案的电信管理机构报告，配合相关部门进行的调查处理。

电信管理机构应当对报告或者发现的可能违反本规定的行为的影响进行评估；影响特别重大的，相关省、自治区、直辖市通信管理局应当向工业和信息化部报告。电信管理机构在依据本规定作出处理决定前，可以要求电信业务经营者和互联网信息服务提供者暂停有关行为，电信业务经营者和互联网信息服务提供者应当执行。

第十五条 电信业务经营者、互联网信息服务提供者应当对其工作人员进行用户个人信息保护相关知识、技能和安全责任培训。

第十六条 电信业务经营者、互联网信息服务提供者应当对用户个人信息保护情况每年至少进行一次自查，记录自查情况，及时消除自查中发现的安全隐患。

第四章 监督检查

第十七条 电信管理机构应当对电信业务经营者、互联网信息服务提供者保护用户个人信息的情况实施监督检查。

电信管理机构实施监督检查时，可以要求电信业务经营者、互联网信息服务提供者提供相关材料，进入其生产经营场所调查情况，电信业务经营者、互联网信息服务提供者应当予以配合。

电信管理机构实施监督检查，应当记录监督检查的情况，不得妨碍电信业务经营者、互联网信息服务提供者正常的经营或者服务活动，不得收取任何费用。

第十八条 电信管理机构及其工作人员对在履行职责中知悉的用户个人信息应当予以保密，不得泄露、篡改或者毁损，不得出售或者非法向他人提供。

第十九条 电信管理机构实施电信业务经营许可及经营许可证年检时，应当对用户个人信息保护情况进行审查。

第二十条 电信管理机构应当将电信业务经营者、互联网信息服务提供者违反本规定的行为记入其社会信用档案并予以公布。

第二十一条 鼓励电信和互联网行业协会依法制定有关用户个人信息保护的

自律性管理制度，引导会员加强自律管理，提高用户个人信息保护水平。

第五章 法律责任

第二十二条 电信业务经营者、互联网信息服务提供者违反第八条、第十二条规定的，由电信管理机构依据职权责令限期改正，予以警告，可以并处一万元以下的罚款。

第二十三条 电信业务经营者、互联网信息服务提供者违反本规定第九条至第十一条、第十三条至第十六条、第十七条第二款规定的，由电信管理机构依据职权责令限期改正，予以警告，可以并处一万元以上三万元以下的罚款，向社会公告；构成犯罪的，依法追究刑事责任。

第二十四条 电信管理机构工作人员在对用户个人信息保护工作实施监督管理的过程中玩忽职守、滥用职权、徇私舞弊的，依法给予处理；构成犯罪的，依法追究刑事责任。

第六章 附 则

第二十五条 本规定自 2013 年 9 月 1 日起施行。

电信业务经营许可管理办法

中华人民共和国工业和信息化部令第 42 号

《电信业务经营许可管理办法》已经 2017 年 6 月 21 日工业和信息化部第 31 次部务会议审议通过，现予公布，自 2017 年 9 月 1 日起施行。工业和信息化部 2009 年 3 月 5 日公布的《电信业务经营许可管理办法》(工业和信息化部令第 5 号)同时废止。

部长 苗圩

2017 年 7 月 3 日

电信业务经营许可管理办法

第一章 总 则

第一条 为了加强电信业务经营许可管理，根据《中华人民共和国电信条例》及其他法律、行政法规的规定，制定本办法。

第二条 在中华人民共和国境内申请、审批、使用和管理电信业务经营许可证(以下简称经营许可证)，适用本办法。

第三条 工业和信息化部和省、自治区、直辖市通信管理局(以下统称电信管

理机构)是经营许可证的审批管理机构。

经营许可证审批管理应当遵循便民、高效、公开、公平、公正的原则。

工业和信息化部建立电信业务综合管理平台(以下简称管理平台)，推进经营许可证的网上申请、审批和管理及相关信息公示、查询、共享， 完善信用管理机制。

第四条 经营电信业务，应当依法取得电信管理机构颁发的经营许可证。

电信业务经营者在电信业务经营活动中，应当遵守经营许可证的规定，接受、配合电信管理机构的监督管理。

电信业务经营者按照经营许可证的规定经营电信业务受法律保护。

第二章 经营许可证的申请

第五条 经营基础电信业务，应当具备下列条件：

(一)经营者为依法设立的专门从事基础电信业务的公司，并且公司的国有股权或者股份不少于 51%；

(二)有业务发展研究报告和组网技术方案；

(三)有与从事经营活动相适应的资金和专业人员；

(四)有从事经营活动的场地、设施及相应的资源；

(五)有为用户提供长期服务的信誉或者能力；

(六)在省、自治区、直辖市范围内经营的， 注册资本最低限额为 1 亿元人民币；在全国或者跨省、自治区、直辖市范围经营的，注册资本最低限额为 10 亿元人民币；

(七)公司及其主要投资者和主要经营管理人员未被列入电信业务经营失信名单；

(八)国家规定的其他条件。

第六条 经营增值电信业务，应当具备下列条件：

(一)经营者为依法设立的公司；

(二)有与开展经营活动相适应的资金和专业人员；

(三)有为用户提供长期服务的信誉或者能力；

(四)在省、自治区、直辖市范围内经营的， 注册资本最低限额为 100 万元人民币；在全国或者跨省、自治区、直辖市范围经营的， 注册资本最低限额为 1000

万元人民币；

(五)有必要的场地、设施及技术方案；

(六)公司及其主要投资者和主要经营管理人员未被列入电信业务经营失信名单；

(七)国家规定的其他条件。

第七条　申请办理基础电信业务经营许可证的，应当向工业和信息化部提交下列申请材料：

(一)公司法定代表人签署的经营基础电信业务的书面申请，内容包括：申请经营电信业务的种类、业务覆盖范围、公司名称和联系方式等；

(二)公司营业执照副本及复印件；

(三)公司概况，包括公司基本情况，拟从事电信业务的机构设置和管理情况、技术力量和经营管理人员情况，与从事经营活动相适应的场地、设施等情况；

(四)公司章程、公司股权结构及股东的有关情况；

(五)业务发展研究报告，包括：经营电信业务的业务发展和实施计划、服务项目、业务覆盖范围、收费方案、预期服务质量、效益分析等；

(六)组网技术方案，包括：网络结构、网络规模、网络建设计划、网络互联方案、技术标准、电信设备的配置、电信资源使用方案等；

(七)为用户提供长期服务和质量保障的措施；

(八)网络与信息安全保障措施；

(九)证明公司信誉的有关材料；

(十)公司法定代表人签署的公司依法经营电信业务的承诺书。

第八条　申请办理增值电信业务经营许可证的，应当向电信管理机构提交下列申请材料：

(一)公司法定代表人签署的经营增值电信业务的书面申请，内容包括：申请经营电信业务的种类、业务覆盖范围、公司名称和联系方式等；

(二)公司营业执照副本及复印件；

(三)公司概况，包括：公司基本情况，拟从事电信业务的人员、场地和设施等情况；

(四)公司章程、公司股权结构及股东的有关情况；

(五)经营电信业务的业务发展和实施计划及技术方案;

(六)为用户提供长期服务和质量保障的措施;

(七)网络与信息安全保障措施;

(八)证明公司信誉的有关材料;

(九)公司法定代表人签署的公司依法经营电信业务的承诺书。

申请经营的电信业务依照法律、行政法规及国家有关规定须经有关主管部门事先审核同意的，应当提交有关主管部门审核同意的文件。

第三章 经营许可证的审批

第九条 经营许可证分为《基础电信业务经营许可证》和《增值电信业务经营许可证》两类。其中，《增值电信业务经营许可证》分为《跨地区增值电信业务经营许可证》和省、自治区、直辖市范围内的《增值电信业务经营许可证》。

《基础电信业务经营许可证》和《跨地区增值电信业务经营许可证》由工业和信息化部审批。省、自治区、直辖市范围内的《增值电信业务经营许可证》由省、自治区、直辖市通信管理局审批。

外商投资电信企业的经营许可证，由工业和信息化部根据《外商投资电信企业管理规定》审批。

第十条 工业和信息化部应当对申请经营基础电信业务的申请材料进行审查。申请材料齐全、符合法定形式的， 应当向申请人出具受理申请通知书。申请材料不齐全或者不符合法定形式的，应当当场或者在五日内一次告知申请人需要补正的全部内容。

工业和信息化部受理申请之后，应当组织专家对第七条第五项、第六项、第八项申请材料进行评审，形成评审意见。

工业和信息化部应当自受理申请之日起 180 日内审查完毕，作出批准或者不予批准的决定。予以批准的，颁发《基础电信业务经营许可证》。不予批准的，应当书面通知申请人并说明理由。

第十一条 电信管理机构应当对申请经营增值电信业务的申请材料进行审查。申请材料齐全、符合法定形式的， 应当向申请人出具受理申请通知书。申请材料不齐全或者不符合法定形式的，应当当场或者在五日内一次告知申请人需要补正的全部内容。

电信管理机构根据管理需要，可以组织专家对第八条第五项、第六项和第七项申请材料进行评审，形成评审意见。

电信管理机构应当自收到全部申请材料之日起 60 日内审查完毕，作出批准或者不予批准的决定。予以批准的， 颁发《跨地区增值电信业务经营许可证》或者省、自治区、直辖市范围内的《增值电信业务经营许可证》。不予批准的，应当书面通知申请人并说明理由。

第十二条 电信管理机构需要对申请材料实质内容进行核实的，可以自行或者委托其他机构对申请人实地查验，申请人应当配合。

电信管理机构组织专家评审的，专家评审时间不计算在本办法第十条第三款和第十一条第三款规定的审查期限内。

第十三条 经营许可证由正文和附件组成。

经营许可证正文应当载明公司名称、法定代表人、业务种类(服务项目)、业务覆盖范围、有效期限、发证机关、发证日期、经营许可证编号等内容。

经营许可证附件可以规定特别事项，由电信管理机构对电信业务经营行为、电信业务经营者权利义务等作出特别要求。

经营许可证应当加盖发证机关印章。

工业和信息化部可以根据实际情况，调整经营许可证的内容，重新公布。

第十四条 《基础电信业务经营许可证》的有效期，根据电信业务种类分为 5 年、10 年。

《跨地区增值电信业务经营许可证》和省、自治区、直辖市范围内的《增值电信业务经营许可证》的有效期为 5 年。

第十五条 经营许可证由公司法定代表人领取，或者由其委托的公司其他人员凭委托书领取。

第四章 经营许可证的使用

第十六条 电信业务经营者应当按照经营许可证所载明的电信业务种类，在规定的业务覆盖范围内，按照经营许可证的规定经营电信业务。

电信业务经营者应当在公司主要经营场所、网站主页、业务宣传材料等显著位置标明其经营许可证编号。

第十七条 获准经营无线电通信业务的，应当按照国家无线电管理相关规定，

持经营许可证向无线电管理机构申请取得无线电频率使用许可。

第十八条 电信业务经营者经发证机关批准，可以授权其持股比例(包括直接持有和间接持有)不少于 51%并符合经营电信业务条件的公司经营其获准经营的电信业务。发证机关应当在电信业务经营者的经营许可证中载明该被授权公司的名称、法定代表人、业务种类、业务覆盖范围等内容。

获准跨地区经营基础电信业务的公司在一个地区不能授权两家或者两家以上公司经营同一项基础电信业务。

第十九条 任何单位和个人不得伪造、涂改、冒用和以任何方式转让经营许可证。

第五章 经营行为的规范

第二十条 基础电信业务经营者应当按照公开、平等的原则为取得经营许可证的电信业务经营者提供经营相关电信业务所需的电信服务和电信资源，不得为无经营许可证的单位或者个人提供用于经营电信业务的电信资源或者提供网络接入、业务接入服务。

第二十一条 电信业务经营者不得以任何方式实施不正当竞争。

第二十二条 为增值电信业务经营者提供网络接入、代理收费和业务合作的基础电信业务经营者，应当对相应增值电信业务的内容、收费、合作行为等进行规范、管理，并建立相应的发现、监督和处置制度及措施。

第二十三条 基础电信业务经营者调整与增值电信业务经营者之间的合作条件的，应当事先征求相关增值电信业务经营者的意见。

有关意见征求情况及记录应当留存，并在电信管理机构监督检查时予以提供。

第二十四条 提供接入服务的增值电信业务经营者应当遵守下列规定：

(一)应当租用取得相应经营许可证的基础电信业务经营者提供的电信服务或者电信资源从事业务经营活动，不得向其他从事接入服务的增值电信业务经营者转租所获得的电信服务或者电信资源；

(二)为用户办理接入服务手续时，应当要求用户提供真实身份信息并予以查验；

(三)不得为未依法取得经营许可证或者履行非经营性互联网信息服务备案手续的单位或者个人提供接入或者代收费等服务；

(四)按照电信管理机构的规定，建立相应的业务管理系统，并按要求实现同电信管理机构相应系统对接，定期报送有关业务管理信息；

(五)对所接入网站传播违法信息的行为进行监督，发现传播明显属于《中华人民共和国电信条例》第五十六条规定的信息的， 应当立即停止接入和代收费等服务，保存有关记录，并向国家有关机关报告；

(六)按照电信管理机构的要求终止或者暂停对违法网站的接入服务。

第二十五条 电信管理机构建立电信业务市场监测制度。相关电信业务经营者应当按照规定向电信管理机构报送相应的监测信息。

第二十六条 电信业务经营者应当按照国家和电信管理机构的规定，明确相应的网络与信息安全管理机构和专职网络与信息安全管理人员，建立网络与信息安全保障、网络安全防护、违法信息监测处置、新业务安全评估、网络安全监测预警、突发事件应急处置、用户信息安全保护等制度， 并具备相应的技术保障措施。

第六章 经营许可证的变更、撤销、吊销和注销

第二十七条 经营许可证有效期届满需要继续经营的，应当提前 90 日向原发证机关提出延续经营许可证的申请；不再继续经营的，应当提前 90 日向原发证机关报告，并做好善后工作。

未在前款规定期限内提出延续经营许可证的申请，或者在经营许可证有效期内未开通电信业务的，有效期届满不予延续。

第二十八条 电信业务经营者或者其授权经营电信业务的公司，遇有因合并或者分立、股东变化等导致经营主体需要变更的情形，或者业务范围需要变化的，应当自公司作出决定之日起 30 日内向原发证机关提出申请。

电信业务经营者变更经营主体、股东的，应当符合本办法第五条、第六条、第九条第三款的有关规定。

第二十九条 在经营许可证的有效期内，变更公司名称、法定代表人、注册资本的，应当在完成公司的工商变更登记手续之日起 30 日内向原发证机关申请办理电信业务经营许可证变更手续。

第三十条 在经营许可证的有效期内，电信业务经营者需要终止经营的，应当符合下列条件：

(一)终止经营基础电信业务的，应当符合电信管理机构确定的电信行业管理总体布局；

(二)有可行的用户妥善处理方案并已妥善处理用户善后问题。

第三十一条 在经营许可证的有效期内，电信业务经营者需要终止经营的，应当向原发证机关提交下列申请材料：

(一)公司法定代表人签署并加盖印章的终止经营电信业务书面申请，内容包括：公司名称、联系方式、经营许可证编号、申请终止经营的电信业务种类、业务覆盖范围等；

(二)公司股东会或者股东大会关于同意终止经营电信业务的决定；

(三)公司法定代表人签署的做好用户善后处理工作的承诺书；

(四)公司关于解决用户善后问题的情况说明，内容包括：用户处理方案、社会公示情况说明、用户意见汇总、实施计划等；

(五)公司的经营许可证原件、营业执照复印件。

原发证机关收到终止经营电信业务的申请后应当向社会公示，公示期为 30 日。自公示期结束 60 日内，原发证机关应当完成审查工作，作出予以批准或者不予批准的决定。对于符合终止经营电信业务条件的，原发证机关应当予以批准，收回并注销电信业务经营许可证或者注销相应的电信业务种类、业务覆盖范围；对于不符合终止经营电信业务条件的，原发证机关应当不予批准，书面通知申请人并说明理由。

第三十二条 有下列情形之一的，发证机关或者其上级机关可以撤销经营许可证：

(一)发证机关工作人员滥用职权、玩忽职守作出准予行政许可决定的；

(二)超越法定职权或者违反法定程序作出准予行政许可决定的；

(三)对不具备申请资格或者不符合申请条件的申请人准予行政许可的；

(四)依法可以撤销经营许可证的其他情形。

第三十三条 有下列情形之一的，发证机关应当注销经营许可证：

(一)电信业务经营者依法终止的；

(二)经营许可证有效期届满未延续的；

(三)电信业务经营者被有关机关依法处罚或者因不可抗力，导致电信业务经

营许可事项无法实施的；

(四)经营许可证依法被撤销、吊销的；

(五)法律、法规规定应当注销经营许可证的其他情形。

第三十四条 发证机关吊销、撤销或者注销电信业务经营者的经营许可证后，应当向社会公布。

电信业务经营者被吊销、撤销或者注销经营许可证的， 应当按照国家有关规定做好善后工作。

被吊销、撤销或者注销经营许可证的，应当将经营许可证交回原发证机关。

第七章 经营许可的监督检查

第三十五条 电信业务经营者应当在每年第一季度通过管理平台向发证机关报告下列信息：

(一)上一年度的电信业务经营情况；

(二)网络建设、业务发展、人员及机构变动情况；

(三)服务质量情况；

(四)网络与信息安全保障制度和措施执行情况；

(五)执行国家和电信管理机构有关规定及经营许可证特别事项的情况；

(六)发证机关要求报送的其他信息。

前款第一项至第三项规定的信息(涉及商业秘密的信息除外)应当向社会公示，第五项、第六项规定的信息由电信业务经营者选择是否向社会公示。

电信业务经营者应当对本条第一款规定的年报信息的真实性负责，不得弄虚作假或者隐瞒真实情况。

第三十六条 电信管理机构建立随机抽查机制，对电信业务经营者的年报信息、日常经营活动、执行国家和电信管理机构有关规定的情况等进行检查。

电信管理机构可以采取书面检查、实地核查、网络监测等方式， 并可以委托第三方机构开展有关检查工作。

电信管理机构在抽查中发现电信业务经营者有违反电信管理规定的违法行为的，应当依法处理。

第三十七条 电信管理机构根据随机抽查、日常监督检查及行政处罚记录等情况，建立电信业务经营不良名单和电信业务经营失信名单。

电信业务经营不良名单和失信名单应当定期通过管理平台更新并向社会公示。

第三十八条 电信管理机构发现电信业务经营者未按照本办法第三十五条的规定报告年报信息的，应当要求其限期报告。电信业务经营者未按照电信管理机构要求的期限报告年报信息的，由电信管理机构列入电信业务经营不良名单。

依照前款规定列入电信业务经营不良名单的电信业务经营者，依照本办法规定履行报告年报信息义务的，经电信管理机构确认后移出。

第三十九条 获准跨地区经营电信业务的公司在有关省、自治区、直辖市设立、变更或者撤销分支机构的，应当自作出决定之日起 30 日内通过管理平台向原发证机关和当地电信管理机构报送有关信息。

省、自治区、直辖市通信管理局应当对跨地区电信业务经营者在当地开展电信业务的有关情况进行监督检查，并向工业和信息化部报告有关检查结果。

第四十条 电信管理机构开展监督检查，不得妨碍电信业务经营者正常的生产经营活动，不得收取任何费用。

电信管理机构开展监督检查时，应当记录监督检查的情况和处理结果，由监督检查人员签字后归档。

电信管理机构应当通过管理平台公示监督检查情况。

第四十一条 电信管理机构应当通过管理平台向社会公示电信业务经营者受到行政处罚的情况，并向相关基础电信业务经营者和提供接入服务的增值电信业务经营者通报。

第四十二条 电信业务经营者受到电信管理机构行政处罚的，由电信管理机构自作出行政处罚决定之日起 30 日内列入电信业务经营不良名单，但受到电信管理机构吊销经营许可证的处罚或者具有本办法规定直接列入电信业务经营失信名单情形的，直接列入失信名单。

列入电信业务经营不良名单的电信业务经营者，一年内未再次受到电信管理机构行政处罚的，由电信管理机构移出不良名单；三年内再次受到电信管理机构责令停业整顿、吊销经营许可证的处罚， 或者具有工业和信息化部规定的其他情形的，由电信管理机构列入电信业务经营失信名单。

列入电信业务经营失信名单后，三年内未再次受到电信管理机构行政处罚的，

由电信管理机构移出失信名单。

列入或者移出电信业务经营失信名单，应当同时将电信业务经营者的主要经营管理人员列入或者移出。

第四十三条 电信管理机构对列入电信业务经营不良名单和失信名单的电信业务经营者实施重点监管。

基础电信业务经营者和提供接入服务的增值电信业务经营者向其他增值电信业务经营者提供网络接入、代收费和业务合作时， 应当把电信业务经营不良名单和失信名单作为重要考量因素。

第四十四条 任何单位或者个人发现电信业务经营者违反电信管理规定应当受到行政处罚的，可以向有关电信管理机构举报。

第八章 法律责任

第四十五条 隐瞒有关情况或者提供虚假材料申请电信业务经营许可的，电信管理机构不予受理或者不予行政许可，给予警告，申请人在一年内不得再次申请该行政许可。

以欺骗、贿赂等不正当手段取得电信业务经营许可的， 电信管理机构撤销该行政许可，给予警告并直接列入电信业务经营失信名单，并视情节轻重处 5000 元以上 3 万元以下的罚款，申请人在三年内不得再次申请该行政许可；构成犯罪的，依法追究刑事责任。

第四十六条 违反本办法第十六条第一款、第二十八条第一款规定，擅自经营电信业务或者超范围经营电信业务的，依照《中华人民共和国电信条例》第六十九条规定予以处罚，其中情节严重、给予责令停业整顿处罚的， 直接列入电信业务经营失信名单。

第四十七条 违反本办法第十九条规定的，依照《中华人民共和国电信条例》第六十八条规定予以处罚。

第四十八条 违反本办法第四条第二款、第二十条、第二十二条、第二十三条、第二十四条、第二十九条、第三十一条或者第三十五条第三款规定的，由电信管理机构责令改正，给予警告，可以并处 5000 元以上 3 万元以下的罚款。

《中华人民共和国网络安全法》《中华人民共和国电信条例》对前款规定的情形规定法律责任的，电信管理机构从其规定处理。

第四十九条 当事人对电信管理机构作出的行政许可、行政处罚决定不服的，可以依法申请行政复议或者提起行政诉讼。

当事人逾期不申请行政复议也不提起行政诉讼，又不履行行政处罚决定的，由作出行政处罚决定的电信管理机构申请人民法院强制执行，并列入电信业务经营失信名单。

第五十条 电信管理机构的工作人员在经营许可证管理工作中，玩忽职守、滥用职权、徇私舞弊， 构成犯罪的，移交司法机关依法追究刑事责任；尚不构成犯罪的，由所在单位或者上级主管部门依法给予处分。

第九章 附 则

第五十一条 经营许可证由工业和信息化部统一印制。

第五十二条 电信管理机构可以参照本办法组织开展电信业务商用试验活动。

第五十三条 本办法自 2017 年 9 月 1 日起施行。2009 年 3 月 5 日公布的《电信业务经营许可管理办法》(工业和信息化部令第 5 号)同时废止。

工业和信息化部关于发布《电信业务分类目录(2015 年版)》的通告

工信部信管〔2015〕484 号

为适应电信新技术、新业务发展， 进一步推进电信业改革开放，促进电信业务繁荣健康发展，扩大信息消费，规范市场行为，提升服务水平，保障用户权益，依据《中华人民共和国电信条例》，我部对《电信业务分类目录》重新进行了调整。现发布《电信业务分类目录(2015 年版)》，自 2016 年 3 月 1 日起施行。

附件：电信业务分类目录(2015 年版)

工业和信息化部

2015 年 12 月 28 日

工业和信息化部关于修订《电信业务分类目录(2015 年版)》的公告

为贯彻落实中央经济工作会议精神，加快 5G 商用步伐，依据《中华人民共和国电信条例》，我部对《电信业务分类目录(2015 年版)》(以下简称《目录》)进行了修订，现予公告。

《目录》在 A 类“基础电信业务”，“A12 蜂窝移动通信业务”类别下，增设“A12-4 第五代数字蜂窝移动通信业务”业务子类。具体业务表述为：“第五

代数字蜂窝移动通信业务是指利用第五代数字蜂窝移动通信网提供的话音、数据、多媒体通信等业务”。其他业务维持不变。

工业和信息化部

2019 年 6 月 6 日

工业和信息化部关于印发《移动智能终端应用软件预置和分发管理暂行规定》的通知

工信部信管〔2016〕407 号

各相关单位：

现将《移动智能终端应用软件预置和分发管理暂行规定》印发给你们，请遵照执行。

工业和信息化部

2016 年 12 月 16 日

移动智能终端应用软件预置和分发管理暂行规定

为推动移动互联网健康有序发展，构建安全可信的信息通信网络环境，依法维护用户的知情权和选择权，促进大众创业、万众创新，规范移动互联网市场秩序，根据《全国人民代表大会常务委员会关于加强网络信息保护的决定》《中华人民共和国网络安全法》《中华人民共和国电信条例》和《互联网信息服务管理办法》等有关规定，制定本规定。

第一条 工业和信息化部大力推动移动智能终端应用软件发展，鼓励移动智能终端生产企业、互联网信息服务提供者等相关企业积极开发移动智能终端应用软件产品，丰富信息消费内容，引导企业健全相关管理机制。鼓励有关行业协会等依法制定自律性管理制度，共同规范移动智能终端应用软件的预置和分发行为，维护网络安全，加强用户权益保护。

第二条 本规定规范移动智能终端生产企业(以下简称生产企业)的移动智能终端应用软件预置行为，以及互联网信息服务提供者提供的移动智能终端应用软件分发服务。

第三条 工业和信息化部依照本规定对全国范围内移动智能终端应用软件预置与分发服务实施监督管理。省、自治区、直辖市通信管理局(以下统称各地通信主管部门)在工业和信息化部领导下，按照本规定对本行政区域内的移动智能

终端应用软件预置与分发服务实施监督管理。工业和信息化部和各地通信主管部门应进一步完善移动智能终端应用软件预置与分发服务监管制度，强化事中事后管理。

第四条 生产企业和提供移动智能终端应用软件分发服务的互联网信息服务提供者(以下简称互联网信息服务提供者)不得提供或传播含有下列内容的移动智能终端应用软件：

(一)反对宪法所确定的基本原则的；

(二)危害国家安全，泄露国家秘密，颠覆国家政权，破坏国家统一的；

(三)损害国家荣誉和利益的；

(四)煽动民族仇恨、民族歧视，破坏民族团结的；

(五)破坏国家宗教政策，宣扬邪教和封建迷信的；

(六)散布谣言，扰乱社会秩序，破坏社会稳定的；

(七)散布淫秽、色情、赌博、暴力、凶杀、恐怖或者教唆犯罪的；

(八)侮辱或者诽谤他人，侵害他人合法权益的；

(九)含有法律、行政法规禁止的其他内容的。

第五条 生产企业和互联网信息服务提供者应依法依规提供移动智能终端应用软件，采取有效措施，维护网络安全，切实保护用户合法权益。

(一)提供移动智能终端预置软件(以下简称预置软件)的生产企业和互联网信息服务提供者应自觉维护行业公平竞争，依法维护用户的知情权和选择权，不得实施破坏市场竞争秩序、侵犯用户合法权益的行为。

(二)生产企业和互联网信息服务提供者所提供移动智能终端应用软件不得调用与所提供服务无关的终端功能、违法发送商业性电子信息；未经明示且经用户同意，不得实施收集使用用户个人信息、开启应用软件、捆绑推广其他应用软件等侵害用户合法权益或危害网络安全的行为。

(三)为移动智能终端应用软件提供代收费的企业，应当采取必要措施，加强对计费、收费行为的管理，杜绝不明扣费；收费企业应对用户确认信息和计费原始数据至少保存 5 个月，并为用户查询提供方便。

(四)生产企业应约束销售渠道，未经用户同意不得擅自在移动智能终端中安装应用软件，并提示用户终端在销售渠道等环节被装入应用软件的可能性、

风险和应对措施。

第六条 生产企业和互联网信息服务提供者均应明示所提供移动智能终端应用软件相关信息。

(一)生产企业和互联网信息服务提供者均应通过用户提示、企业网站等方式明示所提供移动智能终端应用软件的信息，包括名称、功能描述、卸载方法、开发者信息、软件安装及运行所需权限列表等，明确告知用户应用软件收集、使用用户个人信息的内容、目的、方式和范围等。

(二)生产企业应在终端产品说明书中提供预置软件列表信息，并在终端产品说明书或外包装中标示预置软件详细信息的查询方法。生产企业在提交移动智能终端进网申请时，应提供相关产品符合前述要求的声明。

(三)涉及收费的移动智能终端应用软件应严格遵守明码标价等相关规定，明示收费标准、收费方式，明示内容真实准确、醒目规范，经用户确认后方可扣费。

第七条 生产企业和互联网信息服务提供者应确保除基本功能软件外的移动智能终端应用软件可卸载。

(一)移动智能终端的基本功能软件是指保障移动智能终端硬件和操作系统正常运行的应用软件，主要包括操作系统基本组件、保证智能终端硬件正常运行的应用、基本通信应用、应用软件下载通道等。终端中预置的实现同一功能的基本功能软件，至多有一个可设置为不可卸载。

(二)生产企业和互联网信息服务提供者应确保所提供的除基本功能软件之外的移动智能终端应用软件可由用户方便卸载，且在不影响移动智能终端安全使用的情况下，附属于该软件的资源文件、配置文件和用户数据文件等也应能够被方便卸载。

(三)生产企业应确保已被卸载的预置软件在移动智能终端操作系统升级时不被强行恢复；应保证移动智能终端获得进网许可证前后预置软件的一致性；移动智能终端新增预置软件或有重大功能变化的，应及时向工业和信息化部报告。

第八条 从事应用商店等移动应用分发平台服务的互联网信息服务提供者，以及在移动智能终端中预置了移动应用分发平台的生产企业对所提供的应用软

件负有以下管理责任：

(一)应登记应用软件提供者、运营者、开发者的真实身份、联系方式等信息。

(二)应建立应用软件管理机制，对应用软件进行审核及安全、服务等相关检测，对审核和检测中发现的恶意应用软件等违法违规软件，不得向用户提供；对所提供应用软件进行跟踪监测，及时处理违法违规软件，建立完善用户举报投诉处置措施等。

(三)应要求应用软件提供者在提交应用软件时声明其获取的用户终端权限及用途，并将上述信息向软件下载用户明示。

(四)应留存所提供应用软件，以及该软件有关版本、上线时间、功能简介、用途、MD5(消息摘要算法 5)等校验值、服务器接入等信息以备追溯检测，相关信息的留存时间不短于 60 日。

(五)对于违反本规定第四条要求的应用软件，以及在通信主管部门监督检查中发现的恶意应用软件，相关企业应予以及时下架。

(六)应加强网络安全防护以及对相关人员的教育培训，保障自身系统安全和用户个人信息安全。

第九条 通信主管部门应对生产企业和互联网信息服务提供者落实本规定相关要求情况进行监督检查。

(一)通信主管部门应组织专业检测机构对生产企业预置的和互联网信息服务提供者提供的应用软件开展监督检测和恶意应用软件认定工作，相关企业应给予配合，并提供便捷的获取应用软件的条件。

(二)检测机构应及时将检测和认定报告提交通信主管部门。通信主管部门依据报告，要求并监督相关企业进行整改，通知并监督互联网信息服务提供者下架恶意应用软件。

(三)通信主管部门向社会通报监督检查和检测情况。

(四)对于紧急情况以及互联网信息服务提供者未按要求及时下架违法应用软件的，通信主管部门可依法依规要求有关单位采取处置措施。

第十条 相关企业和社会组织应进一步完善服务保障措施，提高用户权益保护水平。

(一)生产企业和互联网信息服务提供者应建立移动智能终端应用软件投诉举报受理制度，为用户提供便捷的投诉举报方式，接受、验证和处理用户投诉举报。如用户发现移动智能终端应用软件违反本规定要求，可向相关企业投诉举报，企业应在规定和公开承诺的时限内妥善处理；对处理结果不满的，用户可向电信用户申诉受理机构申诉。用户发现恶意应用软件，以及含有法律法规规定的禁止性内容或违法发送商业性电子信息的移动终端应用软件，可向网络不良与垃圾信息举报中心举报。

(二)工业和信息化部鼓励移动智能终端应用软件采用依法设立的电子认证服务机构颁发的数字证书进行签名；指导相关企业对已签名的移动智能终端应用软件采用依法设立的电子认证服务机构颁发的数字证书，进行验证并显著标识。

(三)工业和信息化部支持相关社会组织通过行业自律形式，建立恶意应用软件黑名单，实现黑名单信息在相关企业、专业检测机构以及用户之间的共享。

第十一条 违反本规定的，通信主管部门依据职权责令改正，依法进行处罚，并将生产企业、互联网信息服务提供者违反本规定受到行政处罚的情况记入信誉档案，向社会公布。对涉嫌违法犯罪的应用软件线索，各单位应及时报告公安机关。

第十二条 本规定下列用语的含义是：

移动智能终端是指接入公众移动通信网络、具有操作系统、可由用户自行安装和卸载应用软件的移动通信终端产品。

移动智能终端应用软件(英文简称 APP)包括移动智能终端预置应用软件，以及互联网信息服务提供者提供的可以通过网站、应用商店等移动应用分发平台下载、安装、升级的应用软件。

移动应用分发平台是指网站、应用商店等提供移动智能终端应用软件下载、安装、升级的应用软件平台。

移动智能终端预置应用软件是指由生产企业自行或与互联网信息服务提供者合作在移动智能终端出厂前安装的应用软件。

恶意应用软件是指含有信息窃取、恶意扣费、诱骗欺诈、系统破坏等恶意

行为及其他危害用户权益和网络安全的应用软件。

商业性电子信息是指利用电信网或互联网，向用户介绍、推销商品、服务或者商业投资机会的电子信息。

第十三条 本规定解释权属于工业和信息化部。

第十四条 本规定自 2017 年 7 月 1 日起实施。

工业和信息化部印发关于《互联网域名管理办法》的通知

工业和信息化部令第 43 号

《互联网域名管理办法》已经 2017 年 8 月 16 日工业和信息化部第 32 次部务会议审议通过，现予公布，自 2017 年 11 月 1 日起施行。原信息产业部 2004 年 11 月 5 日公布的《中国互联网络域名管理办法》(原信息产业部令第 30 号)同时废止。

部长 苗圩

2017 年 8 月 24 日

互联网域名管理办法

第一章 总 则

第一条 为了规范互联网域名服务，保护用户合法权益，保障互联网域名系统安全、可靠运行， 推动中文域名和国家顶级域名发展和应用，促进中国互联网健康发展，根据《中华人民共和国行政许可法》《国务院对确需保留的行政审批项目设定行政许可的决定》等规定， 参照国际上互联网域名管理准则，制定本办法。

第二条 在中华人民共和国境内从事互联网域名服务及其运行维护、监督管理等相关活动，应当遵守本办法。

本办法所称互联网域名服务(以下简称域名服务)，是指从事域名根服务器运行和管理、顶级域名运行和管理、域名注册、域名解析等活动。

第三条 工业和信息化部对全国的域名服务实施监督管理，主要职责是：

(一)制定互联网域名管理规章及政策；

(二)制定中国互联网域名体系、域名资源发展规划；

(三)管理境内的域名根服务器运行机构和域名注册管理机构；

(四)负责域名体系的网络与信息安全管理；

(五)依法保护用户个人信息和合法权益;

(六)负责与域名有关的国际协调;

(七)管理境内的域名解析服务;

(八)管理其他与域名服务相关的活动。

第四条 各省、自治区、直辖市通信管理局对本行政区域内的域名服务实施监督管理,主要职责是:

(一)贯彻执行域名管理法律、行政法规、规章和政策;

(二)管理本行政区域内的域名注册服务机构;

(三)协助工业和信息化部对本行政区域内的域名根服务器运行机构和域名注册管理机构进行管理;

(四)负责本行政区域内域名系统的网络与信息安全管理;

(五)依法保护用户个人信息和合法权益;

(六)管理本行政区域内的域名解析服务;

(七)管理本行政区域内其他与域名服务相关的活动。

第五条 中国互联网域名体系由工业和信息化部予以公告。根据域名发展的实际情况,工业和信息化部可以对中国互联网域名体系进行调整。

第六条 “.CN”和“.中国”是中国的国家顶级域名。

中文域名是中国互联网域名体系的重要组成部分。国家鼓励和支持中文域名系统的技术研究和推广应用。

第七条 提供域名服务,应当遵守国家相关法律法规,符合相关技术规范和标准。

第八条 任何组织和个人不得妨碍互联网域名系统的安全和稳定运行。

第二章 域名管理

第九条 在境内设立域名根服务器及域名根服务器运行机构、域名注册管理机构和域名注册服务机构的,应当依据本办法取得工业和信息化部或者省、自治区、直辖市通信管理局(以下统称电信管理机构)的相应许可。

第十条 申请设立域名根服务器及域名根服务器运行机构的,应当具备以下条件:

(一)域名根服务器设置在境内,并且符合互联网发展相关规划及域名系统安

全稳定运行要求；

（二）是依法设立的法人，该法人及其主要出资者、主要经营管理人员具有良好的信用记录；

（三）具有保障域名根服务器安全可靠运行的场地、资金、环境、专业人员和技术能力以及符合电信管理机构要求的信息管理系统；

（四）具有健全的网络与信息安全保障措施，包括管理人员、网络与信息安全管理制度、应急处置预案和相关技术、管理措施等；

（五）具有用户个人信息保护能力、提供长期服务的能力及健全的服务退出机制；

（六）法律、行政法规规定的其他条件。

第十一条　申请设立域名注册管理机构的，应当具备以下条件：

（一）域名管理系统设置在境内，并且持有的顶级域名符合相关法律法规及域名系统安全稳定运行要求；

（二）是依法设立的法人，该法人及其主要出资者、主要经营管理人员具有良好的信用记录；

（三）具有完善的业务发展计划和技术方案以及与从事顶级域名运行管理相适应的场地、资金、专业人员以及符合电信管理机构要求的信息管理系统；

（四）具有健全的网络与信息安全保障措施，包括管理人员、网络与信息安全管理制度、应急处置预案和相关技术、管理措施等；

（五）具有进行真实身份信息核验和用户个人信息保护的能力、提供长期服务的能力及健全的服务退出机制；

（六）具有健全的域名注册服务管理制度和对域名注册服务机构的监督机制；

（七）法律、行政法规规定的其他条件。

第十二条　申请设立域名注册服务机构的，应当具备以下条件：

（一）在境内设置域名注册服务系统、注册数据库和相应的域名解析系统；

（二）是依法设立的法人，该法人及其主要出资者、主要经营管理人员具有良好的信用记录；

（三）具有与从事域名注册服务相适应的场地、资金和专业人员以及符合电信管理机构要求的信息管理系统；

(四)具有进行真实身份信息核验和用户个人信息保护的能力、提供长期服务的能力及健全的服务退出机制;

(五)具有健全的域名注册服务管理制度和对域名注册代理机构的监督机制;

(六)具有健全的网络与信息安全保障措施,包括管理人员、网络与信息安全管理制度、应急处置预案和相关技术、管理措施等;

(七)法律、行政法规规定的其他条件。

第十三条 申请设立域名根服务器及域名根服务器运行机构、域名注册管理机构的,应当向工业和信息化部提交申请材料。申请设立域名注册服务机构的,应当向住所地省、自治区、直辖市通信管理局提交申请材料。

申请材料应当包括:

(一)申请单位的基本情况及其法定代表人签署的依法诚信经营承诺书;

(二)对域名服务实施有效管理的证明材料,包括相关系统及场所、服务能力的证明材料、管理制度、与其他机构签订的协议等;

(三)网络与信息安全保障制度及措施;

(四)证明申请单位信誉的材料。

第十四条 申请材料齐全、符合法定形式的,电信管理机构应当向申请单位出具受理申请通知书;申请材料不齐全或者不符合法定形式的,电信管理机构应当场或者在5个工作日内一次性书面告知申请单位需要补正的全部内容;不予受理的,应当出具不予受理通知书并说明理由。

第十五条 电信管理机构应当自受理之日起20个工作日内完成审查,作出予以许可或者不予许可的决定。20个工作日内不能作出决定的,经电信管理机构负责人批准,可以延长10个工作日,并将延长期限的理由告知申请单位。需要组织专家论证的,论证时间不计入审查期限。

予以许可的,应当颁发相应的许可文件;不予许可的,应当书面通知申请单位并说明理由。

第十六条 域名根服务器运行机构、域名注册管理机构和域名注册服务机构的许可有效期为5年。

第十七条 域名根服务器运行机构、域名注册管理机构和域名注册服务机构的名称、住所、法定代表人等信息发生变更的,应当自变更之日起20日内向原

发证机关办理变更手续。

第十八条 在许可有效期内，域名根服务器运行机构、域名注册管理机构、域名注册服务机构拟终止相关服务的，应当提前 30 日书面通知用户，提出可行的善后处理方案，并向原发证机关提交书面申请。

原发证机关收到申请后，应当向社会公示 30 日。公示期结束 60 日内，原发证机关应当完成审查并做出决定。

第十九条 许可有效期届满需要继续从事域名服务的，应当提前 90 日向原发证机关申请延续；不再继续从事域名服务的，应当提前 90 日向原发证机关报告并做好善后工作。

第二十条 域名注册服务机构委托域名注册代理机构开展市场销售等工作的，应当对域名注册代理机构的工作进行监督和管理。

域名注册代理机构受委托开展市场销售等工作的过程中，应当主动表明代理关系，并在域名注册服务合同中明示相关域名注册服务机构名称及代理关系。

第二十一条 域名注册管理机构、域名注册服务机构应当在境内设立相应的应急备份系统并定期备份域名注册数据。

第二十二条 域名根服务器运行机构、域名注册管理机构、域名注册服务机构应当在其网站首页和经营场所显著位置标明其许可相关信息。域名注册管理机构还应当标明与其合作的域名注册服务机构名单。

域名注册代理机构应当在其网站首页和经营场所显著位置标明其代理的域名注册服务机构名称。

第三章 域名服务

第二十三条 域名根服务器运行机构、域名注册管理机构和域名注册服务机构应当向用户提供安全、方便、稳定的服务。

第二十四条 域名注册管理机构应当根据本办法制定域名注册实施细则并向社会公开。

第二十五条 域名注册管理机构应当通过电信管理机构许可的域名注册服务机构开展域名注册服务。

域名注册服务机构应当按照电信管理机构许可的域名注册服务项目提供服务，不得为未经电信管理机构许可的域名注册管理机构提供域名注册服务。

第二十六条 域名注册服务原则上实行“先申请先注册”，相应域名注册实施细则另有规定的，从其规定。

第二十七条 为维护国家利益和社会公众利益，域名注册管理机构应当建立域名注册保留字制度。

第二十八条 任何组织或者个人注册、使用的域名中，不得含有下列内容：

(一)反对宪法所确定的基本原则的；

(二)危害国家安全，泄露国家秘密，颠覆国家政权，破坏国家统一的；

(三)损害国家荣誉和利益的；

(四)煽动民族仇恨、民族歧视，破坏民族团结的；

(五)破坏国家宗教政策，宣扬邪教和封建迷信的；

(六)散布谣言，扰乱社会秩序，破坏社会稳定的；

(七)散布淫秽、色情、赌博、暴力、凶杀、恐怖或者教唆犯罪的；

(八)侮辱或者诽谤他人，侵害他人合法权益的；

(九)含有法律、行政法规禁止的其他内容的。

域名注册管理机构、域名注册服务机构不得为含有前款所列内容的域名提供服务。

第二十九条 域名注册服务机构不得采用欺诈、胁迫等不正当手段要求他人注册域名。

第三十条 域名注册服务机构提供域名注册服务，应当要求域名注册申请者提供域名持有者真实、准确、完整的身份信息等域名注册信息。

域名注册管理机构和域名注册服务机构应当对域名注册信息的真实性、完整性进行核验。

域名注册申请者提供的域名注册信息不准确、不完整的， 域名注册服务机构应当要求其予以补正。申请者不补正或者提供不真实的域名注册信息的， 域名注册服务机构不得为其提供域名注册服务。

第三十一条 域名注册服务机构应当公布域名注册服务的内容、时限、费用，保证服务质量，提供域名注册信息的公共查询服务。

第三十二条 域名注册管理机构、域名注册服务机构应当依法存储、保护用户个人信息。未经用户同意不得将用户个人信息提供给他人， 但法律、行政法规

另有规定的除外。

第三十三条 域名持有者的联系方式等信息发生变更的，应当在变更后 30 日内向域名注册服务机构办理域名注册信息变更手续。

域名持有者将域名转让给他人的，受让人应当遵守域名注册的相关要求。

第三十四条 域名持有者有权选择、变更域名注册服务机构。变更域名注册服务机构的，原域名注册服务机构应当配合域名持有者转移其域名注册相关信息。

无正当理由的，域名注册服务机构不得阻止域名持有者变更域名注册服务机构。

电信管理机构依法要求停止解析的域名，不得变更域名注册服务机构。

第三十五条 域名注册管理机构和域名注册服务机构应当设立投诉受理机制，并在其网站首页和经营场所显著位置公布投诉受理方式。

域名注册管理机构和域名注册服务机构应当及时处理投诉；不能及时处理的，应当说明理由和处理时限。

第三十六条 提供域名解析服务，应当遵守有关法律、法规、标准， 具备相应的技术、服务和网络与信息安全保障能力， 落实网络与信息安全保障措施，依法记录并留存域名解析日志、维护日志和变更记录， 保障解析服务质量和解析系统安全。涉及经营电信业务的，应当依法取得电信业务经营许可。

第三十七条 提供域名解析服务，不得擅自篡改解析信息。

任何组织或者个人不得恶意将域名解析指向他人的 IP 地址。

第三十八条 提供域名解析服务，不得为含有本办法第二十八条第一款所列内容的域名提供域名跳转。

第三十九条 从事互联网信息服务的，其使用域名应当符合法律法规和电信管理机构的有关规定，不得将域名用于实施违法行为。

第四十条 域名注册管理机构、域名注册服务机构应当配合国家有关部门依法开展的检查工作，并按照电信管理机构的要求对存在违法行为的域名采取停止解析等处置措施。

域名注册管理机构、域名注册服务机构发现其提供服务的域名发布、传输法律和行政法规禁止发布或者传输的信息的，应当立即采取消除、停止解析等处置措施，防止信息扩散，保存有关记录，并向有关部门报告。

第四十一条 域名根服务器运行机构、域名注册管理机构和域名注册服务机构应当遵守国家相关法律、法规和标准， 落实网络与信息安全保障措施，配置必要的网络通信应急设备，建立健全网络与信息安全监测技术手段和应急制度。域名系统出现网络与信息安全事件时，应当在 24 小时内向电信管理机构报告。

因国家安全和处置紧急事件的需要，域名根服务器运行机构、域名注册管理机构和域名注册服务机构应当服从电信管理机构的统一指挥与协调，遵守电信管理机构的管理要求。

第四十二条 任何组织或者个人认为他人注册或者使用的域名侵害其合法权益的，可以向域名争议解决机构申请裁决或者依法向人民法院提起诉讼。

第四十三条 已注册的域名有下列情形之一的，域名注册服务机构应当予以注销，并通知域名持有者：

(一)域名持有者申请注销域名的；

(二)域名持有者提交虚假域名注册信息的；

(三)依据人民法院的判决、域名争议解决机构的裁决，应当注销的；

(四)法律、行政法规规定予以注销的其他情形。

第四章 监督检查

第四十四条 电信管理机构应当加强对域名服务的监督检查。域名根服务器运行机构、域名注册管理机构、域名注册服务机构应当接受、配合电信管理机构的监督检查。

鼓励域名服务行业自律管理，鼓励公众监督域名服务。

第四十五条 域名根服务器运行机构、域名注册管理机构、域名注册服务机构应当按照电信管理机构的要求，定期报送业务开展情况、安全运行情况、网络与信息安全责任落实情况、投诉和争议处理情况等信息。

第四十六条 电信管理机构实施监督检查时，应当对域名根服务器运行机构、域名注册管理机构和域名注册服务机构报送的材料进行审核，并对其执行法律法规和电信管理机构有关规定的情况进行检查。

电信管理机构可以委托第三方专业机构开展有关监督检查活动。

第四十七条 电信管理机构应当建立域名根服务器运行机构、域名注册管理机构和域名注册服务机构的信用记录制度，将其违反本办法并受到行政处罚的行

为记入信用档案。

第四十八条 电信管理机构开展监督检查，不得妨碍域名根服务器运行机构、域名注册管理机构和域名注册服务机构正常的经营和服务活动，不得收取任何费用，不得泄露所知悉的域名注册信息。

第五章 罚 则

第四十九条 违反本办法第九条规定，未经许可擅自设立域名根服务器及域名根服务器运行机构、域名注册管理机构、域名注册服务机构的， 电信管理机构应当根据《中华人民共和国行政许可法》第八十一条的规定，采取措施予以制止，并视情节轻重，予以警告或者处一万元以上三万元以下罚款。

第五十条 违反本办法规定，域名注册管理机构或者域名注册服务机构有下列行为之一的，由电信管理机构依据职权责令限期改正，并视情节轻重，处一万元以上三万元以下罚款，向社会公告：

(一)为未经许可的域名注册管理机构提供域名注册服务，或者通过未经许可的域名注册服务机构开展域名注册服务的；

(二)未按照许可的域名注册服务项目提供服务的；

(三)未对域名注册信息的真实性、完整性进行核验的；

(四)无正当理由阻止域名持有者变更域名注册服务机构的。

第五十一条 违反本办法规定，提供域名解析服务，有下列行为之一的，由电信管理机构责令限期改正，可以视情节轻重处一万元以上三万元以下罚款，向社会公告：

(一)擅自篡改域名解析信息或者恶意将域名解析指向他人 IP 地址的；

(二)为含有本办法第二十八条第一款所列内容的域名提供域名跳转的；

(三)未落实网络与信息安全保障措施的；

(四)未依法记录并留存域名解析日志、维护日志和变更记录的；

(五)未按照要求对存在违法行为的域名进行处置的。

第五十二条 违反本办法第十七条、第十八条第一款、第二十一条、第二十二条、第二十八条第二款、第二十九条、第三十一条、第三十二条、第三十五条第一款、第四十条第二款、第四十一条规定的，由电信管理机构依据职权责令限

期改正，可以并处一万元以上三万元以下罚款，向社会公告。

第五十三条 法律、行政法规对有关违法行为的处罚另有规定的，依照有关法律、行政法规的规定执行。

第五十四条 任何组织或者个人违反本办法第二十八条第一款规定注册、使用域名，构成犯罪的，依法追究刑事责任；尚不构成犯罪的，由有关部门依法予以处罚。

第六章 附 则

第五十五条 本办法下列用语的含义是：

(一)域名：指互联网上识别和定位计算机的层次结构式的字符标识，与该计算机的 IP 地址相对应。

(二)中文域名：指含有中文文字的域名。

(三)顶级域名：指域名体系中根节点下的第一级域的名称。

(四)域名根服务器：指承担域名体系中根节点功能的服务器(含镜像服务器)。

(五)域名根服务器运行机构：指依法获得许可并承担域名根服务器运行、维护和管理工作的机构。

(六)域名注册管理机构：指依法获得许可并承担顶级域名运行和管理工作的机构。

(七)域名注册服务机构：指依法获得许可、受理域名注册申请并完成域名在顶级域名数据库中注册的机构。

(八)域名注册代理机构：指受域名注册服务机构的委托，受理域名注册申请，间接完成域名在顶级域名数据库中注册的机构。

(九)域名管理系统：指域名注册管理机构在境内开展顶级域名运行和管理所需的主要信息系统，包括注册管理系统、注册数据库、域名解析系统、域名信息查询系统、身份信息核验系统等。

(十)域名跳转：指对某一域名的访问跳转至该域名绑定或者指向的其他域名、IP 地址或者网络信息服务等。

第五十六条 本办法中规定的日期，除明确为工作日的以外，均为自然日。

第五十七条 在本办法施行前未取得相应许可开展域名服务的，应当自本办法施行之日起十二个月内，按照本办法规定办理许可手续。

在本办法施行前已取得许可的域名根服务器运行机构、域名注册管理机构和域名注册服务机构，其许可有效期适用本办法第十六条的规定，有效期自本办法施行之日起计算。

第五十八条 本办法自 2017 年 11 月 1 日起施行。2004 年 11 月 5 日公布的《中国互联网络域名管理办法》(原信息产业部令第 30 号)同时废止。本办法施行前公布的有关规定与本办法不一致的，按照本办法执行。

工业和信息化部关于规范互联网信息服务使用域名的通知

工信部信管〔2017〕264 号

各有关单位：

为贯彻落实《中华人民共和国反恐怖主义法》《中华人民共和国网络安全法》《互联网信息服务管理办法》《互联网域名管理办法》等法律法规和规章的要求，进一步规范互联网信息服务域名使用，现就有关事项通知如下：

一、互联网信息服务提供者从事互联网信息服务使用的域名应为其依法依规注册所有。

(一)个人从事互联网信息服务的，域名注册者应为互联网信息服务者本人。

(二)单位从事互联网信息服务的，域名注册者应为单位(含公司股东)、单位主要负责人或高级管理人员。

二、互联网接入服务提供者应当按照《中华人民共和国反恐怖主义法》《中华人民共和国网络安全法》的要求，对互联网信息服务提供者的身份进行查验。互联网信息服务提供者不提供真实身份信息的，互联网接入服务提供者不得为其提供服务。

三、域名注册管理机构、域名注册服务机构应当按照《互联网域名管理办法》和电信主管部门的要求，建设相应的信息管理系统，与“工业和信息化部 ICP/IP 地址/域名信息备案管理系统”(以下简称备案系统)进行对接，报送域名注册相关信息。

四、域名注册管理机构、域名注册服务机构应当进一步加强域名真实身份信息注册管理，不得为未提供真实身份信息的域名提供解析服务。

五、互联网接入服务提供者在为互联网信息服务提供者提供接入服务时，

应通过备案系统查验域名注册者的真实身份信息，不提供真实身份信息的或者提供的身份信息不准确、不完整的，互联网接入服务提供者不得为其提供接入服务。本通知施行前已在备案系统中备案的域名除外。

互联网接入服务提供者应当定期通过备案系统核查互联网信息服务提供者使用域名的状态，对于域名不存在、域名过期且未提供真实身份信息等情形的，互联网接入服务提供者应停止为其提供接入服务。

六、电信主管部门要督促互联网接入服务提供者、域名注册管理机构、域名注册服务机构按照上述要求开展业务，依法处理各类违法违规行为，将处理结果纳入企业信誉管理档案，并向社会公示。

七、本通知自 2018 年 1 月 1 日起施行。

特此通知

2017 年 11 月 27 日

工业和信息化部关于印发《公共互联网网络安全突发事件应急预案》的通知

工信部网安〔2017〕281 号

各省、自治区、直辖市通信管理局，中国电信集团公司、中国移动通信集团公司、中国联合网络通信集团有限公司，国家计算机网络应急技术处理协调中心、中国信息通信研究院、中国软件评测中心、国家工业信息安全发展研究中心，域名注册管理和服务机构、互联网企业、网络安全企业：

为进一步健全公共互联网网络安全突发事件应急机制，提升应对能力，根据《中华人民共和国网络安全法》《国家网络安全事件应急预案》等，制定《公共互联网网络安全突发事件应急预案》。现印发给你们，请结合实际，切实抓好贯彻落实。

工业和信息化部

2017 年 11 月 14 日

公共互联网网络安全突发事件应急预案

1.总则

1.1 编制目的

建立健全公共互联网网络安全突发事件应急组织体系和工作机制，提高公共互联网网络安全突发事件综合应对能力，确保及时有效地控制、减轻和消除

公共互联网网络安全突发事件造成的社会危害和损失，保证公共互联网持续稳定运行和数据安全，维护国家网络空间安全，保障经济运行和社会秩序。

1.2 编制依据

《中华人民共和国突发事件应对法》《中华人民共和国网络安全法》《中华人民共和国电信条例》等法律法规和《国家突发公共事件总体应急预案》《国家网络安全事件应急预案》等相关规定。

1.3 适用范围

本预案适用于面向社会提供服务的基础电信企业、域名注册管理和服务机构(以下简称域名机构)、互联网企业(含工业互联网平台企业)发生网络安全突发事件的应对工作。

本预案所称网络安全突发事件，是指突然发生的，由网络攻击、网络入侵、恶意程序等导致的，造成或可能造成严重社会危害或影响，需要电信主管部门组织采取应急处置措施予以应对的网络中断(拥塞)、系统瘫痪(异常)、数据泄露(丢失)、病毒传播等事件。

本预案所称电信主管部门包括工业和信息化部及各省(自治区、直辖市)通信管理局。

工业和信息化部对国家重大活动期间网络安全突发事件应对工作另有规定的，从其规定。

1.4 工作原则

公共互联网网络安全突发事件应急工作坚持统一领导、分级负责；坚持统一指挥、密切协同、快速反应、科学处置；坚持预防为主，预防与应急相结合；落实基础电信企业、域名机构、互联网服务提供者的主体责任；充分发挥网络安全专业机构、网络安全企业和专家学者等各方面力量的作用。

2.组织体系

2.1 领导机构与职责

在中央网信办统筹协调下，工业和信息化部网络安全和信息化领导小组(以下简称部领导小组)统一领导公共互联网网络安全突发事件应急管理工作，负责特别重大公共互联网网络安全突发事件的统一指挥和协调。

2.2 办事机构与职责

在中央网信办下设的国家网络安全应急办公室统筹协调下，在部领导小组统一领导下，工业和信息化部网络安全应急办公室(以下简称部应急办)负责公共互联网网络安全应急管理事务性工作；及时向部领导小组报告突发事件情况，提出特别重大网络安全突发事件应对措施建议；负责重大网络安全突发事件的统一指挥和协调；根据需要协调较大、一般网络安全突发事件应对工作。

部应急办具体工作由工业和信息化部网络安全管理局承担，有关单位明确负责人和联络员参与部应急办工作。

2.3 其他相关单位职责

各省(自治区、直辖市)通信管理局负责组织、指挥、协调本行政区域相关单位开展公共互联网网络安全突发事件的预防、监测、报告和应急处置工作。

基础电信企业、域名机构、互联网企业负责本单位网络安全突发事件预防、监测、报告和应急处置工作，为其他单位的网络安全突发事件应对提供技术支持。

国家计算机网络应急技术处理协调中心、中国信息通信研究院、中国软件评测中心、国家工业信息安全发展研究中心(以下统称网络安全专业机构)负责监测、报告公共互联网网络安全突发事件和预警信息，为应急工作提供决策支持和技术支撑。

鼓励网络安全企业支撑参与公共互联网网络安全突发事件应对工作。

3.事件分级

根据社会影响范围和危害程度，公共互联网网络安全突发事件分为四级：特别重大事件、重大事件、较大事件、一般事件。

3.1 特别重大事件

符合下列情形之一的，为特别重大网络安全事件：

(1)全国范围大量互联网用户无法正常上网；

(2).CN 国家顶级域名系统解析效率大幅下降；

(3)1 亿以上互联网用户信息泄露；

(4)网络病毒在全国范围大面积爆发；

(5)其他造成或可能造成特别重大危害或影响的网络安全事件。

3.2 重大事件

符合下列情形之一的，为重大网络安全事件：

(1)多个省大量互联网用户无法正常上网；

(2)在全国范围有影响力的网站或平台访问出现严重异常；

(3)大型域名解析系统访问出现严重异常；

(4)1 千万以上互联网用户信息泄露；

(5)网络病毒在多个省范围内大面积爆发；

(6)其他造成或可能造成重大危害或影响的网络安全事件。

3.3 较大事件

符合下列情形之一的，为较大网络安全事件：

(1)1 个省内大量互联网用户无法正常上网；

(2)在省内有影响力的网站或平台访问出现严重异常；

(3)1 百万以上互联网用户信息泄露；

(4)网络病毒在 1 个省范围内大面积爆发；

(5)其他造成或可能造成较大危害或影响的网络安全事件。

3.4 一般事件

符合下列情形之一的，为一般网络安全事件：

(1)1 个地市大量互联网用户无法正常上网；

(2)10 万以上互联网用户信息泄露；

(3)其他造成或可能造成一般危害或影响的网络安全事件。

4.监测预警

4.1 事件监测

基础电信企业、域名机构、互联网企业应当对本单位网络和系统的运行状况进行密切监测，一旦发生本预案规定的网络安全突发事件，应当立即通过电话等方式向部应急办和相关省(自治区、直辖市)通信管理局报告，不得迟报、谎报、瞒报、漏报。

网络安全专业机构、网络安全企业应当通过多种途径监测、收集已经发生的公共互联网网络安全突发事件信息，并及时向部应急办和相关省(自治区、直辖市)通信管理局报告。

报告突发事件信息时，应当说明事件发生时间、初步判定的影响范围和危

害、已采取的应急处置措施和有关建议。

4.2 预警监测

基础电信企业、域名机构、互联网企业、网络安全专业机构、网络安全企业应当通过多种途径监测、收集漏洞、病毒、网络攻击最新动向等网络安全隐患和预警信息，对发生突发事件的可能性及其可能造成的影响进行分析评估；认为可能发生特别重大或重大突发事件的，应当立即向部应急办报告；认为可能发生较大或一般突发事件的，应当立即向相关省(自治区、直辖市)通信管理局报告。

4.3 预警分级

建立公共互联网网络突发事件预警制度，按照紧急程度、发展态势和可能造成的危害程度，公共互联网网络突发事件预警等级分为四级：由高到低依次用红色、橙色、黄色和蓝色标示，分别对应可能发生特别重大、重大、较大和一般网络安全突发事件。

4.4 预警发布

部应急办和各省(自治区、直辖市)通信管理局应当及时汇总分析突发事件隐患和预警信息，必要时组织相关单位、专业技术人员、专家学者进行会商研判。

认为需要发布红色预警的，由部应急办报国家网络安全应急办公室统一发布(或转发国家网络安全应急办公室发布的红色预警)，并报部领导小组；认为需要发布橙色预警的，由部应急办统一发布，并报国家网络安全应急办公室和部领导小组；认为需要发布黄色、蓝色预警的，相关省(自治区、直辖市)通信管理局可在本行政区域内发布，并报部应急办，同时通报地方相关部门。对达不到预警级别但又需要发布警示信息的，部应急办和各省(自治区、直辖市)通信管理局可以发布风险提示信息。

发布预警信息时，应当包括预警级别、起始时间、可能的影响范围和造成的危害、应采取的防范措施、时限要求和发布机关等，并公布咨询电话。面向社会发布预警信息可通过网站、短信、微信等多种形式。

4.5 预警响应

4.5.1 黄色、蓝色预警响应

发布黄色、蓝色预警后，相关省(自治区、直辖市)通信管理局应当针对即将发生的网络安全突发事件的特点和可能造成的危害，采取下列措施：

(1)要求有关单位、机构和人员及时收集、报告有关信息，加强网络安全风险的监测；

(2)组织有关单位、机构和人员加强事态跟踪分析评估，密切关注事态发展，重要情况报部应急办；

(3)及时宣传避免、减轻危害的措施，公布咨询电话，并对相关信息的报道工作进行正确引导。

4.5.2 红色、橙色预警响应

发布红色、橙色预警后，部应急办除采取黄色、蓝色预警响应措施外，还应当针对即将发生的网络安全突发事件的特点和可能造成的危害，采取下列措施：

(1)要求各相关单位实行24 小时值班，相关人员保持通信联络畅通；

(2)组织研究制定防范措施和应急工作方案，协调调度各方资源，做好各项准备工作，重要情况报部领导小组；

(3)组织有关单位加强对重要网络、系统的网络安全防护；

(4)要求相关网络安全专业机构、网络安全企业进入待命状态，针对预警信息研究制定应对方案，检查应急设备、软件工具等，确保处于良好状态。

4.6 预警解除

部应急办和省(自治区、直辖市)通信管理局发布预警后，应当根据事态发展，适时调整预警级别并按照权限重新发布；经研判不可能发生突发事件或风险已经解除的，应当及时宣布解除预警，并解除已经采取的有关措施。相关省(自治区、直辖市)通信管理局解除黄色、蓝色预警后，应及时向部应急办报告。

5.应急处置

5.1 响应分级

公共互联网网络安全突发事件应急响应分为四级：Ⅰ级、Ⅱ级、Ⅲ级、Ⅳ级，分别对应已经发生的特别重大、重大、较大、一般事件的应急响应。

5.2 先行处置

公共互联网网络安全突发事件发生后，事发单位在按照本预案规定立即向电信主管部门报告的同时，应当立即启动本单位应急预案，组织本单位应急队伍和工作人员采取应急处置措施，尽最大努力恢复网络和系统运行，尽可能减少对用户和社会的影响，同时注意保存网络攻击、网络入侵或网络病毒的证据。

5.3 启动响应

I 级响应根据国家有关决定或经部领导小组批准后启动，由部领导小组统一指挥、协调。

II 级响应由部应急办决定启动，由部应急办统一指挥、协调。

Ⅲ级、IV 级响应由相关省(自治区、直辖市)通信管理局决定启动，并负责指挥、协调。

启动 I 级、II 级响应后，部应急办立即将突发事件情况向国家网络安全应急办公室等报告；部应急办和相关单位进入应急状态，实行 24 小时值班，相关人员保持联络畅通，相关单位派员参加部应急办工作；视情在部应急办设立应急恢复、攻击溯源、影响评估、信息发布、跨部门协调、国际协调等工作组。

启动Ⅲ级、IV 级响应后，相关省(自治区、直辖市)通信管理局应及时将相关情况报部应急办。

5.4 事态跟踪

启动 I 级、II 级响应后，事发单位和网络安全专业机构、网络安全企业应当持续加强监测，跟踪事态发展，检查影响范围，密切关注舆情，及时将事态发展变化、处置进展情况、相关舆情报部应急办。省(自治区、直辖市)通信管理局立即全面了解本行政区域受影响情况，并及时报部应急办。基础电信企业、域名机构、互联网企业立即了解自身网络和系统受影响情况，并及时报部应急办。

启动Ⅲ级、IV 级响应后，相关省(自治区、直辖市)通信管理局组织相关单位加强事态跟踪研判。

5.5 决策部署

启动 I 级、II 级响应后，部领导小组或部应急办紧急召开会议，听取各相关方面情况汇报，研究紧急应对措施，对应急处置工作进行决策部署。

针对突发事件的类型、特点和原因，要求相关单位采取以下措施：带宽紧急扩容、控制攻击源、过滤攻击流量、修补漏洞、查杀病毒、关闭端口、启用备份数据、暂时关闭相关系统等；对大规模用户信息泄露事件，要求事发单位及时告知受影响的用户，并告知用户减轻危害的措施；防止发生次生、衍生事件的必要措施；其他可以控制和减轻危害的措施。

做好信息报送。及时向国家网络安全应急办公室等报告突发事件处置进展情况；视情况由部应急办向相关职能部门、相关行业主管部门通报突发事件有关情况，必要时向相关部门请求提供支援。视情况向外国政府部门通报有关情况并请求协助。

注重信息发布。及时向社会公众通告突发事件情况，宣传避免或减轻危害的措施，公布咨询电话，引导社会舆论。未经部应急办同意，各相关单位不得擅自向社会发布突发事件相关信息。

启动III级、IV 级响应后，相关省(自治区、直辖市)通信管理局组织相关单位开展处置工作。处置中需要其他区域提供配合和支持的，接受请求的省(自治区、直辖市)通信管理局应当在权限范围内积极配合并提供必要的支持；必要时可报请部应急办予以协调。

5.6 结束响应

突发事件的影响和危害得到控制或消除后，I 级响应根据国家有关决定或经部领导小组批准后结束；II 级响应由部应急办决定结束，并报部领导小组；III级、IV 级响应由相关省(自治区、直辖市)通信管理局决定结束，并报部应急办。

6.事后总结

6.1 调查评估

公共互联网网络安全突发事件应急响应结束后，事发单位要及时调查突发事件的起因(包括直接原因和间接原因)、经过、责任，评估突发事件造成的影响和损失，总结突发事件防范和应急处置工作的经验教训，提出处理意见和改进措施，在应急响应结束后 10 个工作日内形成总结报告，报电信主管部门。电信主管部门汇总并研究后，在应急响应结束后 20 个工作日内形成报告，按程序上报。

6.2 奖惩问责

工业和信息化部对网络安全突发事件应对工作中作出突出贡献的先进集体和个人给予表彰或奖励。

对不按照规定制定应急预案和组织开展演练，迟报、谎报、瞒报和漏报突发事件重要情况，或在预防、预警和应急工作中有其他失职、渎职行为的单位或个人，由电信主管部门给予约谈、通报或依法、依规给予问责或处分。基础电信企业有关情况纳入企业年度网络与信息安全责任考核。

7.预防与应急准备

7.1 预防保护

基础电信企业、域名机构、互联网企业应当根据有关法律法规和国家、行业标准的规定，建立健全网络安全管理制度，采取网络安全防护技术措施，建设网络安全技术手段，定期进行网络安全检查和风险评估，及时消除隐患和风险。电信主管部门依法开展网络安全监督检查，指导督促相关单位消除安全隐患。

7.2 应急演练

电信主管部门应当组织开展公共互联网网络安全突发事件应急演练，提高相关单位网络安全突发事件应对能力。基础电信企业、大型互联网企业、域名机构要积极参与电信主管部门组织的应急演练，并应每年组织开展一次本单位网络安全应急演练，应急演练情况要向电信主管部门报告。

7.3 宣传培训

电信主管部门、网络安全专业机构组织开展网络安全应急相关法律法规、应急预案和基本知识的宣传教育和培训，提高相关企业和社会公众的网络安全意识和防护、应急能力。基础电信企业、域名机构、互联网企业要面向本单位员工加强网络安全应急宣传教育和培训。鼓励开展各种形式的网络安全竞赛。

7.4 手段建设

工业和信息化部规划建设统一的公共互联网网络安全应急指挥平台，汇集、存储、分析有关突发事件的信息，开展应急指挥调度。指导基础电信企业、大型互联网企业、域名机构和网络安全专业机构等单位规划建设本单位突发事件信息系统，并与工业和信息化部应急指挥平台实现互联互通。

7.5 工具配备

基础电信企业、域名机构、互联网企业和网络安全专业机构应加强对木马查杀、漏洞检测、网络扫描、渗透测试等网络安全应急装备、工具的储备，及时调整、升级软件硬件工具。鼓励研制开发相关技术装备和工具。

8.保障措施

8.1 落实责任

各省(自治区、直辖市)通信管理局、基础电信企业、域名机构、互联网企业、网络安全专业机构要落实网络安全应急工作责任制，把责任落实到单位领导、具体部门、具体岗位和个人，建立健全本单位网络安全应急工作体制机制。

8.2 经费保障

工业和信息化部为部应急办、各省(自治区、直辖市)通信管理局、网络安全专业机构开展公共互联网网络安全突发事件应对工作提供必要的经费保障。基础电信企业、域名机构、大型互联网企业应当安排专项资金，支持本单位网络安全应急队伍建设、手段建设、应急演练、应急培训等工作开展。

8.3 队伍建设

网络安全专业机构要加强网络安全应急技术支撑队伍建设，不断提升网络安全突发事件预防保护、监测预警、应急处置、攻击溯源等能力。基础电信企业、域名机构、大型互联网企业要建立专门的网络安全应急队伍，提升本单位网络安全应急能力。支持网络安全企业提升应急支撑能力，促进网络安全应急产业发展。

8.4 社会力量

建立工业和信息化部网络安全应急专家组，充分发挥专家在应急处置工作中的作用。从网络安全专业机构、相关企业、科研院所、高等学校中选拔网络安全技术人才，形成网络安全技术人才库。

8.5 国际合作

工业和信息化部根据职责建立国际合作渠道，签订国际合作协议，必要时通过国际合作应对公共互联网网络安全突发事件。鼓励网络安全专业机构、基础电信企业、域名机构、互联网企业、网络安全企业开展网络安全国际交流与

合作。

9.附则

9.1 预案管理

本预案原则上每年评估一次，根据实际情况由工业和信息化部适时进行修订。

各省(自治区、直辖市)通信管理局要根据本预案，结合实际制定或修订本行政区域公共互联网网络安全突发事件应急预案，并报工业和信息化部备案。

基础电信企业、域名机构、互联网企业要制定本单位公共互联网网络安全突发事件应急预案。基础电信企业、域名机构、大型互联网企业的应急预案要向电信主管部门备案。

9.2 预案解释

本预案由工业和信息化部网络安全管理局负责解释。

9.3 预案实施时间

本预案自印发之日起实施。2009 年 9 月 29 日印发的《公共互联网网络安全应急预案》同时废止。

工业和信息化部关于印发《电信和互联网行业提升网络数据安全保护能力专项行动方案》的通知

工信厅网安〔2019〕42 号

各省、自治区、直辖市通信管理局，中国信息通信研究院、中国电子信息产业发展研究院、国家工业信息安全发展研究中心、中国电子技术标准化研究院、人民邮电报社、中国工业互联网研究院、中国互联网协会、中国通信标准化协会，中国电信集团有限公司、中国移动通信集团有限公司、中国联合网络通信集团有限公司、中国广播电视网络有限公司，有关互联网企业：

现将《电信和互联网行业提升网络数据安全保护能力专项行动方案》(工信厅网安〔2019〕42 号)印发给你们，请认真抓好贯彻执行。

联系人及电话：苗琳 010-66069800/66069561(传真)

电子邮箱：miaolin@miit.gov.cn

工业和信息化部办公厅

2019 年 6 月 28 日

电信和互联网行业提升网络数据安全保护能力专项行动方案

近年来，随着国家大数据发展战略加快实施，大数据技术创新与应用日趋活跃，产生和集聚了类型丰富多样、应用价值不断提升的海量网络数据，成为数字经济发展的关键生产要素。与此同时，数据过度采集滥用、非法交易及用户数据泄露等数据安全问题日益凸显，做好电信和互联网行业(以下简称行业)网络数据安全管理尤为迫切。为积极应对新形势新情况新问题，切实做好新中国成立 70 周年网络数据安全保障工作，全面提升行业网络数据安全保护能力，制定本方案。

一、总体要求

以习近平新时代中国特色社会主义思想为指导，全面贯彻党的十九大和十九届二中、三中全会精神，严格落实《网络安全法》《全国人民代表大会常务委员会关于加强网络信息保护的决定》《互联网信息服务管理办法》等法律法规，坚持维护数据安全与促进数据开发利用并重，坚持数据分类分级保护，坚持充分发挥政府引导作用、企业主体作用和社会监督作用，立足我部行业网络数据安全监管职责，开展为期一年的行业提升网络数据安全保护能力专项行动(以下简称专项行动)，加快推动构建行业网络数据安全综合保障体系，为建设网络强国、助力数字经济发展提供有力保障和重要支撑。

二、工作目标

(一)通过集中开展数据安全合规性评估、专项治理和监督检查，督促基础电信企业和重点互联网企业强化网络数据安全全流程管理，及时整改消除重大数据泄露、滥用等安全隐患，2019 年 10 月底前完成全部基础电信企业(含专业公司)、50 家重点互联网企业以及 200 款主流 App 数据安全检查，圆满完成新中国成立 70 周年等重大活动网络数据安全保障工作。

(二)基本建立行业网络数据安全保障体系。网络数据安全制度标准体系进一步完善，形成行业网络数据保护目录，制定 15 项以上行业网络数据安全标准规范，贯标试点企业不少于 20 家；行业网络数据安全管理和技术支撑平台基本建成，遴选网络数据安全技术能力创新示范项目不少于 30 个；基础电信企业和重点互联网企业网络数据安全管理体系有效建立。

三、重点任务

(一)加快完善网络数据安全制度标准

1.强化网络数据安全管理制度设计。梳理对标《网络安全法》《电信和互联网用户个人信息保护规定》等法律法规要求，加快建立网络数据分类分级保护、数据安全风险评估、数据安全事件通报处置、数据对外提供使用报告等制度。部署电信和互联网企业按照法律法规要求，开展数据安全管理对标工作，健全完善企业内部网络数据全生命周期安全管理制度。

2.完善网络数据安全标准体系。推动出台行业《网络数据安全标准体系建设指南》，加快完善行业网络数据安全标准体系。制定出台行业重要数据识别指南、网络数据安全防护等重点标准，遴选企业开展贯标试点。指导中国通信标准化协会成立网络数据安全标准专项工作组，加快推动网络数据安全相关标准制定工作。

(二)开展合规性评估和专项治理

3.开展网络数据安全风险评估。出台网络数据安全合规性评估要点，依托互联网新技术新业务安全评估机制，部署基础电信企业(含专业公司)和重点互联网企业结合重点业务类型和场景，开展网络数据安全合规性自评估工作，提升企业网络数据安全风险防范能力。针对物联网、车联网、卫星互联网、人工智能等新技术新应用带来的重大互联网数据安全问题，及时开展行业评估和跨部门联合评估工作。

4.深化 App 违法违规专项治理。持续推进 App 违法违规收集使用个人信息专项治理行动，组织第三方评测机构开展 App 安全滚动式评测，对在网络数据安全和用户信息保护方面存在违法违规行为的 App 及时进行下架和公开曝光。组织开展应用商店安全责任专项部署，督促应用商店落实 App 运营者真实身份信息验证、应用程序安全检测、违法违规 App 下架等责任。创新工作模式，引导鼓励第三方机构开展 App 数据安全管理认证，探索推动应用商店等明确标识并优先推荐通过认证的 App。

5.强化网络数据安全监督执法。将企业网络数据安全责任落实情况、数据安全合规性评估落实情况作为重点内容，纳入 2019 年网络信息安全“双随机一公开”检查和基础电信企业网络与信息安全责任考核检查，采取远程测试、实地检查等方式开展监督检查，督促问题整改。持续开展数据泄露等网络数据安

全和用户信息安全事件监测跟踪与执法调查，对违法违规行为及时采取约谈、公开曝光、行政处罚等措施，将处罚结果纳入电信业务经营不良名单或失信名单。

(三)强化行业网络数据安全管理

6.稳步实施网络数据资源“清单式”管理。开展电信和重点互联网企业网络数据资源调研摸底，依据网络数据重要敏感程度和泄露滥用可能造成的危害，研究形成行业网络数据保护目录，并选取重点企业开展试点应用。指导督促试点企业建立内部网络数据清单和数据分类分级管理制度，对列入目录的网络数据实施重点保护。

7.明确企业网络数据安全职能部门。指导电信和重点互联网企业加强内部网络数据安全组织保障，推动设立或明确网络数据安全管理责任部门和专职人员，负责承担企业内部网络数据安全管理工作，督促协调企业内部各相关主体和环节严格落实操作权限管理、日志记录和安全审计、数据加密、数据脱敏、访问控制、数据容灾备份等数据安全保护措施，组织开展数据安全岗位人员法律法规、知识技能等培训。

8.强化网络数据对外合作安全管理。落实《工业和信息化部关于加强基础电信企业数据安全管理规范清理数据对外合作工作的通知》等相关管理要求，督促企业定期开展网络数据对外合作业务专项排查，及时发现问题消除隐患。研究明确利用行业网络数据进行大数据开发应用的数据安全管理要求，督促企业开展合作方数据安全保障能力动态评估，充分依托合同约束、信用管理等手段强化合作方管理，切实提升网络数据共享安全管理水平。

9.加强行业网络数据安全应急管理。落实工业和信息化部相关应急预案要求，指导企业进一步健全完善企业网络数据安全事件应急处置机制，开展应急演练，落实重大网络数据安全事件报告、调查追责、向社会公告等要求。在新中国成立 70 周年等重大活动保障期间，明确企业数据安全重要岗位职责要求，强化应急响应，及时处置网络数据安全突发情况。

(四)创新推动网络数据安全技术防护能力建设

10.加强网络数据安全技术手段建设。加快建设行业网络数据安全管理和技术支撑平台，支撑开展行业数据备案管理、事件通报、溯源核查、技术检测和

安全认证等工作，提升网络数据安全监管技术支撑保障能力。指导企业加大网络数据安全技术投入，加快完善数据防攻击、防窃取、防泄漏、数据备份和恢复等安全技术保障措施，提升企业网络数据安全保障能力。

11.推动网络数据安全技术创新发展。推动成立大数据安全联盟，打造网络数据安全技术交流、联合攻关和试点应用平台。组织开展网络数据安全技术最佳实践案例征集和试点示范项目评选，加大技术研发、成果转化和解决方案的支持力度，促进网络数据安全先进技术创新和产品服务应用推广。制定发布网络数据安全产业发展白皮书。

12.加强专业支撑队伍建设。成立行业网络数据安全专家委员会，为网络数据安全政策标准制定、关键技术研究、重大网络数据安全风险评估、网络数据安全示范项目评审等提供决策支撑。委托中国信息通信研究院、中国电子信息产业发展研究院、中国电子技术标准化研究院、中国互联网协会、中国通信标准化协会等单位开展面向行业的网络数据安全法律法规和政策标准宣贯、技能培训和测试检查。

(五)强化社会监督和宣传交流

13.强化社会监督和行业自律。依托中国互联网协会 12321 网络不良与垃圾信息举报受理中心，建立网络数据违法违规行为举报平台，及时受理用户投诉举报。强化行业自律，指导中国互联网协会联合基础电信企业、重点互联网企业、第三方机构等签署网络数据安全自律公约，引导企业自觉履行数据安全保护义务，努力提高数据安全保护水平。

14.加强宣传展示和国际交流。充分利用中国互联网大会、中国国际大数据产业博览会、国家网络安全宣传周等，指导相关单位举办网络数据安全论坛，开展网络数据安全主题宣传日等活动，促进网络数据安全管理和技术经验交流，提升全行业数据安全意识。加强数据安全国际交流合作，利用世界互联网大会、中欧数字经济与网络安全会议等，积极开展数据安全管理经验交流和信息共享。

四、工作安排

(一)工作部署阶段(2019 年 7 月)。部制定印发专项行动方案，组织开展宣贯部署，向各单位、各企业制定印发工作任务清单，明确各项任务时间节点和

工作要求。

(二)重点保障阶段(2019 年 8-10 月)。部组织完成电信和重点互联网企业网络数据资源调研摸底，明确数据安全合规性评估要点，指导完成各省级基础电信企业和重点互联网企业重点环节数据安全合规性评估，持续开展 App 违法违规收集使用个人信息专项治理，组织完成对重点企业网络数据安全责任落实情况的监督检查和隐患整改，全力做好新中国成立 70 周年网络数据安全保障工作。

(三)长效建设阶段(2019 年 11 月-2020 年 5 月)。总结固化新中国成立 70 周年网络数据安全保障工作经验，重点围绕关键制度、重点标准、技术手段、示范项目、支撑队伍等方面，加快推进完成重点任务举措，推动建立网络数据安全管理长效机制。

(四)总结提升阶段(2020 年 6-7 月)。各单位、各企业梳理总结专项行动完成情况、工作成效及问题，形成工作总结报部(网络安全管理局)。部组织对专项行动工作情况进行总结通报，对典型经验做法进行推广，巩固相关工作成效。

五、工作要求

(一)加强组织领导。各单位要充分认识加快提升行业网络数据安全保护能力的重要性和紧迫性，结合本单位实际，精心组织，周密部署，迅速行动，确保专项行动顺利开展。部网络安全管理局牵头做好专项行动总体部署、推进落实、督导检查等工作；各地通信管理局结合实际，组织开展属地网络数据安全能力提升专项行动各项工作。

(二)明确任务分工。各企业要明确责任部门和责任人，对照任务清单，坚持问题导向，逐一细化工作措施和责任分工，做到措施到位、责任到人，确保专项行动各项任务落实到位、取得实效。中国信息通信研究院、中国电子信息产业发展研究院、中国电子技术标准化研究院、人民邮电报社、中国互联网协会、中国通信标准化协会等单位要做好相关支撑保障工作。

(三)强化监督检查。部和各地通信管理局组织对各单位、各企业专项行动落实情况进行督导检查，指导督促基础电信企业和互联网企业进一步落实相关制度标准要求，健全完善企业网络数据安全合规管理体系，对存在问题及时督

促整改。

(四)加强宣传通报。各单位、各企业要建立信息通报机制，及时总结专项行动进展和成效，每月底前将工作进展情况、取得成效、问题和建议报部网络安全管理局。大力宣传专项行动新进展、新动态及典型经验做法，营造全行业重视网络数据安全、自觉维护网络数据安全的良好氛围，推动专项行动扎实深入开展。

工业和信息化部关于印发《工业控制系统信息安全防护指南》的通知

工信部信软〔2016〕338 号

为贯彻落实《国务院关于深化制造业与互联网融合发展的指导意见》(国发〔2016〕28 号)，保障工业企业工业控制系统信息安全，制定《工业控制系统信息安全防护指南》，现印发你们。

工业和信息化部指导和管理全国工业企业工控安全防护和保障工作，并根据实际情况对指南进行修订。地方工业和信息化主管部门根据工业和信息化部统筹安排，指导本行政区域内的工业企业制定工控安全防护实施方案，推动企业分期分批达到本指南相关要求。

工业和信息化部

2016 年 10 月 17 日

工业控制系统信息安全防护指南

工业控制系统信息安全事关经济发展、社会稳定和国家安全。为提升工业企业工业控制系统信息安全(以下简称工控安全)防护水平，保障工业控制系统安全，制定本指南。

工业控制系统应用企业以及从事工业控制系统规划、设计、建设、运维、评估的企事业单位适用本指南。

工业控制系统应用企业应从以下十一个方面做好工控安全防护工作。

一、安全软件选择与管理

(一)在工业主机上采用经过离线环境中充分验证测试的防病毒软件或应用程序白名单软件，只允许经过工业企业自身授权和安全评估的软件运行。

(二)建立防病毒和恶意软件入侵管理机制，对工业控制系统及临时接入的设备采取病毒查杀等安全预防措施。

二、配置和补丁管理

(一)做好工业控制网络、工业主机和工业控制设备的安全配置，建立工业控制系统配置清单，定期进行配置审计。

(二)对重大配置变更制定变更计划并进行影响分析，配置变更实施前进行严格安全测试。

(三)密切关注重大工控安全漏洞及其补丁发布，及时采取补丁升级措施。在补丁安装前，需对补丁进行严格的安全评估和测试验证。

三、 边界安全防护

(一)分离工业控制系统的开发、测试和生产环境。

(二)通过工业控制网络边界防护设备对工业控制网络与企业网或互联网之间的边界进行安全防护，禁止没有防护的工业控制网络与互联网连接。

(三)通过工业防火墙、网闸等防护设备对工业控制网络安全区域之间进行逻辑隔离安全防护。

四、物理和环境安全防护

(一)对重要工程师站、数据库、服务器等核心工业控制软硬件所在区域采取访问控制、视频监控、专人值守等物理安全防护措施。

(二)拆除或封闭工业主机上不必要的USB、光驱、无线等接口。若确需使用，通过主机外设安全管理技术手段实施严格访问控制。

五、身份认证

(一)在工业主机登录、应用服务资源访问、工业云平台访问等过程中使用身份认证管理。对于关键设备、系统和平台的访问采用多因素认证。

(二)合理分类设置账户权限，以最小特权原则分配账户权限。

(三)强化工业控制设备、SCADA 软件、工业通信设备等的登录账户及密码，避免使用默认口令或弱口令，定期更新口令。

(四)加强对身份认证证书信息保护力度，禁止在不同系统和网络环境下共享。

六、远程访问安全

(一)原则上严格禁止工业控制系统面向互联网开通HTTP、FTP、Telnet 等高风险通用网络服务。

(二)确需远程访问的，采用数据单向访问控制等策略进行安全加固，对访问时限进行控制，并采用加标锁定策略。

(三)确需远程维护的，采用虚拟专用网络(VPN)等远程接入方式进行。

(四)保留工业控制系统的相关访问日志，并对操作过程进行安全审计。

七、安全监测和应急预案演练

(一)在工业控制网络部署网络安全监测设备，及时发现、报告并处理网络攻击或异常行为。

(二)在重要工业控制设备前端部署具备工业协议深度包检测功能的防护设备，限制违法操作。

(三)制定工控安全事件应急响应预案，当遭受安全威胁导致工业控制系统出现异常或故障时，应立即采取紧急防护措施，防止事态扩大，并逐级报送直至属地省级工业和信息化主管部门，同时注意保护现场，以便进行调查取证。

(四)定期对工业控制系统的应急响应预案进行演练，必要时对应急响应预案进行修订。

八、资产安全

(一)建设工业控制系统资产清单，明确资产责任人，以及资产使用及处置规则。

(二)对关键主机设备、网络设备、控制组件等进行冗余配置。

九、数据安全

(一)对静态存储和动态传输过程中的重要工业数据进行保护，根据风险评估结果对数据信息进行分级分类管理。

(二)定期备份关键业务数据。

(三)对测试数据进行保护。

十、供应链管理

(一)在选择工业控制系统规划、设计、建设、运维或评估等服务商时，优先考虑具备工控安全防护经验的企事业单位，以合同等方式明确服务商应承担的信息安全责任和义务。

(二)以保密协议的方式要求服务商做好保密工作，防范敏感信息外泄。

十一、落实责任

通过建立工控安全管理机制、成立信息安全协调小组等方式，明确工控安全管理责任人，落实工控安全责任制，部署工控安全防护措施。

工业和信息化部办公厅关于印发《工业数据分类分级指南(试行)》的通知

工信厅信发〔2020〕6 号

各省、自治区、直辖市及新疆生产建设兵团工业和信息化主管部门，有关中央企业：

现将《工业数据分类分级指南(试行)》印发给你们，请结合实际，认真贯彻执行。

工业和信息化部办公厅

2020 年 2 月 27 日

工业数据分类分级指南(试行)

第一章 总 则

第一条 为贯彻《促进大数据发展行动纲要》《大数据产业发展规划(2016-2020 年)》有关要求，更好推动《数据管理能力成熟度评估模型》(GB/T36073-2018)贯标和《工业控制系统信息安全防护指南》落实，指导企业提升工业数据管理能力，促进工业数据的使用、流动与共享，释放数据潜在价值，赋能制造业高质量发展，制定本指南。

第二条 本指南所指工业数据是工业领域产品和服务全生命周期产生和应用的数据，包括但不限于工业企业在研发设计、生产制造、经营管理、运维服务等环节中生成和使用的数据，以及工业互联网平台企业(以下简称平台企业)在设备接入、平台运行、工业 APP 应用等过程中生成和使用的数据。

第三条 本指南适用于工业和信息化主管部门、工业企业、平台企业等开展工业数据分类分级工作。涉及国家秘密信息的工业数据，应遵守保密法律法规的规定，不适用本指南。

第四条 工业数据分类分级以提升企业数据管理能力为目标，坚持问题导向、目标导向和结果导向相结合，企业主体、行业指导和属地监管相结合，分类标识、逐类定级和分级管理相结合。

第二章 数据分类

第五条 工业企业结合生产制造模式、平台企业结合服务运营模式，分析梳

理业务流程和系统设备，考虑行业要求、业务规模、数据复杂程度等实际情况，对工业数据进行分类梳理和标识，形成企业工业数据分类清单。

第六条 工业企业工业数据分类维度包括但不限于研发数据域(研发设计数据、开发测试数据等)、生产数据域(控制信息、工况状态、工艺参数、系统日志等)、运维数据域(物流数据、产品售后服务数据等)、管理数据域(系统设备资产信息、客户与产品信息、产品供应链数据、业务统计数据等)、外部数据域(与其他主体共享的数据等)。

第七条 平台企业工业数据分类维度包括但不限于平台运营数据域(物联采集数据、知识库模型库数据、研发数据等)和企业管理数据域(客户数据、业务合作数据、人事财务数据等)。

第三章 数据分级

第八条 根据不同类别工业数据遭篡改、破坏、泄露或非法利用后，可能对工业生产、经济效益等带来的潜在影响，将工业数据分为一级、二级、三级等3个级别。

第九条 潜在影响符合下列条件之一的数据为三级数据：

(一)易引发特别重大生产安全事故或突发环境事件，或造成直接经济损失特别巨大；

(二)对国民经济、行业发展、公众利益、社会秩序乃至国家安全造成严重影响。

第十条 潜在影响符合下列条件之一的数据为二级数据：

(一)易引发较大或重大生产安全事故或突发环境事件，给企业造成较大负面影响，或直接经济损失较大；

(二)引发的级联效应明显，影响范围涉及多个行业、区域或者行业内多个企业，或影响持续时间长，或可导致大量供应商、客户资源被非法获取或大量个人信息泄露；

(三)恢复工业数据或消除负面影响所需付出的代价较大。

第十一条 潜在影响符合下列条件之一的数据为一级数据：

(一)对工业控制系统及设备、工业互联网平台等的正常生产运行影响较小；

(二)给企业造成负面影响较小，或直接经济损失较小；

(三)受影响的用户和企业数量较少、生产生活区域范围较小、持续时间较短；

(四)恢复工业数据或消除负面影响所需付出的代价较小。

第四章 分级管理

第十二条 工业和信息化部负责制定工业数据分类分级制度规范，指导、协调开展工业数据分类分级工作。各地工业和信息化主管部门负责指导和推动辖区内工业数据分类分级工作。有关行业、领域主管部门可参考本指南，指导和推动本行业、本领域工业数据分类分级工作。

第十三条 工业企业、平台企业等企业承担工业数据管理的主体责任，要建立健全相关管理制度，实施工业数据分类分级管理并开展年度复查，并在企业系统、业务等发生重大变更时应及时更新分类分级结果。有条件的企业可结合实际设立数据管理机构，配备专职人员。

第十四条 企业应按照《工业控制系统信息安全防护指南》等要求，结合工业数据分级情况，做好防护工作。

企业针对三级数据采取的防护措施，应能抵御来自国家级敌对组织的大规模恶意攻击；针对二级数据采取的防护措施，应能抵御大规模、较强恶意攻击；针对一级数据采取的防护措施，应能抵御一般恶意攻击。

第十五条 鼓励企业在做好数据管理的前提下适当共享一、二级数据，充分释放工业数据的潜在价值。二级数据只对确需获取该级数据的授权机构及相关人员开放。三级数据原则上不共享，确需共享的应严格控制知悉范围。

第十六条 工业数据遭篡改、破坏、泄露或非法利用时，企业应根据事先制定的应急预案立即进行应急处置。涉及三级数据时，还应将事件及时上报数据所在地的省级工业和信息化主管部门，并于应急工作结束后 30 日内补充上报事件处置情况。

工业和信息化部关于开展纵深推进 APP 侵害用户权益专项整治行动的通知

工信部信管函〔2020〕164 号

各省、自治区、直辖市通信管理局，中国信息通信研究院、中国互联网协会，各相关单位：

按照2020年信息通信行业行风建设暨纠风工作部署，为切实加强用户个人信息保护，为人民群众提供更安全、更健康、更干净的信息环境，我部决定开展纵深推进APP侵害用户权益专项整治行动。专项整治时间为通知印发之日至2020年12月10日。具体事项通知如下：

一、整治目标

依据《网络安全法》、《电信条例》、《规范互联网信息服务市场秩序若干规定》(工业和信息化部令第20号)、《电信和互联网用户个人信息保护规定》(工业和信息化部令第24号)和《移动智能终端应用软件预置和分发管理暂行规定》(工信部信管〔2016〕407号)等规定，深入推进技管结合，加强监督检查，督促相关企业强化APP个人信息保护，及时整改消除违规收集、使用用户个人信息和骚扰用户、欺骗误导用户、应用分发平台管理责任落实不到位等突出问题，净化APP应用空间。2020年8月底前上线运行全国APP技术检测平台管理系统，12月10日前完成覆盖40万款主流APP检测工作。

二、整治对象

(一)APP服务提供者，即互联网信息服务提供者提供的可以下载、安装、升级的应用软件，包括快应用和小程序等新应用形态。

(二)软件工具开发包(SDK)提供者，即集成在手机APP里的第三方工具集合。

(三)应用分发平台，包括网站、应用商店、APP等承担下载、安装、升级等分发服务的各类平台。

三、整治任务

(一)APP、SDK违规处理用户个人信息方面。

1.违规收集个人信息。重点整治APP、SDK未告知用户收集个人信息的目的、方式、范围且未经用户同意，私自收集用户个人信息的行为。

2.超范围收集个人信息。重点整治APP、SDK非服务所必需或无合理应用场景，特别是在静默状态下或在后台运行时，超范围收集个人信息的行为。

3.违规使用个人信息。重点整治APP、SDK未向用户告知且未经用户同意，私自使用个人信息，将用户个人信息用于其提供服务之外的目的，特别是私自向其他应用或服务器发送、共享用户个人信息的行为。

4.强制用户使用定向推送功能。重点整治 APP、SDK 未以显著方式标示且未经用户同意，将收集到的用户搜索、浏览记录、使用习惯等个人信息，用于定向推送或广告精准营销，且未提供关闭该功能选项的行为。

(二)设置障碍、频繁骚扰用户方面。

5.APP 强制、频繁、过度索取权限。重点整治 APP 安装、运行和使用相关功能时，非服务所必需或无合理应用场景下，用户拒绝相关授权申请后，应用自动退出或关闭的行为。重点整治短时长、高频次，在用户明确拒绝权限申请后，频繁弹窗、反复申请与当前服务场景无关权限的行为。重点整治未及时明确告知用户索取权限的目的和用途，提前申请超出其业务功能等权限的行为。

6.APP 频繁自启动和关联启动。重点整治 APP 未向用户告知且未经用户同意，或无合理的使用场景，频繁自启动或关联启动第三方 APP 的行为。

(三)欺骗误导用户方面。

7.欺骗误导用户下载 APP。重点整治通过“偷梁换柱”“移花接木”等方式欺骗误导用户下载 APP，特别是具有分发功能的移动应用程序欺骗误导用户下载非用户所自愿下载 APP 的行为。

8.欺骗误导用户提供个人信息。重点整治非服务所必需或无合理场景，通过积分、奖励、优惠等方式欺骗误导用户提供身份证号码以及个人生物特征信息的行为。

(四)应用分发平台责任落实不到位方面。

9.应用分发平台上的 APP 信息明示不到位。重点整治应用分发平台上未明示 APP 运行所需权限列表及用途，未明示 APP 收集、使用用户个人信息的内容、目的、方式和范围等行为。

10.应用分发平台管理责任落实不到位。重点整治 APP 上架审核不严格、违法违规软件处理不及时和 APP 提供者、运营者、开发者身份信息不真实、联系方式虚假失效等问题。

四、工作要求

(一)开展检测检查。我部将于即日起组织第三方检测机构对 APP、SDK 进行技术检测，对应用分发平台的主体责任落实情况进行监督检查。对第一次检查发现存在问题的企业，我部将责令 5 个工作日内完成整改，对整改不彻底仍然

存在问题的，将采取向社会公告、组织下架、行政处罚以及将受到行政处罚的违规主体纳入电信业务经营不良名单或失信名单等措施；对在 APP 不同版本中反复出现问题的企业，我部将向社会公告，并依法依规开展后续处置工作。

(二)抓好执行落实。各地通信管理局要结合实际开展检查工作，每月 15 日前将违规线索录入全国 APP 技术检测平台管理系统，并按照部工作要求开展相关问题处置。相关企业要及时开展自查自纠，对发现的问题立行立改，举一反三，切实有效保护个人信息。APP 企业要完善用户权益保障制度，加强对所集成 SDK 的管理。应用分发平台要强化平台管理责任，积极配合电信主管部门开展相关监管工作。

(三)推动行业自律。鼓励行业协会组织 APP 开发运营者、应用分发平台、第三方服务提供者、电信设备生产企业、安全厂商等相关单位，制定行业自律公约和技术检测标准，健全第三方评议机制，强化行业规范。

(四)强化手段建设。中国信息通信研究院要大力推进全国APP 技术检测平台管理系统建设，进一步凝聚产业力量，鼓励有条件的企业积极参与平台建设，提升自动化检测水平和能力。各地通信管理局要尽快接入，用好相关技术手段，做到关口前移，及时发现解决问题，不断提升行业治理能力和水平。

(五)畅通投诉渠道。专项整治工作期间，各企业应畅通用户投诉渠道，完善投诉处理服务机制和流程。中国互联网协会应通过互联网信息服务投诉平台(https：//ts.isc.org.cn/)或 12321 举报中心接受群众投诉，及时汇总处理用户反映的相关问题。

工业和信息化部

2020 年 7 月 22 日

工业和信息化部办公厅 国家卫生健康委办公厅关于进一步加强远程医疗网络能力建设的通知

工信厅联通信函〔2020〕251 号

各省、自治区、直辖市通信管理局、卫生健康委，新疆生产建设兵团卫生健康委，各相关企业：

为深入贯彻落实《国务院办公厅关于促进“互联网+医疗健康”发展的意见》(国办发〔2018〕26 号)，推进“互联网+”在医疗健康领域的应用发展，

增强基层卫生防疫能力，现就进一步加强远程医疗网络能力建设有关事项通知如下：

一、扩大网络覆盖

(一)提升基层医疗卫生机构网络覆盖水平。基础电信企业持续推进偏远和贫困地区光纤宽带和 4G 网络建设，进一步扩大网络覆盖范围，不断增强网络能力，加快推动宽带网络普遍覆盖基层医疗卫生机构。

(二)推进 5G 网络覆盖医疗卫生机构。面向有条件的地区和应用需求明确的医疗卫生机构，加快推进 5G 网络建设，充分发挥 5G 网络低时延、大连接、高带宽的特点，应用 5G 切片、边缘计算等先进技术，为远程医疗提供更优网络能力。

(三)推动专线网络资源覆盖二级及以上医院。加快高质量互联网专线、数据专线及虚拟专线(VPN)网络建设，实现专线网络资源覆盖所有二级及以上医院(含妇幼保健院)，具备提供优质专线服务能力。

(四)建立各级医疗卫生机构宽带接入台账。地方卫生健康主管部门会同通信主管部门建立未通宽带医疗卫生机构清单，摸清底数并定期动态跟踪，提升各级医疗卫生机构网络接入率，2022 年实现 98%以上基层医疗卫生机构接入互联网。

二、提高网络能力

(五)推动医疗卫生机构网络普遍提速。持续加强网络基础设施建设，不断增强各级各类医疗卫生机构的网络接入能力。为采用公众互联网接入的医疗卫生机构提速至 100Mb/s 以上，采用互联网专线接入的医疗卫生机构提速至 20Mb/s 以上。

(六)增强各级各类医疗卫生机构的网络能力。基础电信企业持续提升网络承载能力、优化资源配置，针对不同业务需求提供差异化接入服务，推动县级以上医院具备千兆网络接入能力。鼓励各级各类医疗卫生机构根据自身业务开展情况，综合使用数据专线、VPN、互联网专线、公众互联网等多种接入方式，提升医疗活动网络化水平。

(七)丰富远程医疗网络技术手段和服务模式。支持并鼓励社会各有关企业基于公众互联网或专线网络，采用 SD-WAN、实时视频通信、智能网络调度等多

种技术方案，优化网络传输质量。面向医疗卫生机构提供整体远程医疗中心解决方案，实现远程医疗网络、平台、硬件设备的一体化建设，节约建设成本，进一步提升传输质量，实现医联体内部业务的互联共享。

三、推广网络应用

(八)探索 5G 网络在远程医疗中的创新应用。鼓励有条件的医疗卫生机构与基础电信企业合作，建设 5G 智慧医疗健康联合实验室或应用示范基地，推动基于 5G 网络的应用创新和服务创新。鼓励医疗设备厂商开展 5G 网络制式的研发和适配工作，提升专业设备的 5G 接入能力，充分发挥 5G 的技术优势。

(九)建设医疗云计算和大数据应用服务体系。充分利用大数据、云计算、人工智能等新一代信息技术，构建医疗专属云服务，结合区域全民健康信息平台建设，推动各级医疗卫生机构间数据共享互认和业务协同。完善医疗云计算和医疗大数据服务能力评估体系，保障医疗云计算资源、医疗大数据资产全生命周期内合规、可信。持续提升医疗信息化基础能力，实现信息资源共享，为远程会诊、远程影像、远程心电、远程急救、远程病理、远程教学、远程监护等网络应用场景提供技术支撑。

(十)推进“互联网+健康扶贫”试点。支持贫困地区利用远程医疗网络及其平台资源创新健康扶贫工作模式，巩固基本医疗有保障成效。实现远程医疗覆盖所有贫困县，有条件的地区推动远程诊疗覆盖到村、在线医学教育普及到

人、在线慢病管理精准到户，充分利用新一代信息技术提升贫困地区基层医疗卫生服务能力，提高贫困人口的健康水平。

(十一)支持开展远程医疗应用示范。支持各级各类医疗卫生机构与基础电信企业广泛开展合作，推动高质量医疗专网、医疗创新中心建设，开展医疗卫生机构与电信企业合作创新试点示范，总结推广先进经验，以点带面，进一步满足群众医疗服务需求。

(十二)提升远程医疗系统互联互通能力。鼓励有条件的地方和相关企业，研究推进远程医疗系统音视频通讯互联互通机制，提升不同厂商、不同时期建设的远程医疗系统互联互通能力。

(十三)推出医疗卫生机构网络资费优惠政策。鼓励基础电信企业面向医疗卫生机构，特别是贫困地区基层医疗卫生机构，推出互联网宽带和专线接入资

费优惠，资费水平不高于其他企业宽带和专线平均资费水平，减轻医疗卫生机构网络使用负担。

四、加强组织保障

(十四)建立协同工作机制。各地通信主管部门与卫生健康主管部门建立协同工作机制，研究本地加强远程医疗网络能力提升工作方案，组织当地电信企业与医疗卫生机构加强协作，进一步提升医疗信息化水平。

(十五)完善“互联网+医疗健康”网络标准体系。构建“互联网+医疗健康”标准协调机制，重点推进医疗健康网络通用需求、网络架构、通信协议、关键接口、互联互通、网络安全等总体性标准，进一步规范医疗健康网络、医疗信息化服务、信息系统技术能力与服务质量，助力构建公平、有序、开放的医疗健康网络环境。

(十六)加强远程医疗网络质量监测管理。建设远程医疗网络监测管理平台，开展面向远程医疗服务的网络质量监测、安全感知、故障预警和统计分析等工作，面向重要系统、重点链路进行运行状况监测和指标分析汇总，有效支撑上层业务开展。鼓励各地开展省域内远程医疗网络质量的监测管理工作。

工业和信息化部办公厅　国家卫生健康委办公厅

2020 年 10 月 22 日

工业和信息化部关于印发《互联网应用适老化及无障碍改造专项行动方案》的通知

工信部信管〔2020〕200 号

各省、自治区、直辖市通信管理局，中国电信集团有限公司、中国移动通信集团有限公司、中国联合网络通信集团有限公司，中国信息通信研究院，中国互联网协会，其他相关企业：

按照《国务院办公厅印发关于切实解决老年人运用智能技术困难实施方案的通知》(国办发〔2020〕45 号)和《工业和信息化部　中国残疾人联合会关于推进信息无障碍的指导意见》(工信部联信管〔2020〕146 号)部署，为着力解决老年人、残疾人等特殊群体在使用互联网等智能技术时遇到的困难，推动充分兼顾老年人、残疾人需求的信息化社会建设，工业和信息化部决定自 2021 年 1 月起，在全国范围内组织开展为期一年的互联网应用适老化及无障碍改造专

项行动。现将《互联网应用适老化和无障碍改造专项行动方案》印发给你们，请结合实际认真贯彻落实。

附件：互联网应用适老化及无障碍改造专项行动方案

工业和信息化部

2020 年 12 月 24 日

工业和信息化部办公厅关于进一步抓好互联网应用适老化及无障碍改造专项行动实施工作的通知

工信厅信管函〔2021〕67 号

各省、自治区、直辖市通信管理局，中国电信集团有限公司、中国移动通信集团有限公司、中国联合网络通信集团有限公司，中国信息通信研究院，中国互联网协会，各相关单位及企业：

为抓好《工业和信息化部关于印发互联网应用适老化及无障碍改造专项行动方案的通知》（工信部信管〔2020〕200 号，以下简称《行动方案》）实施，加快推进互联网应用适老化及无障碍改造专项行动，助力老年人、残疾人等重点受益群体平等便捷地获取、使用互联网应用信息，现将有关事项通知如下：

一、关于改造标准规范

（一）互联网网站。请参照《互联网网站适老化通用设计规范》（附件 1）、国家标准 GB/T 37668-2019《信息技术 互联网内容无障碍可访问性技术要求与测试方法》和行业标准 YD/T1822-2008《信息无障碍 身体机能差异人群 网站无障碍评级测试方法》相关技术要求进行适老化及无障碍改造，由中国互联网协会负责具体指导和技术支撑等工作。（2021 年 9 月 30 日前完成）

（二）移动互联网应用（APP）。请参照《移动互联网应用（APP）适老化通用设计规范》（附件 2）和国家标准GB/T 37668-2019《信息技术 互联网内容无障碍可访问性技术要求与测试方法》相关技术要求进行适老化及无障碍改造，由中国信息通信研究院负责具体指导和技术支撑等工作。（2021 年 9 月 30 日前完成）

二、关于评测要求

相关互联网网站、APP 完成适老化及无障碍改造后，可分别向中国互联网协会、中国信息通信研究院申请评测。评测要求及具体指标详见《互联网应用

适老化及无障碍水平评测体系》(附件 3)。工业和信息化部统一向社会公布评测结果。(2021 年 10 月 31 日前完成)

三、关于标识授予

相关互联网网站、APP 通过评测后，由中国互联网协会、中国信息通信研究院分别授予信息无障碍标识(♿)，有效期为两年。各互联网网站、APP 完成改造后要继续做好后续版本的维护优化工作。工业和信息化部将组织对最新版本的互联网网站、APP 的适老化及无障碍改造情况进行抽查，授予单位根据抽查结果延续或撤销已授予的标识。(2021 年 11 月 30 日前完成)

四、关于纳入企业信用评价

工业和信息化部与各地通信管理局按照“谁发证、谁备案、谁记分”的原则，依企业申请，根据互联网网站、APP 的评测结果及标识授予情况，对在适老化及无障碍改造工作中表现突出的，在“企业信用评价”中予以信用加分。(2021 年 12 月 31 日前完成)

五、关于成果宣传

请各单位积极运用多种渠道，向社会充分宣传互联网应用适老化及无障碍改造成果。鼓励有条件的单位开设专门宣传频道，普及信息无障碍知识和通用设计理念，共同助力营造良好舆论氛围，推动信息无障碍事业持续发展。

请各单位严格按照《行动方案》及本通知要求，加强协作，积极融合运用新技术，共同助力提升互联网应用适老化及无障碍化普及率，切实让重点受益群体在信息化发展中享受到更多的获得感、幸福感、安全感。

联系方式：工业和信息化部 冯鹏一 刘如旭 010-68206135 010-66024197(传真)

中国信息通信研究院 丁丽婷

010-62305212 dingliting@caict.ac.cn

中国互联网协会 黄畅

010-68208792 changhu7142@vip.sina.com

附件：

1.互联网网站适老化通用设计规范

2.移动互联网应用(APP)适老化通用设计规范

3.互联网应用适老化及无障碍水平评测体系

工业和信息化部办公厅

2021 年 4 月 6 日

附件 1：

互联网网站适老化通用设计规范

一、适用范围

本规范规定了互联网网站适老化通用设计规范和技术要求，适用于各种终端的适老化网站设计，也适用于网站的适老化改造与技术开发。

二、服务原则

1.以人为本的人机交互

应做到界面元素的简约化、服务形式的差异化、信息内容的扁平化、功能标识的统一化和操作流程的一致性，并符合《信息技术 互联网内容无障碍可访问性技术要求与测试方法》等国家标准。

2.提供多种的操作方式

计算机网站至少提供全程键盘和特大鼠标这两种操作方式，移动网站应增加快速定位、语音阅读等规范性的适老化智能手势。在兼容性方面，网页应为各类辅助技术和语音识别等人工智能技术的访问操作，规范相应的服务功能与对应的标识信息。

3.实现多样的推送形式

在网页提供特大字体、背景色高对比、文字放大和语音阅读服务等辅助阅读的同时，应提供简约界面版本和信息影像化的人工智能推送形式，以支持老年人感知网页内容、获取服务。

4.形成有效的服务闭环

提供适老化服务的计算机和移动网站，应在用户的操作系统桌面上，提供直接进入适老化服务快捷方式或客户端，以形成有效的适老化及无障碍服务的闭环。

三、技术要求

1 可感知性

1.1 标识与描述

1.1.1 整体信息。应设置描述当前页面整体服务类型、信息状况和信息结构的语音阅读引导操作机制，并易于老年用户辨识理解和操作。

1.1.2 区域信息。网页各信息区域应有服务类型和信息内容的描述与介绍，并提供对应的语音阅读服务，便利老年用户在访问过程中随时获得信息。

1.1.3 关联性操作。具有上下文关系或其他关联性关系界面组件的计算机网站、网页，应设有显著的操作引导文字或图片说明，以及相应的语音阅读服务。

1.2 视觉呈现

1.2.1 页面布局。网页布局设计应依照扁平化原则进行，避免阴影、透视、纹理等复杂装饰设计，也可独立提供内容简约的适老化大版块网页样式。

1.2.2 区域辨识。在展现服务信息的网页，对各信息服务区域以色彩差异进行区别，以方便老人用户辨识。

1.2.3 字体大小。在不依赖操作系统和浏览器的前提下，计算机适老化网页应提供网页的放大设置与大字屏幕服务，移动网页至少提供一种 18dp/pt 及以上的大字体。

1.2.4 焦点状态。鼠标，或指点，或键盘操作，或以其他方式聚焦到页面各组件时，该组件应有明显的状态提示。

1.3 听觉感知

1.3.1 语音阅读。适老化页面各组件和文本信息均应提供在线的语音阅读的适老化服务，至少要在正文页面中实现。

1.3.2 阅读控制。语音阅读服务应有开启和关闭阅读的设置，并可被辅助技术操作和控制，避免出现服务冲突。

说明：计算机网页的上述服务，应支持经过安全性和适配技术评估的第三方语音阅读技术，以及与操作系统适配好的第三方读屏软件。

1.4 非文本处理

1.4.1 非文本链接。以非文本形式的链接，应提供语音阅读其链接的目的或链接用途的适老化服务。

1.4.2 非文本控件。以非文本形式的控件或接受用户输入文本框，应提供语音阅读其目的或用途的适老化服务。

1.4.3 验证码

(1)验证码放大：如网页中存在非文本验证码，应提供相应的验证码放大服务，且验证码的放大倍数不低于 2 倍。包括字符、图形和各类拖拽形式的验证码。

(2)验证码替代：如网页中存在非文本验证码，至少提供一种视觉感官以外的验证码，如系统推送的语音验证码。

说明：以上两种形式需要同时存在。

1.4.4 验证码时效。有时效限制且不超过 3 分钟时长的验证码，应为用户提供语音告知时效的服务，并提供延长时效设置。时效延长设置时长不低于原时效的 2 倍以上。

2 可操作性

2.1 可操作性要求

在没有安全风险的条件下，适老化用户界面应开放组件访问接口，并可被语音控制或其他智能技术操作。

2.2 操作接口

2.2.1 结构数据。适老化界面组件应是层次清晰、信息完整的关系结构。

2.2.2 接口开放。无财务交易或用户信息完全风险的网页，应开放其内容的关系结构访问接口，支持语音控制等智能软件操作。

2.3 多媒体控制

多媒体播放控制。视频、音频等多媒体信息的播放控制，可通过键盘或智能手势完成。

2.4 广告插件及诱导类按键限制

2.4.1 禁止广告插件。提供适老化服务的网页或独立的适老化网站，网页中严禁出现广告内容及插件，也不能随机出现广告或临时性的广告弹窗。

2.4.2 禁止诱导类按键。提供适老化服务的网页或独立的适老化网站中无诱导下载、诱导付款等诱导式按键。

2.5 漂浮窗体控制

2.5.1 漂浮窗体时机。网页中如有漂浮窗体，尽可能在网页加载时与网页同步出现，并提供一个长期关闭的机制。

2.5.2 临时漂浮窗体。如网页需要临时出现漂浮窗体，应有一种告知方式，并提供一个长期关闭的机制。

说明：本要求是针对宣传类且无指向链接的漂浮窗要求，对面向当前用户办理业务的告知类窗体不做限制。

2.6 信息输入处理

2.6.1 错误预防。对于会导致使用者发生法律承诺或财务交易的网页，提交动作是可逆的，且提交可在 10 分钟内予以撤销，或在 10 分钟内支持修改和再次提交。

说明：该细则不包括对于商家促销且影响其他用户公平等形式的财务交易(如秒杀活动)。

2.6.2 区域辨识。网页中的各信息服务区域，任一表现形式(如纯文字、大版块等)，应设有功能、目的和内容的语音告知服务，方便老年用户理解和进行下一步操作。

3 可理解性

3.1 信息及操作表达

3.1.1 专业词语与新词语。提供适老化服务的网站栏目或服务，避免采用专业词语或网络新词语作为访问目标和结果表达。如确有必要，应在用户操作前给予必要的提示。

3.1.2 交互的统一性。经适老化设计的网页界面，其组件的操作流程应与用户的常规操作流程认知保持一致。

3.1.3 识别的一致性。提供适老化服务的网站，避免修改公认的通用名称或功能标识，如确有必要，则应提供必要的说明机制。

3.1.4 位置告知和纠错。应提供告知当前状态、位置和组件关系的机制以指导用户操作，并设有撤销上一步操作的动作。

4 兼容性

4.1 兼容性要求

适老化版本应兼容各主流操作系统和各主流浏览器、盲用读屏等各种辅助软件，以及语音识别等智能技术的访问和操作。

4.2 界面组件

4.2.1 组件样式。适老化页面的组件样式应支持主流浏览器和主流操作系统，不应因用户使用的浏览器或操作系统不同而发生变化。

4.2.2 组件服务。适老化网页的组件服务数据内容，可以按照老年人生活实际需求情况进行提供。如在适老化网页上提供“社保查询、天气查询”等组件。

5 特别性要求

5.1 口述网页结构服务。应对当前网页的信息结构、区域组成和服务功能的整体描述提供语音阅读服务。

5.2 实时读屏服务。应提供用户操作一致的语音阅读服务，并提供开启和关闭切换设置，以避免与语音识别等智能软件冲突。

5.3 完整性服务。提供适老化服务的计算机网站和移动网站，应提供直接进入适老化服务的网站快捷通道或客户端。

附件 2：

移动互联网应用 (APP)适老化通用设计规范

一、适用范围

各企业在提供适老化服务时，可根据实际情况，将适老版界面内嵌在 APP 中或开发单独的适老版 APP，并保障服务的可持续运营。本规范中所列条目，除特别说明适用范围(如适老版界面、单独的适老版 APP)外，其余条目为共性要求。

二、技术要求

1.可感知性

1.1 字型大小调整

在移动应用中，建议使用无衬线字体，应可对字型大小进行调整(随系统设置调整，或移动应用内部具备字体大小设置选项)，主要功能及主要界面的文字信息(不包含字幕、文本图像以及与移动应用功能效果相关的文本)最大字体不小于 30 dp/pt，适老版界面及单独的适老版 APP 中的主要文字信息不小于 18 dp/pt，同时兼顾移动应用适用场景和显示效果。

1.2 行间距

段落内文字的行距至少为 1.3 倍，且段落间距至少比行距大 1.3 倍，同时

兼顾移动应用适用场景和显示效果。

1.3 对比度

文本/文本图像呈现方式、图标等元素间的对比度至少为 4.5：1(字号大于 18 dp/pt 时文本及文本图像对比度至少为 3：1)。

1.4 颜色用途

文本颜色不是作为传达信息、表明动作、提示响应等区分视觉元素的唯一手段。例如，在用户输入密码错误的情景下，可使用文字或语音形式直接提示用户输入有误，避免仅使用颜色作为提示手段。

1.5 验证码

如果移动应用中存在非文本验证码(如拼图类、选图类验证方式)等老年人不易理解的验证方式，则应提供可被不同类型感官(视觉、听觉等)接受的替代表现形式，例如文字或语音形式，以适应老年人的使用需求。

2.可操作性

2.1 组件焦点大小

适老版界面中的主要组件可点击焦点区域尺寸不小于 60 × 60dp/pt，其他页面下的主要组件可点击焦点区域尺寸不小于 44 × 44dp/pt；单独的适老版 APP 中首页主要组件可点击焦点区域尺寸不小于 48 × 48dp/pt，其他页面下的主要组件可点击焦点区域尺寸不小于 44 × 44dp/pt。

2.2 手势操作

在移动应用中，应对用户进行手势导航或者操作的结果提供反馈提示；避免需 3 个或以上手指才能完成的复杂手势操作。

2.3 充足操作时间

在移动应用中，如果限时不是活动的必要部分或关键要素，且不会导致用户发生法律承诺或财务交易，则应为用户的操作留下充足时间，在用户操作完毕前界面不发生变化。

2.4 浮窗

在移动应用中，若内容产生新窗口 (包含但不限于弹窗)，应设置易于用户关闭窗口的按钮。关闭按钮只可在左上、右上、中央底部，且最小点击响应区域不能小于 44×44dp/pt dp/pt。

3.可理解性

3.1 提示机制

在用户安装移动应用时，应为适老化设置、老年人常用功能提供显著的引导提示。

内嵌适老版界面的移动应用首页需具备显著入口，支持切换至适老版，或在首次进入时给予显著切换提示，且在“设置”中提供“长辈版”入口。具备搜索功能的移动应用应将“长辈版”作为标准功能名，用户可通过搜索功能直达，同时设置“亲情版”、“关爱版”、“关怀版”等别名作为搜索关键字。

4.兼容性

4.1 辅助技术

移动应用程序不应禁止或限制终端厂商已适配好的辅助设备(如读屏软件等)的接入与使用。在辅助工具开启时，移动应用内容中所有功能性组件均能正常工作：按钮可正常访问；输入框能正常进行输入；多媒体能正常播放；在页面局部更新后，移动应用内容中新增的功能性组件也应能正常工作。

5.安全性

5.1 广告插件及诱导类按键限制

5.1.1 禁止广告插件。适老版界面、单独的适老版 APP 中严禁出现广告内容及插件，也不能随机出现广告或临时性的广告弹窗。

5.1.2 禁止诱导类按键。移动应用程序中无诱导下载、诱导付款等诱导式按键。

5.2 保障老年用户个人信息安全

移动应用程序进行个人信息处理时应遵循最小必要原则，即处理个人信息应当有明确、合理的目的，并应当限于实现处理目的的最小范围，不得进行与处理目的无关的个人信息处理，以保障老年用户个人信息安全。具体收集信息(如位置信息、图片信息等)行为，应符合《常见类型移动互联网应用程序必要个人信息范围规定》《APP 收集使用个人信息最小必要评估规范》要求。

附件 3：

互联网应用适老化及无障碍水平评测体系

根据《工业和信息化部关于印发互联网应用适老化及无障碍改造专项行动

方案的通知》（工信部信管〔2020〕200 号)要求，按照“用户体验与技术手段并重”的原则，结合相关国家标准、行业标准及适老化通用设计规范，建立本评测体系。

互联网应用适老化及无障碍水平的评测体系由用户满意度评价、技术评价和自我评价三部分构成。总分值为 100 分，60 分以上为合格，即通过评测。

评测指标	权重	评测依据
用户满意度评价	40%	组织老年人、残疾人满意度评价团，以问卷调查、上手体验、电话访谈等方式开展满意度调查，形成用户满意度评价报告。其中，网站方面重点调查老年人、残疾人等重点受益群体对网页内容可访问性、访问操作效率性的满意度；APP 方面重点调查老年人残疾人等重点受益群体使用 APP 的主观感受，包括功能的可感知性、可操作性、可理解性。
评测指标	权重	评测依据
技术评价	40%	网站方面，以 GB/T37668-2019《信息技术 互联网内容无障碍可访问性技术要求与测试方法》、YD/T1822-2008《信息无障碍 身体机能差异人群 网站无障碍评级测试方法》及《互联网网站适老化通用设计规范》为依据，通过自动化检测工具、人工检测等手段展开评测。
		APP 方面，以 GB/T37668-2019《信息技术 互联网内容无障碍可访问性技术要求与测试方法》《移动互联网应用 (APP)适老化通用设计规范》为依据，通过自动化检测工具、人工检测等手段展开评测。
自我评价	20%	参与改造的企业、单位根据专项行动要求进行自我评价，并提交评价报告。

工业和信息化部、国家互联网信息办公室、公安部关于印发网络产品安全漏洞管理规定的通知

工信部联网安〔2021〕66 号

各省、自治区、直辖市及新疆生产建设兵团工业和信息化主管部门、网信办、公安厅(局)，各省、自治区、直辖市通信管理局：

现将《网络产品安全漏洞管理规定》予以发布，自 2021 年 9 月 1 日起施行。

工业和信息化部

国家互联网信息办公室

公安部

2021 年 7 月 12 日

网络产品安全漏洞管理规定

第一条 为了规范网络产品安全漏洞发现、报告、修补和发布等行为，防范网络安全风险，根据《中华人民共和国网络安全法》，制定本规定。

第二条 中华人民共和国境内的网络产品(含硬件、软件)提供者和网络运营者，以及从事网络产品安全漏洞发现、收集、发布等活动的组织或者个人，应当遵守本规定。

第三条 国家互联网信息办公室负责统筹协调网络产品安全漏洞管理工作。工业和信息化部负责网络产品安全漏洞综合管理，承担电信和互联网行业网络产品安全漏洞监督管理。公安部负责网络产品安全漏洞监督管理，依法打击利用网络产品安全漏洞实施的违法犯罪活动。

有关主管部门加强跨部门协同配合，实现网络产品安全漏洞信息实时共享，对重大网络产品安全漏洞风险开展联合评估和处置。

第四条 任何组织或者个人不得利用网络产品安全漏洞从事危害网络安全的活动，不得非法收集、出售、发布网络产品安全漏洞信息；明知他人利用网络产品安全漏洞从事危害网络安全的活动的，不得为其提供技术支持、广告推广、支付结算等帮助。

第五条 网络产品提供者、网络运营者和网络产品安全漏洞收集平台应当建立健全网络产品安全漏洞信息接收渠道并保持畅通，留存网络产品安全漏洞信息接收日志不少于 6 个月。

第六条 鼓励相关组织和个人向网络产品提供者通报其产品存在的安全漏洞。

第七条 网络产品提供者应当履行下列网络产品安全漏洞管理义务，确保其产品安全漏洞得到及时修补和合理发布，并指导支持产品用户采取防范措施：

(一)发现或者获知所提供网络产品存在安全漏洞后，应当立即采取措施并组织对安全漏洞进行验证，评估安全漏洞的危害程度和影响范围；对属于其上游产品或者组件存在的安全漏洞，应当立即通知相关产品提供者。

(二)应当在 2 日内向工业和信息化部网络安全威胁和漏洞信息共享平台报送相关漏洞信息。报送内容应当包括存在网络产品安全漏洞的产品名称、型号、版本以及漏洞的技术特点、危害和影响范围等。

(三)应当及时组织对网络产品安全漏洞进行修补，对于需要产品用户(含下游厂商)采取软件、固件升级等措施的，应当及时将网络产品安全漏洞风险及修补方式告知可能受影响的产品用户，并提供必要的技术支持。

工业和信息化部网络安全威胁和漏洞信息共享平台同步向国家网络与信息安全信息通报中心、国家计算机网络应急技术处理协调中心通报相关漏洞信息。

鼓励网络产品提供者建立所提供网络产品安全漏洞奖励机制，对发现并通报所提供网络产品安全漏洞的组织或者个人给予奖励。

第八条 网络运营者发现或者获知其网络、信息系统及其设备存在安全漏洞后，应当立即采取措施，及时对安全漏洞进行验证并完成修补。

第九条 从事网络产品安全漏洞发现、收集的组织或者个人通过网络平台、媒体、会议、竞赛等方式向社会发布网络产品安全漏洞信息的，应当遵循必要、真实、客观以及有利于防范网络安全风险的原则，并遵守以下规定：

(一)不得在网络产品提供者提供网络产品安全漏洞修补措施之前发布漏洞信息；认为有必要提前发布的，应当与相关网络产品提供者共同评估协商，并向工业和信息化部、公安部报告，由工业和信息化部、公安部组织评估后进行发布。

(二)不得发布网络运营者在用的网络、信息系统及其设备存在安全漏洞的细节情况。

(三)不得刻意夸大网络产品安全漏洞的危害和风险，不得利用网络产品安全漏洞信息实施恶意炒作或者进行诈骗、敲诈勒索等违法犯罪活动。

(四)不得发布或者提供专门用于利用网络产品安全漏洞从事危害网络安全活动的程序和工具。

(五)在发布网络产品安全漏洞时，应当同步发布修补或者防范措施。

(六)在国家举办重大活动期间，未经公安部同意，不得擅自发布网络产品安全漏洞信息。

(七)不得将未公开的网络产品安全漏洞信息向网络产品提供者之外的境外组织或者个人提供。

(八)法律法规的其他相关规定。

第十条 任何组织或者个人设立的网络产品安全漏洞收集平台，应当向工业和信息化部备案。工业和信息化部及时向公安部、国家互联网信息办公室通报相关漏洞收集平台，并对通过备案的漏洞收集平台予以公布。

鼓励发现网络产品安全漏洞的组织或者个人向工业和信息化部网络安全威胁和漏洞信息共享平台、国家网络与信息安全信息通报中心漏洞平台、国家计算机网络应急技术处理协调中心漏洞平台、中国信息安全测评中心漏洞库报送网络产品安全漏洞信息。

第十一条 从事网络产品安全漏洞发现、收集的组织应当加强内部管理，采取措施防范网络产品安全漏洞信息泄露和违规发布。

第十二条 网络产品提供者未按本规定采取网络产品安全漏洞补救或者报告措施的，由工业和信息化部、公安部依据各自职责依法处理；构成《中华人民共和国网络安全法》第六十条规定情形的，依照该规定予以处罚。

第十三条 网络运营者未按本规定采取网络产品安全漏洞修补或者防范措施的，由有关主管部门依法处理；构成《中华人民共和国网络安全法》第五十九条规定情形的，依照该规定予以处罚。

第十四条 违反本规定收集、发布网络产品安全漏洞信息的，由工业和信息化部、公安部依据各自职责依法处理；构成《中华人民共和国网络安全法》第六十二条规定情形的，依照该规定予以处罚。

第十五条 利用网络产品安全漏洞从事危害网络安全活动，或者为他人利用网络产品安全漏洞从事危害网络安全的活动提供技术支持的，由公安机关依法处理；构成《中华人民共和国网络安全法》第六十三条规定情形的，依照该规

定予以处罚；构成犯罪的，依法追究刑事责任。

第十六条 本规定自 2021 年 9 月 1 日起施行。

工业和信息化部关于加强智能网联汽车生产企业及产品准入管理的意见

工信部通装〔2021〕103 号

各省、自治区、直辖市及新疆生产建设兵团工业和信息化主管部门，各省、自治区、直辖市通信管理局，有关汽车生产企业：

为加强智能网联汽车生产企业及产品准入管理，维护公民生命、财产安全和公共安全，促进智能网联汽车产业健康可持续发展，根据《中华人民共和国道路交通安全法》《中华人民共和国网络安全法》《中华人民共和国数据安全法》《道路机动车辆生产企业及产品准入管理办法》等规定，提出以下意见。

一、总体要求

坚持以习近平新时代中国特色社会主义思想为指导，深入贯彻党的十九大和十九届二中、三中、四中、五中全会精神，落实立足新发展阶段、贯彻新发展理念、构建新发展格局、推动高质量发展的要求，压实企业主体责任，加强汽车数据安全、网络安全、软件升级、功能安全和预期功能安全管理，保证产品质量和生产一致性，推动智能网联汽车产业高质量发展。

二、加强数据和网络安全管理

(一)强化数据安全管理能力。企业应当建立健全汽车数据安全管理制度，依法履行数据安全保护义务，明确责任部门和负责人。建立数据资产管理台账，实施数据分类分级管理，加强个人信息与重要数据保护。建设数据安全保护技术措施，确保数据持续处于有效保护和合法利用的状态，依法依规落实数据安全风险评估、数据安全事件报告等要求。在中华人民共和国境内运营中收集和产生的个人信息和重要数据应当按照有关法律法规规定在境内存储。需要向境外提供数据的，应当通过数据出境安全评估。

(二)加强网络安全保障能力。企业应当建立汽车网络安全管理制度，依法落实网络安全等级保护制度和车联网卡实名登记管理要求，明确网络安全责任部门和负责人。具备保障汽车电子电气系统、组件和功能免受网络威胁的技术措施，具备汽车网络安全风险监测、网络安全缺陷和漏洞等发现和处置技术条件，确保车辆及其功能处于被保护的状态，保障车辆安全运行。依法依规落实

网络安全事件报告和处置要求。

三、规范软件在线升级

(三)强化企业管理能力。企业生产具有在线升级(又称OTA 升级)功能的汽车产品的，应当建立与汽车产品及升级活动相适应的管理能力，具有在线升级安全影响评估、测试验证、实施过程保障、信息记录等能力，确保车辆进行在线升级时处于安全状态，并向车辆用户告知在线升级的目的、内容、所需时长、注意事项、升级结果等信息。

(四)保证产品生产一致性。企业实施在线升级活动前，应当确保汽车产品符合国家法律法规、技术标准及技术规范等相关要求并向工业和信息化部备案，涉及安全、节能、环保、防盗等技术参数变更的应提前向工业和信息化部申报，保证汽车产品生产一致性。未经审批，不得通过在线等软件升级方式新增或更新汽车自动驾驶功能。

四、加强产品管理

(五)严格履行告知义务。企业生产具有驾驶辅助和自动驾驶功能的汽车产品的，应当明确告知车辆功能及性能限制、驾驶员职责、人机交互设备指示信息、功能激活及退出方法和条件等信息。

(六)加强组合驾驶辅助功能产品安全管理。企业生产具有组合驾驶辅助功能的汽车产品的，应采取脱手检测等技术措施，保障驾驶员始终在执行相应的动态驾驶任务。组合驾驶辅助功能是指驾驶自动化系统在其设计运行条件下，持续地执行车辆横向和纵向运动控制，并具备相应的目标和事件探测与响应能力。

(七)加强自动驾驶功能产品安全管理。企业生产具有自动驾驶功能的汽车产品的，应当确保汽车产品至少满足以下要求：

1.应能自动识别自动驾驶系统失效以及是否持续满足设计运行条件，并能采取风险减缓措施以达到最小风险状态。

2.应具备人机交互功能，显示自动驾驶系统运行状态。在特定条件下需要驾驶员执行动态驾驶任务的，应具备识别驾驶员执行动态驾驶任务能力的功能。车辆应能够依法依规合理使用灯光信号、声音等方式与其他道路使用者进行交互。

3.应具有事件数据记录系统和自动驾驶数据记录系统，满足相关功能、性能和安全性要求，用于事故重建、责任判定及原因分析等。其中，自动驾驶数据记录系统记录的数据应包括车辆及系统基本信息、车辆状态及动态信息、自动驾驶系统运行信息、行车环境信息、驾乘人员操作及状态信息、故障信息等。

4.应满足功能安全、预期功能安全、网络安全等过程保障要求，以及模拟仿真、封闭场地、实际道路、网络安全、软件升级、数据记录等测试要求，避免车辆在设计运行条件内发生可预见且可预防的安全事故。

(八)确保可靠的时空信息服务。企业应当确保汽车产品具有安全、可靠的卫星定位及授时功能，可有效提供位置、速度、时间等信息，并应满足相关要求，鼓励支持接受北斗卫星导航系统信号。

五、保障措施

(九)建立自查机制。企业应当加强自查，发现生产、销售的汽车产品存在数据安全、网络安全、在线升级安全、驾驶辅助和自动驾驶安全等严重问题的，应当依法依规立即停止相关产品的生产、销售，采取措施进行整改，并及时向工业和信息化部及所在地工业和信息化、电信主管部门报告。

(十)加强监督实施。工业和信息化部指导有关机构做好智能网联汽车生产企业及产品准入技术审查等工作。各地工业和信息化、电信主管部门要与相关部门协同配合，按照《道路机动车辆生产企业及产品准入管理办法》有关要求，做好对本意见落实情况的监督检查。

(十一)夯实基础能力。工业和信息化部会同各地相关部门、有关企业进一步完善智能网联汽车标准体系建设，加快推动汽车数据安全、网络安全、在线升级、驾驶辅助、自动驾驶等标准规范制修订。鼓励第三方服务机构和企业加强相关测试验证和检验检测能力建设，不断提升智能网联汽车相关技术和网络安全、数据安全水平。

工业和信息化部

2021 年 7 月 30 日

工业和信息化部关于加强车联网网络安全和数据安全工作的通知

工信部网安〔2021〕134 号

各省、自治区、直辖市及新疆生产建设兵团工业和信息化主管部门，各省、自治区、直辖市通信管理局，中国电信集团有限公司、中国移动通信集团有限公司、中国联合网络通信集团有限公司，有关智能网联汽车生产企业、车联网服务平台运营企业，有关标准化技术组织：

车联网是新一代网络通信技术与汽车、电子、道路交通运输等领域深度融合的新兴产业形态。智能网联汽车是搭载先进的车载传感器、控制器、执行器等装置，并融合现代通信与网络技术，实现车与车、路、人、云端等智能信息交换、共享，具备复杂环境感知、智能决策、协同控制等功能，可实现“安全、高效、舒适、节能”行驶的新一代汽车。在产业快速发展的同时，车联网安全风险日益凸显，车联网安全保障体系亟须健全完善。为推进实施《新能源汽车产业发展规划(2021-2035 年)》，加强车联网网络安全和数据安全管理工作，现将有关事项通知如下：

一、网络安全和数据安全基本要求

(一)落实安全主体责任。各相关企业要建立网络安全和数据安全管理制度，明确负责人和管理机构，落实网络安全和数据安全保护责任。强化企业内部监督管理，加大资源保障力度，及时发现并解决安全隐患。加强网络安全和数据安全宣传、教育和培训。

(二)全面加强安全保护。各相关企业要采取管理和技术措施，按照车联网网络安全和数据安全相关标准要求，加强汽车、网络、平台、数据等安全保护，监测、防范、及时处置网络安全风险和威胁，确保数据处于有效保护和合法利用状态，保障车联网安全稳定运行。

二、加强智能网联汽车安全防护

(三)保障车辆网络安全。智能网联汽车生产企业要加强整车网络安全架构设计。加强车内系统通信安全保障，强化安全认证、分域隔离、访问控制等措施，防范伪装、重放、注入、拒绝服务等攻击。加强车载信息交互系统、汽车网关、电子控制单元等关键设备和部件安全防护和安全检测。加强诊断接口(OBD)、通用串行总线(USB)端口、充电端口等的访问和权限管理。

(四)落实安全漏洞管理责任。智能网联汽车生产企业要落实《网络产品安全漏洞管理规定》有关要求，明确本企业漏洞发现、验证、分析、修补、报告

等工作程序。发现或获知汽车产品存在漏洞后，应立即采取补救措施，并向工业和信息化部网络安全威胁和漏洞信息共享平台报送漏洞信息。对需要用户采取软件、固件升级等措施修补漏洞的，应当及时将漏洞风险及修补方式告知可能受影响的用户，并提供必要技术支持。

三、加强车联网网络安全防护

(五)加强车联网网络设施和网络系统安全防护能力。各相关企业要严格落实网络安全分级防护要求，加强网络设施和网络系统资产管理，合理划分网络安全域，加强访问控制管理，做好网络边界安全防护，采取防范木马病毒和网络攻击、网络侵入等危害车联网安全行为的技术措施。自行或者委托检测机构定期开展网络安全符合性评测和风险评估，及时消除风险隐患。

(六)保障车联网通信安全。各相关企业要建立车联网身份认证和安全信任机制，强化车载通信设备、路侧通信设备、服务平台等安全通信能力，采取身份认证、加密传输等必要的技术措施，防范通信信息伪造、数据篡改、重放攻击等安全风险，保障车与车、车与路、车与云、车与设备等场景通信安全。鼓励相关企业、机构接入工业和信息化部车联网安全信任根管理平台，协同推动跨车型、跨设施、跨企业互联互认互通。

(七)开展车联网安全监测预警。国家加强车联网网络安全监测平台建设，开展网络安全威胁、事件的监测预警通报和安全保障服务。各相关企业要建立网络安全监测预警机制和技术手段，对智能网联汽车、车联网服务平台及联网系统开展网络安全相关监测，及时发现网络安全事件或异常行为，并按照规定留存相关的网络日志不少于 6 个月。

(八)做好车联网安全应急处置。智能网联汽车生产企业、车联网服务平台运营企业要建立网络安全应急响应机制，制定网络安全事件应急预案，定期开展应急演练，及时处置安全威胁、网络攻击、网络侵入等网络安全风险。在发生危害网络安全的事件时，立即启动应急预案，采取相应的补救措施，并按照《公共互联网网络安全突发事件应急预案》等规定向有关主管部门报告。

(九)做好车联网网络安全防护定级备案。智能网联汽车生产企业、车联网服务平台运营企业要按照车联网网络安全防护相关标准，对所属网络设施和系统开展网络安全防护定级工作，并向所在省(区、市)通信管理局备案。对新建

网络设施和系统，应当在规划设计阶段确定网络安全防护等级。各省(区、市)通信管理局会同工业和信息化主管部门做好定级备案审核工作。

四、加强车联网服务平台安全防护

(十)加强平台网络安全管理。车联网服务平台运营企业要采取必要的安全技术措施，加强智能网联汽车、路侧设备等平台接入安全，主机、数据存储系统等平台设施安全，以及资源管理、服务访问接口等平台应用安全防护能力，防范网络侵入、数据窃取、远程控制等安全风险。涉及在线数据处理与交易处理、信息服务业务等电信业务的，应依法取得电信业务经营许可。认定为关键信息基础设施的，要落实《关键信息基础设施安全保护条例》有关规定，并按照国家有关标准使用商用密码进行保护，自行或者委托商用密码检测机构开展商用密码应用安全性评估。

(十一)加强在线升级服务(OTA)安全和漏洞检测评估。智能网联汽车生产企业要建立在线升级服务软件包安全验证机制，采用安全可信的软件。开展在线升级软件包网络安全检测，及时发现产品安全漏洞。加强在线升级服务安全校验能力，采取身份认证、加密传输等技术措施，保障传输环境和执行环境的网络安全。加强在线升级服务全过程的网络安全监测和应急响应，定期评估网络安全状况，防范软件被伪造、篡改、损毁、泄露和病毒感染等网络安全风险。

(十二)强化应用程序安全管理。智能网联汽车生产企业、车联网服务平台运营企业要建立车联网应用程序开发、上线、使用、升级等安全管理制度，提升应用程序身份鉴别、通信安全、数据保护等安全能力。加强车联网应用程序安全检测，及时处置安全风险，防范恶意应用程序攻击和传播。

五、加强数据安全保护

(十三)加强数据分类分级管理。按照“谁主管、谁负责，谁运营、谁负责”的原则，智能网联汽车生产企业、车联网服务平台运营企业要建立数据管理台账，实施数据分类分级管理，加强个人信息与重要数据保护。定期开展数据安全风险评估，强化隐患排查整改，并向所在省(区、市)通信管理局、工业和信息化主管部门报备。所在省(区、市)通信管理局、工业和信息化主管部门要对企业履行数据安全保护义务进行监督检查。

(十四)提升数据安全技术保障能力。智能网联汽车生产企业、车联网服务

平台运营企业要采取合法、正当方式收集数据，针对数据全生命周期采取有效技术保护措施，防范数据泄露、毁损、丢失、篡改、误用、滥用等风险。各相关企业要强化数据安全监测预警和应急处置能力建设，提升异常流动分析、违规跨境传输监测、安全事件追踪溯源等水平；及时处置数据安全事件，向所在省(区、市)通信管理局、工业和信息化主管部门报告较大及以上数据安全事件，并配合开展相关监督检查，提供必要技术支持。

(十五)规范数据开发利用和共享使用。智能网联汽车生产企业、车联网服务平台运营企业要合理开发利用数据资源，防范在使用自动化决策技术处理数据时，侵犯用户隐私权和知情权。明确数据共享和开发利用的安全管理和责任要求，对数据合作方数据安全保护能力进行审核评估，对数据共享使用情况进行监督管理。

(十六)强化数据出境安全管理。智能网联汽车生产企业、车联网服务平台运营企业需向境外提供在中华人民共和国境内收集和产生的重要数据的，应当依法依规进行数据出境安全评估并向所在省(区、市)通信管理局、工业和信息化主管部门报备。各省(区、市)通信管理局会同工业和信息化主管部门做好数据出境备案、安全评估等工作。

六、健全安全标准体系

(十七)加快车联网安全标准建设。加快编制车联网网络安全和数据安全标准体系建设指南。全国通信标准化技术委员会、全国汽车标准化技术委员会等要加快组织制定车联网防护定级、服务平台防护、汽车漏洞分类分级、通信交互认证、数据分类分级、事件应急响应等标准规范及相关检测评估、认证标准。鼓励各相关企业、社会团体制定高于国家标准或行业标准相关技术要求的企业标准、团体标准。

特此通知。

工业和信息化部

2021 年 9 月 15 日

工业和信息化部关于开展信息通信服务感知提升行动的通知

工信部信管函〔2021〕292 号

各省、自治区、直辖市通信管理局，中国电信集团有限公司、中国移动通

信集团有限公司、中国联合网络通信集团有限公司、中国广播电视网络集团有限公司，相关互联网企业，中国信息通信研究院：

为推动信息通信行业进一步改善服务质量，提升服务水平，工业和信息化部决定自即日起到 2022 年 3 月底，开展信息通信服务感知提升行动(简称“524”行动)。有关事项通知如下：

一、总体要求

坚持以习近平新时代中国特色社会主义思想为指导，贯彻以人民为中心的发展思想，按照党中央、国务院决策部署，聚焦影响用户感知的信息通信服务环节，推动实现服务举措“五优化”，建立个人信息保护“双清单”，实现服务能力“四提升”。到 2022 年 3 月底，信息通信行业综合服务明显改善，用户获得感、幸福感和安全感进一步提升。

二、重点任务

(一)服务举措“五优化”。

1.优化资费套餐设置展示方式。基础电信企业应在自有营业厅、掌厅、网厅、资费专区、代理渠道提供面向公众市场在售的资费套餐，以及面向老年人、残疾人的优惠资费套餐查询入口。全面梳理在售套餐名称，避免引发理解歧义。及时提醒用户套餐内流量使用情况，合理设置套餐外流量单价。(2021 年 12 月底前完成)

2.优化双千兆服务宣传方式。基础电信企业应进一步落实 5G 服务“四个提醒机制”和“四条营销红线”要求。应在宽带服务合同中明确接入上行、下行理论速率，按照承诺提供服务，确保用户接入速率达标，并采用适当方式向用户告知硬件设备、环境因素等对宽带网速的影响。(2021 年 12 月底前完成)

3.优化隐私政策和权限调用展示方式。互联网企业(首批实施的企业名单见附件)应以简洁、清晰、易懂的方式，向用户提供 APP 产品隐私政策摘要；涉及调用用户终端中相册、通讯录、位置等敏感权限的，还应当以适当方式告知用户调用该权限的目的，充分保障用户知情权。(2021 年 12 月底前完成)

4.优化 APP 开屏弹窗信息展示方式。互联网企业应在其 APP 开屏信息和弹窗信息窗口设置明显、有效的关闭按钮，按钮大小、位置、颜色应易于操作辨认，让用户“找得到，关得了”。APP 开屏信息窗口不得使用整屏图片、视频等

作为跳转链接，诱导用户点击或易造成用户误点击，给用户带来不便。(2021 年 12 月底前完成)

5.优化网盘类服务提供方式。相关企业应优化产品服务资费介绍，清晰明示存储空间、传输速率、功能权益及资费水平等内容，不得进行误导宣传。在同一网络条件下，向免费用户提供的上传和下载的最低速率应确保满足基本的下载需求。(2021 年 12 月底前完成)

(二)建立个人信息保护“双清单”。

各相关企业应建立已收集个人信息清单和与第三方共享个人信息清单(首批设立“双清单”的企业名单见附件)，并在 APP 二级菜单中展示，方便用户查询。(2021 年 12 月底前完成)

已收集个人信息清单应简洁、清晰列出 APP(包括内嵌第三方软件工具开发包 SDK)已经收集到的用户个人信息基本情况，包括信息种类、使用目的、使用场景等。

与第三方共享个人信息清单应简洁、清晰列出 APP 与第三方共享的用户个人信息基本情况，包括与第三方共享的个人信息种类、使用目的、使用场景和共享方式等。

(三)服务能力“四提升”。

1.提升跨区域通办能力。基础电信企业新增“亲情网”和“固移融合”服务跨区域通办。在同一基础电信企业网内，归属地不同的手机号码组成亲情网，实现跨省办理。实现省内跨本地网固定宽带和手机号码融合，鼓励具备能力的基础电信企业积极推动实现跨省办理。(2021 年 12 月底前完成)

2.提升携号转网服务能力。基础电信企业在履行前期对外承诺开放渠道基础上，在全国范围内新开放可办理携出服务营业厅 10000 家，并将可办理携出服务营业厅情况及时向社会公示，营业厅应合理布局，让用户少跑路。实现携入服务的网上办理和携出用户异地营业厅话费余额退还服务，鼓励具备能力的基础电信企业实现异地营业厅办理携入服务。(2021 年 12 月底前完成)

3.提升客服热线响应能力。从事互联网信息服务的企业应建立客服热线电话，并在网站、APP 等显著位置公示客服热线电话号码。鼓励具备条件的企业提供充足的人工客服坐席(首批实施的企业名单见附件)，并向老年人提供人工

直连热线服务，客服热线力争达到月均响应时限最长为 30 秒，人工服务的应答率超过 85%。（2022 年 3 月底前完成）

4.提升 APP 关键责任链个人信息保护能力。鼓励应用商店为本平台 APP 提供检测服务，及时向 APP 开发者反馈相关问题并督促改正，防止违规 APP 上架。内嵌 SDK 在非服务所必须或无合理应用场景下，不得自启动或关联启动；APP 开发者、内嵌SDK 应提供相应功能，由用户自主选择是否开启关联启动。（2021 年 12 月底前完成）

三、保障措施

（一）强化组织落实。各单位要高度重视信息通信服务质量提升工作，把维护用户合法权益放在首要位置，加强组织领导，完善管理制度，明确任务分工，夯实主体责任，采取有力措施，确保各项工作取得实效。

（二）加强监督指导。工业和信息化部建立跟踪、约谈、排名、社会公示机制，及时交流、推广典型案例和成功做法。各地通信管理局要加强监督指导，督促属地企业按时保质完成任务。中国信息通信研究院要跟踪监测各项重点任务完成情况，为监管工作提供有效支撑。

（三）推动协同共治。推进政府监管、社会监督、企业自律、用户参与的协同共治，形成服务提质与感知提升良性互动。各相关企业要以此次信息通信服务感知提升行动为契机，充分发挥主动性和创造性，创新服务模式及方法，为用户提供更周全、更贴心、更便捷的服务。

（四）建立长效机制。各相关企业要建立健全内部管理长效机制，巩固深化各项工作成效，努力满足用户需求。工业和信息化部将组织各地通信管理局适时开展“回头看”，确保信息通信服务感知提升行动落到实处、见到实效。

附件：首批设立“双清单”、提升客服热线响应能力、优化隐私政策和权限调用展示方式的互联网企业名单

工业和信息化部

2021 年 11 月 1 日

工业和信息化部办公厅关于印发车联网网络安全和数据安全标准体系建设指南的通知

工信厅科〔2022〕5 号

各省、自治区、直辖市及计划单列市工业和信息化主管部门、通信管理局，有关行业协会、标准化技术组织和专业机构：

现将《车联网网络安全和数据安全标准体系建设指南》印发给你们，请结合本行业(领域)、本地区实际，在标准化工作中贯彻执行。

附件：《车联网网络安全和数据安全标准体系建设指南》.pdf

工业和信息化部办公厅

2022 年 2 月 25 日

工业和信息化部关于印发《网络产品安全漏洞收集平台备案管理办法》的通知

工信部网安〔2022〕146 号

各省、自治区、直辖市及新疆生产建设兵团工业和信息化主管部门，各省、自治区、直辖市通信管理局，有关网络产品安全漏洞收集平台运营单位：

现将《网络产品安全漏洞收集平台备案管理办法》印发给你们，请认真遵照执行。

工业和信息化部

2022 年 10 月 25 日

网络产品安全漏洞收集平台备案管理办法

第一条 为规范网络产品安全漏洞收集平台备案管理，根据《中华人民共和国网络安全法》《中华人民共和国数据安全法》《网络产品安全漏洞管理规定》，制定本办法。

第二条 中华人民共和国境内的网络产品安全漏洞收集平台的备案管理工作，适用本办法。

本办法所称网络产品安全漏洞收集平台(以下简称漏洞收集平台)，是指相关组织或者个人设立的收集非自身网络产品安全漏洞的公共互联网平台，仅用于修补自身网络产品、网络和系统安全漏洞用途的除外。

第三条 漏洞收集平台备案通过工业和信息化部网络安全威胁和漏洞信息共享平台开展，采用网上备案方式进行。

第四条 拟设立漏洞收集平台的组织或个人，应当通过工业和信息化部网络安全威胁和漏洞信息共享平台如实填报网络产品安全漏洞收集平台备案登记信息，主要包括：

(一)漏洞收集平台的名称、首页网址和互联网信息服务(ICP)许可或备案号，用于发布漏洞信息的相关网址、社交软件公众号等互联网发布渠道；

(二)主办单位或主办个人的名称或姓名、证件号码，以及漏洞收集平台主要负责人和联系人的姓名、联系方式；

(三)漏洞收集的范围和方式、漏洞验证评估规则、通知相关责任主体修补漏洞规则、漏洞发布规则、注册用户的身份核实规则及分类分级管理规则等；

(四)通过工业和信息化部通信网络安全防护管理系统，取得的网络安全等级保护备案相关材料；

(五)依据有关国家标准和行业标准，实施平台管理等情况；

(六)有关主管部门要求提交的其他需要说明的信息。

第五条 工业和信息化部在收到漏洞收集平台提交的备案信息后，填报信息齐全、符合法定要求的，应当在 10 个工作日内予以备案，向其发放备案编号，将备案信息通报公安部和国家互联网信息办公室，并通过工业和信息化部网络安全威胁和漏洞信息共享平台向社会公布有关备案信息。

拟设立漏洞收集平台的组织或个人应对所填报信息的真实性负责，发现备案信息不真实、不完整的，工业和信息化部在 10 个工作日内通知漏洞收集平台予以补正。

完成备案的漏洞收集平台应当在其网站主页底部位置标明其备案编号。

第六条 备案信息发生变化的，应当自信息变化之日起 30 日内通过工业和信息化部网络安全威胁和漏洞信息共享平台履行备案变更手续。

第七条 不再从事漏洞收集业务的，应当在业务终止之日通过工业和信息化部网络安全威胁和漏洞信息共享平台履行备案注销手续。

第八条 漏洞收集平台应在上线前完成备案，已上线运行的漏洞收集平台应在本办法施行之日起 10 个工作日内进行备案。

第九条 工业和信息化部设立举报渠道，社会公众可通过工业和信息化部网络安全威胁和漏洞信息共享平台电话、邮箱等方式，对漏洞收集平台涉嫌违反法律法规的行为进行举报。经核查属实的，将依法依规对漏洞收集平台予以处理。

第十条 本办法自 2023 年 1 月 1 日起施行。

工业和信息化部关于印发《工业和信息化领域数据安全管理办法(试行)》的通知

工信部网安〔2022〕166 号

各省、自治区、直辖市、计划单列市及新疆生产建设兵团工业和信息化主管部门，各省、自治区、直辖市通信管理局，青海、宁夏无线电管理机构，部属各单位，部属各高校，各有关企业：

现将《工业和信息化领域数据安全管理办法(试行)》印发给你们，请认真遵照执行。

工业和信息化部

2022 年 12 月 8 日

工业和信息化领域数据安全管理办法(试行)

第一章 总 则

第一条 为了规范工业和信息化领域数据处理活动，加强数据安全管理，保障数据安全，促进数据开发利用，保护个人、组织的合法权益，维护国家安全和发展利益，根据《中华人民共和国数据安全法》《中华人民共和国网络安全法》《中华人民共和国个人信息保护法》《中华人民共和国国家安全法》《中华人民共和国民法典》等法律法规，制定本办法。

第二条 在中华人民共和国境内开展的工业和信息化领域数据处理活动及其安全监管，应当遵守相关法律、行政法规和本办法的要求。

第三条 工业和信息化领域数据包括工业数据、电信数据和无线电数据等。

工业数据是指工业各行业各领域在研发设计、生产制造、经营管理、运行维护、平台运营等过程中产生和收集的数据。

电信数据是指在电信业务经营活动中产生和收集的数据。

无线电数据是指在开展无线电业务活动中产生和收集的无线电频率、台(站)等电波参数数据。

工业和信息化领域数据处理者是指数据处理活动中自主决定处理目的、处理方式的工业企业、软件和信息技术服务企业、取得电信业务经营许可证的电信业务经营者和无线电频率、台(站)使用单位等工业和信息化领域各类主体。工业和信息化领域数据处理者按照所属行业领域可分为工业数据处理者、电信

数据处理者、无线电数据处理者等。数据处理活动包括但不限于数据收集、存储、使用、加工、传输、提供、公开等活动。

第四条 在国家数据安全工作协调机制统筹协调下，工业和信息化部负责督促指导各省、自治区、直辖市及计划单列市、新疆生产建设兵团工业和信息化主管部门，各省、自治区、直辖市通信管理局和无线电管理机构(以下统称地方行业监管部门)开展数据安全监管，对工业和信息化领域的数据处理活动和安全保护进行监督管理。

地方行业监管部门分别负责对本地区工业、电信、无线电数据处理者的数据处理活动和安全保护进行监督管理。

工业和信息化部及地方行业监管部门统称为行业监管部门。

行业监管部门按照有关法律、行政法规，依法配合有关部门开展的数据安全监管相关工作。

第五条 行业监管部门鼓励数据开发利用和数据安全技术研究，支持推广数据安全产品和服务，培育数据安全企业、研究和服务机构，发展数据安全产业，提升数据安全保障能力，促进数据的创新应用。

工业和信息化领域数据处理者研究、开发、使用数据新技术、新产品、新服务，应当有利于促进经济社会和行业发展，符合社会公德和伦理。

第六条 行业监管部门推进工业和信息化领域数据开发利用和数据安全标准体系建设，组织开展相关标准制修订及推广应用工作。

第二章 数据分类分级管理

第七条 工业和信息化部组织制定工业和信息化领域数据分类分级、重要数据和核心数据识别认定、数据分级防护等标准规范，指导开展数据分类分级管理工作，制定行业重要数据和核心数据具体目录并实施动态管理。

地方行业监管部门分别组织开展本地区工业和信息化领域数据分类分级管理及重要数据和核心数据识别工作，确定本地区重要数据和核心数据具体目录并上报工业和信息化部，目录发生变化的，应当及时上报更新。

工业和信息化领域数据处理者应当定期梳理数据，按照相关标准规范识别重要数据和核心数据并形成本单位的具体目录。

第八条 根据行业要求、特点、业务需求、数据来源和用途等因素，工业和

信息化领域数据分类类别包括但不限于研发数据、生产运行数据、管理数据、运维数据、业务服务数据等。

根据数据遭到篡改、破坏、泄露或者非法获取、非法利用，对国家安全、公共利益或者个人、组织合法权益等造成的危害程度，工业和信息化领域数据分为一般数据、重要数据和核心数据三级。

工业和信息化领域数据处理者可在此基础上细分数据的类别和级别。

第九条 危害程度符合下列条件之一的数据为一般数据：

(一)对公共利益或者个人、组织合法权益造成较小影响，社会负面影响小；

(二)受影响的用户和企业数量较少、生产生活区域范围较小、持续时间较短，对企业经营、行业发展、技术进步和产业生态等影响较小；

(三)其他未纳入重要数据、核心数据目录的数据。

第十条 危害程度符合下列条件之一的数据为重要数据：

(一)对政治、国土、军事、经济、文化、社会、科技、电磁、网络、生态、资源、核安全等构成威胁，影响海外利益、生物、太空、极地、深海、人工智能等与国家安全相关的重点领域；

(二)对工业和信息化领域发展、生产、运行和经济利益等造成严重影响；

(三)造成重大数据安全事件或生产安全事故，对公共利益或者个人、组织合法权益造成严重影响，社会负面影响大；

(四)引发的级联效应明显，影响范围涉及多个行业、区域或者行业内多个企业，或者影响持续时间长，对行业发展、技术进步和产业生态等造成严重影响；

(五)经工业和信息化部评估确定的其他重要数据。

第十一条 危害程度符合下列条件之一的数据为核心数据：

(一)对政治、国土、军事、经济、文化、社会、科技、电磁、网络、生态、资源、核安全等构成严重威胁，严重影响海外利益、生物、太空、极地、深海、人工智能等与国家安全相关的重点领域；

(二)对工业和信息化领域及其重要骨干企业、关键信息基础设施、重要资源等造成重大影响；

(三)对工业生产运营、电信网络和互联网运行服务、无线电业务开展等造成重大损害，导致大范围停工停产、大面积无线电业务中断、大规模网络与服务瘫痪、大量业务处理能力丧失等；

(四)经工业和信息化部评估确定的其他核心数据。

第十二条 工业和信息化领域数据处理者应当将本单位重要数据和核心数据目录向本地区行业监管部门备案。备案内容包括但不限于数据来源、类别、级别、规模、载体、处理目的和方式、使用范围、责任主体、对外共享、跨境传输、安全保护措施等基本情况，不包括数据内容本身。

地方行业监管部门应当在工业和信息化领域数据处理者提交备案申请的二十个工作日内完成审核工作，备案内容符合要求的，予以备案，同时将备案情况报工业和信息化部；不予备案的应当及时反馈备案申请人并说明理由。备案申请人应当在收到反馈情况后的十五个工作日内再次提交备案申请。

备案内容发生重大变化的，工业和信息化领域数据处理者应当在发生变化的三个月内履行备案变更手续。重大变化是指某类重要数据和核心数据规模(数据条目数量或者存储总量等)变化 30%以上，或者其它备案内容发生变化。

第三章 数据全生命周期安全管理

第十三条 工业和信息化领域数据处理者应当对数据处理活动负安全主体责任，对各类数据实行分级防护，不同级别数据同时被处理且难以分别采取保护措施的，应当按照其中级别最高的要求实施保护，确保数据持续处于有效保护和合法利用的状态。

(一)建立数据全生命周期安全管理制度，针对不同级别数据，制定数据收集、存储、使用、加工、传输、提供、公开等环节的具体分级防护要求和操作规程；

(二)根据需要配备数据安全管理人员，统筹负责数据处理活动的安全监督管理，协助行业监管部门开展工作；

(三)合理确定数据处理活动的操作权限，严格实施人员权限管理；

(四)根据应对数据安全事件的需要，制定应急预案，并开展应急演练；

(五)定期对从业人员开展数据安全教育和培训；

(六)法律、行政法规等规定的其他措施。

工业和信息化领域重要数据和核心数据处理者，还应当：

(一)建立覆盖本单位相关部门的数据安全工作体系，明确数据安全负责人和管理机构，建立常态化沟通与协作机制。本单位法定代表人或者主要负责人是数据安全第一责任人，领导团队中分管数据安全的成员是直接责任人；

(二)明确数据处理关键岗位和岗位职责，并要求关键岗位人员签署数据安全责任书，责任书内容包括但不限于数据安全岗位职责、义务、处罚措施、注意事项等内容；

(三)建立内部登记、审批等工作机制，对重要数据和核心数据的处理活动进行严格管理并留存记录。

第十四条 工业和信息化领域数据处理者收集数据应当遵循合法、正当的原则，不得窃取或者以其他非法方式收集数据。

数据收集过程中，应当根据数据安全级别采取相应的安全措施，加强重要数据和核心数据收集人员、设备的管理，并对收集来源、时间、类型、数量、频度、流向等进行记录。

通过间接途径获取重要数据和核心数据的，工业和信息化领域数据处理者应当与数据提供方通过签署相关协议、承诺书等方式，明确双方法律责任。

第十五条 工业和信息化领域数据处理者应当按照法律、行政法规规定和用户约定的方式、期限进行数据存储。存储重要数据和核心数据的，应当采用校验技术、密码技术等措施进行安全存储，并实施数据容灾备份和存储介质安全管理，定期开展数据恢复测试。

第十六条 工业和信息化领域数据处理者利用数据进行自动化决策的，应当保证决策的透明度和结果公平合理。使用、加工重要数据和核心数据的，还应当加强访问控制。

工业和信息化领域数据处理者提供数据处理服务，涉及经营电信业务的，应当按照相关法律、行政法规规定取得电信业务经营许可。

第十七条 工业和信息化领域数据处理者应当根据传输的数据类型、级别和应用场景，制定安全策略并采取保护措施。传输重要数据和核心数据的，应当采取校验技术、密码技术、安全传输通道或者安全传输协议等措施。

第十八条 工业和信息化领域数据处理者对外提供数据，应当明确提供的范

围、类别、条件、程序等。提供重要数据和核心数据的，应当与数据获取方签订数据安全协议，对数据获取方数据安全保护能力进行核验，采取必要的安全保护措施。

第十九条 工业和信息化领域数据处理者应当在数据公开前分析研判可能对国家安全、公共利益产生的影响，存在重大影响的不得公开。

第二十条 工业和信息化领域数据处理者应当建立数据销毁制度，明确销毁对象、规则、流程和技术等要求，对销毁活动进行记录和留存。个人、组织按照法律规定、合同约定等请求销毁的，工业和信息化领域数据处理者应当销毁相应数据。

工业和信息化领域数据处理者销毁重要数据和核心数据后，不得以任何理由、任何方式对销毁数据进行恢复，引起备案内容发生变化的，应当履行备案变更手续。

第二十一条 工业和信息化领域数据处理者在中华人民共和国境内收集和产生的重要数据和核心数据，法律、行政法规有境内存储要求的，应当在境内存储，确需向境外提供的，应当依法依规进行数据出境安全评估。

工业和信息化部根据有关法律和中华人民共和国缔结或者参加的国际条约、协定，或者按照平等互惠原则，处理外国工业、电信、无线电执法机构关于提供工业和信息化领域数据的请求。非经工业和信息化部批准，工业和信息化领域数据处理者不得向外国工业、电信、无线电执法机构提供存储于中华人民共和国境内的工业和信息化领域数据。

第二十二条 工业和信息化领域数据处理者因兼并、重组、破产等原因需要转移数据的，应当明确数据转移方案，并通过电话、短信、邮件、公告等方式通知受影响用户。涉及重要数据和核心数据备案内容发生变化的，应当履行备案变更手续。

第二十三条 工业和信息化领域数据处理者委托他人开展数据处理活动的，应当通过签订合同协议等方式，明确委托方与受托方的数据安全责任和义务。委托处理重要数据和核心数据的，应当对受托方的数据安全保护能力、资质进行核验。

除法律、行政法规等另有规定外，未经委托方同意，受托方不得将数据提

供给第三方。

第二十四条 跨主体提供、转移、委托处理核心数据的，工业和信息化领域数据处理者应当评估安全风险，采取必要的安全保护措施，并由本地区行业监管部门审查后报工业和信息化部。工业和信息化部按照有关规定进行审查。

第二十五条 工业和信息化领域数据处理者应当在数据全生命周期处理过程中，记录数据处理、权限管理、人员操作等日志。日志留存时间不少于六个月。

第四章 数据安全监测预警与应急管理

第二十六条 工业和信息化部建立数据安全风险监测机制，组织制定数据安全监测预警接口和标准，统筹建设数据安全监测预警技术手段，形成监测、预警、处置、溯源等能力，与相关部门加强信息共享。

地方行业监管部门分别建设本地区数据安全风险监测预警机制，组织开展数据安全风险监测，按照有关规定及时发布预警信息，通知本地区工业和信息化领域数据处理者及时采取应对措施。

工业和信息化领域数据处理者应当开展数据安全风险监测，及时排查安全隐患，采取必要的措施防范数据安全风险。

第二十七条 工业和信息化部建立数据安全风险信息上报和共享机制，统一汇集、分析、研判、通报数据安全风险信息，鼓励安全服务机构、行业组织、科研机构等开展数据安全风险信息上报和共享。

地方行业监管部门分别汇总分析本地区数据安全风险，及时将可能造成重大及以上安全事件的风险上报工业和信息化部。

工业和信息化领域数据处理者应当及时将可能造成较大及以上安全事件的风险向本地区行业监管部门报告。

第二十八条 工业和信息化部制定工业和信息化领域数据安全事件应急预案，组织协调重要数据和核心数据安全事件应急处置工作。

地方行业监管部门分别组织开展本地区数据安全事件应急处置工作。涉及重要数据和核心数据的安全事件，应当立即上报工业和信息化部，并及时报告事件发展和处置情况。

工业和信息化领域数据处理者在数据安全事件发生后，应当按照应急预

案，及时开展应急处置，涉及重要数据和核心数据的安全事件，第一时间向本地区行业监管部门报告，事件处置完成后在规定期限内形成总结报告，每年向本地区行业监管部门报告数据安全事件处置情况。

工业和信息化领域数据处理者对发生的可能损害用户合法权益的数据安全事件，应当及时告知用户，并提供减轻危害措施。

第二十九条 工业和信息化部委托相关行业组织建立工业和信息化领域数据安全违法行为投诉举报渠道，地方行业监管部门分别建立本地区数据安全违法行为投诉举报机制或渠道，依法接收、处理投诉举报，根据工作需要开展执法调查。鼓励工业和信息化领域数据处理者建立用户投诉处理机制。

第五章 数据安全检测、认证、评估管理

第三十条 工业和信息化部指导、鼓励具备相应资质的机构，依据相关标准开展行业数据安全检测、认证工作。

第三十一条 工业和信息化部制定行业数据安全评估管理制度，开展评估机构管理工作。制定行业数据安全评估规范，指导评估机构开展数据安全风险评估、出境安全评估等工作。

地方行业监管部门分别负责组织开展本地区数据安全评估工作。

工业和信息化领域重要数据和核心数据处理者应当自行或委托第三方评估机构，每年对其数据处理活动至少开展一次风险评估，及时整改风险问题，并向本地区行业监管部门报送风险评估报告。

第六章 监督检查

第三十二条 行业监管部门对工业和信息化领域数据处理者落实本办法要求的情况进行监督检查。

工业和信息化领域数据处理者应当对行业监管部门监督检查予以配合。

第三十三条 工业和信息化部在国家数据安全工作协调机制指导下，开展工业和信息化领域数据安全审查相关工作。

第三十四条 行业监管部门及其委托的数据安全评估机构工作人员对在履行职责中知悉的个人信息和商业秘密等，应当严格保密，不得泄露或者非法向他人提供。

第七章 法律责任

第三十五条 行业监管部门在履行数据安全监督管理职责中，发现数据处理活动存在较大安全风险的，可以按照规定权限和程序对工业和信息化领域数据处理者进行约谈，并要求采取措施进行整改，消除隐患。

第三十六条 有违反本办法规定行为的，由行业监管部门按照相关法律法规，根据情节严重程度给予没收违法所得、罚款、暂停业务、停业整顿、吊销业务许可证等行政处罚；构成犯罪的，依法追究刑事责任。

第八章 附 则

第三十七条 中央企业应当督促指导所属企业，在重要数据和核心数据目录备案、核心数据跨主体处理风险评估、风险信息上报、年度数据安全事件处置报告、重要数据和核心数据风险评估等工作中履行属地管理要求，还应当全面梳理汇总企业集团本部、所属公司的数据安全相关情况，并及时报送工业和信息化部。

第三十八条 开展涉及个人信息的数据处理活动，还应当遵守有关法律、行政法规的规定。

第三十九条 涉及军事、国家秘密信息等数据处理活动，按照国家有关规定执行。

第四十条 工业和信息化领域政务数据处理活动的具体办法，由工业和信息化部另行规定。

第四十一条 国防科技工业、烟草领域数据安全管理由国家国防科技工业局、国家烟草专卖局负责，具体制度参照本办法另行制定。

第四十二条 本办法自 2023 年 1 月 1 日起施行。

工业和信息化部 国家互联网信息办公室关于进一步规范移动智能终端应用软件预置行为的通告

工信部联信管函〔2022〕269 号

为进一步规范移动智能终端应用软件预置行为，保护用户权益，提升移动互联网应用服务供给水平，构建更加安全、更有活力的产业生态，促进移动互联网持续繁荣发展，根据《中华人民共和国网络安全法》《中华人民共和国个人信息保护法》《中华人民共和国电信条例》，现将有关事项通告如下：

一、本通告所称预置应用软件，是指由生产企业预置，在移动智能终端主

屏幕和辅助屏界面内存在用户交互入口，为满足用户应用需求而提供的、可独立使用的软件程序。

二、移动智能终端应用软件预置行为应遵循依法合规、用户至上、安全便捷、最小必要的原则，依据谁预置、谁负责的要求，落实企业主体责任，尊重并依法维护用户知情权、选择权，保障用户合法权益。

三、生产企业应确保移动智能终端中除基本功能软件外的预置应用软件均可卸载，并提供安全便捷的卸载方式供用户选择。

四、基本功能软件限于以下范围：

(一)操作系统基本组件：系统设置、文件管理；

(二)保证智能终端硬件正常运行的应用：多媒体摄录；

(三)基本通信应用：接打电话、收发短信、通讯录、浏览器；

(四)应用软件下载通道：应用商店。

实现同一基本功能的预置应用软件，至多有一个可设置为不可卸载。

五、生产企业应完善移动智能终端权限管理机制，提升操作系统安全性，采取技术和管理措施预防在产品流通环节发生置换操作系统和安装应用软件的行为。

六、生产企业应按照《移动智能终端应用软件预置和分发管理暂行规定》(工信部信管〔2016〕407 号)有关规定，保证预置应用软件安全合规，明示所提供预置应用软件的相关信息，履行登记、审核、监测、留存、下架等全链条管理责任，完善投诉受理制度等服务保障措施，及时处理用户投诉，落实个人信息保护责任。

七、工业和信息化部会同国家互联网信息办公室加强对预置应用软件的监督检查。对违反本通告的行为，依照有关法律法规规定进行处理。

八、本通告自 2023 年 1 月 1 日起执行。

特此通告。

工业和信息化部 国家互联网信息办公室

2022 年 11 月 30 日

工业和信息化部关于进一步提升移动互联网应用服务能力的通知

工信部信管函〔2023〕26 号

近年来，工业和信息化部大力推动提升移动互联网应用服务质量，切实维护用户合法权益，取得积极社会成效，但部分企业服务行为不规范、相关环节责任落实不到位等问题仍时有发生。为优化服务供给，改善用户体验，维护良好的信息消费环境，促进行业高质量发展，依据《个人信息保护法》《电信条例》《规范互联网信息服务市场秩序若干规定》《电信和互联网用户个人信息保护规定》等相关法律法规规章，现就有关事项通知如下：

一、提升全流程服务感知，保护用户合法权益

(一)规范安装卸载行为

1.确保知情同意安装。向用户推荐下载 APP 应遵循公开、透明原则，真实、准确、完整地明示开发运营者、产品功能、隐私政策、权限列表等必要信息，并同步提供明显的取消选项，经用户确认同意后方可下载安装，切实保障用户知情权、选择权。不得通过“偷梁换柱”“强制捆绑”“静默下载”等方式欺骗误导用户下载安装。

2.规范网页推荐下载行为。在用户浏览页面内容时，未经用户同意或主动选择，不得自动或强制下载 APP，或以折叠显示、主动弹窗、频繁提示等方式强迫用户下载、打开 APP，影响用户正常浏览信息。无正当理由，不得将下载 APP 与阅读网页内容相绑定。

3.实现便捷卸载。除基本功能软件外，APP 应当可便捷卸载，不得以空白名称、透明图标、后台隐藏等方式恶意阻挠用户卸载。

(二)优化服务体验

4.窗口关闭用户可选。开屏和弹窗信息窗口提供清晰有效的关闭按钮，保证用户可以便捷关闭；不得频繁弹窗干扰用户正常使用，或利用“全屏热力图”、高灵敏度“摇一摇”等易造成误触发的方式诱导用户操作。

5.服务事项提前告知。清晰明示产品功能权益及资费等内容，存在开通会员、收费等附加条件的，应当显著提示。未经明示，不得在提供产品服务过程中擅自添加限制性条件，并以此为由终止用户正常使用的产品功能和服务，或降低服务体验。

6.启动运行场景合理。在非服务所必需或无合理场景下，不得自启动和关联启动其它 APP，或进行唤醒、调用、更新等行为。

7.服务续期及时提醒。采取自动续订、自动续费方式提供服务的，应当征得用户同意，不得默认勾选、强制捆绑开通。在自动续订、自动续费前 5 日以短信、消息推送等显著方式提醒用户，服务期间提供便捷的随时退订方式和自动续订、自动续费取消途径。

(三)加强个人信息保护

8.坚持合法正当必要原则。从事个人信息处理活动，应具有明确合理的目的，不得仅以服务体验、产品研发、算法推荐、风险控制等为由，强制要求用户同意超范围或者与服务场景无关的个人信息处理行为。用户拒绝提供非当前服务所必需的个人信息时，不得影响用户使用该服务的基本功能。

9.明示个人信息处理规则。通过简洁、清晰、易懂的方式告知用户个人信息处理规则，如发生变动，应及时告知用户最新情况。突出显示敏感个人信息的处理目的、方式和范围，建立已收集个人信息清单，不得采用默认勾选、缩小文字、冗长文本等方式诱导用户同意个人信息处理规则。

10.合理申请使用权限。在对应业务功能启动时，动态申请所需权限，不得要求用户一揽子同意多个非本业务功能的必要权限。在调用终端相册、通讯录、位置等权限时，同步告知用户申请该权限的目的。未经用户同意，不得更改用户未授权权限状态。

(四)响应用户诉求

11.设立客服热线。鼓励互联网企业建立客服热线，主要互联网企业在网站、APP 显著位置公示客服热线电话号码，简化人工服务转接程序。鼓励提高客服热线响应能力，月均响应时限最长为 30 秒，人工服务应答率超过 85%。

12.妥善处理用户投诉。公布有效联系方式，接受用户投诉。按照规范要求答复互联网信息服务投诉平台上的投诉，确保 15 日内处理完成，提高投诉处理满意率。鼓励在 APP 中设置用户满意度测评链接，引导用户参与测评。

二、提升全链条管理能力，营造健康服务生态

(一)落实 APP 开发运营者主体责任

1.完善内部管理机制。明确用户服务和权益保护的牵头管理部门和负责人，建立全生命周期个人信息保护机制，健全考核问责制度，将相关法规政策要求落实到产品研发、推广和运营各环节，不断提高合规水平。定期对个人信

息保护措施及执行情况等进行合规审计，有效防范风险隐患。

2.增强技术保障能力。采取访问控制、技术加密、去标识化等安全技术措施，加强前端和后端安全防护。主动监测发现个人信息泄露、窃取、篡改、毁损、丢失、非法使用等风险威胁，及时响应处置要求。

3.加强软件开发工具(SDK)使用管理。使用SDK 前对其进行个人信息保护能力评估，通过合同等形式明确约定各方权利和义务，确保个人信息处理依法合规。集中展示并及时更新嵌入的 SDK 名称、功能及其处理个人信息的规则。共同处理用户个人信息，侵害用户权益造成损害的，依法承担相应责任。

(二)强化平台分发管理

4.严格 APP 上架审核。准确登记并核验 APP 开发运营者的真实身份和联系方式、APP 的主要功能及用途等基本信息，并对拟上架 APP 进行技术检测。相关审核应明确负责人，并留存审核日志记录，不符合要求的不予上架。全量公示在架 APP，并在显著位置标明 APP 名称及功能、开发运营者、版本号、所需获取的用户终端权限列表及用途、个人信息处理规则等信息。尚未建立分发明示界面的，应将 APP 下载链接到应用商店，引导用户从正规渠道下载所分发的 APP。

5.强化在架 APP 巡查。加强对 APP 的动态巡查，确保公示信息真实准确。对与公示信息不一致，或采用“热更新、热切换”等方式擅自更改 APP 主要功能、申请的权限、个人信息收集使用的场景和范围等违规 APP，应当停止提供服务。

6.完善分发管理机制。建立 APP 开发运营者信用评价、风险提示等机制，鼓励对分发 APP 进行电子签名认证，实现上架应用、分发行为全流程可溯源。加强与面向移动互联网应用程序的检测及认证公共服务平台联动，做好信息上报、监测溯源、信息共享、响应处置工作。

(三)规范SDK 应用服务

7.建立信息公示机制。公开明示 SDK 名称、开发者、版本号、主要功能、使用说明等基本信息，以及个人信息处理规则。SDK 独立采集、传输、存储个人信息的，应当单独作出说明。鼓励发挥 SDK 管理服务平台作用，引导 APP 开发运营者使用合规的 SDK。

8.优化功能配置。遵循最小必要原则，根据不同应用场景或用途，明确SDK 功能和对应的个人信息收集范围，并向APP 开发运营者提供功能模块及个人信息收集的配置选项，不得一揽子过度收集个人信息。

9.加强服务协同。在产品使用全生命周期过程中，通过明确易懂的方式主动向 APP 开发运营者提供合规使用指南，引导 APP 开发运营者正确合理使用，共同提高合规水平。当个人信息处理规则变更或发现风险时，及时更新并告知APP 开发运营者。

(四)筑牢终端安全防线

10.强化 APP 运行管理。为用户提供 APP 自启动和关联启动的关闭功能，以及便捷的相关设备识别码重置选项，加强对 APP 静默下载、热更新的监测，防范未经用户同意私自启动、下载、安装等行为。

11.加强 APP 行为记录提醒。增强对权限调用行为的记录能力，为用户查询权限调用情况提供便利。建立通讯录、麦克风、相机、位置、剪切板等权限在用状态的明显提示机制，保障用户及时准确了解个人信息收集状态。

12.提高 APP 风险预警能力。推动开展 APP 电子签名认证，并向用户进行预警提示，提高对仿冒、不良、违规等风险 APP 的识别能力。

(五)夯实接入企业责任

13.准确登记信息。在为 APP、SDK 提供网络接入服务时，登记并核验APP、SDK 开发运营者的真实身份、联系方式等信息，提高溯源能力。

14.确保有效处置。按照电信监管部门要求，依法对违规 APP、SDK 采取停止接入等必要措施，有效阻止其侵害用户权益的违规行为。

三、工作要求

(一)抓好组织落实。各单位要坚持以人民为中心的发展思想，提高政治站位，强化责任担当，细化分解任务，认真抓好本通知的贯彻实施，确保取得实效。相关企业要落实主体责任，对照本通知要求开展自查自纠，切实维护用户合法权益。同时，健全长效机制，创新模式方法，不断提升移动互联网应用服务水平，不断增强用户的获得感、幸福感、安全感。

(二)加强指导监督。工业和信息化部健全完善测评、通报、排名、公示机制，推动工作扎实有序开展，及时总结、推广优秀案例和经验做法。各地通信

管理局要加强监督检查，指导督促属地企业落实本通知各项要求。对落实不到位或出现违规行为的，依法采取责令限期整改、向社会公告、组织下架等措施，严肃问责查处。

(三)强化技术运用。 中国信息通信研究院要组织产业力量，综合运用人工智能、大数据等新技术新手段，升级打造面向移动互联网应用程序的全国检测及认证公共服务平台，持续完善平台功能，做好技术检测、监测服务和监管支撑工作。积极推广应用电子签名认证等可溯源技术手段，促进提高服务管理能力。

(四)推动行业自律。鼓励行业协会及相关机构制定行业自律公约、技术标准、服务规范，加强评估认证和人才培养。进一步畅通渠道倾听群众意见，促进各方交流互动，引导企业依法合规经营，不断优化改进服务，营造争先创优、互促共进的良好环境，以高质量服务促进高质量发展。

工业和信息化部

2023 年 2 月 6 日

工业和信息化部 国家金融监督管理总局关于促进网络安全保险规范健康发展的意见

工信部联网安〔2023〕95 号

各省、自治区、直辖市及计划单列市、新疆生产建设兵团工业和信息化主管部门，各银保监局，各相关单位：

网络安全保险是为网络安全风险提供保险保障的新兴险种，日益成为转移、防范网络安全风险的重要工具，在推进网络安全社会化服务体系建设中发挥着重要作用。为深入贯彻《中华人民共和国网络安全法》《中华人民共和国数据安全法》等相关法律法规，加快推动网络安全产业和金融服务融合创新，引导网络安全保险健康有序发展，培育网络安全保险新业态，促进企业加强网络安全风险管理，推动网络安全产业高质量发展，现提出如下意见。

一、建立健全网络安全保险政策标准体系

(一)完善网络安全保险政策制度。加强网络安全产业政策对网络安全保险的支持，推动网络安全技术服务赋能网络安全保险发展，引导关键信息基础设施保护、新兴融合领域网络安全保障等充分运用网络安全保险。加强保险业政

策对网络安全保险的支持，指导网络安全保险创新发展，引导开发符合网络安全特点规律的保险产品。推动健全完善财政政策，充分利用地方首台(套)、首版(次)等现有政策，提供保险减税、保险购买补贴等措施。

(二)健全网络安全保险标准规范。支持网络安全产业和保险业加强合作，建立覆盖网络安全保险服务全生命周期的标准体系，统一行业术语规范，明确核保、承保、理赔等主要环节基本流程和通用要求。研究制定承保前重点行业领域网络安全风险量化评估相关标准，规范安全风险评估要求；承保中网络安全监测管理服务相关标准，规范监测预警方法；承保后理赔服务实施要求相关标准，规范网络安全保险售后服务。

二、加强网络安全保险产品服务创新

(三)丰富网络安全保险产品。鼓励保险公司面向不同行业场景的差异化网络安全风险管理需求，开发多元化网络安全保险产品。面向重点行业企业开发网络安全财产损失险、责任险和综合险等，提升企业网络安全风险应对能力。面向信息技术产品开发产品责任险，面向网络安全产品开发网络安全专门保险，为信息网络技术产品提供保险保障。面向网络安全服务开发职业责任险等产品，转移专业技术人员在安全服务过程中因人为操作可能引发的安全风险。

(四)创新发展网络安全保险服务。鼓励网络安全保险服务机构协同合作，探索构建以网络安全保险为核心的全流程网络安全风险管理解决方案。充分发挥保险机构专业优势，联合网络安全企业、基础电信运营商等加快网络安全保险与网络安全服务融合创新。充分发挥网络安全企业、专业网络安全测评机构技术优势，联合保险公司提升网络安全保险服务能力。

三、强化网络安全技术赋能保险发展

(五)开展网络安全风险量化评估。围绕电信和互联网行业典型事件以及工业互联网、车联网、物联网等新兴场景开展网络安全风险研究。探索建立网络安全风险量化评估模型，加强网络安全风险影响规模预测、经济损失等分析。支持网络安全企业、专业网络安全测评机构等研发网络安全风险量化评估技术，开发轻量化网络安全风险量化评估工具，鼓励保险机构建立网络安全风险理赔数据库，支撑网络安全风险精准定价。

(六)加强网络安全风险监测能力。开展网络安全保险全生命周期风险监

测，覆盖事前、事中、事后等重要环节。鼓励网络安全企业、专业网络安全测评机构等充分发挥网络安全风险监测技术优势，充分利用安全技术手段，针对网络安全漏洞、恶意网络资源、网络安全事件等开展网络安全威胁实时监测，及时发现网络安全风险隐患，提升网络安全风险监测预警、应急处置等能力。

四、促进网络安全产业需求释放

(七)推广网络安全保险服务应用。面向电信和互联网、能源、金融、医疗卫生等重点行业，以及工业互联网、车联网、物联网等新兴融合领域，围绕网络安全与信息技术产品服务供给侧和需求侧两类主体，充分发挥网络安全产业、网络安全保险相关联盟协会等作用，开展网络安全保险服务试点，形成可复制、可推广的网络安全保险服务模式，促进网络安全保险推广应用。

(八)推动企业网络安全风险应对能力提升。鼓励重点行业企业完善网络安全风险管理机制，推动电信和互联网、制造业、能源、金融、交通、水利、教育等重点行业企业积极利用网络安全保险工具，有效转移、防范网络安全风险，提升网络基础设施、重要信息系统和数据的安全防护能力。支持中小企业通过网络安全保险服务监控风险敞口，建立健全网络安全风险管理体系，不断加强中小企业网络安全防护能力。

五、培育网络安全保险发展生态

(九)培育优质网络安全保险企业。鼓励网络安全企业、保险机构积极参与网络安全保险生态建设，开展网络安全保险优秀案例征集、网络安全保险应用示范等活动，培育一批专业能力突出的保险机构，发展一批技术支撑能力领先的网络安全企业、专业网络安全测评机构等，建设一批网络安全保险创新联合体，培育网络安全保险发展良性生态。

(十)宣传推广网络安全保险服务。充分发挥相关行业联盟协会、重点企业带动作用，整合资源优势，促进网络安全产业和金融服务要素流动，开展网络安全保险教育培训，引导加强从业人员自律，规范网络安全保险推广应用。用好网络和数据安全产业高峰论坛、网络安全技术应用试点示范等活动，宣传普及网络安全保险，举办网络安全保险主题活动，加强经验总结和交流推广，营造促进网络安全保险规范健康发展的浓厚氛围。

工业和信息化部

国家金融监督管理总局

2023 年 7 月 2 日

工业和信息化部关于开展移动互联网应用程序备案工作的通知

工信部信管〔2023〕105 号

各省、自治区、直辖市通信管理局，中国信息通信研究院、中国互联网协会，基础电信企业，公益性互联单位、互联网接入服务提供者、互联网数据中心服务提供者、内容分发网络服务提供者，移动互联网应用程序分发平台(含小程序、快应用等分发)、智能终端生产企业、互联网信息服务提供者：

为落实《中华人民共和国反电信网络诈骗法》《互联网信息服务管理办法》(国务院令第 292 号)等法律法规要求，促进互联网行业规范健康发展，进一步做好移动互联网信息服务管理，现组织开展移动互联网应用程序(以下简称 APP)备案工作。有关事项通知如下：

一、总体要求

以习近平新时代中国特色社会主义思想为指导，深入学习贯彻习近平总书记关于网络强国的重要思想、习近平总书记关于打击治理电信网络诈骗犯罪工作的重要指示批示精神，坚持依法行政、公开透明、便民高效原则，维护网络安全和公共利益，保护公民和组织合法权益，促进互联网行业规范健康发展。

二、工作内容

(一)在中华人民共和国境内从事互联网信息服务的 APP 主办者，应当依照《中华人民共和国反电信网络诈骗法》《互联网信息服务管理办法》(国务院令第 292 号)等规定履行备案手续，未履行备案手续的，不得从事 APP 互联网信息服务。

(二)工业和信息化部对全国 APP 备案工作进行监督指导，省、自治区、直辖市通信管理局负责实施监督 APP 备案管理工作。

(三)APP 主办者使用的域名、IP 地址等网络资源应当符合《互联网域名管理办法》(工业和信息化部令第 43 号)《互联网 IP 地址备案管理办法》(原信息产业部令第 34 号)《工业和信息化部关于规范互联网信息服务使用域名的通知》(工信部信管〔2017〕264 号)等管理要求。

(四)APP 主办者应当如实填报《互联网信息服务备案登记表》(以下简称

《备案登记表》)以及有关承诺书。

从事新闻、出版、教育、影视、宗教等 APP 互联网信息服务的主办者，在履行备案手续时，还应向其住所所在地省级通信管理局提交相关主管部门审核同意的文件。

电信主管部门可根据实际情况，对《备案登记表》和有关承诺书内容进行调整。

(五)APP 主办者应当向其住所所在地省级通信管理局履行备案手续，由其网络接入服务提供者、APP 分发平台(以下简称分发平台)通过“国家互联网基础资源管理系统”(即 ICP/IP 地址/域名信息备案管理系统，以下简称备案系统)，采取网上提交申请、查验审核方式进行。

(六)网络接入服务提供者、分发平台应对拟从事 APP 互联网信息服务组织或个人的用户真实身份、网络资源等信息进行查验，不得在明知或应知信息不准确情况下，为其代为履行备案手续。

(七)省级通信管理局在收到 APP 主办者提交的备案材料后，材料齐全并准确的，应在二十个工作日内予以备案，向其发放备案编号，并通过备案系统向社会公布备案信息；材料不齐全或不准确的，不予备案，并说明理由。

(八)APP 主办者应当在 APP 显著位置标明其备案编号，并在备案编号下方按要求链接备案系统网址，供公众查询核对。分发平台应在显著位置标明其分发的 APP 备案编号信息，并向电信主管部门报送分发的 APP 有关信息。

APP 信息发生变更、注销等情况，APP 主办者应当向原备案机关履行变更、注销等手续。

(九)网络接入服务提供者、分发平台、智能终端生产企业不得为未履行备案手续的 APP 提供网络接入、分发、预置等服务。

(十)APP 主办者、网络接入服务提供者、分发平台、智能终端生产企业应当建立健全违法违规信息监测和处置机制，发现法律、行政法规禁止发布或者传输的信息，应当立即停止传输该信息，采取消除等处置措施，防止信息扩散，保存有关记录，并向电信主管部门报告，依据电信主管部门要求进行处置。

三、工作安排

(一)工作准备阶段(2023 年 8 月底前)。各省、自治区、直辖市通信管理局组织辖区内 APP 主办者、网络接入服务提供者、分发平台等明确管理要求，制定实施计划，确保有关工作稳步推进。网络接入服务提供者、分发平台应按照要求，建设和升级企业侧备案系统，完成与部侧备案系统对接测试，具备对 APP 信息报备和核验等功能。

(二)存量 APP 备案阶段(2023 年 9 月-2024 年 3 月)。在本通知发布前已开展业务的 APP 应按照本通知要求，通过其网络接入服务提供者、分发平台向其住所所在地省级通信管理局履行备案手续。其中，对于已履行网站备案手续的，仅需补充完善其 APP 有关信息，无需重复填报主办者真实身份信息。对于没有网站备案信息的，按照本通知规定履行备案手续。

在本通知发布后拟开展业务的 APP，应按照本通知要求先履行备案手续后再开展业务。

(三)监督检查阶段(2024 年 4 月-2024 年 6 月)。工业和信息化部组织开展 APP 备案检查工作，各省、自治区、直辖市通信管理局及时督促有关单位填报、补充、更新 APP 备案信息，对网络接入服务提供者、分发平台、智能终端生产企业接入、分发、预置的 APP 开展检查。对未履行备案程序、从事违法违规活动的 APP，各省、自治区、直辖市通信管理局应按照相关法律法规规定处理。

(四)常态化工作阶段(2024 年 7 月至长期)。各省、自治区、直辖市通信管理局定期组织网络接入服务提供者、分发平台、智能终端生产企业开展 APP 备案信息准确性考核工作，采取有效技术措施加强 APP 合规管理，提升移动互联网监管水平。

四、工作要求

(一)提高政治站位，加强组织领导。各单位要充分认识 APP 备案工作对于强化互联网基础管理、促进互联网行业规范健康发展、深化防范治理电信网络诈骗工作成效、维护网络与信息安全的重要意义，按照工作部署，强化主体责任落实，确保各项工作按时保质完成。

(二)压实主体责任，严格工作落实。各通信管理局要加强对企业的督导检查，及时发现问题隐患和薄弱环节。网络接入服务提供者、分发平台、智能终

端生产企业要强化工作落实和责任考核，及时处理工作中遇到的问题，并向电信主管部门报告。

(三)强化技术保障，提供有力支撑。中国信息通信研究院、中国互联网协会要做好备案系统建设运维工作，强化 APP 备案数据共享和分析能力，积极配合电信主管部门做好 APP 备案管理工作的问题解答、宣传引导等工作，有效支撑 APP 各项监管工作。

附件：互联网信息服务备案登记表.wps

工业和信息化部

2023 年 7 月 21 日

工业和信息化部 国家标准化管理委员会关于印发《工业领域数据安全标准体系建设指南(2023 版)》的通知

工信部联科〔2023〕250 号

各省、自治区、直辖市及计划单列市、新疆生产建设兵团工业和信息化主管部门、通信管理局、市场监管局(厅、委)，有关行业协会、中央企业、标准化技术组织、标准化专业机构：

为切实发挥标准对推动工业领域数据安全的技术引领和规范指导，工业和信息化部、国家标准化管理委员会依据《中华人民共和国数据安全法》《工业和信息化领域数据安全管理办法(试行)》等法律法规和政策文件要求，组织编制了《工业领域数据安全标准体系建设指南(2023 版)》。现印发给你们，请结合本地区、本行业、本领域实际，在标准化工作中贯彻执行。

附件：《工业领域数据安全标准体系建设指南(2023 版)》

工业和信息化部

国家标准化管理委员会

2023 年 12 月 19 日

工业和信息化部关于印发《工业和信息化领域数据安全风险评估实施细则(试行)》的通知

工信部网安〔2024〕82 号

各省、自治区、直辖市、计划单列市及新疆生产建设兵团工业和信息化主管部

门，各省、自治区、直辖市通信管理局，青海、宁夏无线电管理机构，部属各单位，部属各高校，各有关企业：

现将《工业和信息化领域数据安全风险评估实施细则(试行)》印发给你们，请认真遵照执行。

工业和信息化部

2024 年 5 月 10 日

工业和信息化领域数据安全风险评估实施细则(试行)

第一条 根据《中华人民共和国数据安全法》《中华人民共和国网络安全法》等法律，按照《工业和信息化领域数据安全管理办法(试行)》有关要求，为引导工业和信息化领域数据处理者规范开展数据安全风险评估工作，提升数据安全管理水平，维护国家安全和发展利益，制定本细则。

第二条 本细则适用于对中华人民共和国境内工业和信息化领域重要数据和核心数据处理者数据处理活动开展的数据安全风险评估。

第三条 工业和信息化部统一管理、监督和指导工业和信息化领域数据安全风险评估工作，组织开展相关评估标准制修订及推广应用。

各省、自治区、直辖市及计划单列市、新疆生产建设兵团工业和信息化主管部门，各省、自治区、直辖市通信管理局和无线电管理机构(以下统称地方行业监管部门)依据职责分别负责监督管理本地区工业、电信、无线电重要数据和核心数据处理者开展数据安全风险评估工作。

工业和信息化部及地方行业监管部门统称为行业监管部门。

第四条 重要数据和核心数据处理者按照及时、客观、有效的原则开展数据安全风险评估，形成真实、完整、准确的评估报告，并对评估结果负责。

第五条 重要数据和核心数据处理者按照国家法律法规、行业监管部门有关规定以及评估标准，对数据处理活动的目的和方式、业务场景、安全保障措施、风险影响等要素，开展数据安全风险评估，重点评估以下内容：

(一)数据处理目的、方式、范围是否合法、正当、必要；

(二)数据安全管理制度、流程策略的制定和落实情况；

(三)数据安全组织架构、岗位配备和职责履行情况；

(四)数据安全技术防护能力建设及应用情况；

(五)数据处理活动相关人员是否熟悉数据安全相关政策法规、是否具备数据安全知识技能、是否接受数据安全相关教育培训等情况;

(六)发生数据遭到篡改、破坏、泄露、丢失或者被非法获取、非法利用等安全事件,对国家安全、公共利益的影响范围、程度等风险;

(七)涉及数据提供、委托处理、转移的,数据获取方或受托方的安全保障能力、责任义务约束和履行情况;

(八)涉及国家法律法规中规定需要申报的数据出境安全评估情形,履行数据出境安全评估要求情况。

第六条 重要数据和核心数据处理者每年至少开展一次数据安全风险评估,评估结果有效期为一年,以评估报告首次出具日期计算。评估报告应当包括数据处理者基本情况、评估团队基本情况、重要数据的种类和数量、开展数据处理活动的情况、数据安全风险评估环境,以及数据处理活动分析、合规性评估、安全风险分析、评估结论及应对措施等。

在有效期内出现以下情形之一的,重要数据和核心数据处理者应当及时对发生变化及其影响的部分开展风险评估:

(一)新增跨主体提供、委托处理、转移核心数据的;

(二)重要数据、核心数据安全状态发生变化对数据安全造成不利影响的,包括但不限于数据处理目的、方式、适用范围和安全制度策略等发生重大调整的;

(三)发生涉及重要数据、核心数据的安全事件的;

(四)重要数据和核心数据目录备案内容发生重大变化的;

(五)行业监管部门要求进行评估的其他情形。

第七条 重要数据和核心数据处理者可以自行或者委托具有工业和信息化数据安全工作能力的第三方评估机构开展评估。评估过程应当建立至少包括组织管理、业务运营、技术保障、安全合规等人员的专业化评估团队,制定完备的评估工作方案,配备有效的技术评测工具。

第八条 重要数据和核心数据处理者委托第三方评估机构开展数据安全风险评估的,可以通过订立合同或者其他具有法律效力的文件,明确双方的权利和责任,向第三方评估机构提供必需的材料和条件,确保相关材料的真实性和完

整性，并确认评估结果。

第九条 重要数据和核心数据处理者对评估中发现的数据安全风险隐患，应当及时采取适当措施消除或降低风险隐患。

第十条 重要数据和核心数据处理者应当在评估工作完成后的 10 个工作日内，向本地区行业监管部门报送评估报告。

中央企业督促指导所属企业履行属地数据安全风险评估及评估报告报送要求，并将梳理汇总的企业集团本部、所属公司的评估报告报送工业和信息化部。

地方行业监管部门将本地区本领域重要数据和核心数据处理者的评估结果报送工业和信息化部。

第十一条 地方行业监管部门发现不符合法律法规和有关规定的，应当及时通知重要数据和核心数据处理者依法予以改正。地方行业监管部门于 12 月 25 日前，将本地区本年度评估报告接收和审核情况报送工业和信息化部。工业和信息化部视情对评估报告组织抽查审核。

涉及跨主体提供、转移、委托处理核心数据的，地方行业监管部门应当在数据处理者提交评估报告的 20 个工作日内完成审查，并报工业和信息化部按照国家有关规定进行复核。

第十二条 鼓励熟悉工业和信息化领域数据安全工作，满足资质要求的认证机构开展第三方评估机构的能力认证。

相关认证机构配备相应的人员和技术保障能力，建立第三方评估机构能力认证制度，明确第三方评估机构在管理体系、人员能力、工具设施、评估领域等方面的规范要求，跟踪管理第三方评估机构的服务质量，督促第三方评估机构独立、公正、客观、科学地开展数据安全风险评估工作。

第十三条 第三方评估机构应当履行下列义务：

(一)对评估工作中知悉的国家秘密、重要数据和核心数据的目录与内容、商业秘密、个人隐私，以及与数据处理者签署的保密协议中约定的保密信息等严格保密；

(二)严格按照国家法律法规、行业监管部门有关规定以及评估标准，公正、独立地开展评估并出具评估报告，全面、准确、客观地反映重要数据和核

心数据处理者的数据安全风险状况，提供务实有效的风险整改建议措施；

(三)除重要数据和核心数据处理者书面同意或者法律、行政法规另有规定外，不得向其他组织或个人提供评估中收集掌握的相关信息。

第十四条 工业和信息化部根据技术能力、人员配备、信誉资质等情况，择优遴选通过能力认证的第三方评估机构，建立工业和信息化领域数据安全风险评估支撑机构库。地方行业监管部门可以参照建立本地区数据安全风险评估支撑机构库。

行业监管部门根据工作需要，可以自行或组织数据安全风险评估支撑机构库中的机构，对重要数据和核心数据处理者的数据处理活动开展专项风险评估，或对重要数据和核心数据处理者的风险评估工作落实情况进行监督检查。

重要数据和核心数据处理者对行业监管部门发起的专项风险评估及监督检查应当予以配合，并对评估发现的相关问题及时进行改正。

第十五条 行业监管部门对于违反国家认证认可相关规定的认证机构，将相关线索移交市场监督管理部门处理。

行业监管部门对第三方评估机构的评估活动进行监督

管理，对违反法律法规、未按行业规定和标准开展评估活动、未履行保密义务的第三方评估机构，视情按照规定权限和程序进行约谈、通报，认证机构应根据通报信息，对不符合认证要求的第三方评估机构依法暂停直至撤销其相应认证证书。

第十六条 有违反本实施细则行为的，由行业监管部门按照相关法律法规，根据情节严重程度给予行政处罚；构成犯罪的，依法追究刑事责任。

第十七条 行业监管部门及委托支撑机构的工作人员对在履行职责中知悉的国家秘密、商业秘密、个人信息、评估工作信息等，负有保密义务。

第十八条 对一般数据处理者数据处理活动开展的数据安全风险评估可参照本细则实施。涉及军事、国家秘密信息等数据处理活动，按照国家有关规定执行。

第十九条 本细则自 2024 年 6 月 1 日起施行。

第四章 国家互联网信息办公室

国务院关于授权国家互联网信息办公室负责互联网信息内容管理工作的通知

国发〔2014〕33 号

各省、自治区、直辖市人民政府，国务院各部委、各直属机构：

为促进互联网信息服务健康有序发展，保护公民、法人和其他组织的合法权益，维护国家安全和公共利益，授权重新组建的国家互联网信息办公室负责全国互联网信息内容管理工作，并负责监督管理执法。

国 务 院

2014 年 8 月 26 日

互联网政务应用安全管理规定

(2024 年 2 月 19 日中央网络安全和信息化委员会办公室、中央机构编制委员会办公室、工业和信息化部、公安部制定 2024 年 5 月 15 日发布)

第一章 总 则

第一条 为保障互联网政务应用安全，根据《中华人民共和国网络安全法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》《党委(党组)网络安全工作责任制实施办法》等，制定本规定。

第二条 各级党政机关和事业单位(简称机关事业单位)建设运行互联网政务应用，应当遵守本规定。

本规定所称互联网政务应用，是指机关事业单位在互联网上设立的门户网站，通过互联网提供公共服务的移动应用程序(含小程序)、公众账号等，以及互联网电子邮件系统。

第三条 建设运行互联网政务应用应当依照有关法律、行政法规的规定以及国家标准的强制性要求，落实网络安全与互联网政务应用“同步规划、同步建设、同步使用”原则，采取技术措施和其他必要措施，防范内容篡改、攻击致瘫、数据窃取等风险，保障互联网政务应用安全稳定运行和数据安全。

第二章 开办和建设

第四条 机关事业单位开办网站应当按程序完成开办审核和备案工作。一个党政机关最多开设一个门户网站。

中央机构编制管理部门、国务院电信部门、国务院公安部门加强数据共享，优化工作流程，减少填报材料，缩短开办周期。

机关事业单位开办网站，应当将运维和安全保障经费纳入预算。

第五条 一个党政机关网站原则上只注册一个中文域名和一个英文域名，域名应当以“.gov.cn”或“.政务”为后缀。非党政机关网站不得注册使用“.gov.cn”或“.政务”的域名。

事业单位网站的域名应当以“.cn”或“.公益”为后缀。

机关事业单位不得将已注册的网站域名擅自转让给其他单位或个人使用。

第六条 机关事业单位移动应用程序应当在已备案的应用程序分发平台或机关事业单位网站分发。

第七条 机构编制管理部门为机关事业单位制发专属电子证书或纸质证书。机关事业单位通过应用程序分发平台分发移动应用程序，应当向平台运营者提供电子证书或纸质证书用于身份核验；开办微博、公众号、视频号、直播号等公众账号，应当向平台运营者提供电子证书或纸质证书用于身份核验。

第八条 互联网政务应用的名称优先使用实体机构名称、规范简称，使用其他名称的，原则上采取区域名加职责名的命名方式，并在显著位置标明实体机构名称。具体命名规范由中央机构编制管理部门制定。

第九条 中央机构编制管理部门为机关事业单位设置专属网上标识，非机关事业单位不得使用。

机关事业单位网站应当在首页底部中间位置加注网上标识。中央网络安全和信息化委员会办公室会同中央机构编制管理部门协调应用程序分发平台以及公众账号信息服务平台，在移动应用程序下载页面、公众账号显著位置加注网上标识。

第十条 各地区、各部门应当对本地区、本部门党政机关网站建设进行整体规划，推进集约化建设。

县级党政机关各部门以及乡镇党政机关原则上不单独建设网站，可利用上级党政机关网站平台开设网页、栏目、发布信息。

第十一条 互联网政务应用应当支持开放标准，充分考虑对用户端的兼容性，不得要求用户使用特定浏览器、办公软件等用户端软硬件系统访问。

机关事业单位通过互联网提供公共服务，不得绑定单一互联网平台，不得将用户下载安装、注册使用特定互联网平台作为获取服务的前提条件。

第十二条 互联网政务应用因机构调整等原因需变更开办主体的，应当及时

变更域名或注册备案信息。不再使用的，应当及时关闭服务，完成数据归档和删除，注销域名和注册备案信息。

第三章 信息安全

第十三条 机关事业单位通过互联网政务应用发布信息，应当健全信息发布审核制度，明确审核程序，指定机构和在编人员负责审核工作，建立审核记录档案；应当确保发布信息内容的权威性、真实性、准确性、及时性和严肃性，严禁发布违法和不良信息。

第十四条 机关事业单位通过互联网政务应用转载信息，应当与政务等履行职能的活动相关，并评估内容的真实性和客观性。转载页面上要准确清晰标注转载来源网站、转载时间、转载链接等，充分考虑图片、内容等知识产权保护问题。

第十五条 机关事业单位发布信息内容需要链接非互联网政务应用的，应当确认链接的资源与政务等履行职能的活动相关，或属于便民服务的范围；应当定期检查链接的有效性和适用性，及时处置异常链接。党政机关门户网站应当采取技术措施，做到在用户点击链接跳转到非党政机关网站时，予以明确提示。

第十六条 机关事业单位应当采取安全保密防控措施，严禁发布国家秘密、工作秘密，防范互联网政务应用数据汇聚、关联引发的泄密风险。应当加强对互联网政务应用存储、处理、传输工作秘密的保密管理。

第四章 网络和数据安全

第十七条 建设互联网政务应用应当落实网络安全等级保护制度和国家密码应用管理要求，按照有关标准规范开展定级备案、等级测评工作，落实安全建设整改加固措施，防范网络和数据安全风险。

中央和国家机关、地市级以上地方党政机关门户网站，以及承载重要业务应用的机关事业单位网站、互联网电子邮件系统等，应当符合网络安全等级保护第三级安全保护要求。

第十八条 机关事业单位应当自行或者委托具有相应资质的第三方网络安全服务机构，对互联网政务应用网络和数据安全每年至少进行一次安全检测评估。

互联网政务应用系统升级、新增功能以及引入新技术新应用，应当在上线前进行安全检测评估。

第十九条 互联网政务应用应当设置访问控制策略。对于面向机关事业单位工作人员使用的功能和互联网电子邮箱系统，应当对接入的 IP 地址段或设备实施访问限制，确需境外访问的，按照白名单方式开通特定时段、特定设备或账号的访问权限。

第二十条 机关事业单位应当留存互联网政务应用相关的防火墙、主机等设备的运行日志，以及应用系统的访问日志、数据库的操作日志，留存时间不少于 1 年，并定期对日志进行备份，确保日志的完整性、可用性。

第二十一条 机关事业单位应当按照国家、行业领域有关数据安全和个人信息保护的要求，对互联网政务应用数据进行分类分级管理，对重要数据、个人信息、商业秘密进行重点保护。

第二十二条 机关事业单位通过互联网政务应用收集的个人信息、商业秘密和其他未公开资料，未经信息提供方同意不得向第三方提供或公开，不得用于履行法定职责以外的目的。

第二十三条 为互联网政务应用提供服务的数据中心、云计算服务平台等应当设在境内。

第二十四条 党政机关建设互联网政务应用采购云计算服务，应当选取通过国家云计算服务安全评估的云平台，并加强对所采购云计算服务的使用管理。

第二十五条 机关事业单位委托外包单位开展互联网政务应用开发和运维时，应当以合同等手段明确外包单位网络和数据安全责任，并加强日常监督管理和考核问责；督促外包单位严格按照约定使用、存储、处理数据。未经委托的机关事业单位同意，外包单位不得转包、分包合同任务，不得访问、修改、披露、利用、转让、销毁数据。

机关事业单位应当建立严格的授权访问机制，操作系统、数据库、机房等最高管理员权限必须由本单位在编人员专人负责，不得擅自委托外包单位人员管理使用；应当按照最小必要原则对外包单位人员进行精细化授权，在授权期满后及时收回权限。

第二十六条 机关事业单位应当合理建设或利用社会化专业灾备设施，对互

联网政务应用重要数据和信息系统等进行容灾备份。

第二十七条 机关事业单位应当加强互联网政务应用开发安全管理，使用外部代码应当经过安全检测。建立业务连续性计划，防范因供应商服务变更等对升级改造、运维保障等带来的风险。

第二十八条 互联网政务应用使用内容分发网络(CDN)服务的，应当要求服务商将境内用户的域名解析地址指向其境内节点，不得指向境外节点。

第二十九条 互联网政务应用应当使用安全连接方式访问，涉及的电子认证服务应当由依法设立的电子政务电子认证服务机构提供。

第三十条 互联网政务应用应当对注册用户进行真实身份信息认证。国家鼓励互联网政务应用支持用户使用国家网络身份认证公共服务进行真实身份信息注册。

对与人身财产安全、社会公共利益等相关的互联网政务应用和电子邮件系统，应当采取多因素鉴别提高安全性，采取超时退出、限制登录失败次数、账号与终端绑定等技术手段防范账号被盗用风险，鼓励采用电子证书等身份认证措施。

第五章 电子邮件安全

第三十一条 鼓励各地区、各部门通过统一建设、共享使用的模式，建设机关事业单位专用互联网电子邮件系统，作为工作邮箱，为本地区、本行业机关事业单位提供电子邮件服务。党政机关自建的互联网电子邮件系统的域名应当以“.gov.cn”或“.政务”为后缀，事业单位自建的互联网电子邮件系统的域名应当以“.cn”或“.公益”为后缀。

机关事业单位工作人员不得使用工作邮箱违规存储、处理、传输、转发国家秘密。

第三十二条 机关事业单位应当建立工作邮箱账号的申请、发放、变更、注销等流程，严格账号审批登记，定期开展账号清理。

第三十三条 机关事业单位互联网电子邮件系统应当关闭邮件自动转发、自动下载附件功能。

第三十四条 机关事业单位互联网电子邮件系统应当具备恶意邮件(含本单位内部发送的邮件)检测拦截功能，对恶意邮箱账号、恶意邮件服务器 IP 以及

恶意邮件主题、正文、链接、附件等进行检测和拦截。应当支持钓鱼邮件威胁情报共享，将发现的钓鱼邮件信息报送至主管部门和属地网信部门，按照有关部门下发的钓鱼邮件威胁情报，配置相应防护策略预置拦截钓鱼邮件。

第三十五条 鼓励机关事业单位基于商用密码技术对电子邮件数据的存储进行安全保护。

第六章 监测预警和应急处置

第三十六条 中央网络安全和信息化委员会办公室会同国务院电信主管部门、公安部门和其他有关部门，组织对地市级以上党政机关互联网政务应用开展安全监测。

各地区、各部门应当对本地区、本行业机关事业单位互联网政务应用开展日常监测和安全检查。

机关事业单位应当建立完善互联网政务应用安全监测能力，实时监测互联网政务应用运行状态和网络安全事件情况。

第三十七条 互联网政务应用发生网络安全事件时，机关事业单位应当按照有关规定向相关部门报告。

第三十八条 中央网络安全和信息化委员会办公室统筹协调重大网络安全事件的应急处置。

互联网政务应用发生或可能发生网络安全事件时，机关事业单位应当立即启动本单位网络安全应急预案，及时处置网络安全事件，消除安全隐患，防止危害扩大。

第三十九条 机构编制管理部门会同网信部门开展针对假冒仿冒互联网政务应用的扫描监测，受理相关投诉举报。网信部门会同电信主管部门，及时对监测发现或网民举报的假冒仿冒互联网政务应用采取停止域名解析、阻断互联网连接和下线处理等措施。公安部门负责打击假冒仿冒互联网政务应用相关违法犯罪活动。

第七章 监督管理

第四十条 中央网络安全和信息化委员会办公室负责统筹协调互联网政务应用安全管理工作。中央机构编制管理部门负责互联网政务应用开办主体身份核验、名称管理和标识管理工作。国务院电信主管部门负责互联网政务应用域名

监督管理和互联网信息服务(ICP)备案工作。国务院公安部门负责监督检查指导互联网政务应用网络安全等级保护和相关安全管理工作。

各地区、各部门承担本地区、本行业机关事业单位互联网政务应用安全管理责任，指定一名负责人分管相关工作，加强对互联网政务应用安全工作的组织领导。

第四十一条 对违反或者未能正确履行本规定相关要求的，按照《党委(党组)网络安全工作责任制实施办法》等文件，依规依纪追究当事人和有关领导的责任。

第八章 附 则

第四十二条 列入关键信息基础设施的互联网门户网站、移动应用程序、公众账号，以及电子邮件系统的安全管理工作，参照本规定有关内容执行。

第四十三条 本规定由中央网络安全和信息化委员会办公室、中央机构编制委员会办公室、工业和信息化部、公安部负责解释。

第四十四条 本规定自 2024 年 7 月 1 日起施行。

汽车数据安全管理若干规定(试行)

国家互联网信息办公室、中华人民共和国国家发展和改革委员会、中华人民共和国工业和信息化部、中华人民共和国公安部、中华人民共和国交通运输部令

第 7 号

《汽车数据安全管理若干规定(试行)》已经 2021 年 7 月 5 日国家互联网信息办公室 2021 年第 10 次室务会议审议通过，并经国家发展和改革委员会、工业和信息化部、公安部、交通运输部同意，现予公布，自 2021 年 10 月 1 日起施行。

国家互联网信息办公室主任 庄 荣 文

国家发展和改革委员会主任 何 立 峰

工业和信息化部部长 肖 亚 庆

公安部部长 赵 克 志

交通运输部部长 李 小 鹏

2021 年 8 月 16 日

汽车数据安全管理若干规定(试行)

第一条 为了规范汽车数据处理活动，保护个人、组织的合法权益，维护国家安全和社会公共利益，促进汽车数据合理开发利用，根据《中华人民共和国网络安全法》、《中华人民共和国数据安全法》等法律、行政法规，制定本规定。

第二条 在中华人民共和国境内开展汽车数据处理活动及其安全监管，应当遵守相关法律、行政法规和本规定的要求。

第三条 本规定所称汽车数据，包括汽车设计、生产、销售、使用、运维等过程中的涉及个人信息数据和重要数据。

汽车数据处理，包括汽车数据的收集、存储、使用、加工、传输、提供、公开等。

汽车数据处理者，是指开展汽车数据处理活动的组织，包括汽车制造商、零部件和软件供应商、经销商、维修机构以及出行服务企业等。

个人信息，是指以电子或者其他方式记录的与已识别或者可识别的车主、驾驶人、乘车人、车外人员等有关的各种信息，不包括匿名化处理后的信息。

敏感个人信息，是指一旦泄露或者非法使用，可能导致车主、驾驶人、乘车人、车外人员等受到歧视或者人身、财产安全受到严重危害的个人信息，包括车辆行踪轨迹、音频、视频、图像和生物识别特征等信息。

重要数据是指一旦遭到篡改、破坏、泄露或者非法获取、非法利用，可能危害国家安全、公共利益或者个人、组织合法权益的数据，包括：

(一)军事管理区、国防科工单位以及县级以上党政机关等重要敏感区域的地理信息、人员流量、车辆流量等数据；

(二)车辆流量、物流等反映经济运行情况的数据；

(三)汽车充电网的运行数据；

(四)包含人脸信息、车牌信息等的车外视频、图像数据；

(五)涉及个人信息主体超过 10 万人的个人信息；

(六)国家网信部门和国务院发展改革、工业和信息化、公安、交通运输等有关部门确定的其他可能危害国家安全、公共利益或者个人、组织合法权益的数据。

第四条 汽车数据处理者处理汽车数据应当合法、正当、具体、明确，与汽

车的设计、生产、销售、使用、运维等直接相关。

第五条 利用互联网等信息网络开展汽车数据处理活动，应当落实网络安全等级保护等制度，加强汽车数据保护，依法履行数据安全义务。

第六条 国家鼓励汽车数据依法合理有效利用，倡导汽车数据处理者在开展汽车数据处理活动中坚持：

(一)车内处理原则，除非确有必要不向车外提供；

(二)默认不收集原则，除非驾驶人自主设定，每次驾驶时默认设定为不收集状态；

(三)精度范围适用原则，根据所提供功能服务对数据精度的要求确定摄像头、雷达等的覆盖范围、分辨率；

(四)脱敏处理原则，尽可能进行匿名化、去标识化等处理。

第七条 汽车数据处理者处理个人信息应当通过用户手册、车载显示面板、语音、汽车使用相关应用程序等显著方式，告知个人以下事项：

(一)处理个人信息的种类，包括车辆行踪轨迹、驾驶习惯、音频、视频、图像和生物识别特征等；

(二)收集各类个人信息的具体情境以及停止收集的方式和途径；

(三)处理各类个人信息的目的、用途、方式；

(四)个人信息保存地点、保存期限，或者确定保存地点、保存期限的规则；

(五)查阅、复制其个人信息以及删除车内、请求删除已经提供给车外的个人信息的方式和途径；

(六)用户权益事务联系人的姓名和联系方式；

(七)法律、行政法规规定的应当告知的其他事项。

第八条 汽车数据处理者处理个人信息应当取得个人同意或者符合法律、行政法规规定的其他情形。

因保证行车安全需要，无法征得个人同意采集到车外个人信息且向车外提供的，应当进行匿名化处理，包括删除含有能够识别自然人的画面，或者对画面中的人脸信息等进行局部轮廓化处理等。

第九条 汽车数据处理者处理敏感个人信息，应当符合以下要求或者符合法

律、行政法规和强制性国家标准等其他要求：

(一)具有直接服务于个人的目的，包括增强行车安全、智能驾驶、导航等；

(二)通过用户手册、车载显示面板、语音以及汽车使用相关应用程序等显著方式告知必要性以及对个人的影响；

(三)应当取得个人单独同意，个人可以自主设定同意期限；

(四)在保证行车安全的前提下，以适当方式提示收集状态，为个人终止收集提供便利；

(五)个人要求删除的，汽车数据处理者应当在十个工作日内删除。

汽车数据处理者具有增强行车安全的目的和充分的必要性，方可收集指纹、声纹、人脸、心律等生物识别特征信息。

第十条 汽车数据处理者开展重要数据处理活动，应当按照规定开展风险评估，并向省、自治区、直辖市网信部门和有关部门报送风险评估报告。

风险评估报告应当包括处理的重要数据的种类、数量、范围、保存地点与期限、使用方式，开展数据处理活动情况以及是否向第三方提供，面临的数据安全风险及其应对措施等。

第十一条 重要数据应当依法在境内存储，因业务需要确需向境外提供的，应当通过国家网信部门会同国务院有关部门组织的安全评估。未列入重要数据的涉及个人信息数据的出境安全管理，适用法律、行政法规的有关规定。

我国缔结或者参加的国际条约、协定有不同规定的，适用该国际条约、协定，但我国声明保留的条款除外。

第十二条 汽车数据处理者向境外提供重要数据，不得超出出境安全评估时明确的目的、范围、方式和数据种类、规模等。

国家网信部门会同国务院有关部门以抽查等方式核验前款规定事项，汽车数据处理者应当予以配合，并以可读等便利方式予以展示。

第十三条 汽车数据处理者开展重要数据处理活动，应当在每年十二月十五日前向省、自治区、直辖市网信部门和有关部门报送以下年度汽车数据安全管理情况：

(一)汽车数据安全管理负责人、用户权益事务联系人的姓名和联系方式；

(二)处理汽车数据的种类、规模、目的和必要性;

(三)汽车数据的安全防护和管理措施，包括保存地点、期限等;

(四)向境内第三方提供汽车数据情况;

(五)汽车数据安全事件和处置情况;

(六)汽车数据相关的用户投诉和处理情况;

(七)国家网信部门会同国务院工业和信息化、公安、交通运输等有关部门明确的其他汽车数据安全管理情况。

第十四条 向境外提供重要数据的汽车数据处理者应当在本规定第十三条要求的基础上，补充报告以下情况:

(一)接收者的基本情况;

(二)出境汽车数据的种类、规模、目的和必要性;

(三)汽车数据在境外的保存地点、期限、范围和方式;

(四)涉及向境外提供汽车数据的用户投诉和处理情况;

(五)国家网信部门会同国务院工业和信息化、公安、交通运输等有关部门明确的向境外提供汽车数据需要报告的其他情况。

第十五条 国家网信部门和国务院发展改革、工业和信息化、公安、交通运输等有关部门依据职责，根据处理数据情况对汽车数据处理者进行数据安全评估，汽车数据处理者应当予以配合。

参与安全评估的机构和人员不得披露评估中获悉的汽车数据处理者商业秘密、未公开信息，不得将评估中获悉的信息用于评估以外目的。

第十六条 国家加强智能(网联)汽车网络平台建设，开展智能(网联)汽车入网运行和安全保障服务等，协同汽车数据处理者加强智能(网联)汽车网络和汽车数据安全防护。

第十七条 汽车数据处理者开展汽车数据处理活动，应当建立投诉举报渠道，设置便捷的投诉举报入口，及时处理用户投诉举报。

开展汽车数据处理活动造成用户合法权益或者公共利益受到损害的，汽车数据处理者应当依法承担相应责任。

第十八条 汽车数据处理者违反本规定的，由省级以上网信、工业和信息化、公安、交通运输等有关部门依照《中华人民共和国网络安全法》、《中华人

民共和国数据安全法》等法律、行政法规的规定进行处罚；构成犯罪的，依法追究刑事责任。

第十九条 本规定自 2021 年 10 月 1 日起施行。

互联网宗教信息服务管理办法

国家宗教事务局、国家互联网信息办公室、工业和信息化部、公安部、国家安全部令第 17 号

《互联网宗教信息服务管理办法》已经国家宗教事务局按规定程序审议通过，并经国家互联网信息办公室、工业和信息化部、公安部、国家安全部同意，现予公布，自 2022 年 3 月 1 日起施行。

国家宗教事务局局长 王作安

国家互联网信息办公室主任 庄荣文

工业和信息化部部长 肖亚庆

公 安 部 部 长 赵克志

国家安全部部长 陈文清

2021 年 12 月 3 日

互联网宗教信息服务管理办法

第一章 总 则

第一条 为了规范互联网宗教信息服务，保障公民宗教信仰自由，根据《中华人民共和国网络安全法》《互联网信息服务管理办法》《宗教事务条例》等法律法规，制定本办法。

第二条 在中华人民共和国境内从事互联网宗教信息服务，适用本办法。

本办法所称互联网宗教信息服务，包括互联网宗教信息发布服务、转载服务、传播平台服务以及其他与互联网宗教信息相关的服务。

第三条 从事互联网宗教信息服务，应当遵守宪法、法律、法规和规章，践行社会主义核心价值观，坚持我国宗教独立自主自办原则，坚持我国宗教中国化方向，积极引导宗教与社会主义社会相适应，维护宗教和顺、社会和谐、民族和睦。

第四条 互联网宗教信息服务管理坚持保护合法、制止非法、遏制极端、抵御渗透、打击犯罪的原则。

第五条 宗教事务部门依法对互联网宗教信息服务进行监督管理，网信部门、电信主管部门、公安机关、国家安全机关等在各自职责范围内依法负责有关行政管理工作。

省级以上人民政府宗教事务部门应当会同网信部门、电信主管部门、公安机关、国家安全机关等建立互联网宗教信息服务管理协调机制。

第二章 互联网宗教信息服务许可

第六条 通过互联网站、应用程序、论坛、博客、微博客、公众账号、即时通信工具、网络直播等形式，以文字、图片、音视频等方式向社会公众提供宗教教义教规、宗教知识、宗教文化、宗教活动等信息的服务，应当取得互联网宗教信息服务许可，并具备下列条件：

(一)申请人是在中华人民共和国境内依法设立的法人组织或者非法人组织，其法定代表人或者主要负责人是具有中国国籍的内地居民；

(二)有熟悉国家宗教政策法规和相关宗教知识的信息审核人员；

(三)有健全的互联网宗教信息服务管理制度；

(四)有健全的信息安全管理制度和安全可控的技术保障措施；

(五)有与服务相匹配的场所、设施和资金；

(六)申请人及其法定代表人或者主要负责人近 3 年内无犯罪记录、无违反国家宗教事务管理有关规定的行为。

境外组织或者个人及其在境内成立的组织不得在境内从事互联网宗教信息服务。

第七条 从事互联网宗教信息服务，应当向所在地省、自治区、直辖市人民政府宗教事务部门提出申请，填报互联网宗教信息服务申请表，并提交下列材料：

(一)申请人依法设立或者登记备案的材料以及法定代表人或者主要负责人身份证件；

(二)宗教信息审核人员参加宗教政策法规和相关宗教知识的教育培训，以及具备审核能力的情况说明；

(三)互联网宗教信息服务管理制度、信息安全管理制度和技术保障措施材料；

(四)用于从事互联网宗教信息服务的场所、设施和资金情况说明;

(五)申请人及其法定代表人或者主要负责人近 3 年内无犯罪记录和无违反国家宗教事务管理有关规定情况承诺书;

(六)拟从事互联网宗教信息服务的栏目、功能设置和域名注册相关材料。

申请提供互联网宗教信息传播平台服务的,还应当提交平台注册用户管理规章制度、用户协议范本、投诉举报处理机制等。用户协议范本涉及互联网宗教信息服务的内容应当符合本办法有关规定。

互联网宗教信息服务申请表式样由国家宗教事务局制定。

全国性宗教团体及其举办的宗教院校从事互联网宗教信息服务,应当向国家宗教事务局提出申请。

第八条 从事互联网宗教信息服务所使用的名称,除与申请人名称相同以外,不得使用宗教团体、宗教院校和宗教活动场所等名称,不得含有法律、行政法规禁止的内容。

第九条 省级以上人民政府宗教事务部门自受理申请之日起 20 日内作出批准或者不予批准的决定。作出批准决定的,核发《互联网宗教信息服务许可证》;作出不予批准决定的,应当书面通知申请人并说明理由。

《互联网宗教信息服务许可证》由国家宗教事务局印制。

申请人取得《互联网宗教信息服务许可证》后,还应当按照国家互联网信息服务管理有关规定办理相关手续。

第十条 从事互联网宗教信息服务,应当在显著位置明示《互联网宗教信息服务许可证》编号。

第十一条 申请人取得《互联网宗教信息服务许可证》后,发生影响许可条件重大事项的,应当报原发证机关审核批准;其他事项变更,应当向原发证机关备案。

第十二条 终止互联网宗教信息服务的,应当自终止之日起 30 日内,到原发证机关办理注销手续。

第十三条 《互联网宗教信息服务许可证》有效期 3 年。有效期届满后拟继续从事互联网宗教信息服务的,应当在有效期届满 30 日前,向原发证机关重新提出申请。

第三章 互联网宗教信息服务管理

第十四条 互联网宗教信息不得含有下列内容：

(一)利用宗教煽动颠覆国家政权、反对中国共产党的领导，破坏社会主义制度、国家统一、民族团结和社会稳定，宣扬极端主义、恐怖主义、民族分裂主义和宗教狂热的；

(二)利用宗教妨碍国家司法、教育、婚姻、社会管理等制度实施的；

(三)利用宗教宣扬邪教和封建迷信，或者利用宗教损害公民身体健康，欺骗、胁迫取得财物的；

(四)违背我国宗教独立自主自办原则的；

(五)破坏不同宗教之间、同一宗教内部以及信教公民与不信教公民之间和睦相处的；

(六)歧视、侮辱信教公民或者不信教公民，损害信教公民或者不信教公民合法权益的；

(七)从事违法宗教活动或者为违法宗教活动提供便利的；

(八)诱导未成年人信教，或者组织、强迫未成年人参加宗教活动的；

(九)以宗教名义进行商业宣传，经销、发送宗教用品、宗教内部资料性出版物和非法出版物的；

(十)假冒宗教教职人员开展活动的；

(十一)有关法律、行政法规和国家规定禁止的其他内容的。

第十五条 取得《互联网宗教信息服务许可证》的宗教团体、宗教院校和寺观教堂，可以且仅限于通过其依法自建的互联网站、应用程序、论坛等由宗教教职人员、宗教院校教师讲经讲道，阐释教义教规中有利于社会和谐、时代进步、健康文明的内容，引导信教公民爱国守法。参与讲经讲道的人员实行实名管理。

第十六条 取得《互联网宗教信息服务许可证》的宗教院校，可以且仅限于通过其依法自建的专用互联网站、应用程序、论坛等开展面向宗教院校学生、宗教教职人员的宗教教育培训。专用互联网站、应用程序、论坛等对外须使用虚拟专用网络连接，并对参加教育培训的人员进行身份验证。

第十七条 除本办法第十五条、第十六条规定的情形外，任何组织或者个人

不得在互联网上传教，不得开展宗教教育培训、发布讲经讲道内容或者转发、链接相关内容，不得在互联网上组织开展宗教活动，不得以文字、图片、音视频等方式直播或者录播拜佛、烧香、受戒、诵经、礼拜、弥撒、受洗等宗教仪式。

第十八条 任何组织或者个人不得在互联网上成立宗教组织、设立宗教院校和宗教活动场所、发展教徒。

第十九条 任何组织或者个人不得在互联网上以宗教名义开展募捐。

宗教团体、宗教院校和宗教活动场所发起设立的慈善组织在互联网上开展慈善募捐，应当符合《中华人民共和国慈善法》相关规定。

第二十条 提供互联网宗教信息传播平台服务的，应当与平台注册用户签订协议，核验注册用户真实身份信息。

第二十一条 未取得《互联网宗教信息服务许可证》的互联网信息传播平台，应当加强平台注册用户管理，不得为用户提供互联网宗教信息发布服务。

第二十二条 从事互联网宗教信息服务，发现违反本办法规定的信息的，应当立即停止传输该信息，采取消除等处置措施，防止信息扩散，保存有关记录，并向有关主管部门报告。

第二十三条 宗教事务部门应当加强对互联网宗教信息服务的日常指导、监督、检查，建立互联网宗教信息服务违规档案、失信联合惩戒对象名单和约谈制度，加强对互联网宗教信息服务相关从业人员的专业培训，接受对违法从事互联网宗教信息服务的举报，研判互联网宗教信息，会同网信部门、电信主管部门、公安机关、国家安全机关依法处置违法行为。

第二十四条 网信部门应当加强互联网信息内容管理，依法处置违法互联网宗教信息。

第二十五条 电信主管部门应当加强互联网行业监管，依法配合处置违法从事互联网宗教信息服务的行为。

第二十六条 公安机关应当依法加强互联网信息服务安全监督管理，防范和处置互联网宗教信息服务中的违法犯罪活动。

第二十七条 国家安全机关应当依法防范和处置境外机构、组织、个人，以及境内机构、组织、个人与境外机构、组织、个人相勾结在互联网上利用宗教

进行的危害国家安全活动。

第四章 法律责任

第二十八条 申请人隐瞒有关情况或者提供虚假材料申请互联网宗教信息服务许可的，宗教事务部门不予受理或者不予许可，已经许可的应当依法撤销许可，并给予警告。

擅自从事互联网宗教信息服务的，由宗教事务部门会同电信主管部门依据职责责令停止相关服务活动。

第二十九条 违反本办法第十条、第十一条、第十四条、第十五条、第十六条、第十七条、第十八条、第十九条规定的，由宗教事务部门责令限期改正；拒不改正的，会同网信部门、电信主管部门、公安机关、国家安全机关等依照有关法律、行政法规的规定给予处罚。

第三十条 互联网宗教信息传播平台注册用户违反本办法规定的，由宗教事务部门会同网信部门、公安机关责令互联网宗教信息传播平台提供者依法依约采取警示整改、限制功能直至关闭账号等处置措施。

第三十一条 违反本办法规定，同时还违反《互联网信息服务管理办法》及国家对互联网新闻信息服务、互联网视听节目服务、网络出版服务等相关管理规定的，由宗教事务部门、网信部门、电信主管部门、公安机关、广播电视主管部门、电影主管部门、出版主管部门等依法处置。

第三十二条 国家工作人员在互联网宗教信息服务管理工作中滥用职权、玩忽职守、徇私舞弊，依法给予处分。

第三十三条 违反本办法规定，构成违反治安管理行为的，依法给予治安管理处罚；构成犯罪的，依法追究刑事责任。

第五章 附 则

第三十四条 本办法施行前已经从事互联网宗教信息服务的，应当自本办法施行之日起 6 个月内依照本办法有关规定办理相关手续。

第三十五条 本办法由国家宗教事务局、国家互联网信息办公室、工业和信息化部、公安部和国家安全部负责解释。

第三十六条 本办法自 2022 年 3 月 1 日起施行。

网络安全审查办法

国家互联网信息办公室

中华人民共和国国家发展和改革委员会

中华人民共和国工业和信息化部

中华人民共和国公安部

中华人民共和国国家安全部

中华人民共和国财政部

中华人民共和国商务部

中国人民银行

国家市场监督管理总局

国家广播电视总局

中国证券监督管理委员会

国家保密局

国家密码管理局

令

第 8 号

《网络安全审查办法》已经 2021 年 11 月 16 日国家互联网信息办公室 2021 年第 20 次室务会议审议通过，并经国家发展和改革委员会、工业和信息化部、公安部、国家安全部、财政部、商务部、中国人民银行、国家市场监督管理总局、国家广播电视总局、中国证券监督管理委员会、国家保密局、国家密码管理局同意，现予公布，自 2022 年 2 月 15 日起施行。

国家互联网信息办公室主任 庄荣文

国家发展和改革委员会主任 何立峰

工业和信息化部部长 肖亚庆

公安部部长 赵克志

国家安全部部长 陈文清

财政部部长 刘 昆

商务部部长 王文涛

中国人民银行行长 易 纲

国家市场监督管理总局局长 张 工

国家广播电视总局局长 聂辰席

中国证券监督管理委员会主席 易会满

国家保密局局长 李兆宗

国家密码管理局局长 刘东方

2021 年 12 月 28 日

网络安全审查办法

第一条 为了确保关键信息基础设施供应链安全，保障网络安全和数据安全，维护国家安全，根据《中华人民共和国国家安全法》、《中华人民共和国网络安全法》、《中华人民共和国数据安全法》、《关键信息基础设施安全保护条例》，制定本办法。

第二条 关键信息基础设施运营者采购网络产品和服务，网络平台运营者开展数据处理活动，影响或者可能影响国家安全的，应当按照本办法进行网络安全审查。

前款规定的关键信息基础设施运营者、网络平台运营者统称为当事人。

第三条 网络安全审查坚持防范网络安全风险与促进先进技术应用相结合、过程公正透明与知识产权保护相结合、事前审查与持续监管相结合、企业承诺与社会监督相结合，从产品和服务以及数据处理活动安全性、可能带来的国家安全风险等方面进行审查。

第四条 在中央网络安全和信息化委员会领导下，国家互联网信息办公室会同中华人民共和国国家发展和改革委员会、中华人民共和国工业和信息化部、中华人民共和国公安部、中华人民共和国国家安全部、中华人民共和国财政部、中华人民共和国商务部、中国人民银行、国家市场监督管理总局、国家广播电视总局、中国证券监督管理委员会、国家保密局、国家密码管理局建立国家网络安全审查工作机制。

网络安全审查办公室设在国家互联网信息办公室，负责制定网络安全审查相关制度规范，组织网络安全审查。

第五条 关键信息基础设施运营者采购网络产品和服务的，应当预判该产品和服务投入使用后可能带来的国家安全风险。影响或者可能影响国家安全的， 应当向网络安全审查办公室申报网络安全审查。

关键信息基础设施安全保护工作部门可以制定本行业、本领域预判指南。

第六条 对于申报网络安全审查的采购活动，关键信息基础设施运营者应当通过采购文件、协议等要求产品和服务提供者配合网络安全审查， 包括承诺不利用提供产品和服务的便利条件非法获取用户数据、非法控制和操纵用户设备， 无正当理由不中断产品供应或者必要的技术支持服务等。

第七条 掌握超过 100 万用户个人信息的网络平台运营者赴国外上市，必须向网络安全审查办公室申报网络安全审查。

第八条 当事人申报网络安全审查，应当提交以下材料：

(一)申报书；

(二)关于影响或者可能影响国家安全的分析报告；

(三)采购文件、协议、拟签订的合同或者拟提交的首次公开募股(IPO)等上市申请文件；

(四)网络安全审查工作需要的其他材料。

第九条 网络安全审查办公室应当自收到符合本办法第八条规定的审查申报材料起 10 个工作日内，确定是否需要审查并书面通知当事人。

第十条 网络安全审查重点评估相关对象或者情形的以下国家安全风险因素：

(一)产品和服务使用后带来的关键信息基础设施被非法控制、遭受干扰或者破坏的风险；

(二)产品和服务供应中断对关键信息基础设施业务连续性的危害；

(三)产品和服务的安全性、开放性、透明性、来源的多样性， 供应渠道的可靠性以及因为政治、外交、贸易等因素导致供应中断的风险；

(四)产品和服务提供者遵守中国法律、行政法规、部门规章情况；

(五)核心数据、重要数据或者大量个人信息被窃取、泄露、毁损以及非法利用、非法出境的风险；

(六)上市存在关键信息基础设施、核心数据、重要数据或者大量个人信息被外国政府影响、控制、恶意利用的风险，以及网络信息安全风险；

(七)其他可能危害关键信息基础设施安全、网络安全和数据安全的因素。

第十一条 网络安全审查办公室认为需要开展网络安全审查的，应当自向当事人发出书面通知之日起 30 个工作日内完成初步审查，包括形成审查结论建议

和将审查结论建议发送网络安全审查工作机制成员单位、相关部门征求意见； 情况复杂的，可以延长 15 个工作日。

第十二条 网络安全审查工作机制成员单位和相关部门应当自收到审查结论建议之日起 15 个工作日内书面回复意见。

网络安全审查工作机制成员单位、相关部门意见一致的，网络安全审查办公室以书面形式将审查结论通知当事人；意见不一致的，按照特别审查程序处理，并通知当事人。

第十三条 按照特别审查程序处理的，网络安全审查办公室应当听取相关单位和部门意见，进行深入分析评估，再次形成审查结论建议，并征求网络安全审查工作机制成员单位和相关部门意见，按程序报中央网络安全和信息化委员会批准后，形成审查结论并书面通知当事人。

第十四条 特别审查程序一般应当在 90 个工作日内完成，情况复杂的可以延长。

第十五条 网络安全审查办公室要求提供补充材料的，当事人、产品和服务提供者应当予以配合。提交补充材料的时间不计入审查时间。

第十六条 网络安全审查工作机制成员单位认为影响或者可能影响国家安全的网络产品和服务以及数据处理活动，由网络安全审查办公室按程序报中央网络安全和信息化委员会批准后，依照本办法的规定进行审查。

为了防范风险，当事人应当在审查期间按照网络安全审查要求采取预防和消减风险的措施。

第十七条 参与网络安全审查的相关机构和人员应当严格保护知识产权，对在审查工作中知悉的商业秘密、个人信息， 当事人、产品和服务提供者提交的未公开材料，以及其他未公开信息承担保密义务；未经信息提供方同意，不得向无关方披露或者用于审查以外的目的。

第十八条 当事人或者网络产品和服务提供者认为审查人员有失客观公正，或者未能对审查工作中知悉的信息承担保密义务的，可以向网络安全审查办公室或者有关部门举报。

第十九条 当事人应当督促产品和服务提供者履行网络安全审查中作出的承诺。

网络安全审查办公室通过接受举报等形式加强事前事中事后监督。

第二十条 当事人违反本办法规定的，依照《中华人民共和国网络安全法》、《中华人民共和国数据安全法》的规定处理。

第二十一条 本办法所称网络产品和服务主要指核心网络设备、重要通信产品、高性能计算机和服务器、大容量存储设备、大型数据库和应用软件、网络安全设备、云计算服务， 以及其他对关键信息基础设施安全、网络安全和数据安全有重要影响的网络产品和服务。

第二十二条 涉及国家秘密信息的，依照国家有关保密规定执行。

国家对数据安全审查、外商投资安全审查另有规定的，应当同时符合其规定。

第二十三条 本办法自 2022 年 2 月 15 日起施行。2020 年 4 月 13 日公布的《网络安全审查办法》(国家互联网信息办公室、国家发展和改革委员会、工业和信息化部、公安部、国家安全部、财政部、商务部、中国人民银行、国家市场监督管理总局、国家广播电视总局、国家保密局、国家密码管理局令第 6 号)同时废止。

互联网信息服务算法推荐管理规定

国家互联网信息办公室

中华人民共和国工业和信息化部

中华人民共和国公安部

国家市场监督管理总局

令

第 9 号

《互联网信息服务算法推荐管理规定》已经 2021 年 11 月 16 日国家互联网信息办公室 2021 年第 20 次室务会议审议通过，并经工业和信息化部、公安部、国家市场监督管理总局同意，现予公布，自 2022 年 3 月 1 日起施行。

国家互联网信息办公室主任 庄荣文

工业和信息化部部长 肖亚庆

公安部部长 赵克志

国家市场监督管理总局局长 张 工

2021 年 12 月 31 日

互联网信息服务算法推荐管理规定

第一章 总 则

第一条 为了规范互联网信息服务算法推荐活动，弘扬社会主义核心价值观，维护国家安全和社会公共利益，保护公民、法人和其他组织的合法权益， 促进互联网信息服务健康有序发展，根据《中华人民共和国网络安全法》、《中华人民共和国数据安全法》、《中华人民共和国个人信息保护法》、《互联网信息服务管理办法》等法律、行政法规，制定本规定。

第二条 在中华人民共和国境内应用算法推荐技术提供互联网信息服务(以下简称算法推荐服务)，适用本规定。法律、行政法规另有规定的， 依照其规定。

前款所称应用算法推荐技术，是指利用生成合成类、个性化推送类、排序精选类、检索过滤类、调度决策类等算法技术向用户提供信息。

第三条 国家网信部门负责统筹协调全国算法推荐服务治理和相关监督管理工作。国务院电信、公安、市场监管等有关部门依据各自职责负责算法推荐服务监督管理工作。

地方网信部门负责统筹协调本行政区域内的算法推荐服务治理和相关监督管理工作。地方电信、公安、市场监管等有关部门依据各自职责负责本行政区域内的算法推荐服务监督管理工作。

第四条 提供算法推荐服务，应当遵守法律法规，尊重社会公德和伦理，遵守商业道德和职业道德，遵循公正公平、公开透明、科学合理和诚实信用的原则。

第五条 鼓励相关行业组织加强行业自律，建立健全行业标准、行业准则和自律管理制度，督促指导算法推荐服务提供者制定完善服务规范、依法提供服务并接受社会监督。

第二章 信息服务规范

第六条 算法推荐服务提供者应当坚持主流价值导向，优化算法推荐服务机制，积极传播正能量，促进算法应用向上向善。

算法推荐服务提供者不得利用算法推荐服务从事危害国家安全和社会公共利益、扰乱经济秩序和社会秩序、侵犯他人合法权益等法律、行政法规禁止的活动，不得利用算法推荐服务传播法律、行政法规禁止的信息， 应当采取措施防范和抵制传播不良信息。

第七条 算法推荐服务提供者应当落实算法安全主体责任，建立健全算法机制机理审核、科技伦理审查、用户注册、信息发布审核、数据安全和个人信息保护、反电信网络诈骗、安全评估监测、安全事件应急处置等管理制度和技术措施，制定并公开算法推荐服务相关规则，配备与算法推荐服务规模相适应的专业人员和技术支撑。

第八条 算法推荐服务提供者应当定期审核、评估、验证算法机制机理、模型、数据和应用结果等， 不得设置诱导用户沉迷、过度消费等违反法律法规或者违背伦理道德的算法模型。

第九条 算法推荐服务提供者应当加强信息安全管理，建立健全用于识别违法和不良信息的特征库，完善入库标准、规则和程序。发现未作显著标识的算法生成合成信息的，应当作出显著标识后，方可继续传输。

发现违法信息的，应当立即停止传输，采取消除等处置措施，防止信息扩散，保存有关记录，并向网信部门和有关部门报告。发现不良信息的， 应当按照网络信息内容生态治理有关规定予以处置。

第十条 算法推荐服务提供者应当加强用户模型和用户标签管理，完善记入用户模型的兴趣点规则和用户标签管理规则，不得将违法和不良信息关键词记入用户兴趣点或者作为用户标签并据以推送信息。

第十一条 算法推荐服务提供者应当加强算法推荐服务版面页面生态管理，建立完善人工干预和用户自主选择机制，在首页首屏、热搜、精选、榜单类、弹窗等重点环节积极呈现符合主流价值导向的信息。

第十二条 鼓励算法推荐服务提供者综合运用内容去重、打散干预等策略，并优化检索、排序、选择、推送、展示等规则的透明度和可解释性， 避免对用户产生不良影响，预防和减少争议纠纷。

第十三条 算法推荐服务提供者提供互联网新闻信息服务的，应当依法取得互联网新闻信息服务许可，规范开展互联网新闻信息采编发布服务、转载服务和传播平台服务，不得生成合成虚假新闻信息，不得传播非国家规定范围内的单位发布的新闻信息。

第十四条 算法推荐服务提供者不得利用算法虚假注册账号、非法交易账号、操纵用户账号或者虚假点赞、评论、转发，不得利用算法屏蔽信息、过度推荐、

操纵榜单或者检索结果排序、控制热搜或者精选等干预信息呈现， 实施影响网络舆论或者规避监督管理行为。

第十五条 算法推荐服务提供者不得利用算法对其他互联网信息服务提供者进行不合理限制，或者妨碍、破坏其合法提供的互联网信息服务正常运行， 实施垄断和不正当竞争行为。

第三章 用户权益保护

第十六条 算法推荐服务提供者应当以显著方式告知用户其提供算法推荐服务的情况，并以适当方式公示算法推荐服务的基本原理、目的意图和主要运行机制等。

第十七条 算法推荐服务提供者应当向用户提供不针对其个人特征的选项，或者向用户提供便捷的关闭算法推荐服务的选项。用户选择关闭算法推荐服务的，算法推荐服务提供者应当立即停止提供相关服务。

算法推荐服务提供者应当向用户提供选择或者删除用于算法推荐服务的针对其个人特征的用户标签的功能。

算法推荐服务提供者应用算法对用户权益造成重大影响的，应当依法予以说明并承担相应责任。

第十八条 算法推荐服务提供者向未成年人提供服务的，应当依法履行未成年人网络保护义务，并通过开发适合未成年人使用的模式、提供适合未成年人特点的服务等方式，便利未成年人获取有益身心健康的信息。

算法推荐服务提供者不得向未成年人推送可能引发未成年人模仿不安全行为和违反社会公德行为、诱导未成年人不良嗜好等可能影响未成年人身心健康的信息，不得利用算法推荐服务诱导未成年人沉迷网络。

第十九条 算法推荐服务提供者向老年人提供服务的，应当保障老年人依法享有的权益，充分考虑老年人出行、就医、消费、办事等需求， 按照国家有关规定提供智能化适老服务，依法开展涉电信网络诈骗信息的监测、识别和处置， 便利老年人安全使用算法推荐服务。

第二十条 算法推荐服务提供者向劳动者提供工作调度服务的，应当保护劳动者取得劳动报酬、休息休假等合法权益， 建立完善平台订单分配、报酬构成及支付、工作时间、奖惩等相关算法。

第二十一条 算法推荐服务提供者向消费者销售商品或者提供服务的，应当保护消费者公平交易的权利，不得根据消费者的偏好、交易习惯等特征， 利用算法在交易价格等交易条件上实施不合理的差别待遇等违法行为。

第二十二条 算法推荐服务提供者应当设置便捷有效的用户申诉和公众投诉、举报入口，明确处理流程和反馈时限，及时受理、处理并反馈处理结果。

第四章 监督管理

第二十三条 网信部门会同电信、公安、市场监管等有关部门建立算法分级分类安全管理制度，根据算法推荐服务的舆论属性或者社会动员能力、内容类别、用户规模、算法推荐技术处理的数据重要程度、对用户行为的干预程度等对算法推荐服务提供者实施分级分类管理。

第二十四条 具有舆论属性或者社会动员能力的算法推荐服务提供者应当在提供服务之日起十个工作日内通过互联网信息服务算法备案系统填报服务提供者的名称、服务形式、应用领域、算法类型、算法自评估报告、拟公示内容等信息，履行备案手续。

算法推荐服务提供者的备案信息发生变更的，应当在变更之日起十个工作日内办理变更手续。

算法推荐服务提供者终止服务的，应当在终止服务之日起二十个工作日内办理注销备案手续，并作出妥善安排。

第二十五条 国家和省、自治区、直辖市网信部门收到备案人提交的备案材料后，材料齐全的，应当在三十个工作日内予以备案，发放备案编号并进行公示；材料不齐全的，不予备案，并应当在三十个工作日内通知备案人并说明理由。

第二十六条 完成备案的算法推荐服务提供者应当在其对外提供服务的网站、应用程序等的显著位置标明其备案编号并提供公示信息链接。

第二十七条 具有舆论属性或者社会动员能力的算法推荐服务提供者应当按照国家有关规定开展安全评估。

第二十八条 网信部门会同电信、公安、市场监管等有关部门对算法推荐服务依法开展安全评估和监督检查工作，对发现的问题及时提出整改意见并限期整改。

算法推荐服务提供者应当依法留存网络日志，配合网信部门和电信、公安、

市场监管等有关部门开展安全评估和监督检查工作，并提供必要的技术、数据等支持和协助。

第二十九条 参与算法推荐服务安全评估和监督检查的相关机构和人员对在履行职责中知悉的个人隐私、个人信息和商业秘密应当依法予以保密， 不得泄露或者非法向他人提供。

第三十条 任何组织和个人发现违反本规定行为的，可以向网信部门和有关部门投诉、举报。收到投诉、举报的部门应当及时依法处理。

第五章 法律责任

第三十一条 算法推荐服务提供者违反本规定第七条、第八条、第九条第一款、第十条、第十四条、第十六条、第十七条、第二十二条、第二十四条、第二十六条规定，法律、行政法规有规定的， 依照其规定；法律、行政法规没有规定的，由网信部门和电信、公安、市场监管等有关部门依据职责给予警告、通报批评，责令限期改正；拒不改正或者情节严重的，责令暂停信息更新，并处一万元以上十万元以下罚款。构成违反治安管理行为的， 依法给予治安管理处罚；构成犯罪的，依法追究刑事责任。

第三十二条 算法推荐服务提供者违反本规定第六条、第九条第二款、第十一条、第十三条、第十五条、第十八条、第十九条、第二十条、第二十一条、第二十七条、第二十八条第二款规定的， 由网信部门和电信、公安、市场监管等有关部门依据职责，按照有关法律、行政法规和部门规章的规定予以处理。

第三十三条 具有舆论属性或者社会动员能力的算法推荐服务提供者通过隐瞒有关情况、提供虚假材料等不正当手段取得备案的， 由国家和省、自治区、直辖市网信部门予以撤销备案，给予警告、通报批评； 情节严重的，责令暂停信息更新，并处一万元以上十万元以下罚款。

具有舆论属性或者社会动员能力的算法推荐服务提供者终止服务未按照本规定第二十四条第三款要求办理注销备案手续，或者发生严重违法情形受到责令关闭网站、吊销相关业务许可证或者吊销营业执照等行政处罚的，由国家和省、自治区、直辖市网信部门予以注销备案。

第六章 附 则

第三十四条 本规定由国家互联网信息办公室会同工业和信息化部、公安部、

国家市场监督管理总局负责解释。

第三十五条 本规定自 2022 年 3 月 1 日起施行。

互联网信息服务深度合成管理规定

国家互联网信息办公室

中华人民共和国工业和信息化部

中华人民共和国公安部

令

第 12 号

《互联网信息服务深度合成管理规定》已经 2022 年 11 月 3 日国家互联网信息办公室 2022 年第 21 次室务会议审议通过，并经工业和信息化部、公安部同意，现予公布，自 2023 年 1 月 10 日起施行。

国家互联网信息办公室主任 庄荣文

工业和信息化部部长 金壮龙

公安部部长 王小洪

2022 年 11 月 25 日

互联网信息服务深度合成管理规定

第一章 总 则

第一条 为了加强互联网信息服务深度合成管理，弘扬社会主义核心价值观，维护国家安全和社会公共利益，保护公民、法人和其他组织的合法权益，根据《中华人民共和国网络安全法》、《中华人民共和国数据安全法》、《中华人民共和国个人信息保护法》、《互联网信息服务管理办法》等法律、行政法规，制定本规定。

第二条 在中华人民共和国境内应用深度合成技术提供互联网信息服务(以下简称深度合成服务)，适用本规定。法律、行政法规另有规定的， 依照其规定。

第三条 国家网信部门负责统筹协调全国深度合成服务的治理和相关监督管理工作。国务院电信主管部门、公安部门依据各自职责负责深度合成服务的监督管理工作。

地方网信部门负责统筹协调本行政区域内的深度合成服务的治理和相关监督管理工作。地方电信主管部门、公安部门依据各自职责负责本行政区域内的深度合成服务的监督管理工作。

第四条 提供深度合成服务，应当遵守法律法规，尊重社会公德和伦理道德，坚持正确政治方向、舆论导向、价值取向，促进深度合成服务向上向善。

第五条 鼓励相关行业组织加强行业自律，建立健全行业标准、行业准则和自律管理制度，督促指导深度合成服务提供者和技术支持者制定完善业务规范、依法开展业务和接受社会监督。

第二章 一般规定

第六条 任何组织和个人不得利用深度合成服务制作、复制、发布、传播法律、行政法规禁止的信息， 不得利用深度合成服务从事危害国家安全和利益、损害国家形象、侵害社会公共利益、扰乱经济和社会秩序、侵犯他人合法权益等法律、行政法规禁止的活动。

深度合成服务提供者和使用者不得利用深度合成服务制作、复制、发布、传播虚假新闻信息。转载基于深度合成服务制作发布的新闻信息的， 应当依法转载互联网新闻信息稿源单位发布的新闻信息。

第七条 深度合成服务提供者应当落实信息安全主体责任，建立健全用户注册、算法机制机理审核、科技伦理审查、信息发布审核、数据安全、个人信息保护、反电信网络诈骗、应急处置等管理制度，具有安全可控的技术保障措施。

第八条 深度合成服务提供者应当制定和公开管理规则、平台公约， 完善服务协议，依法依约履行管理责任，以显著方式提示深度合成服务技术支持者和使用者承担信息安全义务。

第九条 深度合成服务提供者应当基于移动电话号码、身份证件号码、统一社会信用代码或者国家网络身份认证公共服务等方式，依法对深度合成服务使用者进行真实身份信息认证，不得向未进行真实身份信息认证的深度合成服务使用者提供信息发布服务。

第十条 深度合成服务提供者应当加强深度合成内容管理，采取技术或者人工方式对深度合成服务使用者的输入数据和合成结果进行审核。

深度合成服务提供者应当建立健全用于识别违法和不良信息的特征库，完善入库标准、规则和程序，记录并留存相关网络日志。

深度合成服务提供者发现违法和不良信息的，应当依法采取处置措施，保存有关记录，及时向网信部门和有关主管部门报告；对相关深度合成服务使用者依

法依约采取警示、限制功能、暂停服务、关闭账号等处置措施。

第十一条 深度合成服务提供者应当建立健全辟谣机制，发现利用深度合成服务制作、复制、发布、传播虚假信息的， 应当及时采取辟谣措施，保存有关记录，并向网信部门和有关主管部门报告。

第十二条 深度合成服务提供者应当设置便捷的用户申诉和公众投诉、举报入口，公布处理流程和反馈时限，及时受理、处理和反馈处理结果。

第十三条 互联网应用商店等应用程序分发平台应当落实上架审核、日常管理、应急处置等安全管理责任， 核验深度合成类应用程序的安全评估、备案等情况；对违反国家有关规定的，应当及时采取不予上架、警示、暂停服务或者下架等处置措施。

第三章 数据和技术管理规范

第十四条 深度合成服务提供者和技术支持者应当加强训练数据管理，采取必要措施保障训练数据安全；训练数据包含个人信息的，应当遵守个人信息保护的有关规定。

深度合成服务提供者和技术支持者提供人脸、人声等生物识别信息编辑功能的，应当提示深度合成服务使用者依法告知被编辑的个人，并取得其单独同意。

第十五条 深度合成服务提供者和技术支持者应当加强技术管理，定期审核、评估、验证生成合成类算法机制机理。

深度合成服务提供者和技术支持者提供具有以下功能的模型、模板等工具的，应当依法自行或者委托专业机构开展安全评估：

(一)生成或者编辑人脸、人声等生物识别信息的；

(二)生成或者编辑可能涉及国家安全、国家形象、国家利益和社会公共利益的特殊物体、场景等非生物识别信息的。

第十六条 深度合成服务提供者对使用其服务生成或者编辑的信息内容，应当采取技术措施添加不影响用户使用的标识，并依照法律、行政法规和国家有关规定保存日志信息。

第十七条 深度合成服务提供者提供以下深度合成服务，可能导致公众混淆或者误认的，应当在生成或者编辑的信息内容的合理位置、区域进行显著标识，向公众提示深度合成情况：

(一)智能对话、智能写作等模拟自然人进行文本的生成或者编辑服务;

(二)合成人声、仿声等语音生成或者显著改变个人身份特征的编辑服务;

(三)人脸生成、人脸替换、人脸操控、姿态操控等人物图像、视频生成或者显著改变个人身份特征的编辑服务;

(四)沉浸式拟真场景等生成或者编辑服务;

(五)其他具有生成或者显著改变信息内容功能的服务。

深度合成服务提供者提供前款规定之外的深度合成服务的,应当提供显著标识功能,并提示深度合成服务使用者可以进行显著标识。

第十八条 任何组织和个人不得采用技术手段删除、篡改、隐匿本规定第十六条和第十七条规定的深度合成标识。

第四章 监督检查与法律责任

第十九条 具有舆论属性或者社会动员能力的深度合成服务提供者,应当按照《互联网信息服务算法推荐管理规定》履行备案和变更、注销备案手续。

深度合成服务技术支持者应当参照前款规定履行备案和变更、注销备案手续。

完成备案的深度合成服务提供者和技术支持者应当在其对外提供服务的网站、应用程序等的显著位置标明其备案编号并提供公示信息链接。

第二十条 深度合成服务提供者开发上线具有舆论属性或者社会动员能力的新产品、新应用、新功能的,应当按照国家有关规定开展安全评估。

第二十一条 网信部门和电信主管部门、公安部门依据职责对深度合成服务开展监督检查。深度合成服务提供者和技术支持者应当依法予以配合, 并提供必要的技术、数据等支持和协助。

网信部门和有关主管部门发现深度合成服务存在较大信息安全风险的,可以按照职责依法要求深度合成服务提供者和技术支持者采取暂停信息更新、用户账号注册或者其他相关服务等措施。深度合成服务提供者和技术支持者应当按照要求采取措施,进行整改,消除隐患。

第二十二条 深度合成服务提供者和技术支持者违反本规定的,依照有关法律、行政法规的规定处罚;造成严重后果的,依法从重处罚。

构成违反治安管理行为的,由公安机关依法给予治安管理处罚;构成犯罪的,依法追究刑事责任。

第五章 附 则

第二十三条 本规定中下列用语的含义：

深度合成技术，是指利用深度学习、虚拟现实等生成合成类算法制作文本、图像、音频、视频、虚拟场景等网络信息的技术，包括但不限于：

(一)篇章生成、文本风格转换、问答对话等生成或者编辑文本内容的技术；

(二)文本转语音、语音转换、语音属性编辑等生成或者编辑语音内容的技术；

(三)音乐生成、场景声编辑等生成或者编辑非语音内容的技术；

(四)人脸生成、人脸替换、人物属性编辑、人脸操控、姿态操控等生成或者编辑图像、视频内容中生物特征的技术；

(五)图像生成、图像增强、图像修复等生成或者编辑图像、视频内容中非生物特征的技术；

(六)三维重建、数字仿真等生成或者编辑数字人物、虚拟场景的技术。

深度合成服务提供者，是指提供深度合成服务的组织、个人。

深度合成服务技术支持者，是指为深度合成服务提供技术支持的组织、个人。

深度合成服务使用者，是指使用深度合成服务制作、复制、发布、传播信息的组织、个人。

训练数据，是指被用于训练机器学习模型的标注或者基准数据集。

沉浸式拟真场景，是指应用深度合成技术生成或者编辑的、可供参与者体验或者互动的、具有高度真实感的虚拟场景。

第二十四条 深度合成服务提供者和技术支持者从事网络出版服务、网络文化活动和网络视听节目服务的，应当同时符合新闻出版、文化和旅游、广播电视主管部门的规定。

第二十五条 本规定自 2023 年 1 月 10 日起施行。

生成式人工智能服务管理暂行办法

国家互联网信息办公室

中华人民共和国国家发展和改革委员会

中华人民共和国教育部

中华人民共和国科学技术部

中华人民共和国工业和信息化部

中华人民共和国公安部

国家广播电视总局

令

第 15 号

《生成式人工智能服务管理暂行办法》已经 2023 年 5 月 23 日国家互联网信息办公室 2023 年第 12 次室务会会议审议通过，并经国家发展和改革委员会、教育部、科学技术部、工业和信息化部、公安部、国家广播电视总局同意， 现予公布，自 2023 年 8 月 15 日起施行。

国家互联网信息办公室主任 庄荣文

国家发展和改革委员会主任 郑栅洁

教育部部长 怀进鹏

科学技术部部长 王志刚

工业和信息化部部长 金壮龙

公安部部长 王小洪

国家广播电视总局局长 曹淑敏

2023 年 7 月 10 日

生成式人工智能服务管理暂行办法

第一章 总 则

第一条 为了促进生成式人工智能健康发展和规范应用，维护国家安全和社会公共利益，保护公民、法人和其他组织的合法权益， 根据《中华人民共和国网络安全法》、《中华人民共和国数据安全法》、《中华人民共和国个人信息保护法》、《中华人民共和国科学技术进步法》等法律、行政法规，制定本办法。

第二条 利用生成式人工智能技术向中华人民共和国境内公众提供生成文本、图片、音频、视频等内容的服务(以下称生成式人工智能服务)，适用本办法。

国家对利用生成式人工智能服务从事新闻出版、影视制作、文艺创作等活动另有规定的，从其规定。

行业组织、企业、教育和科研机构、公共文化机构、有关专业机构等研发、应用生成式人工智能技术，未向境内公众提供生成式人工智能服务的，不适用本办法的规定。

第三条 国家坚持发展和安全并重、促进创新和依法治理相结合的原则，采取有效措施鼓励生成式人工智能创新发展，对生成式人工智能服务实行包容审慎和分类分级监管。

第四条 提供和使用生成式人工智能服务，应当遵守法律、行政法规，尊重社会公德和伦理道德，遵守以下规定：

(一)坚持社会主义核心价值观，不得生成煽动颠覆国家政权、推翻社会主义制度，危害国家安全和利益、损害国家形象， 煽动分裂国家、破坏国家统一和社会稳定，宣扬恐怖主义、极端主义， 宣扬民族仇恨、民族歧视， 暴力、淫秽色情，以及虚假有害信息等法律、行政法规禁止的内容；

(二)在算法设计、训练数据选择、模型生成和优化、提供服务等过程中， 采取有效措施防止产生民族、信仰、国别、地域、性别、年龄、职业、健康等歧视；

(三)尊重知识产权、商业道德， 保守商业秘密，不得利用算法、数据、平台等优势，实施垄断和不正当竞争行为；

(四)尊重他人合法权益，不得危害他人身心健康，不得侵害他人肖像权、名誉权、荣誉权、隐私权和个人信息权益；

(五)基于服务类型特点，采取有效措施，提升生成式人工智能服务的透明度，提高生成内容的准确性和可靠性。

第二章 技术发展与治理

第五条 鼓励生成式人工智能技术在各行业、各领域的创新应用，生成积极健康、向上向善的优质内容，探索优化应用场景，构建应用生态体系。

支持行业组织、企业、教育和科研机构、公共文化机构、有关专业机构等在生成式人工智能技术创新、数据资源建设、转化应用、风险防范等方面开展协作。

第六条 鼓励生成式人工智能算法、框架、芯片及配套软件平台等基础技术的自主创新，平等互利开展国际交流与合作，参与生成式人工智能相关国际规则制定。

推动生成式人工智能基础设施和公共训练数据资源平台建设。促进算力资源协同共享，提升算力资源利用效能。推动公共数据分类分级有序开放， 扩展高质量的公共训练数据资源。鼓励采用安全可信的芯片、软件、工具、算力和数据资源。

第七条 生成式人工智能服务提供者(以下称提供者)应当依法开展预训练、优化训练等训练数据处理活动，遵守以下规定：

(一)使用具有合法来源的数据和基础模型；

(二)涉及知识产权的，不得侵害他人依法享有的知识产权；

(三)涉及个人信息的，应当取得个人同意或者符合法律、行政法规规定的其他情形；

(四)采取有效措施提高训练数据质量，增强训练数据的真实性、准确性、客观性、多样性；

(五)《中华人民共和国网络安全法》、《中华人民共和国数据安全法》、《中华人民共和国个人信息保护法》等法律、行政法规的其他有关规定和有关主管部门的相关监管要求。

第八条 在生成式人工智能技术研发过程中进行数据标注的，提供者应当制定符合本办法要求的清晰、具体、可操作的标注规则；开展数据标注质量评估，抽样核验标注内容的准确性；对标注人员进行必要培训，提升尊法守法意识，监督指导标注人员规范开展标注工作。

第三章 服务规范

第九条 提供者应当依法承担网络信息内容生产者责任，履行网络信息安全义务。涉及个人信息的，依法承担个人信息处理者责任，履行个人信息保护义务。

提供者应当与注册其服务的生成式人工智能服务使用者(以下称使用者)签订服务协议，明确双方权利义务。

第十条 提供者应当明确并公开其服务的适用人群、场合、用途，指导使用者科学理性认识和依法使用生成式人工智能技术，采取有效措施防范未成年人用户过度依赖或者沉迷生成式人工智能服务。

第十一条 提供者对使用者的输入信息和使用记录应当依法履行保护义务，不得收集非必要个人信息，不得非法留存能够识别使用者身份的输入信息和使用记录，不得非法向他人提供使用者的输入信息和使用记录。

提供者应当依法及时受理和处理个人关于查阅、复制、更正、补充、删除其个人信息等的请求。

第十二条 提供者应当按照《互联网信息服务深度合成管理规定》对图片、

视频等生成内容进行标识。

第十三条 提供者应当在其服务过程中，提供安全、稳定、持续的服务，保障用户正常使用。

第十四条 提供者发现违法内容的，应当及时采取停止生成、停止传输、消除等处置措施，采取模型优化训练等措施进行整改，并向有关主管部门报告。

提供者发现使用者利用生成式人工智能服务从事违法活动的，应当依法依约采取警示、限制功能、暂停或者终止向其提供服务等处置措施，保存有关记录，并向有关主管部门报告。

第十五条 提供者应当建立健全投诉、举报机制，设置便捷的投诉、举报入口，公布处理流程和反馈时限，及时受理、处理公众投诉举报并反馈处理结果。

第四章 监督检查和法律责任

第十六条 网信、发展改革、教育、科技、工业和信息化、公安、广播电视、新闻出版等部门，依据各自职责依法加强对生成式人工智能服务的管理。

国家有关主管部门针对生成式人工智能技术特点及其在有关行业和领域的服务应用，完善与创新发展相适应的科学监管方式，制定相应的分类分级监管规则或者指引。

第十七条 提供具有舆论属性或者社会动员能力的生成式人工智能服务的，应当按照国家有关规定开展安全评估，并按照《互联网信息服务算法推荐管理规定》履行算法备案和变更、注销备案手续。

第十八条 使用者发现生成式人工智能服务不符合法律、行政法规和本办法规定的，有权向有关主管部门投诉、举报。

第十九条 有关主管部门依据职责对生成式人工智能服务开展监督检查，提供者应当依法予以配合，按要求对训练数据来源、规模、类型、标注规则、算法机制机理等予以说明，并提供必要的技术、数据等支持和协助。

参与生成式人工智能服务安全评估和监督检查的相关机构和人员对在履行职责中知悉的国家秘密、商业秘密、个人隐私和个人信息应当依法予以保密， 不得泄露或者非法向他人提供。

第二十条 对来源于中华人民共和国境外向境内提供生成式人工智能服务不符合法律、行政法规和本办法规定的， 国家网信部门应当通知有关机构采取技术

措施和其他必要措施予以处置。

第二十一条 提供者违反本办法规定的，由有关主管部门依照《中华人民共和国网络安全法》、《中华人民共和国数据安全法》、《中华人民共和国个人信息保护法》、《中华人民共和国科学技术进步法》等法律、行政法规的规定予以处罚；法律、行政法规没有规定的， 由有关主管部门依据职责予以警告、通报批评， 责令限期改正；拒不改正或者情节严重的，责令暂停提供相关服务。

构成违反治安管理行为的，依法给予治安管理处罚；构成犯罪的，依法追究刑事责任。

第五章 附 则

第二十二条 本办法下列用语的含义是：

(一)生成式人工智能技术，是指具有文本、图片、音频、视频等内容生成能力的模型及相关技术。

(二)生成式人工智能服务提供者，是指利用生成式人工智能技术提供生成式人工智能服务(包括通过提供可编程接口等方式提供生成式人工智能服务)的组织、个人。

(三)生成式人工智能服务使用者，是指使用生成式人工智能服务生成内容的组织、个人。

第二十三条 法律、行政法规规定提供生成式人工智能服务应当取得相关行政许可的，提供者应当依法取得许可。

外商投资生成式人工智能服务，应当符合外商投资相关法律、行政法规的规定。

第二十四条 本办法自 2023 年 8 月 15 日起施行。

网络暴力信息治理规定

国家互联网信息办公室

中华人民共和国公安部

中华人民共和国文化和旅游部

国家广播电视总局

令

第 17 号

《网络暴力信息治理规定》已经 2023 年 12 月 25 日国家互联网信息办公室 2023 年第 28 次室务会会议审议通过，并经公安部、文化和旅游部、国家广播电视总局同意，现予公布，自 2024 年 8 月 1 日起施行。

国家互联网信息办公室主任 庄荣文

公安部部长 王小洪

文化和旅游部部长 孙业礼

国家广播电视总局局长 曹淑敏

2024 年 6 月 12 日

网络暴力信息治理规定

第一章 总 则

第一条 为了治理网络暴力信息，营造良好网络生态，保障公民合法权益，维护社会公共利益，根据《中华人民共和国网络安全法》、《中华人民共和国个人信息保护法》、《中华人民共和国治安管理处罚法》、《互联网信息服务管理办法》等法律、行政法规，制定本规定。

第二条 中华人民共和国境内的网络暴力信息治理活动，适用本规定。

第三条 网络暴力信息治理坚持源头防范、防控结合、标本兼治、协同共治的原则。

第四条 国家网信部门负责统筹协调全国网络暴力信息治理和相关监督管理工作。国务院公安、文化和旅游、广播电视等有关部门依据各自职责开展网络暴力信息的监督管理工作。

地方网信部门负责统筹协调本行政区域内网络暴力信息治理和相关监督管理工作。地方公安、文化和旅游、广播电视等有关部门依据各自职责开展本行政区域内网络暴力信息的监督管理工作。

第五条 鼓励网络相关行业组织加强行业自律，开展网络暴力信息治理普法宣传，督促指导网络信息服务提供者加强网络暴力信息治理并接受社会监督，为遭受网络暴力信息侵害的用户提供帮扶救助等支持。

第二章 一般规定

第六条 网络信息服务提供者和用户应当坚持社会主义核心价值观，遵守法律法规，尊重社会公德和伦理道德，促进形成积极健康、向上向善的网络文化，

维护良好网络生态。

第七条 网络信息服务提供者应当履行网络信息内容管理主体责任，建立完善网络暴力信息治理机制，健全用户注册、账号管理、个人信息保护、信息发布审核、监测预警、识别处置等制度。

第八条 网络信息服务提供者为用户提供信息发布、即时通讯等服务的，应当依法对用户进行真实身份信息认证。用户不提供真实身份信息的， 网络信息服务提供者不得为其提供相关服务。

网络信息服务提供者应当加强用户账号信息管理，为遭受网络暴力信息侵害的相关主体提供账号信息认证协助，防范和制止假冒、仿冒、恶意关联相关主体进行违规注册或者发布信息。

第九条 网络信息服务提供者应当制定和公开管理规则、平台公约， 与用户签订服务协议，明确网络暴力信息治理相关权利义务，并依法依约履行治理责任。

第十条 任何组织和个人不得制作、复制、发布、传播涉网络暴力违法信息，应当防范和抵制制作、复制、发布、传播涉网络暴力不良信息。

任何组织和个人不得利用网络暴力事件实施蹭炒热度、推广引流等营销炒作行为，不得通过批量注册或者操纵用户账号等形式组织制作、复制、发布、传播网络暴力信息。

明知他人从事涉网络暴力信息违法犯罪活动的，任何组织和个人不得为其提供数据、技术、流量、资金等支持和协助。

第十一条 网络信息服务提供者应当定期发布网络暴力信息治理公告，并将相关工作情况列入网络信息内容生态治理工作年度报告。

第三章 预防预警

第十二条 网络信息服务提供者应当在国家网信部门和国务院有关部门指导下细化网络暴力信息分类标准规则，建立健全网络暴力信息特征库和典型案例样本库，采用人工智能、大数据等技术手段和人工审核相结合的方式加强对网络暴力信息的识别监测。

第十三条 网络信息服务提供者应当建立健全网络暴力信息预警模型，综合事件类别、针对主体、参与人数、信息内容、发布频次、环节场景、举报投诉等因素，及时发现预警网络暴力信息风险。

网络信息服务提供者发现存在网络暴力信息风险的，应当及时回应社会关切，引导用户文明互动、理性表达，并对异常账号及时采取真实身份信息动态核验、弹窗提示、违规警示、限制流量等措施；发现相关信息内容浏览、搜索、评论、举报量显著增长等情形的，还应当及时向有关部门报告。

第十四条 网络信息服务提供者应当建立健全用户账号信用管理体系，将涉网络暴力信息违法违规情形记入用户信用记录，依法依约降低账号信用等级或者列入黑名单，并据以限制账号功能或者停止提供相关服务。

第四章 信息和账号处置

第十五条 网络信息服务提供者发现涉网络暴力违法信息的，或者在其服务的醒目位置、易引起用户关注的重点环节发现涉网络暴力不良信息的， 应当立即停止传输，采取删除、屏蔽、断开链接等处置措施， 保存有关记录，向有关部门报告。发现涉嫌违法犯罪的， 应当及时向公安机关报案，并提供相关线索，依法配合开展侦查、调查和处置等工作。

第十六条 互联网新闻信息服务提供者应当坚持正确政治方向、舆论导向、价值取向，加强网络暴力信息治理的公益宣传。

互联网新闻信息服务提供者不得通过夸大事实、过度渲染、片面报道等方式采编发布、转载涉网络暴力新闻信息。对互联网新闻信息提供跟帖评论服务的，应当实行先审后发。

互联网新闻信息服务提供者采编发布、转载涉网络暴力新闻信息不真实或者不公正的，应当立即公开更正，消除影响。

第十七条 网络信息服务提供者应当加强网络视听节目、网络表演等服务内容的管理，发现含有网络暴力信息的网络视听节目、网络表演等服务的， 应当及时删除信息或者停止提供相关服务；应当加强对网络直播、短视频等服务的内容审核，及时阻断含有网络暴力信息的网络直播，处置含有网络暴力信息的短视频。

第十八条 网络信息服务提供者应当加强对跟帖评论信息内容的管理，对以评论、回复、留言、弹幕、点赞等方式制作、复制、发布、传播网络暴力信息的，应当及时采取删除、屏蔽、关闭评论、停止提供相关服务等处置措施。

第十九条 网络信息服务提供者应当加强对网络论坛社区和网络群组的管理，禁止用户在版块、词条、超话、群组等环节制作、复制、发布、传播网络暴力信

息，禁止以匿名投稿、隔空喊话等方式创建含有网络暴力信息的论坛社区和群组账号。

网络论坛社区、网络群组的建立者和管理者应当履行管理责任， 发现用户制作、复制、发布、传播网络暴力信息的，应当依法依约采取限制发言、移出群组等管理措施。

第二十条 公众账号生产运营者应当建立健全发布推广、互动评论等全过程信息内容安全审核机制，发现账号跟帖评论等环节存在网络暴力信息的，应当及时采取举报、处置等措施。

第二十一条 对违反本规定第十条的用户，网络信息服务提供者应当依法依约采取警示、删除信息、限制账号功能、关闭账号等处置措施，并保存相关记录；对组织、煽动、多次发布网络暴力信息的， 网络信息服务提供者还应当依法依约采取列入黑名单、禁止重新注册等处置措施。

对借网络暴力事件实施营销炒作等行为的，除前款规定外，还应当依法依约采取清理订阅关注账号、暂停营利权限等处置措施。

第二十二条 对组织、煽动制作、复制、发布、传播网络暴力信息的网络信息内容多渠道分发服务机构，网络信息服务提供者应当依法依约对该机构及其管理的账号采取警示、暂停营利权限、限制提供服务、入驻清退等处置措施。

第五章 保护机制

第二十三条 网络信息服务提供者应当建立健全网络暴力信息防护功能，提供便利用户设置屏蔽陌生用户或者特定用户、本人发布信息可见范围、禁止转载或者评论本人发布信息等网络暴力信息防护选项。

网络信息服务提供者应当完善私信规则，提供便利用户设置仅接收好友私信或者拒绝接收所有私信等网络暴力信息防护选项，鼓励提供智能屏蔽私信或者自定义私信屏蔽词等功能。

第二十四条 网络信息服务提供者发现用户面临网络暴力信息风险的，应当及时通过显著方式提示用户，告知用户可以采取的防护措施。

网络信息服务提供者发现网络暴力信息风险涉及以下情形的，还应当为用户提供网络暴力信息防护指导和保护救助服务，协助启动防护措施，并向网信、公安等有关部门报告：

(一)网络暴力信息侵害未成年人、老年人、残疾人等用户合法权益的;

(二)网络暴力信息侵犯用户个人隐私的;

(三)若不及时采取措施,可能造成用户人身、财产损害等严重后果的其他情形。

第二十五条 网络信息服务提供者发现、处置网络暴力信息的,应当及时保存信息内容、浏览评论转发数量等数据。网络信息服务提供者应当向用户提供网络暴力信息快捷取证等功能,依法依约为用户维权提供便利。

公安、网信等有关部门依法调取证据的, 网络信息服务提供者应当及时提供必要的技术支持和协助。

第二十六条 网络信息服务提供者应当自觉接受社会监督,优化投诉、举报程序,在服务显著位置设置专门的网络暴力信息快捷投诉、举报入口, 公布处理流程,及时受理、处理公众投诉、举报并反馈处理结果。

网络信息服务提供者应当结合投诉、举报内容以及相关证明材料及时研判。对属于网络暴力信息的投诉、举报, 应当依法处理并反馈结果;对因证明材料不充分难以准确判断的,应当及时告知用户补充证明材料;对不属于网络暴力信息的投诉、举报, 应当按照其他类型投诉、举报的受理要求予以处理并反馈结果。

第二十七条 网络信息服务提供者应当优先处理涉未成年人网络暴力信息的投诉、举报。发现涉及侵害未成年人用户合法权益的网络暴力信息风险的, 应当按照法律法规和本规定要求及时采取措施,提供相应保护救助服务,并向有关部门报告。

网络信息服务提供者应当设置便利未成年人及其监护人行使通知删除网络暴力信息权利的功能、渠道, 接到相关通知后,应当及时采取删除、屏蔽、断开链接等必要的措施,防止信息扩散。

第六章 监督管理和法律责任

第二十八条 网信部门会同公安、文化和旅游、广播电视等有关部门依法对网络信息服务提供者的网络暴力信息治理情况进行监督检查。

网络信息服务提供者对网信部门和有关部门依法实施的监督检查应当予以配合。

第二十九条 网信部门会同公安、文化和旅游、广播电视等有关部门建立健

全信息共享、会商通报、取证调证、案件督办等工作机制， 协同治理网络暴力信息。

公安机关对于网信、文化和旅游、广播电视等部门移送的涉网络暴力信息违法犯罪线索，应当及时进行审查，并对符合立案条件的及时立案侦查、调查。

第三十条 违反本规定的，依照《中华人民共和国网络安全法》、《中华人民共和国个人信息保护法》、《中华人民共和国治安管理处罚法》、《互联网信息服务管理办法》等法律、行政法规的规定予以处罚。

法律、行政法规没有规定的， 由网信、公安、文化和旅游、广播电视等有关部门依据职责给予警告、通报批评， 责令限期改正，可以并处一万元以上十万元以下罚款；涉及危害公民生命健康安全且有严重后果的，并处十万元以上二十万元以下罚款。

对组织、煽动制作、复制、发布、传播网络暴力信息或者利用网络暴力事件实施恶意营销炒作等行为的组织和个人，应当依法从重处罚。

第三十一条 违反本规定，给他人造成损害的，依法承担民事责任；构成违反治安管理行为的，依法给予治安管理处罚；构成犯罪的，依法追究刑事责任。

第七章 附 则

第三十二条 本规定所称网络暴力信息，是指通过网络以文本、图像、音频、视频等形式对个人集中发布的，含有侮辱谩骂、造谣诽谤、煽动仇恨、威逼胁迫、侵犯隐私，以及影响身心健康的指责嘲讽、贬低歧视等内容的违法和不良信息。

第三十三条 依法通过网络检举、揭发他人违法犯罪，或者依法实施舆论监督的，不适用本规定。

第三十四条 本规定自 2024 年 8 月 1 日起施行。

互联网新闻信息服务管理规定

国家互联网信息办公室令第 1 号

《互联网新闻信息服务管理规定》已经国家互联网信息办公室室务会议审议通过，现予公布，自 2017 年 6 月 1 日起施行。

主任 徐麟

2017 年 5 月 2 日

互联网新闻信息服务管理规定

第一章 总 则

第一条 为加强互联网信息内容管理，促进互联网新闻信息服务健康有序发展，根据《中华人民共和国网络安全法》《互联网信息服务管理办法》《国务院关于授权国家互联网信息办公室负责互联网信息内容管理工作的通知》，制定本规定。

第二条 在中华人民共和国境内提供互联网新闻信息服务，适用本规定。

本规定所称新闻信息，包括有关政治、经济、军事、外交等社会公共事务的报道、评论，以及有关社会突发事件的报道、评论。

第三条 提供互联网新闻信息服务，应当遵守宪法、法律和行政法规，坚持为人民服务、为社会主义服务的方向，坚持正确舆论导向，发挥舆论监督作用，促进形成积极健康、向上向善的网络文化，维护国家利益和公共利益。

第四条 国家互联网信息办公室负责全国互联网新闻信息服务的监督管理执法工作。地方互联网信息办公室依据职责负责本行政区域内互联网新闻信息服务的监督管理执法工作。

第二章 许可

第五条 通过互联网站、应用程序、论坛、博客、微博客、公众账号、即时通信工具、网络直播等形式向社会公众提供互联网新闻信息服务， 应当取得互联网新闻信息服务许可，禁止未经许可或超越许可范围开展互联网新闻信息服务活动。

前款所称互联网新闻信息服务，包括互联网新闻信息采编发布服务、转载服务、传播平台服务。

第六条 申请互联网新闻信息服务许可，应当具备下列条件：

(一)在中华人民共和国境内依法设立的法人；

(二)主要负责人、总编辑是中国公民；

(三)有与服务相适应的专职新闻编辑人员、内容审核人员和技术保障人员；

(四)有健全的互联网新闻信息服务管理制度；

(五)有健全的信息安全管理制度和安全可控的技术保障措施；

(六)有与服务相适应的场所、设施和资金。

申请互联网新闻信息采编发布服务许可的，应当是新闻单位(含其控股的单

位)或新闻宣传部门主管的单位。

符合条件的互联网新闻信息服务提供者实行特殊管理股制度，具体实施办法由国家互联网信息办公室另行制定。

提供互联网新闻信息服务，还应当依法向电信主管部门办理互联网信息服务许可或备案手续。

第七条 任何组织不得设立中外合资经营、中外合作经营和外资经营的互联网新闻信息服务单位。

互联网新闻信息服务单位与境内外中外合资经营、中外合作经营和外资经营的企业进行涉及互联网新闻信息服务业务的合作，应当报经国家互联网信息办公室进行安全评估。

第八条 互联网新闻信息服务提供者的采编业务和经营业务应当分开，非公有资本不得介入互联网新闻信息采编业务。

第九条 申请互联网新闻信息服务许可，申请主体为中央新闻单位(含其控股的单位)或中央新闻宣传部门主管的单位的， 由国家互联网信息办公室受理和决定；申请主体为地方新闻单位(含其控股的单位)或地方新闻宣传部门主管的单位的，由省、自治区、直辖市互联网信息办公室受理和决定；申请主体为其他单位的，经所在地省、自治区、直辖市互联网信息办公室受理和初审后， 由国家互联网信息办公室决定。

国家或省、自治区、直辖市互联网信息办公室决定批准的， 核发《互联网新闻信息服务许可证》。《互联网新闻信息服务许可证》有效期为三年。有效期届满，需继续从事互联网新闻信息服务活动的，应当于有效期届满三十日前申请续办。

省、自治区、直辖市互联网信息办公室应当定期向国家互联网信息办公室报告许可受理和决定情况。

第十条 申请互联网新闻信息服务许可，应当提交下列材料：

(一)主要负责人、总编辑为中国公民的证明；

(二)专职新闻编辑人员、内容审核人员和技术保障人员的资质情况；

(三)互联网新闻信息服务管理制度；

(四)信息安全管理制度和技术保障措施；

(五)互联网新闻信息服务安全评估报告；

(六)法人资格、场所、资金和股权结构等证明;

(七)法律法规规定的其他材料。

第三章 运行

第十一条 互联网新闻信息服务提供者应当设立总编辑，总编辑对互联网新闻信息内容负总责。总编辑人选应当具有相关从业经验， 符合相关条件，并报国家或省、自治区、直辖市互联网信息办公室备案。

互联网新闻信息服务相关从业人员应当依法取得相应资质，接受专业培训、考核。互联网新闻信息服务相关从业人员从事新闻采编活动， 应当具备新闻采编人员职业资格，持有国家新闻出版广电总局统一颁发的新闻记者证。

第十二条 互联网新闻信息服务提供者应当健全信息发布审核、公共信息巡查、应急处置等信息安全管理制度，具有安全可控的技术保障措施。

第十三条 互联网新闻信息服务提供者为用户提供互联网新闻信息传播平台服务，应当按照《中华人民共和国网络安全法》的规定， 要求用户提供真实身份信息。用户不提供真实身份信息的， 互联网新闻信息服务提供者不得为其提供相关服务。

互联网新闻信息服务提供者对用户身份信息和日志信息负有保密的义务，不得泄露、篡改、毁损，不得出售或非法向他人提供。

互联网新闻信息服务提供者及其从业人员不得通过采编、发布、转载、删除新闻信息，干预新闻信息呈现或搜索结果等手段谋取不正当利益。

第十四条 互联网新闻信息服务提供者提供互联网新闻信息传播平台服务，应当与在其平台上注册的用户签订协议，明确双方权利义务。

对用户开设公众账号的，互联网新闻信息服务提供者应当审核其账号信息、服务资质、服务范围等信息， 并向所在地省、自治区、直辖市互联网信息办公室分类备案。

第十五条 互联网新闻信息服务提供者转载新闻信息，应当转载中央新闻单位或省、自治区、直辖市直属新闻单位等国家规定范围内的单位发布的新闻信息，注明新闻信息来源、原作者、原标题、编辑真实姓名等， 不得歪曲、篡改标题原意和新闻信息内容，并保证新闻信息来源可追溯。

互联网新闻信息服务提供者转载新闻信息，应当遵守著作权相关法律法规的

规定，保护著作权人的合法权益。

第十六条 互联网新闻信息服务提供者和用户不得制作、复制、发布、传播法律、行政法规禁止的信息内容。

互联网新闻信息服务提供者提供服务过程中发现含有违反本规定第三条或前款规定内容的，应当依法立即停止传输该信息、采取消除等处置措施， 保存有关记录，并向有关主管部门报告。

第十七条 互联网新闻信息服务提供者变更主要负责人、总编辑、主管单位、股权结构等影响许可条件的重大事项，应当向原许可机关办理变更手续。

互联网新闻信息服务提供者应用新技术、调整增设具有新闻舆论属性或社会动员能力的应用功能，应当报国家或省、自治区、直辖市互联网信息办公室进行互联网新闻信息服务安全评估。

第十八条 互联网新闻信息服务提供者应当在明显位置明示互联网新闻信息服务许可证编号。

互联网新闻信息服务提供者应当自觉接受社会监督，建立社会投诉举报渠道，设置便捷的投诉举报入口，及时处理公众投诉举报。

第四章 监督检查

第十九条 国家和地方互联网信息办公室应当建立日常检查和定期检查相结合的监督管理制度，依法对互联网新闻信息服务活动实施监督检查，有关单位、个人应当予以配合。

国家和地方互联网信息办公室应当健全执法人员资格管理制度。执法人员开展执法活动，应当依法出示执法证件。

第二十条 任何组织和个人发现互联网新闻信息服务提供者有违反本规定行为的，可以向国家和地方互联网信息办公室举报。

国家和地方互联网信息办公室应当向社会公开举报受理方式，收到举报后，应当依法予以处置。互联网新闻信息服务提供者应当予以配合。

第二十一条 国家和地方互联网信息办公室应当建立互联网新闻信息服务网络信用档案，建立失信黑名单制度和约谈制度。

国家互联网信息办公室会同国务院电信、公安、新闻出版广电等部门建立信息共享机制，加强工作沟通和协作配合，依法开展联合执法等专项监督检查活动。

第五章 法律责任

第二十二条 违反本规定第五条规定，未经许可或超越许可范围开展互联网新闻信息服务活动的，由国家和省、自治区、直辖市互联网信息办公室依据职责责令停止相关服务活动，处一万元以上三万元以下罚款。

第二十三条 互联网新闻信息服务提供者运行过程中不再符合许可条件的，由原许可机关责令限期改正；逾期仍不符合许可条件的，暂停新闻信息更新；《互联网新闻信息服务许可证》有效期届满仍不符合许可条件的，不予换发许可证。

第二十四条 互联网新闻信息服务提供者违反本规定第七条第二款、第八条、第十一条、第十二条、第十三条第三款、第十四条、第十五条第一款、第十七条、第十八条规定的，由国家和地方互联网信息办公室依据职责给予警告，责令限期改正；情节严重或拒不改正的，暂停新闻信息更新，处五千元以上三万元以下罚款；构成犯罪的，依法追究刑事责任。

第二十五条 互联网新闻信息服务提供者违反本规定第三条、第十六条第一款、第十九条第一款、第二十条第二款规定的， 由国家和地方互联网信息办公室依据职责给予警告，责令限期改正；情节严重或拒不改正的，暂停新闻信息更新，处二万元以上三万元以下罚款；构成犯罪的，依法追究刑事责任。

第二十六条 互联网新闻信息服务提供者违反本规定第十三条第一款、第十六条第二款规定的，由国家和地方互联网信息办公室根据《中华人民共和国网络安全法》的规定予以处理。

第六章 附 则

第二十七条 本规定所称新闻单位，是指依法设立的报刊社、广播电台、电视台、通讯社和新闻电影制片厂。

第二十八条 违反本规定，同时违反互联网信息服务管理规定的，由国家和地方互联网信息办公室根据本规定处理后，转由电信主管部门依法处置。

国家对互联网视听节目服务、网络出版服务等另有规定的， 应当同时符合其规定。

第二十九条 本规定自 2017 年 6 月 1 日起施行。本规定施行之前颁布的有关规定与本规定不一致的，按照本规定执行。

区块链信息服务管理规定

国家互联网信息办公室令第 3 号

《区块链信息服务管理规定》已经国家互联网信息办公室室务会议审议通过，现予公布，自 2019 年 2 月 15 日起施行。

主任 庄荣文

2019 年 1 月 10 日

区块链信息服务管理规定

第一条 为了规范区块链信息服务活动，维护国家安全和社会公共利益，保护公民、法人和其他组织的合法权益，促进区块链技术及相关服务的健康发展，根据《中华人民共和国网络安全法》《互联网信息服务管理办法》和《国务院关于授权国家互联网信息办公室负责互联网信息内容管理工作的通知》，制定本规定。

第二条 在中华人民共和国境内从事区块链信息服务，应当遵守本规定。法律、行政法规另有规定的，遵照其规定。

本规定所称区块链信息服务，是指基于区块链技术或者系统，通过互联网站、应用程序等形式，向社会公众提供信息服务。

本规定所称区块链信息服务提供者，是指向社会公众提供区块链信息服务的主体或者节点，以及为区块链信息服务的主体提供技术支持的机构或者组织；本规定所称区块链信息服务使用者，是指使用区块链信息服务的组织或者个人。

第三条 国家互联网信息办公室依据职责负责全国区块链信息服务的监督管理执法工作。省、自治区、直辖市互联网信息办公室依据职责负责本行政区域内区块链信息服务的监督管理执法工作。

第四条 鼓励区块链行业组织加强行业自律，建立健全行业自律制度和行业准则，指导区块链信息服务提供者建立健全服务规范，推动行业信用评价体系建设，督促区块链信息服务提供者依法提供服务、接受社会监督， 提高区块链信息服务从业人员的职业素养，促进行业健康有序发展。

第五条 区块链信息服务提供者应当落实信息内容安全管理责任，建立健全用户注册、信息审核、应急处置、安全防护等管理制度。

第六条 区块链信息服务提供者应当具备与其服务相适应的技术条件，对于法律、行政法规禁止的信息内容， 应当具备对其发布、记录、存储、传播的即时

和应急处置能力，技术方案应当符合国家相关标准规范。

第七条 区块链信息服务提供者应当制定并公开管理规则和平台公约，与区块链信息服务使用者签订服务协议，明确双方权利义务，要求其承诺遵守法律规定和平台公约。

第八条 区块链信息服务提供者应当按照《中华人民共和国网络安全法》的规定，对区块链信息服务使用者进行基于组织机构代码、身份证件号码或者移动电话号码等方式的真实身份信息认证。用户不进行真实身份信息认证的， 区块链信息服务提供者不得为其提供相关服务。

第九条 区块链信息服务提供者开发上线新产品、新应用、新功能的，应当按照有关规定报国家和省、自治区、直辖市互联网信息办公室进行安全评估。

第十条 区块链信息服务提供者和使用者不得利用区块链信息服务从事危害国家安全、扰乱社会秩序、侵犯他人合法权益等法律、行政法规禁止的活动， 不得利用区块链信息服务制作、复制、发布、传播法律、行政法规禁止的信息内容。

第十一条 区块链信息服务提供者应当在提供服务之日起十个工作日内通过国家互联网信息办公室区块链信息服务备案管理系统填报服务提供者的名称、服务类别、服务形式、应用领域、服务器地址等信息，履行备案手续。

区块链信息服务提供者变更服务项目、平台网址等事项的， 应当在变更之日起五个工作日内办理变更手续。

区块链信息服务提供者终止服务的，应当在终止服务三十个工作日前办理注销手续，并作出妥善安排。

第十二条 国家和省、自治区、直辖市互联网信息办公室收到备案人提交的备案材料后，材料齐全的，应当在二十个工作日内予以备案，发放备案编号，并通过国家互联网信息办公室区块链信息服务备案管理系统向社会公布备案信息；材料不齐全的，不予备案，在二十个工作日内通知备案人并说明理由。

第十三条 完成备案的区块链信息服务提供者应当在其对外提供服务的互联网站、应用程序等的显著位置标明其备案编号。

第十四条 国家和省、自治区、直辖市互联网信息办公室对区块链信息服务备案信息实行定期查验，区块链信息服务提供者应当在规定时间内登录区块链信息服务备案管理系统，提供相关信息。

第十五条 区块链信息服务提供者提供的区块链信息服务存在信息安全隐患的，应当进行整改，符合法律、行政法规等相关规定和国家相关标准规范后方可继续提供信息服务。

第十六条 区块链信息服务提供者应当对违反法律、行政法规规定和服务协议的区块链信息服务使用者，依法依约采取警示、限制功能、关闭账号等处置措施，对违法信息内容及时采取相应的处理措施，防止信息扩散，保存有关记录，并向有关主管部门报告。

第十七条 区块链信息服务提供者应当记录区块链信息服务使用者发布内容和日志等信息，记录备份应当保存不少于六个月，并在相关执法部门依法查询时予以提供。

第十八条 区块链信息服务提供者应当配合网信部门依法实施的监督检查，并提供必要的技术支持和协助。

区块链信息服务提供者应当接受社会监督，设置便捷的投诉举报入口，及时处理公众投诉举报。

第十九条 区块链信息服务提供者违反本规定第五条、第六条、第七条、第九条、第十一条第二款、第十三条、第十五条、第十七条、第十八条规定的，由国家和省、自治区、直辖市互联网信息办公室依据职责给予警告，责令限期改正，改正前应当暂停相关业务；拒不改正或者情节严重的，并处五千元以上三万元以下罚款；构成犯罪的，依法追究刑事责任。

第二十条 区块链信息服务提供者违反本规定第八条、第十六条规定的，由国家和省、自治区、直辖市互联网信息办公室依据职责， 按照《中华人民共和国网络安全法》的规定予以处理。

第二十一条 区块链信息服务提供者违反本规定第十条的规定，制作、复制、发布、传播法律、行政法规禁止的信息内容的， 由国家和省、自治区、直辖市互联网信息办公室依据职责给予警告，责令限期改正，改正前应当暂停相关业务；拒不改正或者情节严重的，并处二万元以上三万元以下罚款；构成犯罪的，依法追究刑事责任。

区块链信息服务使用者违反本规定第十条的规定，制作、复制、发布、传播法律、行政法规禁止的信息内容的， 由国家和省、自治区、直辖市互联网信息办

公室依照有关法律、行政法规的规定予以处理。

第二十二条 区块链信息服务提供者违反本规定第十一条第一款的规定，未按照本规定履行备案手续或者填报虚假备案信息的，由国家和省、自治区、直辖市互联网信息办公室依据职责责令限期改正；拒不改正或者情节严重的，给予警告，并处一万元以上三万元以下罚款。

第二十三条 在本规定公布前从事区块链信息服务的，应当自本规定生效之日起二十个工作日内依照本规定补办有关手续。

第二十四条 本规定自 2019 年 2 月 15 日起施行。

儿童个人信息网络保护规定

国家互联网信息办公室令第 4 号

《儿童个人信息网络保护规定》已经国家互联网信息办公室室务会议审议通过，现予公布，自 2019 年 10 月 1 日起施行。

主任 庄荣文

2019 年 8 月 22 日

儿童个人信息网络保护规定

第一条 为了保护儿童个人信息安全，促进儿童健康成长，根据《中华人民共和国网络安全法》《中华人民共和国未成年人保护法》等法律法规，制定本规定。

第二条 本规定所称儿童，是指不满十四周岁的未成年人。

第三条 在中华人民共和国境内通过网络从事收集、存储、使用、转移、披露儿童个人信息等活动，适用本规定。

第四条 任何组织和个人不得制作、发布、传播侵害儿童个人信息安全的信息。

第五条 儿童监护人应当正确履行监护职责，教育引导儿童增强个人信息保护意识和能力，保护儿童个人信息安全。

第六条 鼓励互联网行业组织指导推动网络运营者制定儿童个人信息保护的行业规范、行为准则等，加强行业自律，履行社会责任。

第七条 网络运营者收集、存储、使用、转移、披露儿童个人信息的，应当遵循正当必要、知情同意、目的明确、安全保障、依法利用的原则。

第八条　网络运营者应当设置专门的儿童个人信息保护规则和用户协议，并指定专人负责儿童个人信息保护。

第九条　网络运营者收集、使用、转移、披露儿童个人信息的，应当以显著、清晰的方式告知儿童监护人，并应当征得儿童监护人的同意。

第十条　网络运营者征得同意时，应当同时提供拒绝选项，并明确告知以下事项：

(一)收集、存储、使用、转移、披露儿童个人信息的目的、方式和范围；

(二)儿童个人信息存储的地点、期限和到期后的处理方式；

(三)儿童个人信息的安全保障措施；

(四)拒绝的后果；

(五)投诉、举报的渠道和方式；

(六)更正、删除儿童个人信息的途径和方法；

(七)其他应当告知的事项。

前款规定的告知事项发生实质性变化的，应当再次征得儿童监护人的同意。

第十一条　网络运营者不得收集与其提供的服务无关的儿童个人信息，不得违反法律、行政法规的规定和双方的约定收集儿童个人信息。

第十二条　网络运营者存储儿童个人信息，不得超过实现其收集、使用目的所必需的期限。

第十三条　网络运营者应当采取加密等措施存储儿童个人信息，确保信息安全。

第十四条　网络运营者使用儿童个人信息，不得违反法律、行政法规的规定和双方约定的目的、范围。因业务需要，确需超出约定的目的、范围使用的，应当再次征得儿童监护人的同意。

第十五条　网络运营者对其工作人员应当以最小授权为原则，严格设定信息访问权限，控制儿童个人信息知悉范围。工作人员访问儿童个人信息的，应当经过儿童个人信息保护负责人或者其授权的管理人员审批，记录访问情况，并采取技术措施，避免违法复制、下载儿童个人信息。

第十六条　网络运营者委托第三方处理儿童个人信息的，应当对受委托方及委托行为等进行安全评估，签署委托协议，明确双方责任、处理事项、处理期限、

处理性质和目的等，委托行为不得超出授权范围。

前款规定的受委托方，应当履行以下义务：

(一)按照法律、行政法规的规定和网络运营者的要求处理儿童个人信息；

(二)协助网络运营者回应儿童监护人提出的申请；

(三)采取措施保障信息安全，并在发生儿童个人信息泄露安全事件时，及时向网络运营者反馈；

(四)委托关系解除时及时删除儿童个人信息；

(五)不得转委托；

(六)其他依法应当履行的儿童个人信息保护义务。

第十七条 网络运营者向第三方转移儿童个人信息的，应当自行或者委托第三方机构进行安全评估。

第十八条 网络运营者不得披露儿童个人信息，但法律、行政法规规定应当披露或者根据与儿童监护人的约定可以披露的除外。

第十九条 儿童或者其监护人发现网络运营者收集、存储、使用、披露的儿童个人信息有错误的，有权要求网络运营者予以更正。网络运营者应当及时采取措施予以更正。

第二十条 儿童或者其监护人要求网络运营者删除其收集、存储、使用、披露的儿童个人信息的，网络运营者应当及时采取措施予以删除，包括但不限于以下情形：

(一)网络运营者违反法律、行政法规的规定或者双方的约定收集、存储、使用、转移、披露儿童个人信息的；

(二)超出目的范围或者必要期限收集、存储、使用、转移、披露儿童个人信息的；

(三)儿童监护人撤回同意的；

(四)儿童或者其监护人通过注销等方式终止使用产品或者服务的。

第二十一条 网络运营者发现儿童个人信息发生或者可能发生泄露、毁损、丢失的，应当立即启动应急预案，采取补救措施；造成或者可能造成严重后果的，应当立即向有关主管部门报告，并将事件相关情况以邮件、信函、电话、推送通知等方式告知受影响的儿童及其监护人，难以逐一告知的，应当采取合理、有效

的方式发布相关警示信息。

第二十二条 网络运营者应当对网信部门和其他有关部门依法开展的监督检查予以配合。

第二十三条 网络运营者停止运营产品或者服务的，应当立即停止收集儿童个人信息的活动，删除其持有的儿童个人信息，并将停止运营的通知及时告知儿童监护人。

第二十四条 任何组织和个人发现有违反本规定行为的，可以向网信部门和其他有关部门举报。

网信部门和其他有关部门收到相关举报的，应当依据职责及时进行处理。

第二十五条 网络运营者落实儿童个人信息安全管理责任不到位，存在较大安全风险或者发生安全事件的，由网信部门依据职责进行约谈，网络运营者应当及时采取措施进行整改，消除隐患。

第二十六条 违反本规定的，由网信部门和其他有关部门依据职责，根据《中华人民共和国网络安全法》《互联网信息服务管理办法》等相关法律法规规定处理；构成犯罪的，依法追究刑事责任。

第二十七条 违反本规定被追究法律责任的，依照有关法律、行政法规的规定记入信用档案，并予以公示。

第二十八条 通过计算机信息系统自动留存处理信息且无法识别所留存处理的信息属于儿童个人信息的，依照其他有关规定执行。

第二十九条 本规定自 2019 年 10 月 1 日起施行。

网络信息内容生态治理规定

国家互联网信息办公室令第 5 号

《网络信息内容生态治理规定》已经国家互联网信息办公室室务会议审议通过，现予公布，自 2020 年 3 月 1 日起施行。

主任 庄荣文

2019 年 12 月 15 日

网络信息内容生态治理规定

第一章 总 则

第一条 为了营造良好网络生态，保障公民、法人和其他组织的合法权益，

维护国家安全和公共利益，根据《中华人民共和国国家安全法》《中华人民共和国网络安全法》《互联网信息服务管理办法》等法律、行政法规，制定本规定。

第二条 中华人民共和国境内的网络信息内容生态治理活动，适用本规定。

本规定所称网络信息内容生态治理，是指政府、企业、社会、网民等主体，以培育和践行社会主义核心价值观为根本，以网络信息内容为主要治理对象，以建立健全网络综合治理体系、营造清朗的网络空间、建设良好的网络生态为目标，开展的弘扬正能量、处置违法和不良信息等相关活动。

第三条 国家网信部门负责统筹协调全国网络信息内容生态治理和相关监督管理工作，各有关主管部门依据各自职责做好网络信息内容生态治理工作。

地方网信部门负责统筹协调本行政区域内网络信息内容生态治理和相关监督管理工作，地方各有关主管部门依据各自职责做好本行政区域内网络信息内容生态治理工作。

第二章 网络信息内容生产者

第四条 网络信息内容生产者应当遵守法律法规，遵循公序良俗，不得损害国家利益、公共利益和他人合法权益。

第五条 鼓励网络信息内容生产者制作、复制、发布含有下列内容的信息：

(一)宣传习近平新时代中国特色社会主义思想，全面准确生动解读中国特色社会主义道路、理论、制度、文化的；

(二)宣传党的理论路线方针政策和中央重大决策部署的；

(三)展示经济社会发展亮点，反映人民群众伟大奋斗和火热生活的；

(四)弘扬社会主义核心价值观，宣传优秀道德文化和时代精神，充分展现中华民族昂扬向上精神风貌的；

(五)有效回应社会关切，解疑释惑，析事明理，有助于引导群众形成共识的；

(六)有助于提高中华文化国际影响力， 向世界展现真实立体全面的中国的；

(七)其他讲品味讲格调讲责任、讴歌真善美、促进团结稳定等的内容。

第六条 网络信息内容生产者不得制作、复制、发布含有下列内容的违法信息：

(一)反对宪法所确定的基本原则的；

(二)危害国家安全，泄露国家秘密，颠覆国家政权，破坏国家统一的；

(三)损害国家荣誉和利益的;

(四)歪曲、丑化、亵渎、否定英雄烈士事迹和精神， 以侮辱、诽谤或者其他方式侵害英雄烈士的姓名、肖像、名誉、荣誉的;

(五)宣扬恐怖主义、极端主义或者煽动实施恐怖活动、极端主义活动的;

(六)煽动民族仇恨、民族歧视，破坏民族团结的;

(七)破坏国家宗教政策，宣扬邪教和封建迷信的;

(八)散布谣言，扰乱经济秩序和社会秩序的;

(九)散布淫秽、色情、赌博、暴力、凶杀、恐怖或者教唆犯罪的;

(十)侮辱或者诽谤他人，侵害他人名誉、隐私和其他合法权益的;

(十一)法律、行政法规禁止的其他内容。

第七条 网络信息内容生产者应当采取措施，防范和抵制制作、复制、发布含有下列内容的不良信息:

(一)使用夸张标题，内容与标题严重不符的;

(二)炒作绯闻、丑闻、劣迹等的;

(三)不当评述自然灾害、重大事故等灾难的;

(四)带有性暗示、性挑逗等易使人产生性联想的;

(五)展现血腥、惊悚、残忍等致人身心不适的;

(六)煽动人群歧视、地域歧视等的;

(七)宣扬低俗、庸俗、媚俗内容的;

(八)可能引发未成年人模仿不安全行为和违反社会公德行为、诱导未成年人不良嗜好等的;

(九)其他对网络生态造成不良影响的内容。

第三章 网络信息内容服务平台

第八条 网络信息内容服务平台应当履行信息内容管理主体责任，加强本平台网络信息内容生态治理，培育积极健康、向上向善的网络文化。

第九条 网络信息内容服务平台应当建立网络信息内容生态治理机制，制定本平台网络信息内容生态治理细则，健全用户注册、账号管理、信息发布审核、跟帖评论审核、版面页面生态管理、实时巡查、应急处置和网络谣言、黑色产业链信息处置等制度。

网络信息内容服务平台应当设立网络信息内容生态治理负责人，配备与业务范围和服务规模相适应的专业人员，加强培训考核，提升从业人员素质。

第十条 网络信息内容服务平台不得传播本规定第六条规定的信息，应当防范和抵制传播本规定第七条规定的信息。

网络信息内容服务平台应当加强信息内容的管理，发现本规定第六条、第七条规定的信息的，应当依法立即采取处置措施，保存有关记录，并向有关主管部门报告。

第十一条 鼓励网络信息内容服务平台坚持主流价值导向，优化信息推荐机制，加强版面页面生态管理，在下列重点环节(包括服务类型、位置版块等)积极呈现本规定第五条规定的信息：

(一)互联网新闻信息服务首页首屏、弹窗和重要新闻信息内容页面等；

(二)互联网用户公众账号信息服务精选、热搜等；

(三)博客、微博客信息服务热门推荐、榜单类、弹窗及基于地理位置的信息服务版块等；

(四)互联网信息搜索服务热搜词、热搜图及默认搜索等；

(五)互联网论坛社区服务首页首屏、榜单类、弹窗等；

(六)互联网音视频服务首页首屏、发现、精选、榜单类、弹窗等；

(七)互联网网址导航服务、浏览器服务、输入法服务首页首屏、榜单类、皮肤、联想词、弹窗等；

(八)数字阅读、网络游戏、网络动漫服务首页首屏、精选、榜单类、弹窗等；

(九)生活服务、知识服务平台首页首屏、热门推荐、弹窗等；

(十)电子商务平台首页首屏、推荐区等；

(十一)移动应用商店、移动智能终端预置应用软件和内置信息内容服务首屏、推荐区等；

(十二)专门以未成年人为服务对象的网络信息内容专栏、专区和产品等；

(十三)其他处于产品或者服务醒目位置、易引起网络信息内容服务使用者关注的重点环节。

网络信息内容服务平台不得在以上重点环节呈现本规定第七条规定的信息。

第十二条 网络信息内容服务平台采用个性化算法推荐技术推送信息的，应

当设置符合本规定第十条、第十一条规定要求的推荐模型，建立健全人工干预和用户自主选择机制。

第十三条 鼓励网络信息内容服务平台开发适合未成年人使用的模式，提供适合未成年人使用的网络产品和服务，便利未成年人获取有益身心健康的信息。

第十四条 网络信息内容服务平台应当加强对本平台设置的广告位和在本平台展示的广告内容的审核巡查，对发布违法广告的，应当依法予以处理。

第十五条 网络信息内容服务平台应当制定并公开管理规则和平台公约，完善用户协议，明确用户相关权利义务，并依法依约履行相应管理职责。

网络信息内容服务平台应当建立用户账号信用管理制度，根据用户账号的信用情况提供相应服务。

第十六条 网络信息内容服务平台应当在显著位置设置便捷的投诉举报入口，公布投诉举报方式，及时受理处置公众投诉举报并反馈处理结果。

第十七条 网络信息内容服务平台应当编制网络信息内容生态治理工作年度报告，年度报告应当包括网络信息内容生态治理工作情况、网络信息内容生态治理负责人履职情况、社会评价情况等内容。

第四章 网络信息内容服务使用者

第十八条 网络信息内容服务使用者应当文明健康使用网络，按照法律法规的要求和用户协议约定，切实履行相应义务，在以发帖、回复、留言、弹幕等形式参与网络活动时，文明互动，理性表达，不得发布本规定第六条规定的信息，防范和抵制本规定第七条规定的信息。

第十九条 网络群组、论坛社区版块建立者和管理者应当履行群组、版块管理责任，依据法律法规、用户协议和平台公约等， 规范群组、版块内信息发布等行为。

第二十条 鼓励网络信息内容服务使用者积极参与网络信息内容生态治理，通过投诉、举报等方式对网上违法和不良信息进行监督，共同维护良好网络生态。

第二十一条 网络信息内容服务使用者和网络信息内容生产者、网络信息内容服务平台不得利用网络和相关信息技术实施侮辱、诽谤、威胁、散布谣言以及侵犯他人隐私等违法行为，损害他人合法权益。

第二十二条 网络信息内容服务使用者和网络信息内容生产者、网络信息内

容服务平台不得通过发布、删除信息以及其他干预信息呈现的手段侵害他人合法权益或者谋取非法利益。

第二十三条 网络信息内容服务使用者和网络信息内容生产者、网络信息内容服务平台不得利用深度学习、虚拟现实等新技术新应用从事法律、行政法规禁止的活动。

第二十四条 网络信息内容服务使用者和网络信息内容生产者、网络信息内容服务平台不得通过人工方式或者技术手段实施流量造假、流量劫持以及虚假注册账号、非法交易账号、操纵用户账号等行为，破坏网络生态秩序。

第二十五条 网络信息内容服务使用者和网络信息内容生产者、网络信息内容服务平台不得利用党旗、党徽、国旗、国徽、国歌等代表党和国家形象的标识及内容，或者借国家重大活动、重大纪念日和国家机关及其工作人员名义等， 违法违规开展网络商业营销活动。

第五章 网络行业组织

第二十六条 鼓励行业组织发挥服务指导和桥梁纽带作用，引导会员单位增强社会责任感，唱响主旋律，弘扬正能量，反对违法信息，防范和抵制不良信息。

第二十七条 鼓励行业组织建立完善行业自律机制，制定网络信息内容生态治理行业规范和自律公约，建立内容审核标准细则，指导会员单位建立健全服务规范、依法提供网络信息内容服务、接受社会监督。

第二十八条 鼓励行业组织开展网络信息内容生态治理教育培训和宣传引导工作，提升会员单位、从业人员治理能力， 增强全社会共同参与网络信息内容生态治理意识。

第二十九条 鼓励行业组织推动行业信用评价体系建设，依据章程建立行业评议等评价奖惩机制，加大对会员单位的激励和惩戒力度，强化会员单位的守信意识。

第六章 监督管理

第三十条 各级网信部门会同有关主管部门，建立健全信息共享、会商通报、联合执法、案件督办、信息公开等工作机制， 协同开展网络信息内容生态治理工作。

第三十一条 各级网信部门对网络信息内容服务平台履行信息内容管理主体

责任情况开展监督检查，对存在问题的平台开展专项督查。

网络信息内容服务平台对网信部门和有关主管部门依法实施的监督检查，应当予以配合。

第三十二条 各级网信部门建立网络信息内容服务平台违法违规行为台账管理制度，并依法依规进行相应处理。

第三十三条 各级网信部门建立政府、企业、社会、网民等主体共同参与的监督评价机制，定期对本行政区域内网络信息内容服务平台生态治理情况进行评估。

第七章 法律责任

第三十四条 网络信息内容生产者违反本规定第六条规定的，网络信息内容服务平台应当依法依约采取警示整改、限制功能、暂停更新、关闭账号等处置措施，及时消除违法信息内容，保存记录并向有关主管部门报告。

第三十五条 网络信息内容服务平台违反本规定第十条、第三十一条第二款规定的，由网信等有关主管部门依据职责，按照《中华人民共和国网络安全法》《互联网信息服务管理办法》等法律、行政法规的规定予以处理。

第三十六条 网络信息内容服务平台违反本规定第十一条第二款规定的，由设区的市级以上网信部门依据职责进行约谈，给予警告，责令限期改正；拒不改正或者情节严重的，责令暂停信息更新，按照有关法律、行政法规的规定予以处理。

第三十七条 网络信息内容服务平台违反本规定第九条、第十二条、第十五条、第十六条、第十七条规定的，由设区的市级以上网信部门依据职责进行约谈，给予警告，责令限期改正；拒不改正或者情节严重的，责令暂停信息更新，按照有关法律、行政法规的规定予以处理。

第三十八条 违反本规定第十四条、第十八条、第十九条、第二十一条、第二十二条、第二十三条、第二十四条、第二十五条规定的， 由网信等有关主管部门依据职责，按照有关法律、行政法规的规定予以处理。

第三十九条 网信部门根据法律、行政法规和国家有关规定，会同有关主管部门建立健全网络信息内容服务严重失信联合惩戒机制，对严重违反本规定的网络信息内容服务平台、网络信息内容生产者和网络信息内容使用者依法依规实施

限制从事网络信息服务、网上行为限制、行业禁入等惩戒措施。

第四十条 违反本规定，给他人造成损害的，依法承担民事责任；构成犯罪的，依法追究刑事责任；尚不构成犯罪的，由有关主管部门依照有关法律、行政法规的规定予以处罚。

第八章 附 则

第四十一条 本规定所称网络信息内容生产者，是指制作、复制、发布网络信息内容的组织或者个人。

本规定所称网络信息内容服务平台，是指提供网络信息内容传播服务的网络信息服务提供者。

本规定所称网络信息内容服务使用者，是指使用网络信息内容服务的组织或者个人。

第四十二条 本规定自 2020 年 3 月 1 日起施行。

互联网用户账号信息管理规定

国家互联网信息办公室令第 10 号

《互联网用户账号信息管理规定》已经 2022 年 6 月 9 日国家互联网信息办公室 2022 年第 11 次室务会议审议通过，现予公布，自 2022 年 8 月 1 日起施行。

国家互联网信息办公室主任 庄荣文

2022 年 6 月 27 日

互联网用户账号信息管理规定

第一章 总 则

第一条 为了加强对互联网用户账号信息的管理，弘扬社会主义核心价值观，维护国家安全和社会公共利益，保护公民、法人和其他组织的合法权益，根据《中华人民共和国网络安全法》、《中华人民共和国个人信息保护法》、《互联网信息服务管理办法》等法律、行政法规，制定本规定。

第二条 互联网用户在中华人民共和国境内的互联网信息服务提供者注册、使用互联网用户账号信息及其管理工作，适用本规定。法律、行政法规另有规定的，依照其规定。

第三条 国家网信部门负责全国互联网用户账号信息的监督管理工作。

地方网信部门依据职责负责本行政区域内的互联网用户账号信息的监督管

理工作。

第四条 互联网用户注册、使用和互联网信息服务提供者管理互联网用户账号信息，应当遵守法律法规，遵循公序良俗，诚实信用，不得损害国家安全、社会公共利益或者他人合法权益。

第五条 鼓励相关行业组织加强行业自律，建立健全行业标准、行业准则和自律管理制度，督促指导互联网信息服务提供者制定完善服务规范、加强互联网用户账号信息安全管理、依法提供服务并接受社会监督。

第二章 账号信息注册和使用

第六条 互联网信息服务提供者应当依照法律、行政法规和国家有关规定，制定和公开互联网用户账号管理规则、平台公约，与互联网用户签订服务协议，明确账号信息注册、使用和管理相关权利义务。

第七条 互联网个人用户注册、使用账号信息，含有职业信息的，应当与个人真实职业信息相一致。

互联网机构用户注册、使用账号信息， 应当与机构名称、标识等相一致，与机构性质、经营范围和所属行业类型等相符合。

第八条 互联网用户注册、使用账号信息，不得有下列情形：

(一)违反《网络信息内容生态治理规定》第六条、第七条规定；

(二)假冒、仿冒、捏造政党、党政军机关、企事业单位、人民团体和社会组织的名称、标识等；

(三)假冒、仿冒、捏造国家(地区)、国际组织的名称、标识等；

(四)假冒、仿冒、捏造新闻网站、报刊社、广播电视机构、通讯社等新闻媒体的名称、标识等， 或者擅自使用“新闻”、“报道”等具有新闻属性的名称、标识等；

(五)假冒、仿冒、恶意关联国家行政区域、机构所在地、标志性建筑物等重要空间的地理名称、标识等；

(六)以损害公共利益或者谋取不正当利益等为目的，故意夹带二维码、网址、邮箱、联系方式等，或者使用同音、谐音、相近的文字、数字、符号和字母等；

(七)含有名不副实、夸大其词等可能使公众受骗或者产生误解的内容；

(八)含有法律、行政法规和国家有关规定禁止的其他内容。

第九条 互联网信息服务提供者为互联网用户提供信息发布、即时通讯等服务的，应当对申请注册相关账号信息的用户进行基于移动电话号码、身份证件号码或者统一社会信用代码等方式的真实身份信息认证。用户不提供真实身份信息，或者冒用组织机构、他人身份信息进行虚假注册的，不得为其提供相关服务。

第十条 互联网信息服务提供者应当对互联网用户在注册时提交的和使用中拟变更的账号信息进行核验，发现违反本规定第七条、第八条规定的， 应当不予注册或者变更账号信息。

对账号信息中含有“中国”、“中华”、“中央”、“全国”、“国家”等内容，或者含有党旗、党徽、国旗、国歌、国徽等党和国家象征和标志的，应当依照法律、行政法规和国家有关规定从严核验。

互联网信息服务提供者应当采取必要措施，防止被依法依约关闭的账号重新注册；对注册与其关联度高的账号信息，应当对相关信息从严核验。

第十一条 对于互联网用户申请注册提供互联网新闻信息服务、网络出版服务等依法需要取得行政许可的互联网信息服务的账号，或者申请注册从事经济、教育、医疗卫生、司法等领域信息内容生产的账号， 互联网信息服务提供者应当要求其提供服务资质、职业资格、专业背景等相关材料， 予以核验并在账号信息中加注专门标识。

第十二条 互联网信息服务提供者应当在互联网用户账号信息页面展示合理范围内的互联网用户账号的互联网协议(IP)地址归属地信息，便于公众为公共利益实施监督。

第十三条 互联网信息服务提供者应当在互联网用户公众账号信息页面，展示公众账号的运营主体、注册运营地址、内容生产类别、统一社会信用代码、有效联系方式、互联网协议(IP)地址归属地等信息。

第三章 账号信息管理

第十四条 互联网信息服务提供者应当履行互联网用户账号信息管理主体责任，配备与服务规模相适应的专业人员和技术能力，建立健全并严格落实真实身份信息认证、账号信息核验、信息内容安全、生态治理、应急处置、个人信息保护等管理制度。

第十五条 互联网信息服务提供者应当建立账号信息动态核验制度，适时核

验存量账号信息，发现不符合本规定要求的，应当暂停提供服务并通知用户限期改正；拒不改正的，应当终止提供服务。

第十六条 互联网信息服务提供者应当依法保护和处理互联网用户账号信息中的个人信息，并采取措施防止未经授权的访问以及个人信息泄露、篡改、丢失。

第十七条 互联网信息服务提供者发现互联网用户注册、使用账号信息违反法律、行政法规和本规定的， 应当依法依约采取警示提醒、限期改正、限制账号功能、暂停使用、关闭账号、禁止重新注册等处置措施， 保存有关记录，并及时向网信等有关主管部门报告。

第十八条 互联网信息服务提供者应当建立健全互联网用户账号信用管理体系，将账号信息相关信用评价作为账号信用管理的重要参考指标，并据以提供相应服务。

第十九条 互联网信息服务提供者应当在显著位置设置便捷的投诉举报入口，公布投诉举报方式，健全受理、甄别、处置、反馈等机制， 明确处理流程和反馈时限，及时处理用户和公众投诉举报。

第四章 监督检查与法律责任

第二十条 网信部门会同有关主管部门，建立健全信息共享、会商通报、联合执法、案件督办等工作机制，协同开展互联网用户账号信息监督管理工作。

第二十一条 网信部门依法对互联网信息服务提供者管理互联网用户注册、使用账号信息情况实施监督检查。互联网信息服务提供者应当予以配合， 并提供必要的技术、数据等支持和协助。

发现互联网信息服务提供者存在较大网络信息安全风险的，省级以上网信部门可以要求其采取暂停信息更新、用户账号注册或者其他相关服务等措施。互联网信息服务提供者应当按照要求采取措施，进行整改，消除隐患。

第二十二条 互联网信息服务提供者违反本规定的，依照有关法律、行政法规的规定处罚。法律、行政法规没有规定的， 由省级以上网信部门依据职责给予警告、通报批评， 责令限期改正，并可以处一万元以上十万元以下罚款。构成违反治安管理行为的，移交公安机关处理；构成犯罪的，移交司法机关处理。

第五章 附 则

第二十三条 本规定下列用语的含义是：

(一)互联网用户账号信息，是指互联网用户在互联网信息服务中注册、使用的名称、头像、封面、简介、签名、认证信息等用于标识用户账号的信息。

(二)互联网信息服务提供者，是指向用户提供互联网信息发布和应用平台服务，包括但不限于互联网新闻信息服务、网络出版服务、搜索引擎、即时通讯、交互式信息服务、网络直播、应用软件下载等互联网服务的主体。

第二十四条 本规定自 2022 年 8 月 1 日施行。本规定施行之前颁布的有关规定与本规定不一致的，按照本规定执行。

数据出境安全评估办法

国家互联网信息办公室令第 11 号

《数据出境安全评估办法》已经 2022 年 5 月 19 日国家互联网信息办公室 2022 年第 10 次室务会议审议通过，现予公布，自 2022 年 9 月 1 日起施行。

国家互联网信息办公室主任 庄荣文

2022 年 7 月 7 日

数据出境安全评估办法

第一条 为了规范数据出境活动，保护个人信息权益，维护国家安全和社会公共利益，促进数据跨境安全、自由流动， 根据《中华人民共和国网络安全法》、《中华人民共和国数据安全法》、《中华人民共和国个人信息保护法》等法律法规，制定本办法。

第二条 数据处理者向境外提供在中华人民共和国境内运营中收集和产生的重要数据和个人信息的安全评估，适用本办法。法律、行政法规另有规定的， 依照其规定。

第三条 数据出境安全评估坚持事前评估和持续监督相结合、风险自评估与安全评估相结合，防范数据出境安全风险，保障数据依法有序自由流动。

第四条 数据处理者向境外提供数据，有下列情形之一的，应当通过所在地省级网信部门向国家网信部门申报数据出境安全评估：

(一)数据处理者向境外提供重要数据；

(二)关键信息基础设施运营者和处理 100 万人以上个人信息的数据处理者向境外提供个人信息；

(三)自上年 1 月 1 日起累计向境外提供 10 万人个人信息或者 1 万人敏感个

人信息的数据处理者向境外提供个人信息；

(四)国家网信部门规定的其他需要申报数据出境安全评估的情形。

第五条 数据处理者在申报数据出境安全评估前，应当开展数据出境风险自评估，重点评估以下事项：

(一)数据出境和境外接收方处理数据的目的、范围、方式等的合法性、正当性、必要性；

(二)出境数据的规模、范围、种类、敏感程度，数据出境可能对国家安全、公共利益、个人或者组织合法权益带来的风险；

(三)境外接收方承诺承担的责任义务，以及履行责任义务的管理和技术措施、能力等能否保障出境数据的安全；

(四)数据出境中和出境后遭到篡改、破坏、泄露、丢失、转移或者被非法获取、非法利用等的风险，个人信息权益维护的渠道是否通畅等；

(五)与境外接收方拟订立的数据出境相关合同或者其他具有法律效力的文件等(以下统称法律文件)是否充分约定了数据安全保护责任义务；

(六)其他可能影响数据出境安全的事项。

第六条 申报数据出境安全评估，应当提交以下材料：

(一)申报书；

(二)数据出境风险自评估报告；

(三)数据处理者与境外接收方拟订立的法律文件；

(四)安全评估工作需要的其他材料。

第七条 省级网信部门应当自收到申报材料之日起 5 个工作日内完成完备性查验。申报材料齐全的， 将申报材料报送国家网信部门；申报材料不齐全的，应当退回数据处理者并一次性告知需要补充的材料。

国家网信部门应当自收到申报材料之日起 7 个工作日内，确定是否受理并书面通知数据处理者。

第八条 数据出境安全评估重点评估数据出境活动可能对国家安全、公共利益、个人或者组织合法权益带来的风险，主要包括以下事项：

(一)数据出境的目的、范围、方式等的合法性、正当性、必要性；

(二)境外接收方所在国家或者地区的数据安全保护政策法规和网络安全环

境对出境数据安全的影响；境外接收方的数据保护水平是否达到中华人民共和国法律、行政法规的规定和强制性国家标准的要求；

(三)出境数据的规模、范围、种类、敏感程度，出境中和出境后遭到篡改、破坏、泄露、丢失、转移或者被非法获取、非法利用等的风险；

(四)数据安全和个人信息权益是否能够得到充分有效保障；

(五)数据处理者与境外接收方拟订立的法律文件中是否充分约定了数据安全保护责任义务；

(六)遵守中国法律、行政法规、部门规章情况；

(七)国家网信部门认为需要评估的其他事项。

第九条 数据处理者应当在与境外接收方订立的法律文件中明确约定数据安全保护责任义务，至少包括以下内容：

(一)数据出境的目的、方式和数据范围， 境外接收方处理数据的用途、方式等；

(二)数据在境外保存地点、期限， 以及达到保存期限、完成约定目的或者法律文件终止后出境数据的处理措施；

(三)对于境外接收方将出境数据再转移给其他组织、个人的约束性要求；

(四)境外接收方在实际控制权或者经营范围发生实质性变化，或者所在国家、地区数据安全保护政策法规和网络安全环境发生变化以及发生其他不可抗力情形导致难以保障数据安全时，应当采取的安全措施；

(五)违反法律文件约定的数据安全保护义务的补救措施、违约责任和争议解决方式；

(六)出境数据遭到篡改、破坏、泄露、丢失、转移或者被非法获取、非法利用等风险时，妥善开展应急处置的要求和保障个人维护其个人信息权益的途径和方式。

第十条 国家网信部门受理申报后，根据申报情况组织国务院有关部门、省级网信部门、专门机构等进行安全评估。

第十一条 安全评估过程中，发现数据处理者提交的申报材料不符合要求的，国家网信部门可以要求其补充或者更正。数据处理者无正当理由不补充或者更正的，国家网信部门可以终止安全评估。

数据处理者对所提交材料的真实性负责，故意提交虚假材料的，按照评估不通过处理，并依法追究相应法律责任。

第十二条 国家网信部门应当自向数据处理者发出书面受理通知书之日起45个工作日内完成数据出境安全评估；情况复杂或者需要补充、更正材料的， 可以适当延长并告知数据处理者预计延长的时间。

评估结果应当书面通知数据处理者。

第十三条 数据处理者对评估结果有异议的，可以在收到评估结果 15 个工作日内向国家网信部门申请复评，复评结果为最终结论。

第十四条 通过数据出境安全评估的结果有效期为 2 年，自评估结果出具之日起计算。在有效期内出现以下情形之一的，数据处理者应当重新申报评估：

(一)向境外提供数据的目的、方式、范围、种类和境外接收方处理数据的用途、方式发生变化影响出境数据安全的， 或者延长个人信息和重要数据境外保存期限的；

(二)境外接收方所在国家或者地区数据安全保护政策法规和网络安全环境发生变化以及发生其他不可抗力情形、数据处理者或者境外接收方实际控制权发生变化、数据处理者与境外接收方法律文件变更等影响出境数据安全的；

(三)出现影响出境数据安全的其他情形。

有效期届满，需要继续开展数据出境活动的，数据处理者应当在有效期届满60个工作日前重新申报评估。

第十五条 参与安全评估工作的相关机构和人员对在履行职责中知悉的国家秘密、个人隐私、个人信息、商业秘密、保密商务信息等数据应当依法予以保密，不得泄露或者非法向他人提供、非法使用。

第十六条 任何组织和个人发现数据处理者违反本办法向境外提供数据的，可以向省级以上网信部门举报。

第十七条 国家网信部门发现已经通过评估的数据出境活动在实际处理过程中不再符合数据出境安全管理要求的，应当书面通知数据处理者终止数据出境活动。数据处理者需要继续开展数据出境活动的， 应当按照要求整改，整改完成后重新申报评估。

第十八条 违反本办法规定的，依据《中华人民共和国网络安全法》、《中华

人民共和国数据安全法》、《中华人民共和国个人信息保护法》等法律法规处理；构成犯罪的，依法追究刑事责任。

第十九条 本办法所称重要数据，是指一旦遭到篡改、破坏、泄露或者非法获取、非法利用等， 可能危害国家安全、经济运行、社会稳定、公共健康和安全等的数据。

第二十条 本办法自 2022 年 9 月 1 日起施行。本办法施行前已经开展的数据出境活动，不符合本办法规定的，应当自本办法施行之日起 6 个月内完成整改。

网信部门行政执法程序规定

国家互联网信息办公室令第 14 号

《网信部门行政执法程序规定》已经 2023 年 2 月 3 日国家互联网信息办公室 2023 年第 2 次室务会议审议通过，现予公布，自 2023 年 6 月 1 日起施行。

国家互联网信息办公室主任 庄荣文

2023 年 3 月 18 日

网信部门行政执法程序规定

第一章 总 则

第一条 为了规范和保障网信部门依法履行职责，保护公民、法人和其他组织的合法权益，维护国家安全和公共利益，根据《中华人民共和国行政处罚法》、《中华人民共和国行政强制法》、《中华人民共和国网络安全法》、《中华人民共和国数据安全法》、《中华人民共和国个人信息保护法》等法律、行政法规， 制定本规定。

第二条 网信部门实施行政处罚等行政执法，适用本规定。

本规定所称网信部门，是指国家互联网信息办公室和地方互联网信息办公室。

第三条 网信部门实施行政执法，应当坚持处罚与教育相结合，做到事实清楚、证据确凿、依据准确、程序合法。

第四条 国家网信部门依法建立本系统的行政执法监督制度。

上级网信部门对下级网信部门实施的行政执法进行监督。

第五条 网信部门应当加强执法队伍和执法能力建设，建立健全执法人员培训、考试考核、资格管理和持证上岗制度。

第六条 网信部门及其执法人员对在执法过程中知悉的国家秘密、商业秘密

或者个人隐私，应当依法予以保密。

第七条 执法人员与案件有直接利害关系或者有其他关系可能影响公正执法的，应当回避。

当事人认为执法人员与案件有直接利害关系或者有其他关系可能影响公正执法的，有权申请回避。

当事人提出回避申请的，网信部门应当依法审查，由网信部门负责人决定。决定作出之前，不停止调查。

第二章 管辖和适用

第八条 行政处罚由违法行为发生地的网信部门管辖。法律、行政法规、部门规章另有规定的，从其规定。

违法行为发生地包括违法行为人相关服务许可地或者备案地，主营业地、登记地，网站建立者、管理者、使用者所在地， 网络接入地，服务器所在地，计算机等终端设备所在地等。

第九条 县级以上网信部门依职权管辖本行政区域内的行政处罚案件。法律、行政法规另有规定的，从其规定。

第十条 对当事人的同一个违法行为，两个以上网信部门都有管辖权的，由最先立案的网信部门管辖。

两个以上网信部门对管辖权有争议的，应当协商解决，协商不成的，报请共同的上一级网信部门指定管辖；也可以直接由共同的上一级网信部门指定管辖。

第十一条 上级网信部门认为必要的，可以直接办理下级网信部门管辖的案件，也可以将本部门管辖的案件交由下级网信部门办理。法律、行政法规、部门规章明确规定案件应当由上级网信部门管辖的，上级网信部门不得将案件交由下级网信部门管辖。

下级网信部门对其管辖的案件由于特殊原因不能行使管辖权的，可以报请上级网信部门管辖或者指定管辖。

设区的市级以下网信部门发现其所管辖的行政处罚案件涉及国家安全等情形的，应当及时报告上一级网信部门，必要时报请上一级网信部门管辖。

第十二条 网信部门发现受理的案件不属于其管辖的，应当及时移送有管辖权的网信部门。

受移送的网信部门应当将案件查处结果及时函告移送案件的网信部门；认为移送不当的，应当报请共同的上一级网信部门指定管辖，不得再次自行移送。

第十三条 上级网信部门接到管辖争议或者报请指定管辖的请示后，应当在十个工作日内作出指定管辖的决定，并书面通知下级网信部门。

第十四条 网信部门发现案件属于其他行政机关管辖的，应当依法移送有关行政机关。

网信部门发现违法行为涉嫌犯罪的，应当及时将案件移送司法机关。司法机关决定立案的，网信部门应当及时办结移交手续。

网信部门应当与司法机关加强协调配合，建立健全案件移送制度，加强证据材料移交、接收衔接，完善案件处理信息通报机制。

第十五条 网信部门对依法应当由原许可、批准的部门作出降低资质等级、吊销许可证件等行政处罚决定的，应当将取得的证据及相关材料送原许可、批准的部门，由其依法作出是否降低资质等级、吊销许可证件等决定。

第十六条 对当事人的同一个违法行为，不得给予两次以上罚款的行政处罚。同一个违法行为违反多个法律规范应当给予罚款处罚的，按照罚款数额高的规定处罚。

第三章 行政处罚程序

第一节 立案

第十七条 网信部门对下列事项应当及时调查处理，并填写案件来源登记表：

(一)在监督检查中发现案件线索的；

(二) 自然人、法人或者其他组织投诉、申诉、举报的；

(三)上级网信部门交办或者下级网信部门报请查处的；

(四)有关机关移送的；

(五)经由其他方式、途径发现的。

第十八条 行政处罚立案应当符合下列条件：

(一)有涉嫌违反法律、行政法规和部门规章的行为，依法应当予以行政处罚；

(二)属于本部门管辖；

(三)在应当给予行政处罚的法定期限内。

符合立案条件的，应当填写立案审批表，连同相关材料，在七个工作日内报

网信部门负责人批准立案，并指定两名以上执法人员为案件承办人。情况特殊的，可以延长至十五个工作日内立案。

对于不予立案的投诉、申诉、举报， 应当将不予立案的相关情况作书面记录留存。

对于其他机关移送的案件，决定不予立案的，应当书面告知移送机关。

不予立案或者撤销立案的，承办人应当制作不予立案审批表或者撤销立案审批表，报网信部门负责人批准。

第二节 调查取证

第十九条 网信部门进行案件调查取证，应当由具有行政执法资格的执法人员实施。执法人员不得少于两人， 并应当主动向当事人或者有关人员出示执法证件。必要时，可以聘请专业人员进行协助。

首次向案件当事人收集、调取证据的， 应当告知其有申请执法人员回避的权利。

向有关单位、个人收集、调取证据时，应当告知其有如实提供证据的义务。被调查对象和有关人员应当如实回答询问，协助和配合调查，及时提供依法应予保存的网络运营者发布的信息、用户发布的信息、日志信息等相关材料， 不得阻挠、干扰案件的调查。

第二十条 网信部门在执法过程中确需有关机关或者其他行政区域网信部门协助调查取证的，应当出具协助调查函，协助调查函应当载明需要协助的具体事项、期限等内容。

收到协助调查函的网信部门对属于本部门职权范围的协助事项应当予以协助，在接到协助调查函之日起十五个工作日内完成相关工作；需要延期完成或者无法协助的，应当及时函告提出协助请求的网信部门。

第二十一条 执法人员应当依法收集与案件有关的证据，包括书证、物证、视听资料、电子数据、证人证言、当事人的陈述、鉴定意见、勘验笔录、现场笔录等。

电子数据是指案件发生过程中形成的，存在于计算机设备、移动通信设备、互联网服务器、移动存储设备、云存储系统等电子设备或者存储介质中， 以数字化形式存储、处理、传输的， 能够证明案件事实的数据。视听资料包括录音资料

和影像资料。存储在电子介质中的录音资料和影像资料，适用电子数据的规定。

证据应当经查证属实，方可作为认定案件事实的根据。

以非法手段取得的证据，不得作为认定案件事实的根据。

第二十二条 立案前调查和监督检查过程中依法取得的证据材料，可以作为案件的证据使用。

对于移送的案件，移送机关依职权调查收集的证据材料，可以作为案件的证据使用。

第二十三条 网信部门在立案前，可以采取询问、勘验、检查、检测、检验、鉴定、调取相关材料等措施，不得限制调查对象的人身、财产权利。

网信部门立案后，可以对涉案物品、设施、场所采取先行登记保存等措施。

第二十四条 网信部门在执法过程中询问当事人或者其他有关人员，应当制作询问笔录，载明时间、地点、事实、经过等内容。询问笔录应当交询问对象或者其他有关人员核对确认，并由执法人员和询问对象或者其他有关人员签名。询问对象和其他有关人员拒绝签名或者无法签名的，应当注明原因。

第二十五条 网信部门对于涉及违法行为的场所、物品、网络应当进行勘验、检查，及时收集、固定书证、物证、视听资料和电子数据。

第二十六条 网信部门可以委托司法鉴定机构就案件中的专门性问题出具鉴定意见；不属于司法鉴定范围的，可以委托有能力或者有条件的机构出具检测报告或者检验报告。

第二十七条 网信部门可以向有关单位、个人调取能够证明案件事实的证据材料，并可以根据需要拍照、录像、复印和复制。

调取的书证、物证应当是原件、原物。调取原件、原物确有困难的， 可以由提交证据的有关单位、个人在复制品上签字或者盖章，注明“此件由×××提供，经核对与原件(物)无异”的字样或者文字说明，注明出证日期、证据出处， 并签名或者盖章。

调取的视听资料、电子数据应当是原始载体或者备份介质。调取原始载体或者备份介质确有困难的，可以收集复制件，并注明制作方法、制作时间、制作人等情况。调取声音资料的，应当附有该声音内容的文字记录。

第二十八条 在证据可能灭失或者以后难以取得的情况下，经网信部门负责

人批准，执法人员可以依法对涉案计算机、服务器、硬盘、移动存储设备、存储卡等涉嫌实施违法行为的物品先行登记保存，制作登记保存物品清单，向当事人出具登记保存物品通知书。先行登记保存期间，当事人和其他有关人员不得损毁、销毁或者转移证据。

网信部门实施先行登记保存的，应当通知当事人或者持有人到场，并在现场笔录中对采取的相关措施情况予以记载。

第二十九条 网信部门对先行登记保存的证据，应当在七个工作日内作出以下处理决定：

(一)需要采取证据保全措施的，采取记录、复制、拍照、录像等证据保全措施后予以返还；

(二)需要检验、检测、鉴定的，送交具有相应资质的机构检验、检测、鉴定；

(三)违法事实不成立，或者先行登记保存的证据与违法事实不具有关联性的，解除先行登记保存。

逾期未作出处理决定的，应当解除先行登记保存。

违法事实成立，依法应当予以没收的，依照法定程序实施行政处罚。

第三十条 网信部门收集、保全电子数据，可以采取现场取证、远程取证和责令有关单位、个人固定和提交等措施。

现场取证、远程取证结束后，应当制作电子取证工作记录。

第三十一条 执法人员在调查取证过程中，应当要求当事人在笔录和其他相关材料上签字、捺指印、盖章或者以其他方式确认。

当事人拒绝到场，拒绝签字、捺指印、盖章或者以其他方式确认， 或者无法找到当事人的，应当由两名执法人员在笔录或者其他材料上注明原因，并邀请其他有关人员作为见证人签字或者盖章，也可以采取录音、录像等方式记录。

第三十二条 对有证据证明是用于违法个人信息处理活动的设备、物品，可以采取查封或者扣押措施。

采取或者解除查封、扣押措施， 应当向网信部门主要负责人书面报告并经批准。情况紧急， 需要当场采取查封、扣押措施的， 执法人员应当在二十四小时内向网信部门主要负责人报告，并补办批准手续。网信部门主要负责人认为不应当采取查封、扣押措施的，应当立即解除。

第三十三条 案件调查终结后，承办人认为违法事实成立，应当予以行政处罚的，撰写案件处理意见报告，草拟行政处罚建议书。

有下列情形之一的，承办人撰写案件处理意见报告，说明拟作处理的理由，报网信部门负责人批准后根据不同情况分别处理：

(一)认为违法事实不能成立，不予行政处罚的；

(二)违法行为情节轻微并及时改正，没有造成危害后果，不予行政处罚的；

(三)初次违法且危害后果轻微并及时改正，可以不予行政处罚的；

(四)当事人有证据足以证明没有主观过错，不予行政处罚的，法律、行政法规另有规定的，从其规定；

(五)案件不属于本部门管辖，应当移送其他行政机关管辖的；

(六)涉嫌犯罪，应当移送司法机关的。

第三十四条 网信部门在进行监督检查或者案件调查时，对已有证据证明违法事实成立的，应当责令当事人立即改正或者限期改正违法行为。

第三十五条 对事实清楚、当事人自愿认错认罚且对违法事实和法律适用没有异议的行政处罚案件，网信部门应当快速办理案件。

第三节 听证

第三十六条 网信部门作出下列行政处罚决定前，应当告知当事人有要求举行听证的权利。当事人要求听证的， 应当在被告知后五个工作日内提出，网信部门应当组织听证。当事人逾期未要求听证的，视为放弃听证的权利：

(一)较大数额罚款；

(二)没收较大数额违法所得、没收较大价值非法财物；

(三)降低资质等级、吊销许可证件；

(四)责令停产停业、责令关闭、限制从业；

(五)其他较重的行政处罚；

(六)法律、行政法规、部门规章规定的其他情形。

第三十七条 网信部门应当在听证的七个工作日前，将听证通知书送达当事人，告知当事人及有关人员举行听证的时间、地点。

听证应当制作听证笔录，交当事人或者其代理人核对无误后签字或者盖章。当事人或者其代理人拒绝签字或者盖章的，由听证主持人在笔录中注明。

除涉及国家秘密、商业秘密或者个人隐私依法予以保密外，听证公开举行。

听证结束后，网信部门应当根据听证笔录，依照本规定第四十二条的规定，作出决定。

第四节 行政处罚决定和送达

第三十八条 网信部门对当事人作出行政处罚决定前，可以根据有关规定对其实施约谈，谈话结束后制作执法约谈笔录。

第三十九条 网信部门作出行政处罚决定前，应当填写行政处罚意见告知书，告知当事人拟作出的行政处罚内容及事实、理由、依据， 并告知当事人依法享有的陈述、申辩等权利。

第四十条 当事人有权进行陈述和申辩。网信部门应当充分听取当事人的意见，对当事人提出的事实、理由和证据， 应当进行复核；当事人提出的事实、理由或者证据成立的，网信部门应当采纳。

网信部门不得因当事人陈述、申辩而给予更重的处罚。

网信部门及其执法人员在作出行政处罚决定前，未依照本规定向当事人告知拟作出的行政处罚内容及事实、理由、依据，或者拒绝听取当事人的陈述、申辩，不得作出行政处罚决定，但当事人明确放弃陈述或者申辩权利的除外。

第四十一条 有下列情形之一，在网信部门负责人作出行政处罚的决定之前，应当由从事行政处罚决定法制审核的人员进行法制审核；未经法制审核或者审核未通过的，不得作出决定：

(一)涉及重大公共利益的；

(二)直接关系当事人或者第三人重大权益，经过听证程序的；

(三)案件情况疑难复杂、涉及多个法律关系的；

(四)法律、行政法规规定应当进行法制审核的其他情形。

法制审核由网信部门确定的负责法制审核的机构实施。网信部门中初次从事行政处罚决定法制审核的人员，应当通过国家统一法律职业资格考试取得法律职业资格。

第四十二条 拟作出的行政处罚决定应当报网信部门负责人审查。网信部门负责人根据不同情况，分别作出如下决定：

(一)确有应受行政处罚的违法行为的，根据情节轻重及具体情况，作出行政

处罚决定；

(二)违法行为轻微，依法可以不予行政处罚的，不予行政处罚；

(三)违法事实不能成立的，不予行政处罚；

(四)违法行为涉嫌犯罪的，移送司法机关。

第四十三条 对情节复杂或者重大违法行为给予行政处罚，网信部门负责人应当集体讨论决定。集体讨论决定的过程应当书面记录。

第四十四条 网信部门作出行政处罚决定，应当制作统一编号的行政处罚决定书。

行政处罚决定书应当载明下列事项：

(一)当事人的姓名或者名称、地址等基本情况；

(二)违反法律、行政法规、部门规章的事实和证据；

(三)行政处罚的种类和依据；

(四)行政处罚的履行方式和期限；

(五)申请行政复议、提起行政诉讼的途径和期限；

(六)作出行政处罚决定的网信部门名称和作出决定的日期。

行政处罚决定中涉及没收有关物品的，还应当附没收物品凭证。

行政处罚决定书必须盖有作出行政处罚决定的网信部门的印章。

第四十五条 网信部门应当自行政处罚案件立案之日起九十日内作出行政处罚决定。

因案情复杂等原因不能在规定期限内作出处理决定的，经本部门负责人批准，可以延长六十日。案情特别复杂或者情况特殊，经延期仍不能作出处理决定的，由上一级网信部门负责人决定是否继续延期，决定继续延期的，应当同时确定延长的合理期限；国家网信部门办理的行政处罚案件需要延期的，由本部门主要负责人批准。

案件处理过程中，听证、检测、检验、鉴定、行政协助等时间不计入本条第一款、第二款规定的期限。

第四十六条 行政处罚决定书应当在宣告后当场交付当事人；当事人不在场的，应当在七个工作日内依照《中华人民共和国民事诉讼法》的有关规定， 将行政处罚决定书送达当事人。

当事人同意并签订确认书的，网信部门可以采用传真、电子邮件等方式， 将行政处罚决定书等送达当事人。

第四章 执行和结案

第四十七条 行政处罚决定书送达后，当事人应当在行政处罚决定书载明的期限内予以履行。

当事人确有经济困难，可以提出延期或者分期缴纳罚款的申请，并提交书面材料。经案件承办人审核， 确定延期或者分期缴纳罚款的期限和金额，报网信部门负责人批准后，可以暂缓或者分期缴纳。

第四十八条 网络运营者违反相关法律、行政法规、部门规章规定，需由电信主管部门关闭网站、吊销相关增值电信业务经营许可证或者取消备案的， 转电信主管部门处理。

第四十九条 当事人对行政处罚决定不服，可以依法申请行政复议或者提起行政诉讼。

当事人对行政处罚决定不服，申请行政复议或者提起行政诉讼的，行政处罚不停止执行，法律另有规定的除外。

当事人申请行政复议或者提起行政诉讼的，加处罚款的数额在行政复议或者行政诉讼期间不予计算。

第五十条 当事人逾期不履行行政处罚决定的，作出行政处罚决定的网信部门可以采取下列措施：

(一)到期不缴纳罚款的，每日按罚款数额的百分之三加处罚款，加处罚款的数额不得超出罚款的数额；

(二)依照《中华人民共和国行政强制法》的规定申请人民法院强制执行。

网信部门批准延期、分期缴纳罚款的， 申请人民法院强制执行的期限，自暂缓或者分期缴纳罚款期限结束之日起计算。

第五十一条 网信部门申请人民法院强制执行的，申请前应当填写履行行政处罚决定催告书，书面催告当事人履行义务，并告知履行义务的期限和方式、依法享有的陈述和申辩权；涉及加处罚款的，应当有明确的金额和给付方式。

当事人进行陈述、申辩的， 网信部门应当对当事人提出的事实、理由和证据进行记录、复核， 并制作陈述申辩笔录、陈述申辩复核意见书。当事人提出的事

实、理由或者证据成立的，网信部门应当采纳。

履行行政处罚决定催告书送达十个工作日后，当事人仍未履行处罚决定的，网信部门可以填写行政处罚强制执行申请书，向所在地有管辖权的人民法院申请强制执行。

第五十二条 行政处罚决定履行或者执行后，有下列情形之一的，执法人员应当填写行政处罚结案报告，将有关案件材料进行整理装订，归档保存：

(一)行政处罚决定履行或者执行完毕的；

(二)人民法院裁定终结执行的；

(三)案件终止调查的；

(四)作出本规定第四十二条第二项至第四项决定的；

(五)其他应当予以结案的情形。

结案后，执法人员应当将案件材料按照档案管理的有关规定立卷归档。案卷归档应当一案一卷、材料齐全、规范有序。

第五十三条 网信部门应当依法以文字、音像等形式，对行政处罚的启动、调查取证、审核、决定、送达、执行等进行全过程记录，归档保存。

第五十四条 网信部门实施行政处罚应当接受社会监督。公民、法人或者其他组织对网信部门实施行政处罚的行为，有权申诉或者检举；网信部门应当认真审查，发现有错误的，应当主动改正。

第五章 附 则

第五十五条 本规定中的期限以时、日计算，开始的时和日不计算在内。期限届满的最后一日是法定节假日的，以法定节假日后的第一日为届满的日期。但是，法律、行政法规另有规定的除外。

第五十六条 本规定中的“以上”、“以下”、“内”均包括本数、本级。

第五十七条 国家网信部门负责制定行政执法相关文书格式范本。各省、自治区、直辖市网信部门可以参照文书格式范本， 制定本行政区域行政执法所适用的文书格式并自行印制。

第五十八条 本规定自 2023 年 6 月 1 日起施行。2017 年 5 月 2 日公布的《互联网信息内容管理行政执法程序规定》(国家互联网信息办公室令第 2 号)同时废止。

促进和规范数据跨境流动规定

国家互联网信息办公室令第 16 号

《促进和规范数据跨境流动规定》已经 2023 年 11 月 28 日国家互联网信息办公室 2023 年第 26 次室务会议审议通过，现予公布，自公布之日起施行。

国家互联网信息办公室主任 庄荣文

2024 年 3 月 22 日

促进和规范数据跨境流动规定

第一条 为了保障数据安全，保护个人信息权益，促进数据依法有序自由流动，根据《中华人民共和国网络安全法》、《中华人民共和国数据安全法》、《中华人民共和国个人信息保护法》等法律法规， 对于数据出境安全评估、个人信息出境标准合同、个人信息保护认证等数据出境制度的施行，制定本规定。

第二条 数据处理者应当按照相关规定识别、申报重要数据。未被相关部门、地区告知或者公开发布为重要数据的，数据处理者不需要作为重要数据申报数据出境安全评估。

第三条 国际贸易、跨境运输、学术合作、跨国生产制造和市场营销等活动中收集和产生的数据向境外提供，不包含个人信息或者重要数据的，免予申报数据出境安全评估、订立个人信息出境标准合同、通过个人信息保护认证。

第四条 数据处理者在境外收集和产生的个人信息传输至境内处理后向境外提供，处理过程中没有引入境内个人信息或者重要数据的，免予申报数据出境安全评估、订立个人信息出境标准合同、通过个人信息保护认证。

第五条 数据处理者向境外提供个人信息，符合下列条件之一的，免予申报数据出境安全评估、订立个人信息出境标准合同、通过个人信息保护认证：

(一)为订立、履行个人作为一方当事人的合同，如跨境购物、跨境寄递、跨境汇款、跨境支付、跨境开户、机票酒店预订、签证办理、考试服务等，确需向境外提供个人信息的；

(二)按照依法制定的劳动规章制度和依法签订的集体合同实施跨境人力资源管理，确需向境外提供员工个人信息的；

(三)紧急情况下为保护自然人的生命健康和财产安全，确需向境外提供个人信息的；

(四)关键信息基础设施运营者以外的数据处理者自当年 1 月 1 日起累计向境外提供不满 10 万人个人信息(不含敏感个人信息)的。

前款所称向境外提供的个人信息，不包括重要数据。

第六条 自由贸易试验区在国家数据分类分级保护制度框架下，可以自行制定区内需要纳入数据出境安全评估、个人信息出境标准合同、个人信息保护认证管理范围的数据清单(以下简称负面清单)，经省级网络安全和信息化委员会批准后，报国家网信部门、国家数据管理部门备案。

自由贸易试验区内数据处理者向境外提供负面清单外的数据，可以免予申报数据出境安全评估、订立个人信息出境标准合同、通过个人信息保护认证。

第七条 数据处理者向境外提供数据，符合下列条件之一的，应当通过所在地省级网信部门向国家网信部门申报数据出境安全评估：

(一)关键信息基础设施运营者向境外提供个人信息或者重要数据；

(二)关键信息基础设施运营者以外的数据处理者向境外提供重要数据，或者自当年 1 月 1 日起累计向境外提供 100 万人以上个人信息(不含敏感个人信息)或者 1 万人以上敏感个人信息。

属于本规定第三条、第四条、第五条、第六条规定情形的，从其规定。

第八条 关键信息基础设施运营者以外的数据处理者自当年 1 月 1 日起累计向境外提供 10 万人以上、不满 100 万人个人信息(不含敏感个人信息)或者不满 1 万人敏感个人信息的，应当依法与境外接收方订立个人信息出境标准合同或者通过个人信息保护认证。

属于本规定第三条、第四条、第五条、第六条规定情形的，从其规定。

第九条 通过数据出境安全评估的结果有效期为 3 年，自评估结果出具之日起计算。有效期届满， 需要继续开展数据出境活动且未发生需要重新申报数据出境安全评估情形的，数据处理者可以在有效期届满前 60 个工作日内通过所在地省级网信部门向国家网信部门提出延长评估结果有效期申请。经国家网信部门批准，可以延长评估结果有效期 3 年。

第十条 数据处理者向境外提供个人信息的，应当按照法律、行政法规的规定履行告知、取得个人单独同意、进行个人信息保护影响评估等义务。

第十一条 数据处理者向境外提供数据的，应当遵守法律、法规的规定，履

行数据安全保护义务，采取技术措施和其他必要措施，保障数据出境安全。发生或者可能发生数据安全事件的，应当采取补救措施，及时向省级以上网信部门和其他有关主管部门报告。

第十二条 各地网信部门应当加强对数据处理者数据出境活动的指导监督，健全完善数据出境安全评估制度，优化评估流程；强化事前事中事后全链条全领域监管，发现数据出境活动存在较大风险或者发生数据安全事件的，要求数据处理者进行整改，消除隐患；对拒不改正或者造成严重后果的，依法追究法律责任。

第十三条 2022 年 7 月 7 日公布的《数据出境安全评估办法》(国家互联网信息办公室令第 11 号)、2023 年 2 月 22 日公布的《个人信息出境标准合同办法》(国家互联网信息办公室令第 13 号)等相关规定与本规定不一致的，适用本规定。

第十四条 本规定自公布之日起施行。

即时通信工具公众信息服务发展管理暂行规定

(国家互联网信息办公室 2014 年 8 月 7 日)

第一条 为进一步推动即时通信工具公众信息服务健康有序发展，保护公民、法人和其他组织的合法权益，维护国家安全和公共利益，根据《全国人民代表大会常务委员会关于维护互联网安全的决定》、《全国人民代表大会常务委员会关于加强网络信息保护的决定》、《最高人民法院、最高人民检察院关于办理利用信息网络实施诽谤等刑事案件适用法律若干问题的解释》、《互联网信息服务管理办法》、《互联网新闻信息服务管理规定》等法律法规，制定本规定。

第二条 在中华人民共和国境内从事即时通信工具公众信息服务，适用本规定。

本规定所称即时通信工具，是指基于互联网面向终端使用者提供即时信息交流服务的应用。本规定所称公众信息服务， 是指通过即时通信工具的公众账号及其他形式向公众发布信息的活动。

第三条 国家互联网信息办公室负责统筹协调指导即时通信工具公众信息服务发展管理工作，省级互联网信息内容主管部门负责本行政区域的相关工作。

互联网行业组织应当积极发挥作用，加强行业自律，推动行业信用评价体系建设，促进行业健康有序发展。

第四条 即时通信工具服务提供者应当取得法律法规规定的相关资质。即时

通信工具服务提供者从事公众信息服务活动，应当取得互联网新闻信息服务资质。

第五条 即时通信工具服务提供者应当落实安全管理责任，建立健全各项制度，配备与服务规模相适应的专业人员，保护用户信息及公民个人隐私，自觉接受社会监督，及时处理公众举报的违法和不良信息。

第六条 即时通信工具服务提供者应当按照“后台实名、前台自愿”的原则，要求即时通信工具服务使用者通过真实身份信息认证后注册账号。

即时通信工具服务使用者注册账号时，应当与即时通信工具服务提供者签订协议，承诺遵守法律法规、社会主义制度、国家利益、公民合法权益、公共秩序、社会道德风尚和信息真实性等“七条底线”。

第七条 即时通信工具服务使用者为从事公众信息服务活动开设公众账号，应当经即时通信工具服务提供者审核，由即时通信工具服务提供者向互联网信息内容主管部门分类备案。

新闻单位、新闻网站开设的公众账号可以发布、转载时政类新闻， 取得互联网新闻信息服务资质的非新闻单位开设的公众账号可以转载时政类新闻。其他公众账号未经批准不得发布、转载时政类新闻。

即时通信工具服务提供者应当对可以发布或转载时政类新闻的公众账号加注标识。

鼓励各级党政机关、企事业单位和各人民团体开设公众账号， 服务经济社会发展，满足公众需求。

第八条 即时通信工具服务使用者从事公众信息服务活动，应当遵守相关法律法规。

对违反协议约定的即时通信工具服务使用者，即时通信工具服务提供者应当视情节采取警示、限制发布、暂停更新直至关闭账号等措施，并保存有关记录，履行向有关主管部门报告义务。

第九条 对违反本规定的行为，由有关部门依照相关法律法规处理。

第十条 本规定自公布之日起施行。

互联网用户账号名称管理规定

（国家互联网信息办公室 2015 年 2 月 4 日）

第一条 为加强对互联网用户账号名称的管理，保护公民、法人和其他组织

的合法权益，根据《国务院关于授权国家互联网信息办公室负责互联网信息内容管理工作的通知》和有关法律、行政法规，制定本规定。

第二条 在中华人民共和国境内注册、使用和管理互联网用户账号名称，适用本规定。

本规定所称互联网用户账号名称，是指机构或个人在博客、微博客、即时通信工具、论坛、贴吧、跟帖评论等互联网信息服务中注册或使用的账号名称。

第三条 国家互联网信息办公室负责对全国互联网用户账号名称的注册、使用实施监督管理，各省、自治区、直辖市互联网信息内容主管部门负责对本行政区域内互联网用户账号名称的注册、使用实施监督管理。

第四条 互联网信息服务提供者应当落实安全管理责任，完善用户服务协议，明示互联网信息服务使用者在账号名称、头像和简介等注册信息中不得出现违法和不良信息，配备与服务规模相适应的专业人员，对互联网用户提交的账号名称、头像和简介等注册信息进行审核，对含有违法和不良信息的，不予注册；保护用户信息及公民个人隐私，自觉接受社会监督，及时处理公众举报的账号名称、头像和简介等注册信息中的违法和不良信息。

第五条 互联网信息服务提供者应当按照“后台实名、前台自愿”的原则，要求互联网信息服务使用者通过真实身份信息认证后注册账号。

互联网信息服务使用者注册账号时，应当与互联网信息服务提供者签订协议，承诺遵守法律法规、社会主义制度、国家利益、公民合法权益、公共秩序、社会道德风尚和信息真实性等七条底线。

第六条 任何机构或个人注册和使用的互联网用户账号名称，不得有下列情形：

(一)违反宪法或法律法规规定的；

(二)危害国家安全，泄露国家秘密，颠覆国家政权，破坏国家统一的；

(三)损害国家荣誉和利益的，损害公共利益的；

(四)煽动民族仇恨、民族歧视，破坏民族团结的；

(五)破坏国家宗教政策，宣扬邪教和封建迷信的；

(六)散布谣言，扰乱社会秩序，破坏社会稳定的；

(七)散布淫秽、色情、赌博、暴力、凶杀、恐怖或者教唆犯罪的；

(八)侮辱或者诽谤他人，侵害他人合法权益的；

(九)含有法律、行政法规禁止的其他内容的。

第七条 互联网信息服务使用者以虚假信息骗取账号名称注册，或其账号头像、简介等注册信息存在违法和不良信息的， 互联网信息服务提供者应当采取通知限期改正、暂停使用、注销登记等措施。

第八条 对冒用、关联机构或社会名人注册账号名称的，互联网信息服务提供者应当注销其账号，并向互联网信息内容主管部门报告。

第九条 对违反本规定的行为，由有关部门依照相关法律规定处理。

第十条 本规定自 2015 年 3 月 1 日施行。

互联网新闻信息服务单位约谈工作规定

(国家互联网信息办公室 2015 年 4 月 28 日)

第一条 为了进一步推进依法治网，促进互联网新闻信息服务单位依法办网、文明办网，规范互联网新闻信息服务，保护公民、法人和其他组织的合法权益，营造清朗网络空间，根据《互联网信息服务管理办法》、《互联网新闻信息服务管理规定》和《国务院关于授权国家互联网信息办公室负责互联网信息内容管理工作的通知》，制定本规定。

第二条 国家互联网信息办公室、地方互联网信息办公室建立互联网新闻信息服务单位约谈制度。

本规定所称约谈，是指国家互联网信息办公室、地方互联网信息办公室在互联网新闻信息服务单位发生严重违法违规情形时，约见其相关负责人，进行警示谈话、指出问题、责令整改纠正的行政行为。

第三条 地方互联网信息办公室负责对本行政区域内的互联网新闻信息服务单位实施约谈，约谈情况应当及时向国家互联网信息办公室报告。

对存在重大违法情形的互联网新闻信息服务单位，由国家互联网信息办公室单独或联合属地互联网信息办公室实施约谈。

第四条 互联网新闻信息服务单位有下列情形之一的，国家互联网信息办公室、地方互联网信息办公室可对其主要负责人、总编辑等进行约谈：

(一)未及时处理公民、法人和其他组织关于互联网新闻信息服务的投诉、举报情节严重的；

(二)通过采编、发布、转载、删除新闻信息等谋取不正当利益的;

(三)违反互联网用户账号名称注册、使用、管理相关规定情节严重的;

(四)未及时处置违法信息情节严重的;

(五)未及时落实监管措施情节严重的;

(六)内容管理和网络安全制度不健全、不落实的;

(七)网站日常考核中问题突出的;

(八)年检中问题突出的;

(九)其他违反相关法律法规规定需要约谈的情形。

第五条 国家互联网信息办公室、地方互联网信息办公室对互联网新闻信息服务单位实施约谈,应当提前告知约谈事由,并约定时间、地点和参加人员等。

国家互联网信息办公室、地方互联网信息办公室实施约谈时, 应当由两名以上执法人员参加,主动出示证件,并记录约谈情况。

第六条 国家互联网信息办公室、地方互联网信息办公室通过约谈,及时指出互联网新闻信息服务单位存在的问题,并提出整改要求。

互联网新闻信息服务单位应当及时落实整改要求,依法提供互联网新闻信息服务。

第七条 国家互联网信息办公室、地方互联网信息办公室应当加强对互联网新闻信息服务单位的监督检查,并对其整改情况进行综合评估,综合评估可以委托第三方开展。

互联网新闻信息服务单位未按要求整改,或经综合评估未达到整改要求的,将依照《互联网信息服务管理办法》、《互联网新闻信息服务管理规定》的有关规定给予警告、罚款、责令停业整顿、吊销许可证等处罚; 互联网新闻信息服务单位被多次约谈仍然存在违法行为的,依法从重处罚。

第八条 国家互联网信息办公室、地方互联网信息办公室可将与互联网新闻信息服务单位的约谈情况向社会公开。

约谈情况记入互联网新闻信息服务单位日常考核和年检档案。

第九条 国家互联网信息办公室、地方互联网信息办公室履行约谈职责时,互联网新闻信息服务单位应当予以配合,不得拒绝、阻挠。

第十条 本规定由国家互联网信息办公室负责解释,自 2015 年 6 月 1 日起实

施。

互联网信息搜索服务管理规定

（国家互联网信息办公室 2016 年 6 月 25 日）

第一条为规范互联网信息搜索服务，促进互联网信息搜索行业健康有序发展，保护公民、法人和其他组织的合法权益， 维护国家安全和公共利益，根据《全国人民代表大会常务委员会关于加强网络信息保护的决定》和《国务院关于授权国家互联网信息办公室负责互联网信息内容管理工作的通知》，制定本规定。

第二条在中华人民共和国境内从事互联网信息搜索服务，适用本规定。

本规定所称互联网信息搜索服务，是指运用计算机技术从互联网上搜集、处理各类信息供用户检索的服务。

第三条国家互联网信息办公室负责全国互联网信息搜索服务的监督管理执法工作。地方互联网信息办公室依据职责负责本行政区域内互联网信息搜索服务的监督管理执法工作。

第四条互联网信息搜索服务行业组织应当建立健全行业自律制度和行业准则，指导互联网信息搜索服务提供者建立健全服务规范，督促互联网信息搜索服务提供者依法提供服务、接受社会监督， 提高互联网信息搜索服务从业人员的职业素养。

第五条互联网信息搜索服务提供者应当取得法律法规规定的相关资质。

第六条互联网信息搜索服务提供者应当落实主体责任，建立健全信息审核、公共信息实时巡查、应急处置及个人信息保护等信息安全管理制度， 具有安全可控的防范措施，为有关部门依法履行职责提供必要的技术支持。

第七条互联网信息搜索服务提供者不得以链接、摘要、快照、联想词、相关搜索、相关推荐等形式提供含有法律法规禁止的信息内容。

第八条互联网信息搜索服务提供者提供服务过程中发现搜索结果明显含有法律法规禁止内容的信息、网站及应用， 应当停止提供相关搜索结果，保存有关记录，并及时向国家或者地方互联网信息办公室报告。

第九条互联网信息搜索服务提供者及其从业人员，不得通过断开相关链接或者提供含有虚假信息的搜索结果等手段，牟取不正当利益。

第十条互联网信息搜索服务提供者应当提供客观、公正、权威的搜索结果，

不得损害国家利益、公共利益，以及公民、法人和其他组织的合法权益。

第十一条互联网信息搜索服务提供者提供付费搜索信息服务，应当依法查验客户有关资质，明确付费搜索信息页面比例上限，醒目区分自然搜索结果与付费搜索信息，对付费搜索信息逐条加注显著标识。

互联网信息搜索服务提供者提供商业广告信息服务，应当遵守相关法律法规。

第十二条互联网信息搜索服务提供者应当建立健全公众投诉、举报和用户权益保护制度，在显著位置公布投诉、举报方式， 主动接受公众监督，及时处理公众投诉、举报，依法承担对用户权益造成损害的赔偿责任。

第十三条本规定自 2016 年 8 月 1 日起施行。

互联网直播服务管理规定

（国家互联网信息办公室 2016 年 11 月 4 日）

第一条 为加强对互联网直播服务的管理，保护公民、法人和其他组织的合法权益，维护国家安全和公共利益，根据《全国人民代表大会常务委员会关于加强网络信息保护的决定》《国务院关于授权国家互联网信息办公室负责互联网信息内容管理工作的通知》《互联网信息服务管理办法》和《互联网新闻信息服务管理规定》，制定本规定。

第二条 在中华人民共和国境内提供、使用互联网直播服务，应当遵守本规定。

本规定所称互联网直播，是指基于互联网，以视频、音频、图文等形式向公众持续发布实时信息的活动；本规定所称互联网直播服务提供者，是指提供互联网直播平台服务的主体；本规定所称互联网直播服务使用者，包括互联网直播发布者和用户。

第三条 提供互联网直播服务，应当遵守法律法规，坚持正确导向，大力弘扬社会主义核心价值观，培育积极健康、向上向善的网络文化， 维护良好网络生态，维护国家利益和公共利益，为广大网民特别是青少年成长营造风清气正的网络空间。

第四条 国家互联网信息办公室负责全国互联网直播服务信息内容的监督管理执法工作。地方互联网信息办公室依据职责负责本行政区域内的互联网直播服务信息内容的监督管理执法工作。国务院相关管理部门依据职责对互联网直播服

务实施相应监督管理。

各级互联网信息办公室应当建立日常监督检查和定期检查相结合的监督管理制度，指导督促互联网直播服务提供者依据法律法规和服务协议规范互联网直播服务行为。

第五条 互联网直播服务提供者提供互联网新闻信息服务的，应当依法取得互联网新闻信息服务资质，并在许可范围内开展互联网新闻信息服务。

开展互联网新闻信息服务的互联网直播发布者，应当依法取得互联网新闻信息服务资质并在许可范围内提供服务。

第六条 通过网络表演、网络视听节目等提供互联网直播服务的，还应当依法取得法律法规规定的相关资质。

第七条 互联网直播服务提供者应当落实主体责任，配备与服务规模相适应的专业人员，健全信息审核、信息安全管理、值班巡查、应急处置、技术保障等制度。提供互联网新闻信息直播服务的，应当设立总编辑。

互联网直播服务提供者应当建立直播内容审核平台，根据互联网直播的内容类别、用户规模等实施分级分类管理， 对图文、视频、音频等直播内容加注或播报平台标识信息，对互联网新闻信息直播及其互动内容实施先审后发管理。

第八条 互联网直播服务提供者应当具备与其服务相适应的技术条件，应当具备即时阻断互联网直播的技术能力，技术方案应符合国家相关标准。

第九条 互联网直播服务提供者以及互联网直播服务使用者不得利用互联网直播服务从事危害国家安全、破坏社会稳定、扰乱社会秩序、侵犯他人合法权益、传播淫秽色情等法律法规禁止的活动，不得利用互联网直播服务制作、复制、发布、传播法律法规禁止的信息内容。

第十条 互联网直播发布者发布新闻信息，应当真实准确、客观公正。转载新闻信息应当完整准确，不得歪曲新闻信息内容，并在显著位置注明来源，保证新闻信息来源可追溯。

第十一条 互联网直播服务提供者应当加强对评论、弹幕等直播互动环节的实时管理，配备相应管理人员。

互联网直播发布者在进行直播时，应当提供符合法律法规要求的直播内容，自觉维护直播活动秩序。

用户在参与直播互动时，应当遵守法律法规，文明互动，理性表达。

第十二条 互联网直播服务提供者应当按照“后台实名、前台自愿”的原则，对互联网直播用户进行基于移动电话号码等方式的真实身份信息认证，对互联网直播发布者进行基于身份证件、营业执照、组织机构代码证等的认证登记。互联网直播服务提供者应当对互联网直播发布者的真实身份信息进行审核，向所在地省、自治区、直辖市互联网信息办公室分类备案， 并在相关执法部门依法查询时予以提供。

互联网直播服务提供者应当保护互联网直播服务使用者身份信息和隐私，不得泄露、篡改、毁损，不得出售或者非法向他人提供。

第十三条 互联网直播服务提供者应当与互联网直播服务使用者签订服务协议，明确双方权利义务，要求其承诺遵守法律法规和平台公约。

互联网直播服务协议和平台公约的必备条款由互联网直播服务提供者所在地省、自治区、直辖市互联网信息办公室指导制定。

第十四条 互联网直播服务提供者应当对违反法律法规和服务协议的互联网直播服务使用者，视情采取警示、暂停发布、关闭账号等处置措施， 及时消除违法违规直播信息内容，保存记录并向有关主管部门报告。

第十五条 互联网直播服务提供者应当建立互联网直播发布者信用等级管理体系，提供与信用等级挂钩的管理和服务。

互联网直播服务提供者应当建立黑名单管理制度，对纳入黑名单的互联网直播服务使用者禁止重新注册账号，并及时向所在地省、自治区、直辖市互联网信息办公室报告。

省、自治区、直辖市互联网信息办公室应当建立黑名单通报制度， 并向国家互联网信息办公室报告。

第十六条 互联网直播服务提供者应当记录互联网直播服务使用者发布内容和日志信息，保存六十日。

互联网直播服务提供者应当配合有关部门依法进行的监督检查，并提供必要的文件、资料和数据。

第十七条 互联网直播服务提供者和互联网直播发布者未经许可或者超出许可范围提供互联网新闻信息服务的，由国家和省、自治区、直辖市互联网信息办

公室依据《互联网新闻信息服务管理规定》予以处罚。

对于违反本规定的其他违法行为，由国家和地方互联网信息办公室依据职责，依法予以处罚；构成犯罪的，依法追究刑事责任。通过网络表演、网络视听节目等提供网络直播服务，违反有关法律法规的，由相关部门依法予以处罚。

第十八条 鼓励支持相关行业组织制定行业公约，加强行业自律，建立健全行业信用评价体系和服务评议制度，促进行业规范发展。

第十九条 互联网直播服务提供者应当自觉接受社会监督，健全社会投诉举报渠道，设置便捷的投诉举报入口，及时处理公众投诉举报。

第二十条 本规定自 2016 年 12 月 1 日起施行。

互联网新闻信息服务许可管理实施细则

（国家互联网信息办公室 2017 年 5 月 22 日）

第一条 为进一步提高互联网新闻信息服务许可管理规范化、科学化水平，促进互联网新闻信息服务健康有序发展，根据《中华人民共和国行政许可法》《互联网新闻信息服务管理规定》（以下简称《规定》），制定本细则。

第二条 国家和省、自治区、直辖市互联网信息办公室实施互联网新闻信息服务许可，适用本细则。

第三条 通过互联网站、应用程序、论坛、博客、微博客、公众账号、即时通信工具、网络直播等形式向社会公众提供互联网新闻信息服务， 应当取得互联网新闻信息服务许可，禁止未经许可或超越许可范围开展互联网新闻信息服务活动。

第四条 互联网新闻信息服务，包括互联网新闻信息采编发布服务、转载服务、传播平台服务。

其中，采编发布服务，是指对新闻信息进行采集、编辑、制作并发布的服务；转载服务，是指选择、编辑并发布其他主体已发布新闻信息的服务； 传播平台服务，是指为用户传播新闻信息提供平台的服务。

获准提供互联网新闻信息采编发布服务的，可以同时提供互联网新闻信息转载服务。获准提供互联网新闻信息传播平台服务， 拟同时提供采编发布服务、转载服务的，应当依法取得互联网新闻信息采编发布、转载服务许可。

第五条 申请互联网新闻信息服务许可的，应当具备下列许可条件：

(一)在中华人民共和国境内依法设立的法人;

(二)主要负责人、总编辑是中国公民;

(三)有与服务相适应的专职新闻编辑人员、内容审核人员和技术保障人员;

(四)有健全的互联网新闻信息服务管理制度;

(五)有健全的信息安全管理制度和安全可控的技术保障措施;

(六)有与服务相适应的场所、设施和资金。

其中，申请互联网新闻信息采编发布服务许可的，应当是新闻单位(含新闻单位控股的单位)或新闻宣传部门主管的单位。新闻单位是指经国家有关部门依法批准设立的报刊社、广播电台、电视台、通讯社和新闻电影制片厂。控股是指出资额、持有股份占企业资本总额或股本总额50%以上，或出资额、持有股份的比例虽然不足50%，但依其出资额或持有股份已足以对企业决议产生重大影响。新闻宣传部门包括各级宣传部门、网信部门、广电部门等。

任何组织不得设立中外合资经营、中外合作经营和外资经营的互联网新闻信息服务单位。

第六条 根据《规定》第十条， 申请互联网新闻信息服务许可的，应当提交下列申请材料:

(一)主要负责人、总编辑为中国公民的证明。包括主要负责人、总编辑的身份证复印件等;

(二)专职新闻编辑人员、内容审核人员和技术保障人员的资质情况。包括相关人员基本情况，以及国家新闻出版广电总局统一颁发的新闻记者证、新闻单位从业证明、相关培训考核证明等材料，具体人员数量应当与所提供的服务相适应;

(三)互联网新闻信息服务管理制度。包括网站总编辑制度、从业人员教育培训和考核制度等;

(四)信息安全管理制度和技术保障措施。包括信息发布审核制度、公共信息巡查制度、应急处置制度、用户个人信息保护制度等， 以及相关技术保障措施的情况;

(五)互联网新闻信息服务安全评估报告。由有关部门或具有相关资质的机构出具的对于申请者信息安全管理制度和技术保障措施的安全评估报告;

(六)法人资格、场所、资金的证明。包括企业营业执照、事业单位法人证书、

服务场所产权证书、租赁合同等材料复印件；

(七)互联网新闻信息服务许可申请书。包括申请表， 以及对拟提供具体服务形式、服务方案的说明等。

第七条 申请互联网新闻信息采编发布服务许可的，除应当提交本细则第六条规定的申请材料外，还应当提交该单位或其控股方为新闻单位的证明，或其主管单位为新闻宣传部门的证明及该主管单位的意见。其中，新闻单位证明包括《报纸出版许可证》、《广播电视播出机构许可证》、《期刊出版许可证》(持有《期刊出版许可证》的， 应当以提供《规定》第二条所称“新闻信息”服务为主营业务)等；主管单位意见内容主要包括，说明申请者与该主管单位的关系、就申请者是否符合许可条件提出评估意见并加盖单位公章等。

申请互联网新闻信息传播平台服务许可的，除应当提交本细则第六条规定的申请材料外，还应当提交平台账号用户管理规章制度、用户协议范本、投诉举报处理机制等。

申请者为企业法人的，除应当提交本细则第六条规定的申请材料外，还应当提供下列股权相关材料：

(一)股权结构图。包括股东名称、股权比例、出资方式、出资时间等信息。股东为非自然人主体的，须逐级追溯到自然人、事业单位以及国有独资公司， 并就实际控制人情况作出说明。股权结构图需加盖单位公章，并由法定代表人签字；

(二)股东证明材料。股东为自然人的， 须提供身份证明材料；股东为非自然人主体的，须提供该主体的名称、组织形式、法定代表人等材料；

(三)公司章程。包括公司章程及历次修改决议；

(四)无外资承诺书。申请者对股权结构图中所有股东均不含外资成分作出的书面承诺；

(五)专业机构意见书。律师事务所或会计师事务所就上述股权材料的真实性、准确性、完整性出具的书面证明，包括验资报告、法律意见书等材料。

第八条 根据《规定》第七条， 互联网新闻信息服务单位与境内外中外合资经营、中外合作经营和外资经营的企业进行涉及互联网新闻信息服务业务的合作，应当报国家互联网信息办公室进行安全评估，并提交以下材料：

(一)拟合作企业的情况。包括该企业基本情况介绍、营业执照等法人资格证

明；

(二)拟合作业务的情况。包括合作意向书、合作发展规划、合作可行性分析报告等材料；

主管单位为新闻宣传部门的，还应当提交该主管单位就该项业务合作的意见。

互联网新闻信息服务单位与境内外中外合资经营、中外合作经营和外资经营的企业进行涉及互联网新闻信息服务业务的合作，可能导致互联网新闻信息服务单位不再符合许可条件的，不予通过安全评估。

第九条 国家和省、自治区、直辖市互联网信息办公室收到申请材料后，应当根据情况依法作出处理：

(一)申请材料齐全、符合要求的，予以受理；

(二) 申请材料不齐全、不符合要求的， 当场或五个工作日内一次性告知申请者应予更正或补充的内容；

(三)对依法不需要取得互联网新闻信息服务许可的，不予受理，并即时告知申请者，退回申请材料；

(四)对申请事项不属于职权范围的，应当即时作出不予受理的决定，并告知申请者向有关行政机关申请。

第十条 依法受理后，国家和省、自治区、直辖市互联网信息办公室按照本细则第五条、第六条、第七条的规定， 对申请材料进行审核，包括申请者是否符合许可条件、材料是否真实等。

审核过程中，国家和省、自治区、直辖市互联网信息办公室可依据实际情况，约见申请者主要负责人、总编辑， 到网站备案地、实际经营地、网站服务器所在地等其他相关场所进行实地检查。

第十一条 国家和省、自治区、直辖市互联网信息办公室应当依据《行政许可法》第四十二条， 在规定期限内依法作出批准或不予批准的决定。批准的， 核发《互联网新闻信息服务许可证》。

省、自治区、直辖市互联网信息办公室应当自作出批准决定之日起七个工作日内，向国家互联网信息办公室报告有关情况。

第十二条 根据《规定》第十七条，互联网新闻信息服务提供者变更以下事项，应当自变更之日起七个工作日内，向原许可机关申请办理变更手续：

(一)变更公司章程、服务场所、网站名称、接入服务提供者等事项;

(二)变更总编辑、主要负责人、股权结构、互联网地址等事项， 或者进行上市、合并、分立;

其中，变更总编辑、主要负责人、股权结构、互联网地址等事项， 或者进行上市、合并、分立， 导致互联网新闻信息服务提供者不再符合许可条件的，根据《规定》第二十三条予以处罚。

互联网新闻信息服务提供者新增服务类别，应当根据《规定》第六条， 依法取得相应的许可。

第十三条 互联网新闻信息服务提供者申请办理本细则第十二条相关变更手续，应当向原许可机关提交以下材料:

(一)变更申请书。包括申请变更事项、变更原因以及其他需要说明的问题，并加盖单位公章;

(二)变更事项材料。提交具体变更事项的说明、证明材料， 包括变更人员基本情况、资格证书、任免证明，或者变更后的营业执照、公司章程、租赁合同等，并加盖单位公章。

变更股权结构的，应当按照本细则第七条规定，提供相关股权材料。涉及上市的，还应当提供有关上市活动具体实施方案、新三板挂牌方案以及战略投资机构有关情况等材料。

涉及许可证所列事项变更的，应当提交许可证原件。

第十四条 《互联网新闻信息服务许可证》有效期为三年。有效期届满，需继续从事互联网新闻信息服务活动的，应当于有效期届满三十日前，按照许可程序，向原许可机关申请续办，并提交以下材料:

(一)许可续办申请书。包括前期从业情况说明、涉及本细则第五条许可条件相关情况的说明，以及其他需要说明的问题，并加盖单位公章;

(二)许可证原件。

主管单位为新闻宣传部门的，还应当提交该主管单位的意见。

《互联网新闻信息服务许可证》有效期届满， 未依法申请续办的，不得继续提供互联网新闻信息服务，原许可证作废。

第十五条 根据《行政许可法》第九条，互联网新闻信息服务许可不得转让。

互联网新闻信息服务提供者不得因业务调整、合并、分立等原因擅自转让许可。

第十六条 互联网新闻信息服务提供者终止服务的，应当自终止服务之日起三十日内向原许可机关办理注销手续，并提交以下材料：

(一)注销申请书。包括注销原因以及其他需要说明的问题，并加盖单位公章；

(二)许可证原件。

第十七条 根据《规定》第十九条，国家和地方互联网信息办公室建立抽查、考核等日常检查和定期检查相结合的监督管理制度，加强对互联网新闻信息服务活动的监督检查，有关单位、个人应当予以配合。

监督检查结果，依法向社会公开，接受社会监督。

第十八条 本细则与《规定》同步施行。

互联网论坛社区服务管理规定

(国家互联网信息办公室 2017 年 8 月 25 日)

第一条 为规范互联网论坛社区服务，促进互联网论坛社区行业健康有序发展，保护公民、法人和其他组织的合法权益，维护国家安全和公共利益，根据《中华人民共和国网络安全法》《国务院关于授权国家互联网信息办公室负责互联网信息内容管理工作的通知》，制定本规定。

第二条 在中华人民共和国境内从事互联网论坛社区服务，适用本规定。

本规定所称互联网论坛社区服务，是指在互联网上以论坛、贴吧、社区等形式，为用户提供互动式信息发布社区平台的服务。

第三条 国家互联网信息办公室负责全国互联网论坛社区服务的监督管理执法工作。地方互联网信息办公室依据职责负责本行政区域内互联网论坛社区服务的监督管理执法工作。

第四条 鼓励互联网论坛社区服务行业组织建立健全行业自律制度和行业准则，指导互联网论坛社区服务提供者建立健全服务规范，督促互联网论坛社区服务提供者依法提供服务、接受社会监督， 提高互联网论坛社区服务从业人员的职业素养。

第五条 互联网论坛社区服务提供者应当落实主体责任，建立健全信息审核、公共信息实时巡查、应急处置及个人信息保护等信息安全管理制度， 具有安全可控的防范措施，配备与服务规模相适应的专业人员，为有关部门依法履行职责提

供必要的技术支持。

第六条 互联网论坛社区服务提供者不得利用互联网论坛社区服务发布、传播法律法规和国家有关规定禁止的信息。

互联网论坛社区服务提供者应当与用户签订协议，明确用户不得利用互联网论坛社区服务发布、传播法律法规和国家有关规定禁止的信息， 情节严重的，服务提供者将封禁或者关闭有关账号、版块； 明确论坛社区版块发起者、管理者应当履行与其权利相适应的义务，对违反法律规定和协议约定、履行责任义务不到位的，服务提供者应当依法依约限制或取消其管理权限，直至封禁或者关闭有关账号、版块。

第七条 互联网论坛社区服务提供者应当加强对其用户发布信息的管理，发现含有法律法规和国家有关规定禁止的信息的，应当立即停止传输该信息，采取消除等处置措施，保存有关记录，并及时向国家或者地方互联网信息办公室报告。

第八条 互联网论坛社区服务提供者应当按照“后台实名、前台自愿”的原则，要求用户通过真实身份信息认证后注册账号，并对版块发起者和管理者实施真实身份信息备案、定期核验等。用户不提供真实身份信息的， 互联网论坛社区服务提供者不得为其提供信息发布服务。

互联网论坛社区服务提供者应当加强对注册用户虚拟身份信息、版块名称简介等的审核管理，不得出现法律法规和国家有关规定禁止的内容。

互联网论坛社区服务提供者应当保护用户身份信息，不得泄露、篡改、毁损，不得非法出售或者非法向他人提供。

第九条 互联网论坛社区服务提供者及其从业人员，不得通过发布、转载、删除信息或者干预呈现结果等手段，谋取不正当利益。

第十条 互联网论坛社区服务提供者开展经营和服务活动，必须遵守法律法规，尊重社会公德，遵守商业道德，诚实信用，承担社会责任。

第十一条 互联网论坛社区服务提供者应当建立健全公众投诉、举报制度，在显著位置公布投诉、举报方式，主动接受公众监督，及时处理公众投诉、举报。国家和地方互联网信息办公室依据职责，对举报受理落实情况进行监督检查。

第十二条 互联网论坛社区服务提供者违反本规定的， 由有关部门依照相关法律法规处理。

第十三条 本规定自 2017 年 10 月 1 日起施行。

互联网群组信息服务管理规定

（国家互联网信息办公室 2017 年 9 月 7 日）

第一条 为规范互联网群组信息服务，维护国家安全和公共利益，保护公民、法人和其他组织的合法权益，根据《中华人民共和国网络安全法》《国务院关于授权国家互联网信息办公室负责互联网信息内容管理工作的通知》，制定本规定。

第二条 在中华人民共和国境内提供、使用互联网群组信息服务，应当遵守本规定。

本规定所称互联网群组，是指互联网用户通过互联网站、移动互联网应用程序等建立的，用于群体在线交流信息的网络空间。本规定所称互联网群组信息服务提供者，是指提供互联网群组信息服务的平台。本规定所称互联网群组信息服务使用者，包括群组建立者、管理者和成员。

第三条 国家互联网信息办公室负责全国互联网群组信息服务的监督管理执法工作。地方互联网信息办公室依据职责负责本行政区域内的互联网群组信息服务的监督管理执法工作。

第四条 互联网群组信息服务提供者和使用者，应当坚持正确导向，弘扬社会主义核心价值观，培育积极健康的网络文化，维护良好网络生态。

第五条 互联网群组信息服务提供者应当落实信息内容安全管理主体责任，配备与服务规模相适应的专业人员和技术能力，建立健全用户注册、信息审核、应急处置、安全防护等管理制度。

互联网群组信息服务提供者应当制定并公开管理规则和平台公约，与使用者签订服务协议，明确双方权利义务。

第六条 互联网群组信息服务提供者应当按照“后台实名、前台自愿”的原则，对互联网群组信息服务使用者进行真实身份信息认证，用户不提供真实身份信息的，不得为其提供信息发布服务。

互联网群组信息服务提供者应当采取必要措施保护使用者个人信息安全，不得泄露、篡改、毁损，不得非法出售或者非法向他人提供。

第七条 互联网群组信息服务提供者应当根据互联网群组的性质类别、成员规模、活跃程度等实行分级分类管理，制定具体管理制度并向国家或省、自治区、

直辖市互联网信息办公室备案，依法规范群组信息传播秩序。

互联网群组信息服务提供者应当建立互联网群组信息服务使用者信用等级管理体系，根据信用等级提供相应服务。

第八条 互联网群组信息服务提供者应当根据自身服务规模和管理能力，合理设定群组成员人数和个人建立群数、参加群数上限。

互联网群组信息服务提供者应设置和显示唯一群组识别编码，对成员达到一定规模的群组要设置群信息页面，注明群组名称、人数、类别等基本信息。

互联网群组信息服务提供者应根据群组规模类别，分级审核群组建立者真实身份、信用等级等建群资质， 完善建群、入群等审核验证功能， 并标注群组建立者、管理者及成员群内身份信息。

第九条 互联网群组建立者、管理者应当履行群组管理责任，依据法律法规、用户协议和平台公约，规范群组网络行为和信息发布，构建文明有序的网络群体空间。

互联网群组成员在参与群组信息交流时，应当遵守法律法规，文明互动、理性表达。

互联网群组信息服务提供者应为群组建立者、管理者进行群组管理提供必要功能权限。

第十条 互联网群组信息服务提供者和使用者不得利用互联网群组传播法律法规和国家有关规定禁止的信息内容。

第十一条 互联网群组信息服务提供者应当对违反法律法规和国家有关规定的互联网群组，依法依约采取警示整改、暂停发布、关闭群组等处置措施， 保存有关记录，并向有关主管部门报告。

互联网群组信息服务提供者应当对违反法律法规和国家有关规定的群组建立者、管理者等使用者， 依法依约采取降低信用等级、暂停管理权限、取消建群资格等管理措施，保存有关记录，并向有关主管部门报告。

互联网群组信息服务提供者应当建立黑名单管理制度，对违法违约情节严重的群组及建立者、管理者和成员纳入黑名单，限制群组服务功能，保存有关记录，并向有关主管部门报告。

第十二条 互联网群组信息服务提供者和使用者应当接受社会公众和行业组

织的监督，建立健全投诉举报渠道，设置便捷举报入口，及时处理投诉举报。国家和地方互联网信息办公室依据职责，对举报受理落实情况进行监督检查。

鼓励互联网行业组织指导推动互联网群组信息服务提供者制定行业公约，加强行业自律，履行社会责任。

第十三条 互联网群组信息服务提供者应当配合有关主管部门依法进行的监督检查，并提供必要的技术支持和协助。

互联网群组信息服务提供者应当按规定留存网络日志不少于六个月。

第十四条 互联网群组信息服务提供者和使用者违反本规定的，由有关部门依照相关法律法规处理。

第十五条 本规定自 2017 年 10 月 8 日起施行。

互联网新闻信息服务新技术新应用安全评估管理规定

（国家互联网信息办公室 2017 年 10 月 30 日）

第一条 为规范开展互联网新闻信息服务新技术新应用安全评估工作，维护国家安全和公共利益，保护公民、法人和其他组织的合法权益， 根据《中华人民共和国网络安全法》《互联网新闻信息服务管理规定》，制定本规定。

第二条 国家和省、自治区、直辖市互联网信息办公室组织开展互联网新闻信息服务新技术新应用安全评估，适用本规定。

本规定所称互联网新闻信息服务新技术新应用（以下简称“新技术新应用”），是指用于提供互联网新闻信息服务的创新性应用（包括功能及应用形式）及相关支撑技术。

本规定所称互联网新闻信息服务新技术新应用安全评估（以下简称“新技术新应用安全评估”），是指根据新技术新应用的新闻舆论属性、社会动员能力及由此产生的信息内容安全风险确定评估等级，审查评价其信息安全管理制度和技术保障措施的活动。

第三条 互联网新闻信息服务提供者调整增设新技术新应用，应当建立健全信息安全管理制度和安全可控的技术保障措施，不得发布、传播法律法规禁止的信息内容。

第四条 国家互联网信息办公室负责全国新技术新应用安全评估工作。省、自治区、直辖市互联网信息办公室依据职责负责本行政区域内新技术新应用安全

评估工作。

国家和省、自治区、直辖市互联网信息办公室可以委托第三方机构承担新技术新应用安全评估的具体实施工作。

第五条 鼓励支持新技术新应用安全评估相关行业组织和专业机构加强自律，建立健全安全评估服务质量评议和信用、能力公示制度，促进行业规范发展。

第六条 互联网新闻信息服务提供者应当建立健全新技术新应用安全评估管理制度和保障制度，按照本规定要求自行组织开展安全评估，为国家和省、自治区、直辖市互联网信息办公室组织开展安全评估提供必要的配合， 并及时完成整改。

第七条 有下列情形之一的，互联网新闻信息服务提供者应当自行组织开展新技术新应用安全评估，编制书面安全评估报告，并对评估结果负责：

(一)应用新技术、调整增设具有新闻舆论属性或社会动员能力的应用功能的；

(二)新技术、新应用功能在用户规模、功能属性、技术实现方式、基础资源配置等方面的改变导致新闻舆论属性或社会动员能力发生重大变化的。

国家互联网信息办公室适时发布新技术新应用安全评估目录，供互联网新闻信息服务提供者自行组织开展安全评估参考。

第八条 互联网新闻信息服务提供者按照本规定第七条自行组织开展新技术新应用安全评估，发现存在安全风险的，应当及时整改，直至消除相关安全风险。

按照本规定第七条规定自行组织开展安全评估的，应当在应用新技术、调整增设应用功能前完成评估。

第九条 互联网新闻信息服务提供者按照本规定第八条自行组织开展新技术新应用安全评估后，应当自安全评估完成之日起 10 个工作日内报请国家或者省、自治区、直辖市互联网信息办公室组织开展安全评估。

第十条 报请国家或者省、自治区、直辖市互联网信息办公室组织开展新技术新应用安全评估，报请主体为中央新闻单位或者中央新闻宣传部门主管的单位的，由国家互联网信息办公室组织开展安全评估；报请主体为地方新闻单位或者地方新闻宣传部门主管的单位的，由省、自治区、直辖市互联网信息办公室组织开展安全评估；报请主体为其他单位的，经所在地省、自治区、直辖市互联网信息办公室组织开展安全评估后，将评估材料及意见报国家互联网信息办公室审核

后形成安全评估报告。

第十一条 互联网新闻信息服务提供者报请国家或者省、自治区、直辖市互联网信息办公室组织开展新技术新应用安全评估，应当提供下列材料，并对提供材料的真实性负责：

(一)服务方案(包括服务项目、服务方式、业务形式、服务范围等)；

(二)产品(服务)的主要功能和主要业务流程，系统组成(主要软硬件系统的种类、品牌、版本、部署位置等概要介绍)；

(三)产品(服务)配套的信息安全管理制度和技术保障措施；

(四)自行组织开展并完成的安全评估报告；

(五)其他开展安全评估所需的必要材料。

第十二条 国家和省、自治区、直辖市互联网信息办公室应当自材料齐备之日起 45 个工作日内组织完成新技术新应用安全评估。

国家和省、自治区、直辖市互联网信息办公室可以采取书面确认、实地核查、网络监测等方式对报请材料进行进一步核实，服务提供者应予配合。

国家和省、自治区、直辖市互联网信息办公室组织完成安全评估后， 应自行或委托第三方机构编制形成安全评估报告。

第十三条 新技术新应用安全评估报告载明的意见认为新技术新应用存在信息安全风险隐患，未能配套必要的安全保障措施手段的，互联网新闻信息服务提供者应当及时进行整改，直至符合法律法规规章等相关规定和国家强制性标准相关要求。在整改完成前， 拟调整增设的新技术新应用不得用于提供互联网新闻信息服务。

服务提供者拒绝整改，或整改后未达法律法规规章等相关规定和国家强制性标准相关要求，而导致不再符合许可条件的，由国家和省、自治区、直辖市互联网信息办公室依据《互联网新闻信息服务管理规定》第二十三条的规定， 责令服务提供者限期改正；逾期仍不符合许可条件的，暂停新闻信息更新；《互联网新闻信息服务许可证》有效期届满仍不符合许可条件的，不予换发许可证。

第十四条 组织开展新技术新应用安全评估的相关单位和人员应当对在履行职责中知悉的国家秘密、商业秘密和个人信息严格保密， 不得泄露、出售或者非法向他人提供。

第十五条 国家和省、自治区、直辖市互联网信息办公室应当建立主动监测管理制度，对新技术新应用加强监测巡查，强化信息安全风险管理，督导企业主体责任落实。

第十六条 互联网新闻信息服务提供者未按照本规定进行安全评估，违反《互联网新闻信息服务管理规定》的，由国家和地方互联网信息办公室依法予以处罚。

第十七条 申请提供互联网新闻信息服务，报请国家或者省、自治区、直辖市互联网信息办公室组织开展新技术新应用安全评估的，参照适用本规定。

第十八条 本规定自 2017 年 12 月 1 日起施行。

互联网新闻信息服务单位内容管理从业人员管理办法

（国家互联网信息办公室 2017 年 10 月 30 日）

第一章 总 则

第一条 为加强对互联网新闻信息服务单位内容管理从业人员（以下简称“从业人员”）的管理，维护从业人员和社会公众的合法权益，促进互联网新闻信息服务健康有序发展，根据《中华人民共和国网络安全法》《互联网新闻信息服务管理规定》，制定本办法。

第二条 本办法所称从业人员，是指互联网新闻信息服务单位中专门从事互联网新闻信息采编发布、转载和审核等内容管理工作的人员。

第三条 本办法所称互联网新闻信息服务单位，是指依法取得互联网新闻信息服务许可，通过互联网站、应用程序、论坛、博客、微博客、公众账号、即时通信工具、网络直播等形式向社会公众提供互联网新闻信息服务的单位。

第四条 国家互联网信息办公室负责全国互联网新闻信息服务单位从业人员教育培训工作的规划指导和从业情况的监督检查。

地方互联网信息办公室依据职责负责本地区互联网新闻信息服务单位从业人员教育培训工作的规划指导和从业情况的监督检查。

第二章 从业人员行为规范

第五条 从业人员应当遵守宪法、法律和行政法规，坚持正确政治方向和舆论导向，贯彻执行党和国家有关新闻舆论工作的方针政策，维护国家利益和公共利益，严格遵守互联网内容管理的法律法规和国家有关规定，促进形成积极健康、向上向善的网络文化，推动构建风清气正的网络空间。

第六条 从业人员应当坚持马克思主义新闻观，坚持社会主义核心价值观，坚持以人民为中心的工作导向，树立群众观点，坚决抵制不良风气和低俗内容。

第七条 从业人员应当恪守新闻职业道德，坚持新闻真实性原则，认真核实新闻信息来源，按规定转载国家规定范围内的单位发布的新闻信息，杜绝编发虚假互联网新闻信息，确保互联网新闻信息真实、准确、全面、客观。

第八条 从业人员不得从事有偿新闻活动。不得利用互联网新闻信息采编发布、转载和审核等工作便利从事广告、发行、赞助、中介等经营活动， 谋取不正当利益。不得利用网络舆论监督等工作便利进行敲诈勒索、打击报复等活动。

第三章 从业人员教育培训

第九条 国家互联网信息办公室组织开展对中央新闻单位(含其控股的单位)和中央新闻宣传部门主管的单位主办的互联网新闻信息服务单位从业人员的教育培训工作。

省、自治区、直辖市互联网信息办公室组织开展对所在地地方新闻单位(含其控股的单位)和地方新闻宣传部门主管的单位、其他单位主办的互联网新闻信息服务单位，以及中央重点新闻网站地方频道从业人员的教育培训工作。

省、自治区、直辖市互联网信息办公室应当按要求向国家互联网信息办公室报告组织开展的从业人员教育培训工作情况。

第十条 互联网新闻信息服务单位应当建立完善从业人员教育培训制度，建立培训档案，加强培训管理，自行组织开展从业人员初任培训、专项培训、定期培训等工作，按要求组织从业人员参加国家和省、自治区、直辖市互联网信息办公室组织开展的教育培训工作。

第十一条 从业人员应当按要求参加国家和省、自治区、直辖市互联网信息办公室组织开展的教育培训，每三年不少于 40 个学时。

从业人员应当接受所在互联网新闻信息服务单位自行组织开展的、每年不少于 40 个学时的教育培训，其中关于马克思主义新闻观的教育培训不少于 10 个学时。

第十二条 从业人员的教育培训内容应当包括马克思主义新闻观，党和国家关于网络安全和信息化、新闻舆论等工作的重要决策部署、政策措施和相关法律法规，从业人员职业道德规范等。

第十三条 互联网新闻信息服务单位自行组织从业人员开展的教育培训工作，应当接受国家和地方互联网信息办公室的指导和监督。有关情况纳入国家和地方互联网信息办公室对该单位的监督检查内容。

第四章 从业人员监督管理

第十四条 国家和地方互联网信息办公室指导互联网新闻信息服务单位建立健全从业人员准入、奖惩、考评、退出等制度。

互联网新闻信息服务单位应当建立健全从业人员劳动人事制度，加强从业人员管理，按照国家和地方互联网信息办公室要求，定期报送从业人员有关信息，并及时报告从业人员变动情况。

第十五条 国家互联网信息办公室建立从业人员统一的管理信息系统，对从业人员基本信息、从业培训经历和奖惩情况等进行记录， 并及时更新、调整。地方互联网信息办公室负责对属地从业人员建立管理信息系统，并将更新、调整情况及时上报上一级互联网信息办公室。

国家和地方互联网信息办公室依法建立从业人员信用档案和黑名单。

第十六条 从业人员从事互联网新闻信息服务活动，存在违反本办法第五条至第八条规定，以及其他违反党和国家新闻舆论领域有关方针政策的行为的，国家或省、自治区、直辖市互联网信息办公室负责对其所在互联网新闻信息服务单位进行约谈，督促该单位对有关人员加强管理和教育培训。

从业人员存在违法行为的，根据有关法律法规依法处理。构成犯罪的， 依法追究刑事责任。

互联网新闻信息服务单位发现从业人员存在违法行为的，应当依法依约对其给予警示、处分直至解除聘用合同或劳动合同，并在 15 个工作日内，按照分级管理、属地管理要求， 将有关情况报告国家或省、自治区、直辖市互联网信息办公室。

第十七条 国家和地方互联网信息办公室将互联网新闻信息服务单位从业人员的从业情况纳入对该单位的监督检查内容。

互联网新闻信息服务单位对从业人员管理不力，造成严重后果，导致其不再符合许可条件的，由国家和地方互联网信息办公室依据《互联网新闻信息服务管理规定》第二十三条有关规定予以处理。

第十八条 从业人员提供互联网新闻信息服务，应当自觉接受社会监督。互联网新闻信息服务单位应当建立举报制度，畅通社会公众监督举报的渠道。

第五章 附 则

第十九条 互联网新闻信息服务单位的主管主办单位或宣传管理部门、新闻出版广电部门有从业人员教育培训、管理工作等方面安排和规定的， 应当同时符合其规定。

本办法所称从业人员，不包括互联网新闻信息服务单位中党务、人事、行政、后勤、经营、工程技术等非直接提供互联网新闻信息服务的人员。

第二十条 本办法自 2017 年 12 月 1 日起施行。

微博客信息服务管理规定

（国家互联网信息办公室 2018 年 2 月 2 日）

第一条 为促进微博客信息服务健康有序发展，保护公民、法人和其他组织的合法权益，维护国家安全和公共利益，根据《中华人民共和国网络安全法》《国务院关于授权国家互联网信息办公室负责互联网信息内容管理工作的通知》，制定本规定。

第二条 在中华人民共和国境内从事微博客信息服务，应当遵守本规定。

本规定所称微博客，是指基于使用者关注机制，主要以简短文字、图片、视频等形式实现信息传播、获取的社交网络服务。

微博客服务提供者是指提供微博客平台服务的主体。微博客服务使用者是指使用微博客平台从事信息发布、互动交流等的行为主体。

微博客信息服务是指提供微博客平台服务及使用微博客平台从事信息发布、传播等行为。

第三条 国家互联网信息办公室负责全国微博客信息服务的监督管理执法工作。地方互联网信息办公室依据职责负责本行政区域内的微博客信息服务的监督管理执法工作。

第四条 微博客服务提供者应当依法取得法律法规规定的相关资质。

向社会公众提供互联网新闻信息服务的，应当依法取得互联网新闻信息服务许可，并在许可范围内开展服务，禁止未经许可或超越许可范围开展互联网新闻信息服务活动。

第五条 微博客服务提供者应当发挥促进经济发展、服务社会大众的积极作用，弘扬社会主义核心价值观，传播先进文化，坚持正确舆论导向，倡导依法上网、文明上网、安全上网。

第六条 微博客服务提供者应当落实信息内容安全管理主体责任，建立健全用户注册、信息发布审核、跟帖评论管理、应急处置、从业人员教育培训等制度及总编辑制度，具有安全可控的技术保障和防范措施，配备与服务规模相适应的管理人员。

微博客服务提供者应当制定平台服务规则，与微博客服务使用者签订服务协议，明确双方权利、义务，要求微博客服务使用者遵守相关法律法规。

第七条 微博客服务提供者应当按照“后台实名、前台自愿”的原则，对微博客服务使用者进行基于组织机构代码、身份证件号码、移动电话号码等方式的真实身份信息认证、定期核验。微博客服务使用者不提供真实身份信息的， 微博客服务提供者不得为其提供信息发布服务。

微博客服务提供者应当保障微博客服务使用者的信息安全，不得泄露、篡改、毁损，不得出售或者非法向他人提供。

第八条 微博客服务使用者申请前台实名认证账号的，应当提供与认证信息相符的有效证明材料。

境内具有组织机构特征的微博客服务使用者申请前台实名认证账号的，应当提供组织机构代码证、营业执照等有效证明材料。

境外组织和机构申请前台实名认证账号的，应当提供驻华机构出具的有效证明材料。

第九条 微博客服务提供者应当按照分级分类管理原则，根据微博客服务使用者主体类型、发布内容、关注者数量、信用等级等制定具体管理制度， 提供相应服务，并向国家或省、自治区、直辖市互联网信息办公室备案。

第十条 微博客服务提供者应当对申请前台实名认证账号的微博客服务使用者进行认证信息审核，并按照注册地向国家或省、自治区、直辖市互联网信息办公室分类备案。微博客服务使用者提供的证明材料与认证信息不相符的， 微博客服务提供者不得为其提供前台实名认证服务。

各级党政机关、企事业单位、人民团体和新闻媒体等组织机构对所开设的前

台实名认证账号发布的信息内容及其跟帖评论负有管理责任。微博客服务提供者应当提供管理权限等必要支持。

第十一条 微博客服务提供者应当建立健全辟谣机制，发现微博客服务使用者发布、传播谣言或不实信息，应当主动采取辟谣措施。

第十二条 微博客服务提供者和微博客服务使用者不得利用微博客发布、传播法律法规禁止的信息内容。

微博客服务提供者发现微博客服务使用者发布、传播法律法规禁止的信息内容，应当依法立即停止传输该信息、采取消除等处置措施， 保存有关记录，并向有关主管部门报告。

第十三条 微博客服务提供者应用新技术、调整增设具有新闻舆论属性或社会动员能力的应用功能，应当报国家或省、自治区、直辖市互联网信息办公室进行安全评估。

第十四条 微博客服务提供者应当自觉接受社会监督，设置便捷的投诉举报入口，及时处理公众投诉举报。

第十五条 国家鼓励和指导互联网行业组织建立健全微博客行业自律制度和行业准则，推动微博客行业信用等级评价和信用体系建设，督促微博客服务提供者依法提供服务、接受社会监督。

第十六条 微博客服务提供者应当遵守国家相关法律法规规定，配合有关部门开展监督管理执法工作，并提供必要的技术支持和协助。

微博客服务提供者应当记录微博客服务使用者日志信息，保存时间不少于六个月。

第十七条 微博客服务提供者违反本规定的， 由有关部门依照相关法律法规处理。

第十八条 本规定自 2018 年 3 月 20 日起施行。

具有舆论属性或社会动员能力的互联网信息服务安全评估规定

（国家互联网信息办公室 2018 年 11 月 15 日）

第一条 为加强对具有舆论属性或社会动员能力的互联网信息服务和相关新技术新应用的安全管理，规范互联网信息服务活动，维护国家安全、社会秩序和公共利益，根据《中华人民共和国网络安全法》《互联网信息服务管理办法》《计

算机信息网络国际联网安全保护管理办法》，制订本规定。

第二条 本规定所称具有舆论属性或社会动员能力的互联网信息服务，包括下列情形：

(一)开办论坛、博客、微博客、聊天室、通讯群组、公众账号、短视频、网络直播、信息分享、小程序等信息服务或者附设相应功能；

(二)开办提供公众舆论表达渠道或者具有发动社会公众从事特定活动能力的其他互联网信息服务。

第三条 互联网信息服务提供者具有下列情形之一的，应当依照本规定自行开展安全评估，并对评估结果负责：

(一)具有舆论属性或社会动员能力的信息服务上线，或者信息服务增设相关功能的；

(二)使用新技术新应用，使信息服务的功能属性、技术实现方式、基础资源配置等发生重大变更，导致舆论属性或者社会动员能力发生重大变化的；

(三)用户规模显著增加，导致信息服务的舆论属性或者社会动员能力发生重大变化的；

(四)发生违法有害信息传播扩散，表明已有安全措施难以有效防控网络安全风险的；

(五)地市级以上网信部门或者公安机关书面通知需要进行安全评估的其他情形。

第四条 互联网信息服务提供者可以自行实施安全评估，也可以委托第三方安全评估机构实施。

第五条 互联网信息服务提供者开展安全评估，应当对信息服务和新技术新应用的合法性，落实法律、行政法规、部门规章和标准规定的安全措施的有效性，防控安全风险的有效性等情况进行全面评估，并重点评估下列内容：

(一)确定与所提供服务相适应的安全管理负责人、信息审核人员或者建立安全管理机构的情况；

(二)用户真实身份核验以及注册信息留存措施；

(三)对用户的账号、操作时间、操作类型、网络源地址和目标地址、网络源端口、客户端硬件特征等日志信息，以及用户发布信息记录的留存措施；

(四)对用户账号和通讯群组名称、昵称、简介、备注、标识， 信息发布、转发、评论和通讯群组等服务功能中违法有害信息的防范处置和有关记录保存措施；

(五)个人信息保护以及防范违法有害信息传播扩散、社会动员功能失控风险的技术措施；

(六)建立投诉、举报制度， 公布投诉、举报方式等信息， 及时受理并处理有关投诉和举报的情况；

(七)建立为网信部门依法履行互联网信息服务监督管理职责提供技术、数据支持和协助的工作机制的情况；

(八)建立为公安机关、国家安全机关依法维护国家安全和查处违法犯罪提供技术、数据支持和协助的工作机制的情况。

第六条 互联网信息服务提供者在安全评估中发现存在安全隐患的，应当及时整改，直至消除相关安全隐患。

经过安全评估，符合法律、行政法规、部门规章和标准的， 应当形成安全评估报告。安全评估报告应当包括下列内容：

(一)互联网信息服务的功能、服务范围、软硬件设施、部署位置等基本情况和相关证照获取情况；

(二)安全管理制度和技术措施落实情况及风险防控效果；

(三)安全评估结论；

(四)其他应当说明的相关情况。

第七条 互联网信息服务提供者应当将安全评估报告通过全国互联网安全管理服务平台提交所在地地市级以上网信部门和公安机关。

具有本规定第三条第一项、第二项情形的， 互联网信息服务提供者应当在信息服务、新技术新应用上线或者功能增设前提交安全评估报告； 具有本规定第三条第三、四、五项情形的，应当自相关情形发生之日起 30 个工作日内提交安全评估报告。

第八条 地市级以上网信部门和公安机关应当依据各自职责对安全评估报告进行书面审查。

发现安全评估报告内容、项目缺失， 或者安全评估方法明显不当的，应当责令互联网信息服务提供者限期重新评估。

发现安全评估报告内容不清的，可以责令互联网信息服务提供者补充说明。

第九条 网信部门和公安机关根据对安全评估报告的书面审查情况，认为有必要的，应当依据各自职责对互联网信息服务提供者开展现场检查。

网信部门和公安机关开展现场检查原则上应当联合实施，不得干扰互联网信息服务提供者正常的业务活动。

第十条 对存在较大安全风险、可能影响国家安全、社会秩序和公共利益的互联网信息服务，省级以上网信部门和公安机关应当组织专家进行评审，必要时可以会同属地相关部门开展现场检查。

第十一条 网信部门和公安机关开展现场检查，应当依照有关法律、行政法规、部门规章的规定进行。

第十二条 网信部门和公安机关应当建立监测管理制度，加强网络安全风险管理，督促互联网信息服务提供者依法履行网络安全义务。

发现具有舆论属性或社会动员能力的互联网信息服务提供者未按本规定开展安全评估的，网信部门和公安机关应当通知其按本规定开展安全评估。

第十三条 网信部门和公安机关发现具有舆论属性或社会动员能力的互联网信息服务提供者拒不按照本规定开展安全评估的，应当通过全国互联网安全管理服务平台向公众提示该互联网信息服务存在安全风险，并依照各自职责对该互联网信息服务实施监督检查，发现存在违法行为的，应当依法处理。

第十四条 网信部门统筹协调具有舆论属性或社会动员能力的互联网信息服务安全评估工作，公安机关的安全评估工作情况定期通报网信部门。

第十五条 网信部门、公安机关及其工作人员对在履行职责中知悉的国家秘密、商业秘密和个人信息应当严格保密，不得泄露、出售或者非法向他人提供。

第十六条 对于互联网新闻信息服务新技术新应用的安全评估，依照《互联网新闻信息服务新技术新应用安全评估管理规定》执行。

第十七条 本规定自 2018 年 11 月 30 日起施行。

金融信息服务管理规定

（国家互联网信息办公室 2018 年 12 月 26 日）

第一条 为加强金融信息服务内容管理，提高金融信息服务质量，促进金融信息服务健康有序发展，保护自然人、法人和非法人组织的合法权益， 维护国家

安全和公共利益，根据《中华人民共和国网络安全法》《互联网信息服务管理办法》《国务院关于授权国家互联网信息办公室负责互联网信息内容管理工作的通知》，制定本规定。

第二条 在中华人民共和国境内从事金融信息服务，应当遵守本规定。

本规定所称金融信息服务，是指向从事金融分析、金融交易、金融决策或者其他金融活动的用户提供可能影响金融市场的信息和／或者金融数据的服务。该服务不同于通讯社服务。

第三条 国家互联网信息办公室负责全国金融信息服务的监督管理执法工作，地方互联网信息办公室依据职责负责本行政区域内的金融信息服务的监督管理执法工作。

第四条 金融信息服务提供者从事互联网新闻信息服务、法定特许或者应予以备案的金融业务应当取得相应资质，并接受有关主管部门的监督管理。

第五条 金融信息服务提供者应当履行主体责任，配备与服务规模相适应的管理人员，建立信息内容审核、信息数据保存、信息安全保障、个人信息保护、知识产权保护等服务规范。

第六条 金融信息服务提供者应当在显著位置准确无误注明信息来源，并确保文字、图像、视频、音频等形式的金融信息来源可追溯。

第七条 金融信息服务提供者应当配备相关专业人员，负责金融信息内容的审核，确保金融信息真实、客观、合法。

第八条 金融信息服务提供者不得制作、复制、发布、传播含有下列内容的信息：

(一)散布虚假金融信息，危害国家金融安全以及社会稳定的；

(二)歪曲国家财政货币政策、金融管理政策， 扰乱经济秩序、损害国家利益的；

(三)教唆他人商业欺诈或经济犯罪，造成社会影响的；

(四)虚构证券、基金、期货、外汇等金融市场事件或新闻的；

(五)宣传有关主管部门禁止的金融产品与服务的；

(六)法律、法规和规章禁止的其他内容。

第九条 金融信息服务提供者应当自觉接受用户监督，设置便捷投诉窗口，

及时妥善处理投诉事宜，并保存有关记录。

第十条 金融信息服务使用者发现金融信息服务提供者所提供的金融信息含有本规定第八条所列内容的，可以向国家或地方互联网信息办公室举报。

第十一条 金融信息服务提供者发现含有本规定第八条所列信息内容的，应当立即终止传输、禁止使用和停止传播该信息内容， 及时采取处置措施，消除相关信息内容，保存完整记录并向国家或地方互联网信息办公室报告。

第十二条 国家和地方互联网信息办公室应当建立日常检查和定期检查相结合的监督管理制度，依法对金融信息服务活动实施监督检查，有关单位、个人应当予以配合。

第十三条 金融信息服务使用者向社会传播金融信息服务提供者提供的金融信息中含有本规定第八条所列内容的，由国家或地方互联网信息办公室以及有关主管部门依法处罚。

第十四条 金融信息服务提供者违反本规定第五条、第六条、第七条、第八条、第九条规定的， 由国家或地方互联网信息办公室依据职责进行约谈、公开谴责、责令改正、列入失信名单； 依法应当予以行政处罚的，由国家或地方互联网信息办公室等有关主管部门给予行政处罚；构成犯罪的，依法追究刑事责任。

第十五条 国家和地方互联网信息办公室根据工作需要，与有关主管部门建立金融信息服务情况通报、信息共享等工作机制，对违法违规行为实施联合惩戒。

第十六条 鼓励金融信息服务提供者建立行业自律组织，制定服务规范，推动行业信用体系建设，促进行业健康有序发展。

第十七条 本规定自 2019 年 2 月 1 日起施行。

互联网用户公众账号信息服务管理规定

（国家互联网信息办公室 2021 年 01 月 22 日）

第一章 总 则

第一条 为了规范互联网用户公众账号信息服务，维护国家安全和公共利益，保护公民、法人和其他组织的合法权益， 根据《中华人民共和国网络安全法》《互联网信息服务管理办法》《网络信息内容生态治理规定》等法律法规和国家有关规定，制定本规定。

第二条 在中华人民共和国境内提供、从事互联网用户公众账号信息服务，

应当遵守本规定。

第三条 国家网信部门负责全国互联网用户公众账号信息服务的监督管理执法工作。地方网信部门依据职责负责本行政区域内互联网用户公众账号信息服务的监督管理执法工作。

第四条 公众账号信息服务平台和公众账号生产运营者应当遵守法律法规，遵循公序良俗，履行社会责任，坚持正确舆论导向、价值取向， 弘扬社会主义核心价值观，生产发布向上向善的优质信息内容，发展积极健康的网络文化，维护清朗网络空间。

鼓励各级党政机关、企事业单位和人民团体注册运营公众账号， 生产发布高质量政务信息或者公共服务信息，满足公众信息需求，推动经济社会发展。

鼓励公众账号信息服务平台积极为党政机关、企事业单位和人民团体提升政务信息发布、公共服务和社会治理水平，提供充分必要的技术支持和安全保障。

第五条 公众账号信息服务平台提供互联网用户公众账号信息服务，应当取得国家法律、行政法规规定的相关资质。

公众账号信息服务平台和公众账号生产运营者向社会公众提供互联网新闻信息服务，应当取得互联网新闻信息服务许可。

第二章 公众账号信息服务平台

第六条 公众账号信息服务平台应当履行信息内容和公众账号管理主体责任，配备与业务规模相适应的管理人员和技术能力，设置内容安全负责人岗位，建立健全并严格落实账号注册、信息内容安全、生态治理、应急处置、网络安全、数据安全、个人信息保护、知识产权保护、信用评价等管理制度。

公众账号信息服务平台应当依据法律法规和国家有关规定，制定并公开信息内容生产、公众账号运营等管理规则、平台公约， 与公众账号生产运营者签订服务协议，明确双方内容发布权限、账号管理责任等权利义务。

第七条 公众账号信息服务平台应当按照国家有关标准和规范，建立公众账号分类注册和分类生产制度，实施分类管理。

公众账号信息服务平台应当依据公众账号信息内容生产质量、信息传播能力、账号主体信用评价等指标，建立分级管理制度，实施分级管理。

公众账号信息服务平台应当将公众账号和内容生产与账号运营管理规则、平

台公约、服务协议等向所在地省、自治区、直辖市网信部门备案； 上线具有舆论属性或者社会动员能力的新技术新应用新功能，应当按照有关规定进行安全评估。

第八条 公众账号信息服务平台应当采取复合验证等措施，对申请注册公众账号的互联网用户进行基于移动电话号码、居民身份证号码或者统一社会信用代码等方式的真实身份信息认证，提高认证准确率。用户不提供真实身份信息的，或者冒用组织机构、他人真实身份信息进行虚假注册的，不得为其提供相关服务。

公众账号信息服务平台应当对互联网用户注册的公众账号名称、头像和简介等进行合法合规性核验，发现账号名称、头像和简介与注册主体真实身份信息不相符的，特别是擅自使用或者关联党政机关、企事业单位等组织机构或者社会知名人士名义的，应当暂停提供服务并通知用户限期改正，拒不改正的，应当终止提供服务；发现相关注册信息含有违法和不良信息的，应当依法及时处置。

公众账号信息服务平台应当禁止被依法依约关闭的公众账号以相同账号名称重新注册；对注册与其关联度高的账号名称，还应当对账号主体真实身份信息、服务资质等进行必要核验。

第九条 公众账号信息服务平台对申请注册从事经济、教育、医疗卫生、司法等领域信息内容生产的公众账号，应当要求用户在注册时提供其专业背景，以及依照法律、行政法规获得的职业资格或者服务资质等相关材料， 并进行必要核验。

公众账号信息服务平台应当对核验通过后的公众账号加注专门标识，并根据用户的不同主体性质，公示内容生产类别、运营主体名称、注册运营地址、统一社会信用代码、联系方式等注册信息，方便社会监督查询。

公众账号信息服务平台应当建立动态核验巡查制度，适时核验生产运营者注册信息的真实性、有效性。

第十条 公众账号信息服务平台应当对同一主体在本平台注册公众账号的数量合理设定上限。对申请注册多个公众账号的用户， 还应当对其主体性质、服务资质、业务范围、信用评价等进行必要核验。

公众账号信息服务平台对互联网用户注册后超过六个月不登录、不使用的公众账号，可以根据服务协议暂停或者终止提供服务。

公众账号信息服务平台应当健全技术手段，防范和处置互联网用户超限量注

册、恶意注册、虚假注册等违规注册行为。

第十一条 公众账号信息服务平台应当依法依约禁止公众账号生产运营者违规转让公众账号。

公众账号生产运营者向其他用户转让公众账号使用权的，应当向平台提出申请。平台应当依据前款规定对受让方用户进行认证核验，并公示主体变更信息。平台发现生产运营者未经审核擅自转让公众账号的，应当及时暂停或者终止提供服务。

公众账号生产运营者自行停止账号运营，可以向平台申请暂停或者终止使用。平台应当按照服务协议暂停或者终止提供服务。

第十二条 公众账号信息服务平台应当建立公众账号监测评估机制，防范账号订阅数、用户关注度、内容点击率、转发评论量等数据造假行为。

公众账号信息服务平台应当规范公众账号推荐订阅关注机制，健全技术手段，及时发现、处置公众账号订阅关注数量的异常变动情况。未经互联网用户知情同意，不得以任何方式强制或者变相强制订阅关注其他用户公众账号。

第十三条 公众账号信息服务平台应当建立生产运营者信用等级管理体系，根据信用等级提供相应服务。

公众账号信息服务平台应当建立健全网络谣言等虚假信息预警、发现、溯源、甄别、辟谣、消除等处置机制， 对制作发布虚假信息的公众账号生产运营者降低信用等级或者列入黑名单。

第十四条 公众账号信息服务平台与生产运营者开展内容供给与账号推广合作，应当规范管理电商销售、广告发布、知识付费、用户打赏等经营行为， 不得发布虚假广告、进行夸大宣传、实施商业欺诈及商业诋毁等，防止违法违规运营。

公众账号信息服务平台应当加强对原创信息内容的著作权保护，防范盗版侵权行为。

平台不得利用优势地位干扰生产运营者合法合规运营、侵犯用户合法权益。

第三章 公众账号生产运营者

第十五条 公众账号生产运营者应当按照平台分类管理规则，在注册公众账号时如实填写用户主体性质、注册地、运营地、内容生产类别、联系方式等基本信息，组织机构用户还应当注明主要经营或者业务范围。

公众账号生产运营者应当遵守平台内容生产和账号运营管理规则、平台公约和服务协议，按照公众账号登记的内容生产类别，从事相关行业领域的信息内容生产发布。

第十六条 公众账号生产运营者应当履行信息内容生产和公众账号运营管理主体责任，依法依规从事信息内容生产和公众账号运营活动。

公众账号生产运营者应当建立健全选题策划、编辑制作、发布推广、互动评论等全过程信息内容安全审核机制，加强信息内容导向性、真实性、合法性审核，维护网络传播良好秩序。

公众账号生产运营者应当建立健全公众账号注册使用、运营推广等全过程安全管理机制，依法、文明、规范运营公众账号， 以优质信息内容吸引公众关注订阅和互动分享，维护公众账号良好社会形象。

公众账号生产运营者与第三方机构开展公众账号运营、内容供给等合作， 应与第三方机构签订书面协议，明确第三方机构信息安全管理义务并督促履行。

第十七条 公众账号生产运营者转载信息内容的，应当遵守著作权保护相关法律法规，依法标注著作权人和可追溯信息来源，尊重和保护著作权人的合法权益。

公众账号生产运营者应当对公众账号留言、跟帖、评论等互动环节进行管理。平台可以根据公众账号的主体性质、信用等级等， 合理设置管理权限，提供相关技术支持。

第十八条 公众账号生产运营者不得有下列违法违规行为：

(一)不以真实身份信息注册，或者注册与自身真实身份信息不相符的公众账号名称、头像、简介等；

(二)恶意假冒、仿冒或者盗用组织机构及他人公众账号生产发布信息内容；

(三)未经许可或者超越许可范围提供互联网新闻信息采编发布等服务；

(四)操纵利用多个平台账号，批量发布雷同低质信息内容，生成虚假流量数据，制造虚假舆论热点；

(五)利用突发事件煽动极端情绪，或者实施网络暴力损害他人和组织机构名誉，干扰组织机构正常运营，影响社会和谐稳定；

(六)编造虚假信息，伪造原创属性，标注不实信息来源，歪曲事实真相，误

导社会公众；

(七)以有偿发布、删除信息等手段， 实施非法网络监督、营销诈骗、敲诈勒索，谋取非法利益；

(八)违规批量注册、囤积或者非法交易买卖公众账号；

(九)制作、复制、发布违法信息，或者未采取措施防范和抵制制作、复制、发布不良信息；

(十)法律、行政法规禁止的其他行为。

第四章 监督管理

第十九条 公众账号信息服务平台应当加强对本平台公众账号信息服务活动的监督管理，及时发现和处置违法违规信息或者行为。

公众账号信息服务平台应当对违反本规定及相关法律法规的公众账号，依法依约采取警示提醒、限制账号功能、暂停信息更新、停止广告发布、关闭注销账号、列入黑名单、禁止重新注册等处置措施， 保存有关记录，并及时向网信等有关主管部门报告。

第二十条 公众账号信息服务平台和生产运营者应当自觉接受社会监督。

公众账号信息服务平台应当在显著位置设置便捷的投诉举报入口和申诉渠道，公布投诉举报和申诉方式，健全受理、甄别、处置、反馈等机制，明确处理流程和反馈时限，及时处理公众投诉举报和生产运营者申诉。

鼓励互联网行业组织开展公众评议，推动公众账号信息服务平台和生产运营者严格自律，建立多方参与的权威调解机制，公平合理解决行业纠纷，依法维护用户合法权益。

第二十一条 各级网信部门会同有关主管部门建立健全协作监管等工作机制，监督指导公众账号信息服务平台和生产运营者依法依规从事相关信息服务活动。

公众账号信息服务平台和生产运营者应当配合有关主管部门依法实施监督检查，并提供必要的技术支持和协助。

公众账号信息服务平台和生产运营者违反本规定的，由网信部门和有关主管部门在职责范围内依照相关法律法规处理。

第五章 附 则

第二十二条 本规定所称互联网用户公众账号，是指互联网用户在互联网站、

应用程序等网络平台注册运营，面向社会公众生产发布文字、图片、音视频等信息内容的网络账号。

本规定所称公众账号信息服务平台，是指为互联网用户提供公众账号注册运营、信息内容发布与技术保障服务的网络信息服务提供者。

本规定所称公众账号生产运营者，是指注册运营公众账号从事内容生产发布的自然人、法人或者非法人组织。

第二十三条 本规定自 2021 年 2 月 22 日起施行。本规定施行之前颁布的有关规定与本规定不一致的，按照本规定执行。

移动互联网应用程序信息服务管理规定

(国家互联网信息办公室 2022 年 6 月 14 日)

第一章 总 则

第一条 为了规范移动互联网应用程序(以下简称应用程序)信息服务，保护公民、法人和其他组织的合法权益， 维护国家安全和公共利益，根据《中华人民共和国网络安全法》、《中华人民共和国数据安全法》、《中华人民共和国个人信息保护法》、《中华人民共和国未成年人保护法》、《互联网信息服务管理办法》、《互联网新闻信息服务管理规定》、《网络信息内容生态治理规定》等法律、行政法规和国家有关规定，制定本规定。

第二条 在中华人民共和国境内提供应用程序信息服务，以及从事互联网应用商店等应用程序分发服务，应当遵守本规定。

本规定所称应用程序信息服务，是指通过应用程序向用户提供文字、图片、语音、视频等信息制作、复制、发布、传播等服务的活动，包括即时通讯、新闻资讯、知识问答、论坛社区、网络直播、电子商务、网络音视频、生活服务等类型。

本规定所称应用程序分发服务，是指通过互联网提供应用程序发布、下载、动态加载等服务的活动，包括应用商店、快应用中心、互联网小程序平台、浏览器插件平台等类型。

第三条 国家网信部门负责全国应用程序信息内容的监督管理工作。地方网信部门依据职责负责本行政区域内应用程序信息内容的监督管理工作。

第四条 应用程序提供者和应用程序分发平台应当遵守宪法、法律和行政法

规，弘扬社会主义核心价值观，坚持正确政治方向、舆论导向和价值取向， 遵循公序良俗，履行社会责任，维护清朗网络空间。

应用程序提供者和应用程序分发平台不得利用应用程序从事危害国家安全、扰乱社会秩序、侵犯他人合法权益等法律法规禁止的活动。

第五条 应用程序提供者和应用程序分发平台应当履行信息内容管理主体责任，积极配合国家实施网络可信身份战略，建立健全信息内容安全管理、信息内容生态治理、数据安全和个人信息保护、未成年人保护等管理制度， 确保网络安全，维护良好网络生态。

第二章 应用程序提供者

第六条 应用程序提供者为用户提供信息发布、即时通讯等服务的，应当对申请注册的用户进行基于移动电话号码、身份证件号码或者统一社会信用代码等方式的真实身份信息认证。用户不提供真实身份信息， 或者冒用组织机构、他人身份信息进行虚假注册的，不得为其提供相关服务。

第七条 应用程序提供者通过应用程序提供互联网新闻信息服务的，应当取得互联网新闻信息服务许可，禁止未经许可或者超越许可范围开展互联网新闻信息服务活动。

应用程序提供者提供其他互联网信息服务，依法须经有关主管部门审核同意或者取得相关许可的，经有关主管部门审核同意或者取得相关许可后方可提供服务。

第八条 应用程序提供者应当对信息内容呈现结果负责，不得生产传播违法信息，自觉防范和抵制不良信息。

应用程序提供者应当建立健全信息内容审核管理机制，建立完善用户注册、账号管理、信息审核、日常巡查、应急处置等管理措施， 配备与服务规模相适应的专业人员和技术能力。

第九条 应用程序提供者不得通过虚假宣传、捆绑下载等行为，通过机器或者人工刷榜、刷量、控评等方式，或者利用违法和不良信息诱导用户下载。

第十条 应用程序应当符合相关国家标准的强制性要求。应用程序提供者发现应用程序存在安全缺陷、漏洞等风险时， 应当立即采取补救措施，按照规定及时告知用户并向有关主管部门报告。

第十一条 应用程序提供者开展应用程序数据处理活动，应当履行数据安全保护义务，建立健全全流程数据安全管理制度，采取保障数据安全技术措施和其他安全措施，加强风险监测，不得危害国家安全、公共利益， 不得损害他人合法权益。

第十二条 应用程序提供者处理个人信息应当遵循合法、正当、必要和诚信原则，具有明确、合理的目的并公开处理规则， 遵守必要个人信息范围的有关规定，规范个人信息处理活动，采取必要措施保障个人信息安全，不得以任何理由强制要求用户同意个人信息处理行为，不得因用户不同意提供非必要个人信息，而拒绝用户使用其基本功能服务。

第十三条 应用程序提供者应当坚持最有利于未成年人的原则，关注未成年人健康成长，履行未成年人网络保护各项义务，依法严格落实未成年人用户账号真实身份信息注册和登录要求，不得以任何形式向未成年人用户提供诱导其沉迷的相关产品和服务，不得制作、复制、发布、传播含有危害未成年人身心健康内容的信息。

第十四条 应用程序提供者上线具有舆论属性或者社会动员能力的新技术、新应用、新功能，应当按照国家有关规定进行安全评估。

第十五条 鼓励应用程序提供者积极采用互联网协议第六版(IPv6)向用户提供信息服务。

第十六条 应用程序提供者应当依据法律法规和国家有关规定，制定并公开管理规则，与注册用户签订服务协议，明确双方相关权利义务。

对违反本规定及相关法律法规及服务协议的注册用户，应用程序提供者应当依法依约采取警示、限制功能、关闭账号等处置措施， 保存记录并向有关主管部门报告。

第三章 应用程序分发平台

第十七条 应用程序分发平台应当在上线运营三十日内向所在地省、自治区、直辖市网信部门备案。办理备案时，应当提交以下材料：

(一)平台运营主体基本情况；

(二)平台名称、域名、接入服务、服务资质、上架应用程序类别等信息；

(三)平台取得的经营性互联网信息服务许可或者非经营性互联网信息服务

备案等材料；

(四)本规定第五条要求建立健全的相关制度文件；

(五)平台管理规则、服务协议等。

省、自治区、直辖市网信部门收到备案材料后，材料齐全的应当予以备案。

国家网信部门及时公布已经履行备案手续的应用程序分发平台名单。

第十八条 应用程序分发平台应当建立分类管理制度，对上架的应用程序实施分类管理，并按类别向其所在地省、自治区、直辖市网信部门备案应用程序。

第十九条 应用程序分发平台应当采取复合验证等措施，对申请上架的应用程序提供者进行基于移动电话号码、身份证件号码或者统一社会信用代码等多种方式相结合的真实身份信息认证。根据应用程序提供者的不同主体性质， 公示提供者名称、统一社会信用代码等信息，方便社会监督查询。

第二十条 应用程序分发平台应当建立健全管理机制和技术手段，建立完善上架审核、日常管理、应急处置等管理措施。

应用程序分发平台应当对申请上架和更新的应用程序进行审核，发现应用程序名称、图标、简介存在违法和不良信息， 与注册主体真实身份信息不相符，业务类型存在违法违规等情况的，不得为其提供服务。

应用程序提供的信息服务属于本规定第七条规定范围的，应用程序分发平台应当对相关许可等情况进行核验；属于本规定第十四条规定范围的，应用程序分发平台应当对安全评估情况进行核验。

应用程序分发平台应当加强对在架应用程序的日常管理，对含有违法和不良信息，下载量、评价指标等数据造假， 存在数据安全风险隐患，违法违规收集使用个人信息，损害他人合法权益等的，不得为其提供服务。

第二十一条 应用程序分发平台应当依据法律法规和国家有关规定，制定并公开管理规则，与应用程序提供者签订服务协议，明确双方相关权利义务。

对违反本规定及相关法律法规及服务协议的应用程序，应用程序分发平台应当依法依约采取警示、暂停服务、下架等处置措施， 保存记录并向有关主管部门报告。

第四章 监督管理

第二十二条 应用程序提供者和应用程序分发平台应当自觉接受社会监督，

设置醒目、便捷的投诉举报入口， 公布投诉举报方式，健全受理、处置、反馈等机制，及时处理公众投诉举报。

第二十三条 鼓励互联网行业组织建立健全行业自律机制，制定完善行业规范和自律公约，指导会员单位建立健全服务规范，依法依规提供信息服务，维护市场公平，促进行业健康发展。

第二十四条 网信部门会同有关主管部门建立健全工作机制，监督指导应用程序提供者和应用程序分发平台依法依规从事信息服务活动。

应用程序提供者和应用程序分发平台应当对网信部门和有关主管部门依法实施的监督检查予以配合，并提供必要的支持和协助。

第二十五条 应用程序提供者和应用程序分发平台违反本规定的，由网信部门和有关主管部门在职责范围内依照相关法律法规处理。

第五章 附 则

第二十六条 本规定所称移动互联网应用程序，是指运行在移动智能终端上向用户提供信息服务的应用软件。

本规定所称移动互联网应用程序提供者，是指提供信息服务的移动互联网应用程序所有者或者运营者。

本规定所称移动互联网应用程序分发平台，是指提供移动互联网应用程序发布、下载、动态加载等分发服务的互联网信息服务提供者。

第二十七条 本规定自 2022 年 8 月 1 日起施行。2016 年 6 月 28 日公布的《移动互联网应用程序信息服务管理规定》同时废止。

互联网弹窗信息推送服务管理规定

（国家互联网信息办公室 工业和信息化部 国家市场监督管理总局 2022 年 9 月 9 日）

第一条 为了规范互联网弹窗信息推送服务，维护国家安全和公共利益，保护公民、法人和其他组织的合法权益， 促进行业健康有序发展，根据《中华人民共和国网络安全法》、《中华人民共和国未成年人保护法》、《中华人民共和国广告法》、《互联网信息服务管理办法》、《互联网新闻信息服务管理规定》、《网络信息内容生态治理规定》等法律法规，制定本规定。

第二条 在中华人民共和国境内提供互联网弹窗信息推送服务，适用本规定。

本规定所称互联网弹窗信息推送服务，是指通过操作系统、应用软件、网站等，以弹出消息窗口形式向互联网用户提供的信息推送服务。

本规定所称互联网弹窗信息推送服务提供者，是指提供互联网弹窗信息推送服务的组织或者个人。

第三条 提供互联网弹窗信息推送服务，应当遵守宪法、法律和行政法规，弘扬社会主义核心价值观，坚持正确政治方向、舆论导向和价值取向， 维护清朗网络空间。

第四条 互联网弹窗信息推送服务提供者应当落实信息内容管理主体责任，建立健全信息内容审核、生态治理、数据安全和个人信息保护、未成年人保护等管理制度。

第五条 提供互联网弹窗信息推送服务的，应当遵守下列要求：

(一)不得推送《网络信息内容生态治理规定》规定的违法和不良信息， 特别是恶意炒作娱乐八卦、绯闻隐私、奢靡炫富、审丑扮丑等违背公序良俗内容， 不得以恶意翻炒为目的，关联某一话题集中推送相关旧闻；

(二)未取得互联网新闻信息服务许可的，不得弹窗推送新闻信息，弹窗推送信息涉及其他互联网信息服务，依法应当经有关主管部门审核同意或者取得相关许可的，应当经有关主管部门审核同意或者取得相关许可；

(三)弹窗推送新闻信息的，应当严格依据国家互联网信息办公室发布的《互联网新闻信息稿源单位名单》，不得超范围转载，不得歪曲、篡改标题原意和新闻信息内容，保证新闻信息来源可追溯；

(四)提升弹窗推送信息多样性，科学设定新闻信息和垂直领域内容占比，体现积极健康向上的主流价值观，不得集中推送、炒作社会热点敏感事件、恶性案件、灾难事故等，引发社会恐慌；

(五)健全弹窗信息推送内容管理规范，完善信息筛选、编辑、推送等工作流程，配备与服务规模相适应的审核力量，加强弹窗信息内容审核；

(六)保障用户权益，以服务协议等明确告知用户弹窗信息推送服务的具体形式、内容频次、取消渠道等， 充分考虑用户体验，科学规划推送频次，不得对普通用户和会员用户进行不合理地差别推送，不得以任何形式干扰或者影响用户关闭弹窗，弹窗信息应当显著标明弹窗信息推送服务提供者身份；

(七)不得设置诱导用户沉迷、过度消费等违反法律法规或者违背伦理道德的算法模型；不得利用算法实施恶意屏蔽信息、过度推荐等行为； 不得利用算法针对未成年人用户进行画像，向其推送可能影响其身心健康的信息；

(八)弹窗推送广告信息的，应当具有可识别性，显著标明“广告”和关闭标志，确保弹窗广告一键关闭；

(九)不得以弹窗信息推送方式呈现恶意引流跳转的第三方链接、二维码等信息，不得通过弹窗信息推送服务诱导用户点击，实施流量造假、流量劫持。

第六条 互联网弹窗信息推送服务提供者应当自觉接受社会监督，设置便捷投诉举报入口，及时处理关于弹窗信息推送服务的公众投诉举报。

第七条 鼓励和指导互联网行业组织建立健全互联网弹窗信息推送服务行业准则，引导行业健康有序发展。

第八条 网信部门会同电信主管部门、市场监管部门等有关部门建立健全协作监管等工作机制，监督指导互联网弹窗信息推送服务提供者依法依规提供服务。

第九条 互联网弹窗信息推送服务提供者违反本规定的，由网信部门、电信主管部门、市场监管部门等有关部门在职责范围内依照相关法律法规规定处理。

第十条 本规定自 2022 年 9 月 30 日起施行。

互联网跟帖评论服务管理规定

(国家互联网信息办公室 2022 年 11 月 16 日)

第一条 为了规范互联网跟帖评论服务，维护国家安全和公共利益，保护公民、法人和其他组织的合法权益，根据《中华人民共和国网络安全法》《网络信息内容生态治理规定》《互联网用户账号信息管理规定》等法律法规和国家有关规定，制定本规定。

第二条 在中华人民共和国境内提供、使用跟帖评论服务，应当遵守本规定。

本规定所称跟帖评论服务，是指互联网站、应用程序以及其他具有舆论属性或社会动员能力的网站平台，以评论、回复、留言、弹幕、点赞等方式，为用户提供发表文字、符号、表情、图片、音视频等信息的服务。

第三条 国家网信部门负责全国跟帖评论服务的监督管理执法工作。地方网信部门依据职责负责本行政区域内跟帖评论服务的监督管理执法工作。

第四条 跟帖评论服务提供者应当严格落实跟帖评论服务管理主体责任，依

法履行以下义务：

(一)按照“后台实名、前台自愿”原则，对注册用户进行基于移动电话号码、身份证件号码或者统一社会信用代码等方式的真实身份信息认证，不得向未认证真实身份信息或者冒用组织机构、他人身份信息的用户提供跟帖评论服务。

(二)建立健全用户个人信息保护制度，处理用户个人信息应当遵循合法、正当、必要和诚信原则， 公开个人信息处理规则，告知个人信息的处理目的、处理方式、处理的个人信息种类、保存期限等事项，并依法取得个人的同意。法律、行政法规另有规定的除外。

(三)对新闻信息提供跟帖评论服务的，应当建立先审后发制度。

(四)提供弹幕方式跟帖评论服务的，应当在同一平台和页面同时提供与之对应的静态版信息内容。

(五)建立健全跟帖评论审核管理、实时巡查、应急处置、举报受理等信息安全管理制度，及时发现处置违法和不良信息，并向网信部门报告。

(六)创新跟帖评论管理方式，研发使用跟帖评论信息安全管理技术，提升违法和不良信息处置能力；及时发现跟帖评论服务存在的安全缺陷、漏洞等风险，采取补救措施，并向网信部门报告。

(七)配备与服务规模相适应的审核编辑队伍，加强跟帖评论审核培训，提高审核编辑人员专业素养。

(八)配合网信部门依法开展监督检查工作，提供必要的技术、数据支持和协助。

第五条 具有舆论属性或社会动员能力的跟帖评论服务提供者上线跟帖评论相关新产品、新应用、新功能的，应当按照国家有关规定开展安全评估。

第六条 跟帖评论服务提供者应当与注册用户签订服务协议，明确跟帖评论的服务与管理细则以及双方跟帖评论发布权限、管理责任等权利义务， 履行互联网相关法律法规告知义务，开展文明上网教育。对公众账号生产运营者， 在服务协议中应当明确其跟帖评论管理权限及相应责任，督促其切实履行管理义务。

第七条 跟帖评论服务提供者应当按照用户服务协议对跟帖评论服务使用者和公众账号生产运营者进行规范管理。对发布违法和不良信息内容的跟帖评论服务使用者，应当依法依约采取警示提醒、拒绝发布、删除信息、限制账号功能、

暂停账号更新、关闭账号、禁止重新注册等处置措施， 并保存相关记录；对未尽到管理义务导致跟帖评论环节出现违法和不良信息内容的公众账号生产运营者，应当根据具体情形，依法依约采取警示提醒、删除信息、暂停跟帖评论区功能直至永久关闭跟帖评论区、限制账号功能、暂停账号更新、关闭账号、禁止重新注册等处置措施，保存相关记录，并及时向网信部门报告。

第八条 跟帖评论服务提供者应当建立用户分级管理制度，对用户的跟帖评论行为开展信用评估，根据信用等级确定服务范围及功能，对严重失信的用户应列入黑名单，停止对列入黑名单的用户提供服务，并禁止其通过重新注册账号等方式使用跟帖评论服务。

第九条 跟帖评论服务使用者应当遵守法律法规，遵循公序良俗，弘扬社会主义核心价值观，不得发布法律法规和国家有关规定禁止的信息内容。

第十条 公众账号生产运营者应当对账号跟帖评论信息内容加强审核管理，及时发现跟帖评论环节违法和不良信息内容，采取举报、处置等必要措施。

第十一条 公众账号生产运营者可按照用户服务协议向跟帖评论服务提供者申请举报、隐藏或者删除违法和不良评论信息、自主关闭账号跟帖评论区等管理权限。跟帖评论服务提供者应当对公众账号生产运营者的跟帖评论管理情况进行信用评估后，根据公众账号的主体性质、信用评估等级等，合理设置管理权限，提供相关技术支持。

第十二条 跟帖评论服务提供者、跟帖评论服务使用者和公众账号生产运营者不得通过发布、删除、推荐跟帖评论信息以及利用软件、雇佣商业机构及人员散布信息等其他干预跟帖评论信息呈现的手段，侵害他人合法权益或公共利益，谋取非法利益，恶意干扰跟帖评论秩序，误导公众舆论。

第十三条 跟帖评论服务提供者应当建立健全跟帖评论违法和不良信息公众投诉举报和跟帖评论服务使用者申诉制度，设置便捷投诉举报和申诉入口，及时受理和处置跟帖评论相关投诉举报和申诉。

跟帖评论服务使用者对被处置的跟帖评论信息存在异议的，有权向跟帖评论服务提供者提出申诉，跟帖评论服务提供者应当按照用户服务协议进行核查处理。

任何组织和个人发现违反本规定行为的，可以向网信部门投诉举报。网信部门收到投诉举报后，应当及时依法处理。

第十四条 各级网信部门应当建立健全日常检查和定期检查相结合的监督管理制度，依法对互联网跟帖评论服务实施监督检查。

第十五条 违反本规定的，由国家和地方网信部门依照相关法律法规处理。

第十六条 本规定自 2022 年 12 月 15 日起施行。2017 年 8 月 25 日公布的《互联网跟帖评论服务管理规定》同时废止。

粤港澳大湾区(内地、香港)个人信息跨境流动标准合同实施指引

国家互联网信息办公室 香港创新科技及工业局公告 2023 年 3 号

落实《中华人民共和国国家互联网信息办公室与香港特别行政区政府创新科技及工业局 关于促进粤港澳大湾区数据跨境流动的合作备忘录》关于“共同制定粤港澳大湾区个人信息跨境标准合同并组织实施，加强个人信息跨境标准合同备案管理”的合作措施，国家互联网信息办公室与香港创新科技及工业局共同制定《粤港澳大湾区(内地、香港)个人信息跨境流动标准合同实施指引》，现予公布。

特此公告。

附件：《粤港澳大湾区(内地、香港)个人信息跨境流动标准合同实施指引》

国家互联网信息办公室 王京涛

香港特区政府创新科技及工业局 孙　东

2023 年 12 月 10 日

粤港澳大湾区(内地、香港)个人信息跨境流动标准合同实施指引

第一条 为促进粤港澳大湾区个人信息跨境安全有序流动，推动粤港澳大湾区高质量发展，落实《中华人民共和国国家互联网信息办公室与香港特别行政区政府创新科技及工业局 关于促进粤港澳大湾区数据跨境流动的合作备忘录》(以下简称备忘录)，国家互联网信息办公室、香港特别行政区政府创新科技及工业局共同制定本实施指引。

第二条 《粤港澳大湾区(内地、香港)个人信息跨境流动标准合同》(以下简称标准合同，见附件 1)为备忘录下有关促进粤港澳大湾区个人信息跨境流动的便利措施。粤港澳大湾区个人信息处理者及接收方可以按照本实施指引要求， 通过订立标准合同的方式进行粤港澳大湾区内内地和香港之间的个人信息跨境流动。被相关部门、地区告知或者公开发布为重要数据的个人信息除外。

个人信息处理者及接收方应注册于(适用于组织)/位于(适用于个人)粤港澳大湾区内地部分，即广东省广州市、深圳市、珠海市、佛山市、惠州市、东莞市、中山市、江门市、肇庆市，或者香港特别行政区。

第三条 通过订立标准合同的方式开展个人信息跨境提供的，应当坚持自主缔约与备案管理相结合、保护个人信息权益与防范风险相结合， 保障个人信息跨境安全、自由流动。

第四条 按照本实施指引，通过订立标准合同跨境提供个人信息的，应当履行标准合同列明的义务和责任，包括满足以下条件：

(一)个人信息处理者跨境提供个人信息前，应当按照个人信息处理者属地法律法规要求告知个人信息主体或者取得个人信息主体的同意；

(二)不得向粤港澳大湾区以外的组织、个人提供。

第五条 个人信息处理者按照本实施指引，通过订立标准合同跨境提供个人信息前，应当开展个人信息保护影响评估，重点评估以下内容：

(一)个人信息处理者和接收方处理个人信息的目的、方式等的合法性、正当性、必要性；

(二)对个人信息主体权益的影响及安全风险；

(三)接收方承诺承担的义务，以及履行义务的管理和技术措施、能力等能否保障跨境提供的个人信息安全。

第六条 标准合同应当严格按照本实施指引附件订立，合同生效后方可开展个人信息跨境提供。

个人信息处理者可以与接收方约定其他条款，但不得与标准合同相冲突。

第七条 跨境提供个人信息的目的、范围、种类、方式，或者接收方处理个人信息的用途、方式发生变化， 延长保存期限，以及发生影响或者可能影响个人信息权益其他情况的，个人信息处理者应当重新开展个人信息保护影响评估，补充或者重新订立标准合同，并履行相应备案手续。

第八条 个人信息处理者及接收方应在标准合同生效之日起 10 个工作日内按照属地向广东省互联网信息办公室或者香港特别行政区政府政府资讯科技总监办公室进行标准合同备案，提交如下材料：

(一)法定代表人身份证件影印件；

(二)承诺书(模板见附件 2)；

(三)标准合同。

个人信息处理者及接收方应当对所备案材料的真实性负责。

第九条 个人信息处理者及接收方接受属地监管机构的监督管理，包括但不限于：

(一)根据标准合同第二条第七项及第十项，个人信息处理者答复监管机构的询问及对合同的义务和责任的履行承担举证责任；

(二)根据标准合同第三条第十二项，接收方应接受监管机构的监督管理，包括服从监管机构作出的决定以及提供已采取必要行动的证明等；

(三)根据标准合同第六条第二项，个人信息处理者解除标准合同时，通知监管机构。

第十条 任何组织和个人发现个人信息处理者或接收方按照本实施指引进行粤港澳大湾区内的个人信息跨境流动，但不履行本实施指引及标准合同要求的义务和责任的，可以向国家互联网信息办公室、广东省互联网信息办公室或者香港特别行政区政府创新科技及工业局、政府资讯科技总监办公室、香港个人资料私隐专员公署投诉、举报。

收到投诉、举报的部门发现个人信息跨境活动存在较大安全风险或者发生个人信息安全事件的，可以要求个人信息处理者或者接收方整改；需要交由其他执法部门处置的，交由相关部门依法处置。

第十一条 个人信息处理者或接收方在处理个人信息时发生个人信息泄露等安全事件的，应立即采取补救措施，按照属地通知国家互联网信息办公室、广东省互联网信息办公室，或者香港特别行政区政府创新科技及工业局、政府资讯科技总监办公室、香港个人资料私隐专员公署。

第十二条 以上规定并不影响内地履行个人信息保护职责的部门和香港个人资料私隐专员公署在职责范围内依法加强个人信息保护和监督管理工作，包括处理与个人信息保护有关的投诉、举报，调查、处理违法个人信息处理活动等。

第十三条 有关部门及其工作人员对在履行职责中知悉的个人隐私、个人信息、商业秘密、保密商务信息等应当依法予以保密， 不得泄露或者非法向他人提供、非法使用。

第十四条　国家互联网信息办公室和香港特别行政区政府创新科技及工业局可以根据实际情况，经协商一致后对本实施指引及附件进行修订。

第十五条　本实施指引自发布之日起生效。

附件 1：粤港澳大湾区(内地、香港)个人信息跨境流动标准合同

关于变更互联网新闻信息服务单位审批备案和外国机构在中国境内提供金融信息服务业务审批实施机关的通知

(国家互联网信息办公室 2015 年 4 月 30 日)

根据《国务院关于授权国家互联网信息办公室负责互联网信息内容管理工作的通知》及有关部门职能调整相关精神，国家互联网信息办公室承担以下审批备案职能：新闻单位设立的登载超出本单位已刊登播发的新闻信息、提供时政类电子公告服务、向公众发送时政类通讯信息的互联网新闻信息服务单位的审批；非新闻单位设立的转载新闻信息、提供时政类电子公告服务、向公众发送时政类通讯信息的互联网新闻信息服务单位的审批；外国机构在中国境内提供金融信息服务业务的审批。省、自治区、直辖市互联网信息办公室负责新闻单位设立的登载本单位已刊登播发新闻信息的互联网新闻信息服务单位的备案。

具体申请材料、审批程序、备案流程等信息可登陆中国网信网(www.cac.gov.cn)查询。联系方式：010-65120744(互联网新闻信息服务)、010-65129305(外国机构在中国境内提供金融信息服务)。

国家互联网信息办公室

2015 年 4 月 29 日

关于开展境内金融信息服务报备工作的通知

各省、自治区、直辖市互联网信息办公室：

为贯彻落实《关于加快建立网络综合治理体系的意见》和《金融信息服务管理规定》要求，提高金融信息服务质量，促进金融信息服务业健康发展，定于 2021 年 8 月起开展境内金融信息服务报备工作，现就有关事项通知如下：

一、报备对象

本通知所称金融信息服务，是指向从事金融分析、金融交易、金融决策或者其他金融活动的用户提供可能影响金融市场的信息和(或者)金融数据的服

务。该服务不同于通讯社服务、互联网新闻信息服务、金融业务服务和征信业务服务。

本通知所称境内机构，是指实际控制人为境内法人(非外商投资企业法人)或自然人，且商事登记在境内的机构。

按照本通知进行报备的金融信息服务，应具备以下特征：为境内机构开展的金融信息服务，主要是以互联网终端或专用终端等特定方式，向金融机构或专业投资者等特定对象，提供包括信息和数据在内的信息业务服务，服务的目的是辅助金融决策。

二、报备原则

按照“自愿申报、统一标准、两级核验”的原则，由境内机构自主决定是否提交报备申请。境内机构商事登记所在地的省级互联网信息办公室初核后，提交国家互联网信息办公室复核。

三、报备定位

报备是对境内机构提供金融信息服务行为的确认，但不对境内机构在提供产品和服务过程中发生的任何法律纠纷承担责任。

境内机构在完成金融信息服务报备后，应严格按照《金融信息服务管理规定》和本通知有关要求提供金融信息服务，不得以已通过金融信息服务报备为名，推脱违法违规从事金融信息服务业务和其他业务的责任。

境内机构如从事金融业务，应按规定取得相应资质，并接受有关主管部门监管。以互联网站、应用程序、论坛、博客、公众账号、即时通信工具、网络直播等形式面向社会公众提供金融资讯的，不属于本通知所称的金融信息服务，有关机构应遵守《互联网新闻信息服务管理规定》等法律法规。

四、报备渠道

报备依托金融信息服务报备系统(以下简称“报备系统”，网址：http://fisbaobei.ifcert.cn)开展，境内机构按要求填报信息、提交材料。

五、报备内容

报备按业务环节分为首次报送、重大事项报告和年度审核。

(一)境内机构首次申请金融信息服务报备，应如实填报下列信息或上传有关材料电子扫描件：

1.机构基本信息、业务范围、服务项目和产品、服务提供方式、用户情况等信息；

2.提供金融信息服务涉及的信息内容发布、信息内容审核、信息数据保存、信息安全保障、个人信息保护、知识产权保护、合作对象资质核验等内部管理制度及执行情况说明；

3.机构设立的证明文本(营业执照)以及已获取的相关许可、资质等信息；

4.机构法定代表人、高级管理人员近三年受到的刑事处罚、行政处罚、监管措施等情况；

5.上一年度财务报表以及审计报告；

6.国家互联网信息办公室规定的其他材料。

(二)境内机构在完成首次报送后，发生下列重大事项，应在重大事项发生后的 10 个工作日内通过报备系统如实填报下列信息或上传有关材料电子扫描件：

1.机构基本信息、业务范围、服务项目和产品、服务提供方式等发生变更；

2.新增服务项目和产品；

3.信息内容发布、信息内容审核、信息数据保存、信息安全保障、个人信息保护、知识产权保护、合作对象资质核验等方面出现重大风险事件；

4.机构或者法定代表人、高级管理人员因涉嫌违法违规被立案调查、司法机关侦查，以及受到刑事处罚、行政处罚、监管措施等；

5.机构发生重大民事纠纷，进行诉讼或仲裁；

6.机构股权结构发生重大变更；

7.对业务发展可能产生重大影响的其他风险事件；

8.国家互联网信息办公室规定的其他重大事项。

(三)境内机构完成首次报送后，应于每年 4 月 30 日前通过报备系统提交年度审核信息。年度审核信息包括机构基本信息、经营情况，已报备产品运行情况，信息内容审核情况，以及国家互联网信息办公室规定的其他事项。

六、报备信息核验

省级互联网信息办公室应在收到境内机构报送信息后 15 个工作日内核验。

对报送信息、材料不完备或者不符合规定的，省级互联网信息办公室应一次性告知需补正的全部内容。境内机构应在收到核验意见后按要求提交补正报送信息，超过 10 个工作日仍未按要求补正的，不予核验通过。

对报送信息、材料完备且符合相关规定的境内机构，省级互联网信息办公室应在核验通过后及时提交国家互联网信息办公室。国家互联网信息办公室经复核并根据需要征求有关部门意见后，完成报备。

国家互联网应急中心作为技术支撑单位，负责金融信息服务报备系统的运营和维护，并协助对境内机构提交的报备材料进行形式核验。

七、报备信息公示和变更

境内机构完成首次报送后，其机构名称、报备编号、主要产品、服务方式等信息，由国家互联网信息办公室通过报备系统向社会公示。境内机构应在所提供服务、产品的明显位置明示报备信息，并链接报备系统网址，供用户查询核对。

境内机构提交重大事项变更和年度审核信息、材料后，省级互联网信息办公室应按照前述报备信息核验的有关要求进行初核，审核通过后提交国家互联网信息办公室复核。对涉及报备公示信息变更的，国家互联网信息办公室予以修改完善。

境内机构因终止金融信息服务、注销商事登记或被市场监管部门吊销营业执照，以及其他不符合报备相关规定的，省级互联网信息办公室应及时提请国家互联网信息办公室注销其金融信息服务报备信息。国家互联网信息办公室复核通过后，注销其报备信息并向社会公示。

八、工作要求

(一)高度重视境内金融信息服务报备工作。开展境内金融信息服务报备是推动境内金融信息服务业健康发展，提升行业影响力的重要基础和关键环节，各省级互联网信息办公室务必高度重视此项工作，明确责任，加强统筹协调，组织开展好报备工作。

(二)分阶段完成境内金融信息服务报备工作。报备工作将常态化开展。请各省级互联网信息办公室于 2021 年 10 月 30 日前完成对现有境内金融信息服务的报备工作，并结合实际建立工作机制，扎实做好常态化工作。

(三)切实指导境内机构做好金融信息服务报备工作。各省级互联网信息办公室应向境内机构认真解读金融信息服务相关政策文件，介绍报备流程和要求，指导境内机构如实填报信息、上传材料，确保资料真实准确，并依法保护境内机构依照本通知提交材料中包含的具有商业价值的信息。

(四)开展审视加强行业管理。金融信息服务事关意识形态安全和金融安全，各省级互联网信息办公室应指导通过报备的境内机构提供审视其所提供金融信息的必要条件。对发现境内机构存在违法违规的情形，依法依规予以处置。

特此通知。

国家互联网信息办公室

2021 年 7 月 25 日

关于进一步压实网站平台信息内容管理主体责任的意见

(国家互联网信息办公室 2021 年 9 月 15 日)

随着信息技术的迅猛发展，互联网已经成为人们了解资讯、获取知识、娱乐交流的重要途径，成为提供社会公共服务和方便群众生产生活的重要载体。网站平台日益成为信息内容生产传播的重要渠道，兼具社会属性和公共属性，在坚持正确价值取向、保障网络内容安全、维护网民合法权益等方面， 具有不可替代的地位和作用。促进网站平台健康有序运行，日益重要而迫切。

近年来，网信系统深入贯彻落实党中央决策部署，在坚持依法管网、依法办网方面取得了长足进步，特别是网站平台积极履行信息内容管理主体责任，在保障信息安全、规范传播秩序、维护良好生态等方面， 发挥了主体作用。同时也要看到，网站平台还存在责任认识不充分、角色定位不准确、履职尽责不到位、制度机制不完善、管理操作不规范等问题，一定程度导致违法和不良信息禁而不绝，网络生态问题时有发生。为进一步压实网站平台信息内容管理主体责任，充分发挥网站平台信息内容管理第一责任人作用，切实提升管网治网水平，现提出如下意见：

一、指导思想

以习近平新时代中国特色社会主义思想特别是习近平总书记关于网络强国的重要思想为指导，全面贯彻落实党的十九大和十九届二中、三中、四中、五中

全会精神，立足新发展阶段，贯彻新发展理念，构建新发展格局，坚持以人民为中心，坚持维护国家利益，统筹规范与发展，以推动互联网行业健康发展为目标，以促进网站平台自我规范管理为着力点，围绕强化网站平台信息内容管理主体责任工作主线，引导推动网站平台准确把握责任，明确工作规范，健全管理制度，完善运行规则，切实防范化解各种风险隐患，积极营造清朗网络空间。

二、主要原则

坚持政治引领。坚持党管互联网，树牢“四个意识”，坚定“四个自信”，做到“两个维护”，切实把政治标准和政治要求贯穿互联网管理全过程、各环节，确保网站平台始终坚持正确的政治方向、舆论导向和价值取向。

坚持问题导向。聚焦各类网络乱象，着力破解网站平台履行信息内容管理主体责任存在的认识偏差、管理失范、能力不足、效果不彰等突出问题，指导督促网站平台补短板、强弱项、提水平。

坚持分类指导。充分体现互联网不同领域的规律，准确把握不同产品功能特点，分领域确定重点职责，分平台抓好重点任务，分环节明确工作标准，促进网站平台规范管理、有效履责。

坚持强化监管。加强源头治理、规则治理，注重风险管理、行为管理，增强监管系统性针对性。把握重点，抓住关键，强化头部网站平台日常管理。以管理促规范，激发网站平台履职尽责的内生动能。

三、重点任务

(一)把握主体责任内涵。网站平台要以弘扬社会主义核心价值观为己任，培育积极健康、向上向善的网络文化，确保网上主旋律高昂、正能量充沛；对信息内容呈现结果负责，严防违法信息生产传播，自觉防范和抵制传播不良信息，确保信息内容安全。建设良好网络秩序，全链条覆盖、全口径管理，规范用户网上行为，遏制各类网络乱象，维护清朗网络空间。健全管理制度机制，准确界定行为边界，切实规范工作流程，强化内部管理约束，做到有规可依、有规必依，保障日常运营规范健康。加强未成年人网络保护，注重保障用户权益，切实维护社会公共利益。

(二)完善平台社区规则。制定和完善适合网站平台特点的社区规则，充分体现法律法规要求，充分体现社会主义核心价值观要求，充分体现行业管理要求。

明确网站平台在内容运营中的权利、责任和义务， 细化处理违规行为的措施、权限、程序， 明晰处置原则和操作标准，切实强化网站平台自身行为约束。完善用户行为准则，编制违法和不良信息清单目录，建立用户信用记录和评价制度，增强用户管理的针对性和有效性，建立并留存处置用户违规行为记录。严格执行社区规则，不得选择性操作，不得差别化对待，不得超范围处置。

(三)加强账号规范管理。制定账号规范管理实施细则，加强账号运行监管，有效规制账号行为。加强账号注册管理，严格落实真实身份信息登记相关要求，强化名称、头像等账号信息合规审核， 强化公众账号主体资质核验，确保公众账号名称和运营主体业务相匹配。加强账号行为管理， 严格分类分级，实现精准管理、重点管理、动态管理。加强对需要关注账号管理， 建立目录清单，制定管理措施，确保规范有序。加大违法违规账号处置力度， 建立黑名单账号数据库，严防违法违规账号转世。全面清理“僵尸号”“空壳号”。

(四)健全内容审核机制。严格落实总编辑负责制度， 明确总编辑信息内容审核权利责任，建立总编辑全产品、全链条信息内容审核把关工作机制。完善人工审核制度，进一步扩大人工审核范围，细化审核标准，完善审核流程，确保审核质量。建立违法违规信息样本库动态更新机制，分级分类设置，定期丰富扩充，提升技术审核效率和质量。健全重点信息多节点召回复核机制， 明确重点信息范围、标准、类别等， 对关系国家安全、国计民生和公共利益等重点领域信息， 增加审核频次，加大审核力度，科学把握内容，确保信息安全。

(五)提升信息内容质量。坚持主流价值导向， 唱响主旋律、传播正能量， 弘扬社会主义先进文化、展示奋发昂扬精神面貌。完善内容生产扶持政策， 采取资金、流量等多种支持方式， 鼓励引导用户生产高质量信息内容。结合网站平台实际，增加主流媒体信息服务订购数量和比例，优化信息内容生产供给。建立信息内容评价体系，注重遴选优质“自媒体”账号、MCN 机构等，丰富网站平台信息来源，保障信息内容健康向上。

(六)规范信息内容传播。强化新闻信息稿源管理， 严格落实互联网新闻信息服务相关法律法规，禁止未经许可的主体提供相关服务，转载新闻信息时，不得歪曲、篡改标题原意和新闻信息内容，保证新闻来源可追溯。优化信息推荐机制，优先推送优质信息内容，坚决防范和抵制不良信息，严禁传播违法信息，切实维

护版面页面良好生态。规范话题设置， 严防蹭热点、伪原创、低俗媚俗、造谣传谣、负面信息集纳等恶意传播行为。健全舆情预警机制，重点关注敏感热点舆情，及时发现不良倾向，进行科学有效引导，防止误导社会公众。建立信息传播人工干预制度规范，严格操作标准，规范操作流程，全过程留痕备查，及时主动向监管部门报告重大事项。

(七)加强重点功能管理。科学设计、有效管理应用领域广、使用频度高的功能。规范热点排行， 健全榜单规则，合理确定构成要素和权重，体现正确价值观导向。优化算法推荐， 明确推荐重点，细化推荐标准，评估推荐效果，按要求开展算法备案。强化弹窗管理， 准确把握推送环节，严格控制推送频次，加强推送内容审核把关。规范搜索呈现， 完善搜索运行规则，建立权威信息内容库，重点领域优先展示权威来源信息，确保搜索结果客观准确。加强群组运行管理， 明确群组负责人权利义务，设定群组人员数量标准，规范群组用户行为。鼓励社会公众参与违法和不良信息举报，畅通投诉举报渠道，健全完善受理处置反馈机制。

(八)坚持依法合规经营。从事互联网新闻信息服务等业务， 应当依法依规履行许可手续，未经许可不得开展相关活动。上线运营具有媒体属性和舆论动员功能的新技术新应用，按规定进行安全评估，通过后方可正式运行。开展数据共享、流量合作等跨平台经营活动，应当符合国家相关政策，有助于正能量信息传播。坚持诚信运营，不得选择性自我优待，不得非正常屏蔽或推送利益相关方信息，不得利用任何形式诱导点击、诱导下载、诱导消费。

(九)严格未成年人网络保护。落实未成年人保护法律法规要求， 结合业务类型和实际，制定未成年人网络保护具体方案，明确目标，细化措施，建立长效机制。加大投入， 开发升级未成年人防沉迷、青少年模式等管理系统， 不断提高系统辨识度，增强识别精准性，合理设置未成年人使用服务的时间、权限等， 提供适合未成年人的优质内容，保障未成年人健康科学用网。面向未成年人提供产品和服务，清晰界定服务内容，高标准治理产品生态，严防不良信息影响未成年人身心健康。严禁借未成年人名义利用网络进行商业炒作牟利。

(十)加强人员队伍建设。配备与业务规模相适应的从业人员， 加大信息内容审核人员数量和比例，不断优化结构，切实保障信息服务质量。严格从业人员行业进入、履职考核、离职登记等各环节管理， 新闻信息服务从业人员依法持证上

岗。针对性开展业务培训， 制定培训计划，建立培训档案，持续提升从业人员能力素质。加强从业人员诚信体系建设， 健全信用管理机制，加大违法违规处罚力度，严格落实从业人员黑名单管理制度。

四、组织保障

(十一)加强组织领导。各地网信部门要充分认识压实网站平台信息内容管理主体责任的重要性和紧迫性，作为管网治网的重要内容，紧抓不放。要切实履行属地管理责任，明确责任分工，组织专门力量，精心谋划部署，精心组织实施。网站平台要提高思想认识，把履行主体责任作为 CEO 工程，列入企业重要议事日程，明确时间表、任务书、路线图，切实抓出成效。

(十二)强化日常监管。加强基础管理， 准确掌握属地网站平台底数，建立网站平台履行主体责任台账。理清管理重点， 及时掌握重点网站平台工作动态。主动发现问题、解决问题， 充分发挥互联网行政执法作用，推动网站平台针对性补齐履行主体责任工作短板。建立定期例会制度，通报典型案例，传递管理要求，推广好的经验做法。

(十三)注重督导检查。各地网信部门要加大督导检查力度， 跟踪评估属地网站平台履行主体责任工作效果，督导检查网站平台各项工作制度机制的制订情况，督导检查网站平台制度机制的落实情况，对存在的各种问题及时纠正处置。网站平台要自查自纠制度机制执行情况，对违规行为及时处罚，每年主动向属地网信部门报告履行主体责任情况，及时报告涉及履行主体责任的重大事项。

关于发布《云计算服务安全评估办法》的公告

国家互联网信息办公室、国家发展和改革委员会、工业和信息化部、财政部

公告 2019 年第 2 号

为提高党政机关、关键信息基础设施运营者采购使用云计算服务的安全可控水平，国家互联网信息办公室、国家发展和改革委员会、工业和信息化部、财政部制定了《云计算服务安全评估办法》，现予以发布。

附件：云计算服务安全评估办法

国家互联网信息办公室 国家发展和改革委员会

工业和信息化部 财政部

2019 年 7 月 2 日

云计算服务安全评估办法

第一条 为提高党政机关、关键信息基础设施运营者采购使用云计算服务的安全可控水平，制定本办法。

第二条 云计算服务安全评估坚持事前评估与持续监督相结合，保障安全与促进应用相统一，依据有关法律法规和政策规定，参照国家有关网络安全标准，发挥专业技术机构、专家作用，客观评价、严格监督云计算服务平台(以下简称“云平台”)的安全性、可控性，为党政机关、关键信息基础设施运营者采购云计算服务提供参考。

本办法中的云平台包括云计算服务软硬件设施及其相关管理制度等。

第三条 云计算服务安全评估重点评估以下内容：

(一)云平台管理运营者(以下简称“云服务商”)的征信、经营状况等基本情况；

(二)云服务商人员背景及稳定性，特别是能够访问客户数据、能够收集相关元数据的人员；

(三)云平台技术、产品和服务供应链安全情况；

(四)云服务商安全管理能力及云平台安全防护情况；

(五)客户迁移数据的可行性和便捷性；

(六)云服务商的业务连续性；

(七)其他可能影响云服务安全的因素。

第四条 国家互联网信息办公室会同国家发展和改革委员会、工业和信息化部、财政部建立云计算服务安全评估工作协调机制(以下简称“协调机制”)，审议云计算服务安全评估政策文件，批准云计算服务安全评估结果，协调处理云计算服务安全评估有关重要事项。

云计算服务安全评估工作协调机制办公室(以下简称“办公室”)设在国家互联网信息办公室网络安全协调局。

第五条 云服务商可申请对面向党政机关、关键信息基础设施提供云计算服务的云平台进行安全评估。

第六条 申请安全评估的云服务商应向办公室提交以下材料：

(一)申报书；

(二)云计算服务系统安全计划;

(三)业务连续性和供应链安全报告;

(四)客户数据可迁移性分析报告;

(五)安全评估工作需要的其他材料。

第七条 办公室受理云服务商申请后,组织专业技术机构参照国家有关标准对云平台进行安全评价。

第八条 专业技术机构应坚持客观、公正、公平的原则,按照国家有关规定,在办公室指导监督下,参照《云计算服务安全指南》《云计算服务安全能力要求》等国家标准,重点评价本办法第三条所述内容,形成评价报告,并对评价结果负责。

第九条 办公室在专业技术机构安全评价基础上,组织云计算服务安全评估专家组进行综合评价。

第十条 云计算服务安全评估专家组根据云服务商申报材料、评价报告等,综合评价云计算服务的安全性、可控性,提出是否通过安全评估的建议。

第十一条 云计算服务安全评估专家组的建议经协调机制审议通过后,办公室按程序报国家互联网信息办公室核准。

云计算服务安全评估结果由办公室发布。

第十二条 云计算服务安全评估结果有效期 3 年。有效期届满需要延续保持评估结果的,云服务商应在届满前至少 6 个月向办公室申请复评。

有效期内,云服务商因股权变更、企业重组等导致实控人或控股权发生变化的,应重新申请安全评估。

第十三条 办公室通过组织抽查、接受举报等形式,对通过评估的云平台开展持续监督,重点监督有关安全控制措施有效性、重大变更、应急响应、风险处置等内容。

通过评估的云平台已不再满足要求的,经协调机制审议、国家互联网信息办公室核准后撤销通过评估的结论。

第十四条 通过评估的云平台停止提供服务时,云服务商应至少提前 6 个月通知客户和办公室,并配合客户做好迁移工作。

第十五条 云服务商对所提供申报材料的真实性负责。在评估过程中拒绝按

要求提供材料或故意提供虚假材料的，按评估不通过处理。

第十六条 未经云服务商同意，参与评估工作的相关机构和人员不得披露云服务商提交的未公开材料以及评估工作中获悉的其他非公开信息，不得将云服务商提供的信息用于评估以外的目的。

第十七条 本办法自 2019 年 9 月 1 日起施行。

关于印发《网络音视频信息服务管理规定》的通知

国信办通字〔2019〕3 号

各省、自治区、直辖市网信办、文化和旅游厅(局)、广播电视局， 新疆生产建设兵团网信办、文化体育广电和旅游局：

为促进网络音视频信息服务健康有序发展，保护公民、法人和其他组织的合法权益，维护国家安全和公共利益，国家互联网信息办公室、文化和旅游部、国家广播电视总局制定了《网络音视频信息服务管理规定》。现印发给你们，请认真遵照执行。

国家互联网信息办公室

文化和旅游部

国家广播电视总局

2019 年 11 月 18 日

网络音视频信息服务管理规定

第一条 为促进网络音视频信息服务健康有序发展，保护公民、法人和其他组织的合法权益，维护国家安全和公共利益，根据《中华人民共和国网络安全法》《互联网信息服务管理办法》《互联网新闻信息服务管理规定》《互联网文化管理暂行规定》《互联网视听节目服务管理规定》，制定本规定。

第二条 在中华人民共和国境内从事网络音视频信息服务，应当遵守本规定。

本规定所称网络音视频信息服务，是指通过互联网站、应用程序等网络平台，向社会公众提供音视频信息制作、发布、传播的服务。

网络音视频信息服务提供者，是指向社会公众提供网络音视频信息服务的组织或者个人。网络音视频信息服务使用者， 是指使用网络音视频信息服务的组织或者个人。

第三条 各级网信、文化和旅游、广播电视等部门依据各自职责开展网络音

视频信息服务的监督管理工作。

第四条 网络音视频信息服务提供者和使用者应当遵守宪法、法律和行政法规，坚持正确政治方向、舆论导向和价值取向， 弘扬社会主义核心价值观，促进形成积极健康、向上向善的网络文化。

第五条 国家鼓励和指导互联网行业组织加强行业自律，建立健全网络音视频信息服务行业标准和行业准则，推动网络音视频信息服务行业信用体系建设，督促网络音视频信息服务提供者依法提供服务、接受社会监督， 提高网络音视频信息服务从业人员职业素养，促进行业健康有序发展。

第六条 网络音视频信息服务提供者应当依法取得法律、行政法规规定的相关资质。

第七条 网络音视频信息服务提供者应当落实信息内容安全管理主体责任，配备与服务规模相适应的专业人员，建立健全用户注册、信息发布审核、信息安全管理、应急处置、从业人员教育培训、未成年人保护、知识产权保护等制度，具有与新技术新应用发展相适应的安全可控的技术保障和防范措施，有效应对网络安全事件，防范网络违法犯罪活动，维护网络数据的完整性、安全性和可用性。

第八条 网络音视频信息服务提供者应当依照《中华人民共和国网络安全法》的规定，对用户进行基于组织机构代码、身份证件号码、移动电话号码等方式的真实身份信息认证。用户不提供真实身份信息的， 网络音视频信息服务提供者不得为其提供信息发布服务。

第九条 任何组织和个人不得利用网络音视频信息服务以及相关信息技术从事危害国家安全、破坏社会稳定、扰乱社会秩序、侵犯他人合法权益等法律法规禁止的活动，不得制作、发布、传播煽动颠覆国家政权、危害政治安全和社会稳定、网络谣言、淫秽色情，以及侵害他人名誉权、肖像权、隐私权、知识产权和其他合法权益等法律法规禁止的信息内容。

第十条 网络音视频信息服务提供者基于深度学习、虚拟现实等新技术新应用上线具有媒体属性或者社会动员功能的音视频信息服务，或者调整增设相关功能的，应当按照国家有关规定开展安全评估。

第十一条 网络音视频信息服务提供者和网络音视频信息服务使用者利用基于深度学习、虚拟现实等的新技术新应用制作、发布、传播非真实音视频信息的，

应当以显著方式予以标识。

网络音视频信息服务提供者和网络音视频信息服务使用者不得利用基于深度学习、虚拟现实等的新技术新应用制作、发布、传播虚假新闻信息。转载音视频新闻信息的，应当依法转载国家规定范围内的单位发布的音视频新闻信息。

第十二条 网络音视频信息服务提供者应当加强对网络音视频信息服务使用者发布的音视频信息的管理，部署应用违法违规音视频以及非真实音视频鉴别技术，发现音视频信息服务使用者制作、发布、传播法律法规禁止的信息内容的，应当依法依约停止传输该信息，采取消除等处置措施，防止信息扩散，保存有关记录，并向网信、文化和旅游、广播电视等部门报告。

网络音视频信息服务提供者发现不符合本规定第十一条第一款要求的信息内容的，应当立即停止传输该信息，以显著方式标识后方可继续传输该信息。

第十三条 网络音视频信息服务提供者应当建立健全辟谣机制，发现网络音视频信息服务使用者利用基于深度学习、虚拟现实等的虚假图像、音视频生成技术制作、发布、传播谣言的， 应当及时采取相应的辟谣措施，并将相关信息报网信、文化和旅游、广播电视等部门备案。

第十四条 网络音视频信息服务提供者应当在与网络音视频信息服务使用者签订的服务协议中，明确双方权利、义务， 要求网络音视频信息服务使用者遵守本规定及相关法律法规。对违反本规定、相关法律法规及服务协议的网络音视频信息服务使用者依法依约采取警示整改、限制功能、暂停更新、关闭账号等处置措施，保存有关记录，并向网信、文化和旅游、广播电视等部门报告。

第十五条 网络音视频信息服务提供者应当自觉接受社会监督，设置便捷的投诉举报入口，公布投诉、举报方式等信息，及时受理并处理公众投诉举报。

第十六条 为网络音视频信息服务提供技术支持的主体应当遵守相关法律法规规定和国家标准规范，采取技术措施和其他必要措施，保障网络安全、稳定运行。

第十七条 各级网信、文化和旅游、广播电视等部门应当建立日常监督检查和定期检查相结合的监督管理制度，指导督促网络音视频信息服务提供者依据法律法规和服务协议规范网络音视频信息服务行为。

网络音视频信息服务提供者应当遵守相关法律法规规定，依法留存网络日志，

配合网信、文化和旅游、广播电视等部门开展监督管理执法工作， 并提供必要的技术、数据支持和协助。

第十八条 网络音视频信息服务提供者和网络音视频信息服务使用者违反本规定的，由网信、文化和旅游、广播电视等部门依照《中华人民共和国网络安全法》《互联网信息服务管理办法》《互联网新闻信息服务管理规定》《互联网文化管理暂行规定》《互联网视听节目服务管理规定》等相关法律法规规定处理；构成违反治安管理行为的，依法给予治安管理处罚；构成犯罪的，依法追究刑事责任。

第十九条 本规定自 2020 年 1 月 1 日起施行。

关于开展 App 违法违规收集使用个人信息专项治理的公告

中央网信办、工业和信息化部、公安部、市场监管总局公告 2019 年第 1 号

近年来，移动互联网应用程序(App)得到广泛应用，在促进经济社会发展、服务民生等方面发挥了不可替代的作用。同时，App 强制授权、过度索权、超范围收集个人信息的现象大量存在，违法违规使用个人信息的问题十分突出，广大网民对此反应强烈。落实《网络安全法》《消费者权益保护法》的要求，为保障个人信息安全，维护广大网民合法权益，中央网信办、工业和信息化部、公安部、市场监管总局决定，自 2019 年 1 月至 12 月，在全国范围组织开展 App 违法违规收集使用个人信息专项治理。现将有关事项公告如下：

一、App 运营者收集使用个人信息时要严格履行《网络安全法》规定的责任义务，对获取的个人信息安全负责，采取有效措施加强个人信息保护。遵循合法、正当、必要的原则，不收集与所提供服务无关的个人信息；收集个人信息时要以通俗易懂、简单明了的方式展示个人信息收集使用规则，并经个人信息主体自主选择同意；不以默认、捆绑、停止安装使用等手段变相强迫用户授权，不得违反法律法规和与用户的约定收集使用个人信息。倡导 App 运营者在定向推送新闻、时政、广告时，为用户提供拒绝接收定向推送的选项。

二、全国信息安全标准化技术委员会、中国消费者协会、中国互联网协会、中国网络空间安全协会，依据法律法规和国家相关标准，编制大众化应用基本业务功能及必要信息规范、App 违法违规收集使用个人信息治理评估要点，组织相关专业机构，对用户数量大、与民众生活密切相关的 App 隐私政策

和个人信息收集使用情况进行评估。

三、有关主管部门加强对违法违规收集使用个人信息行为的监管和处罚，对强制、过度收集个人信息，未经消费者同意、违反法律法规规定和双方约定收集、使用个人信息，发生或可能发生信息泄露、丢失而未采取补救措施，非法出售、非法向他人提供个人信息等行为，按照《网络安全法》《消费者权益保护法》等依法予以处罚，包括责令 App 运营者限期整改；逾期不改的，公开曝光；情节严重的，依法暂停相关业务、停业整顿、吊销相关业务许可证或者吊销营业执照。

四、公安机关开展打击整治网络侵犯公民个人信息违法犯罪专项工作，依法严厉打击针对和利用个人信息的违法犯罪行为。

五、开展 App 个人信息安全认证，鼓励 App 运营者自愿通过 App 个人信息安全认证，鼓励搜索引擎、应用商店等明确标识并优先推荐通过认证的 App。

特此公告。

中央网信信办 工业和信息化部

公安部 市场监管总局

2019 年 1 月 23 日

关于印发《App 违法违规收集使用个人信息行为认定方法》的通知

国信办秘字〔2019〕191 号

各省、自治区、直辖市及新疆生产建设兵团网信办、通信管理局、公安厅(局)、市场监管局(厅、委)：

根据《关于开展 App 违法违规收集使用个人信息专项治理的公告》，为认定 App 违法违规收集使用个人信息行为提供参考，落实《网络安全法》等法律法规，国家互联网信息办公室、工业和信息化部、公安部、市场监管总局联合制定了《App 违法违规收集使用个人信息行为认定方法》。现印发你们，请结合监管和执法工作实际参考执行。

国家互联网信息办公室秘书局

工业和信息化部办公厅

公安部办公厅

市场监管总局办公厅

2019 年 11 月 28 日

App 违法违规收集使用个人信息行为认定方法

根据《关于开展 App 违法违规收集使用个人信息专项治理的公告》，为监督管理部门认定 App 违法违规收集使用个人信息行为提供参考，为 App 运营者自查自纠和网民社会监督提供指引，落实《网络安全法》等法律法规，制定本方法。

一、以下行为可被认定为“未公开收集使用规则”

1.在 App 中没有隐私政策，或者隐私政策中没有收集使用个人信息规则；

2.在 App 首次运行时未通过弹窗等明显方式提示用户阅读隐私政策等收集使用规则；

3.隐私政策等收集使用规则难以访问，如进入 App 主界面后，需多于 4 次点击等操作才能访问到；

4.隐私政策等收集使用规则难以阅读，如文字过小过密、颜色过淡、模糊不清，或未提供简体中文版等。

二、以下行为可被认定为“未明示收集使用个人信息的目的、方式和范围”

1.未逐一列出 App(包括委托的第三方或嵌入的第三方代码、插件)收集使用个人信息的目的、方式、范围等；

2.收集使用个人信息的目的、方式、范围发生变化时， 未以适当方式通知用户，适当方式包括更新隐私政策等收集使用规则并提醒用户阅读等；

3.在申请打开可收集个人信息的权限，或申请收集用户身份证号、银行账号、行踪轨迹等个人敏感信息时，未同步告知用户其目的，或者目的不明确、难以理解；

4.有关收集使用规则的内容晦涩难懂、冗长繁琐， 用户难以理解，如使用大量专业术语等。

三、以下行为可被认定为“未经用户同意收集使用个人信息”

1.征得用户同意前就开始收集个人信息或打开可收集个人信息的权限；

2.用户明确表示不同意后，仍收集个人信息或打开可收集个人信息的权限，或频繁征求用户同意、干扰用户正常使用；

3.实际收集的个人信息或打开的可收集个人信息权限超出用户授权范围；

4.以默认选择同意隐私政策等非明示方式征求用户同意；

5.未经用户同意更改其设置的可收集个人信息权限状态，如 App 更新时自动将用户设置的权限恢复到默认状态；

6.利用用户个人信息和算法定向推送信息，未提供非定向推送信息的选项；

7.以欺诈、诱骗等不正当方式误导用户同意收集个人信息或打开可收集个人信息的权限，如故意欺瞒、掩饰收集使用个人信息的真实目的；

8.未向用户提供撤回同意收集个人信息的途径、方式；

9.违反其所声明的收集使用规则，收集使用个人信息。

四、以下行为可被认定为“违反必要原则，收集与其提供的服务无关的个人信息”

1.收集的个人信息类型或打开的可收集个人信息权限与现有业务功能无关；

2.因用户不同意收集非必要个人信息或打开非必要权限，拒绝提供业务功能；

3.App 新增业务功能申请收集的个人信息超出用户原有同意范围，若用户不同意，则拒绝提供原有业务功能，新增业务功能取代原有业务功能的除外；

4.收集个人信息的频度等超出业务功能实际需要；

5.仅以改善服务质量、提升用户体验、定向推送信息、研发新产品等为由，强制要求用户同意收集个人信息；

6.要求用户一次性同意打开多个可收集个人信息的权限，用户不同意则无法使用。

五、以下行为可被认定为“未经同意向他人提供个人信息”

1.既未经用户同意，也未做匿名化处理，App 客户端直接向第三方提供个人信息，包括通过客户端嵌入的第三方代码、插件等方式向第三方提供个人信息；

2.既未经用户同意，也未做匿名化处理，数据传输至 App 后台服务器后，向第三方提供其收集的个人信息；

3.App 接入第三方应用，未经用户同意，向第三方应用提供个人信息。

六、以下行为可被认定为“未按法律规定提供删除或更正个人信息功能”或“未公布投诉、举报方式等信息”

1.未提供有效的更正、删除个人信息及注销用户账号功能；

2.为更正、删除个人信息或注销用户账号设置不必要或不合理条件；

3.虽提供了更正、删除个人信息及注销用户账号功能， 但未及时响应用户相

应操作，需人工处理的，未在承诺时限内(承诺时限不得超过 15 个工作日，无承诺时限的，以 15 个工作日为限)完成核查和处理；

4.更正、删除个人信息或注销用户账号等用户操作已执行完毕， 但 App 后台并未完成的；

5.未建立并公布个人信息安全投诉、举报渠道，或未在承诺时限内(承诺时限不得超过 15 个工作日，无承诺时限的，以 15 个工作日为限)受理并处理的。

关于印发《常见类型移动互联网应用程序必要个人信息范围规定》的通知

国信办秘字〔2021〕14 号

各省、自治区、直辖市及新疆生产建设兵团网信办、通信管理局、公安厅(局)、市场监管局(厅、委)：

为贯彻落实《中华人民共和国网络安全法》关于“网络运营者收集、使用个人信息，应当遵循合法、正当、必要的原则”“网络运营者不得收集与其提供的服务无关的个人信息”等规定，国家互联网信息办公室、工业和信息化部、公安部、国家市场监督管理总局联合制定了《常见类型移动互联网应用程序必要个人信息范围规定》，明确移动互联网应用程序(App)运营者不得因用户不同意收集非必要个人信息，而拒绝用户使用 App 基本功能服务。

现将《常见类型移动互联网应用程序必要个人信息范围规定》印发给你们，请指导督促本地区 App 运营者抓紧落实，并加强监督检查，及时调查、处理违法违规收集使用个人信息行为，切实维护公民在网络空间的合法权益。

特此通知。

国家互联网信息办公室秘书局

工业和信息化部办公厅

公安部办公厅

国家市场监督管理总局办公厅

2021 年 3 月 12 日

常见类型移动互联网应用程序必要个人信息范围规定

第一条 为了规范移动互联网应用程序(App)收集个人信息行为，保障公民个人信息安全，根据《中华人民共和国网络安全法》，制定本规定。

第二条 移动智能终端上运行的 App 存在收集用户个人信息行为的，应当遵

守本规定。法律、行政法规、部门规章和规范性文件另有规定的，依照其规定。

App 包括移动智能终端预置、下载安装的应用软件，基于应用软件开放平台接口开发的、用户无需安装即可使用的小程序。

第三条 本规定所称必要个人信息，是指保障 App 基本功能服务正常运行所必需的个人信息，缺少该信息 App 即无法实现基本功能服务。具体是指消费侧用户个人信息，不包括服务供给侧用户个人信息。

第四条 App 不得因为用户不同意提供非必要个人信息，而拒绝用户使用其基本功能服务。

第五条 常见类型 App 的必要个人信息范围：

(一)地图导航类，基本功能服务为“定位和导航”，必要个人信息为：位置信息、出发地、到达地。

(二)网络约车类，基本功能服务为“网络预约出租汽车服务、巡游出租汽车电召服务”，必要个人信息包括：

1.注册用户移动电话号码；

2.乘车人出发地、到达地、位置信息、行踪轨迹；

3.支付时间、支付金额、支付渠道等支付信息(网络预约出租汽车服务)。

(三)即时通信类，基本功能服务为“提供文字、图片、语音、视频等网络即时通信服务”，必要个人信息包括：

1.注册用户移动电话号码；

2.账号信息：账号、即时通信联系人账号列表。

(四)网络社区类，基本功能服务为“博客、论坛、社区等话题讨论、信息分享和关注互动”，必要个人信息为：注册用户移动电话号码。

(五)网络支付类，基本功能服务为“网络支付、提现、转账等功能”，必要个人信息包括：

1.注册用户移动电话号码；

2.注册用户姓名、证件类型和号码、证件有效期限、银行卡号码。

(六)网上购物类，基本功能服务为“购买商品”，必要个人信息包括：

1.注册用户移动电话号码；

2.收货人姓名(名称)、地址、联系电话;

3.支付时间、支付金额、支付渠道等支付信息。

(七)餐饮外卖类,基本功能服务为“餐饮购买及外送”,必要个人信息包括:

1.注册用户移动电话号码;

2.收货人姓名(名称)、地址、联系电话;

3.支付时间、支付金额、支付渠道等支付信息。

(八)邮件快件寄递类,基本功能服务为“信件、包裹、印刷品等物品寄递服务”,必要个人信息包括:

1.寄件人姓名、证件类型和号码等身份信息;

2.寄件人地址、联系电话;

3.收件人姓名(名称)、地址、联系电话;

4.寄递物品的名称、性质、数量。

(九)交通票务类,基本功能服务为“交通相关的票务服务及行程管理(如票务购买、改签、退票、行程管理等)”,必要个人信息包括:

1.注册用户移动电话号码;

2.旅客姓名、证件类型和号码、旅客类型。旅客类型通常包括儿童、成人、学生等;

3.旅客出发地、目的地、出发时间、车次/船次/航班号、席别/舱位等级、座位号(如有)、车牌号及车牌颜色(ETC 服务);

4.支付时间、支付金额、支付渠道等支付信息。

(十)婚恋相亲类,基本功能服务为“婚恋相亲”,必要个人信息包括:

1.注册用户移动电话号码;

2.婚恋相亲人的性别、年龄、婚姻状况。

(十一)求职招聘类,基本功能服务为“求职招聘信息交换”,必要个人信息包括:

1.注册用户移动电话号码;

2.求职者提供的简历。

(十二)网络借贷类,基本功能服务为“通过互联网平台实现的用于消费、

日常生产经营周转等的个人申贷服务”，必要个人信息包括：

1.注册用户移动电话号码；

2.借款人姓名、证件类型和号码、证件有效期限、银行卡号码。

(十三)房屋租售类，基本功能服务为“个人房源信息发布、房屋出租或买卖”，必要个人信息包括：

1.注册用户移动电话号码；

2.房源基本信息：房屋地址、面积/户型、期望售价或租金。

(十四)二手车交易类，基本功能服务为“二手车买卖信息交换”，必要个人信息包括：

1.注册用户移动电话号码；

2.购买方姓名、证件类型和号码；

3.出售方姓名、证件类型和号码、车辆行驶证号、车辆识别号码。

(十五)问诊挂号类，基本功能服务为“在线咨询问诊、预约挂号”，必要个人信息包括：

1.注册用户移动电话号码；

2.挂号时需提供患者姓名、证件类型和号码、预约挂号的医院和科室；

3.问诊时需提供病情描述。

(十六)旅游服务类，基本功能服务为“旅游服务产品信息的发布与订购”，必要个人信息包括：

1.注册用户移动电话号码；

2.出行人旅游目的地、旅游时间；

3.出行人姓名、证件类型和号码、联系方式。

(十七)酒店服务类，基本功能服务为“酒店预订”，必要个人信息包括：

1.注册用户移动电话号码；

2.住宿人姓名和联系方式、入住和退房时间、入住酒店名称。

(十八)网络游戏类，基本功能服务为“提供网络游戏产品和服务”，必要个人信息为：注册用户移动电话号码。

(十九)学习教育类，基本功能服务为“在线辅导、网络课堂等”，必要个人信息为：注册用户移动电话号码。

(二十)本地生活类，基本功能服务为“家政维修、家居装修、二手闲置物品交易等日常生活服务”，必要个人信息为：注册用户移动电话号码。

(二十一)女性健康类，基本功能服务为“女性经期管理、备孕育儿、美容美体等健康管理服务”，无须个人信息，即可使用基本功能服务。

(二十二)用车服务类，基本功能服务为“共享单车、共享汽车、租赁汽车等服务”，必要个人信息包括：

1.注册用户移动电话号码；

2.使用共享汽车、租赁汽车服务用户的证件类型和号码，驾驶证件信息；

3.支付时间、支付金额、支付渠道等支付信息；

4.使用共享单车、分时租赁汽车服务用户的位置信息。

(二十三)投资理财类，基本功能服务为“股票、期货、基金、债券等相关投资理财服务”，必要个人信息包括：

1.注册用户移动电话号码；

2.投资理财用户姓名、证件类型和号码、证件有效期限、证件影印件；

3.投资理财用户资金账户、银行卡号码或支付账号。

(二十四)手机银行类，基本功能服务为“通过手机等移动智能终端设备进行银行账户管理、信息查询、转账汇款等服务”，必要个人信息包括：

1.注册用户移动电话号码；

2.用户姓名、证件类型和号码、证件有效期限、证件影印件、银行卡号码、银行预留移动电话号码；

3.转账时需提供收款人姓名、银行卡号码、开户银行信息。

(二十五)邮箱云盘类，基本功能服务为“邮箱、云盘等”，必要个人信息为：注册用户移动电话号码。

(二十六)远程会议类，基本功能服务为“通过网络提供音频或视频会议”，必要个人信息为：注册用户移动电话号码。

(二十七)网络直播类，基本功能服务为“向公众持续提供实时视频、音频、图文等形式信息浏览服务”，无须个人信息，即可使用基本功能服务。

(二十八)在线影音类，基本功能服务为“影视、音乐搜索和播放”，无须个人信息，即可使用基本功能服务。

(二十九)短视频类，基本功能服务为“不超过一定时长的视频搜索、播放”，无须个人信息，即可使用基本功能服务。

(三十)新闻资讯类，基本功能服务为“新闻资讯的浏览、搜索”，无须个人信息，即可使用基本功能服务。

(三十一)运动健身类，基本功能服务为“运动健身训练”，无须个人信息，即可使用基本功能服务。

(三十二)浏览器类，基本功能服务为“浏览互联网信息资源”，无须个人信息，即可使用基本功能服务。

(三十三)输入法类，基本功能服务为“文字、符号等输入”，无须个人信息，即可使用基本功能服务。

(三十四)安全管理类，基本功能服务为“查杀病毒、清理恶意插件、修复漏洞等”，无须个人信息，即可使用基本功能服务。

(三十五)电子图书类，基本功能服务为“电子图书搜索、阅读”，无须个人信息，即可使用基本功能服务。

(三十六)拍摄美化类，基本功能服务为“拍摄、美颜、滤镜等”，无须个人信息，即可使用基本功能服务。

(三十七)应用商店类，基本功能服务为“App 搜索、下载”，无须个人信息，即可使用基本功能服务。

(三十八)实用工具类，基本功能服务为“日历、天气、词典翻译、计算器、遥控器、手电筒、指南针、时钟闹钟、文件传输、文件管理、壁纸铃声、截图录屏、录音、文档处理、智能家居助手、星座性格测试等”，无须个人信息，即可使用基本功能服务。

(三十九)演出票务类，基本功能服务为“演出购票”，必要个人信息包括：

1.注册用户移动电话号码；

2.观演场次、座位号(如有)；

3.支付时间、支付金额、支付渠道等支付信息。

第六条 任何组织和个人发现违反本规定行为的，可以向相关部门举报。

相关部门收到举报后，应当依法予以处理。

第七条 本规定自 2021 年 5 月 1 日起施行。

关于印发《关于加强互联网信息服务算法综合治理的指导意见》的通知

国信办发文〔2021〕7 号

各省、自治区、直辖市网信办、党委宣传部、教育厅(教委)、科技厅(委、局)、通信管理局、公安厅(局)、文化和旅游厅(局)、市场监管局(厅、委)、广播电视局，新疆生产建设兵团网信办、党委宣传部、教育局、科技局、公安局、文化体育广电和旅游局、市场监管局：

为加强互联网信息服务算法综合治理，促进行业健康有序繁荣发展，国家互联网信息办公室、中央宣传部、教育部、科学技术部、工业和信息化部、公安部、文化和旅游部、国家市场监督管理总局、国家广播电视总局等九部委制定了《关于加强互联网信息服务算法综合治理的指导意见》。现印发给你们，请结合实际，认真贯彻执行。

国家互联网信息办公室

中央宣传部

教育部

科学技术部

工业和信息化部

公安部

文化和旅游部

国家市场监督管理总局

国家广播电视总局

2021 年 9 月 17 日

关于加强互联网信息服务算法综合治理的指导意见

近年来，互联网信息服务算法(以下简称“算法”)在加速互联网信息传播、繁荣数字经济、促进社会发展等方面发挥了重要作用。与此同时，算法不合理应用也影响了正常的传播秩序、市场秩序和社会秩序，给维护意识形态安全、社会公平公正和网民合法权益带来挑战。为深入贯彻落实党中央、国务院决策部署，管理好使用好发展好算法应用，全面提升网络综合治理能力，现就加强互联网信息服务算法安全治理提出如下意见。

一、总体要求

(一)指导思想

坚持以习近平新时代中国特色社会主义思想特别是习近平总书记关于网络强国的重要思想为指导，深入贯彻党的十九大和十九届二中、三中、四中、五中全会精神，坚持正能量是总要求、管得住是硬道理、用得好是真本事，以算法安全可信、高质量、创新性发展为导向，建立健全算法安全治理机制，构建完善算法安全监管体系，推进算法自主创新，促进算法健康、有序、繁荣发展，为建设网络强国提供有力支撑。

(二)基本原则

坚持正确导向，强化科技伦理意识、安全意识和底线思维，充分发挥算法服务正能量传播作用，营造风清气正的网络空间；坚持依法治理，加强法律法规建设，创新技术监管模式，打击违法违规行为，建立健全多方参与的算法安全治理机制；坚持风险防控，推进算法分级分类安全管理，有效识别高风险类算法，实施精准治理；坚持权益保障，引导算法应用公平公正、透明可释，充分保障网民合法权益；坚持技术创新，大力推进我国算法创新研究工作，保护算法知识产权，强化自研算法的部署和推广，提升我国算法的核心竞争力。

(三)主要目标

利用三年左右时间，逐步建立治理机制健全、监管体系完善、算法生态规范的算法安全综合治理格局。

——治理机制健全。制定完善互联网信息服务算法安全治理政策法规，算法安全治理的主体权责明确，治理结构高效运行，形成有法可依、多元协同、多方参与的治理机制。

——监管体系完善。创新性地构建形成算法安全风险监测、算法安全评估、科技伦理审查、算法备案管理和涉算法违法违规行为处置等多维一体的监管体系。

——算法生态规范。算法导向正确、正能量充沛，算法应用公平公正、公开透明，算法发展安全可控、自主创新，有效防范算法滥用带来的风险隐患。

二、健全算法安全治理机制

(一)加强算法治理规范。健全算法安全治理政策法规，加快制定算法管理规定，明确算法管理主体、管理范围、管理要求和法律责任等，完善算法安全

治理措施，制定标准、指南等配套文件。

(二)优化算法治理结构。进一步明确政府、企业、行业组织和网民在算法安全治理中的权利、义务和责任，科学合理布局治理组织结构，规范运作、相互衔接，打造形成政府监管、企业履责、行业自律、社会监督的算法安全多元共治局面。

(三)强化统筹协同治理。网信部门会同宣传、教育、科技、工信、公安、文化和旅游、市场监管、广电等部门，建立部门协同联动长效机制，履行监管职责，共同开展算法安全治理工作。

(四)强化企业主体责任。企业应建立算法安全责任制度和科技伦理审查制度，健全算法安全管理组织机构，加强风险防控和隐患排查治理，提升应对算法安全突发事件的能力和水平。企业应强化责任意识，对算法应用产生的结果负主体责任。

(五)强化行业组织自律。互联网信息服务行业应当加强行业自律，积极开展算法科学技术普及工作，逐步组建算法安全治理力量，吸引专业人才队伍，汇聚多方资源投入，承担算法安全治理社会责任，为算法安全治理提供有力支撑。

(六)倡导网民监督参与。鼓励广大网民积极参与算法安全治理工作，切实加强政府、企业、行业组织和网民间的信息交流和有效沟通。政府积极受理网民举报投诉，企业自觉接受社会监督并及时做好结果反馈。

三、构建算法安全监管体系

(七)有效监测算法安全风险。对算法的数据使用、应用场景、影响效果等开展日常监测工作，感知算法应用带来的网络传播趋势、市场规则变化、网民行为等信息，预警算法应用可能产生的不规范、不公平、不公正等隐患，发现算法应用安全问题。

(八)积极开展算法安全评估。组织建立专业技术评估队伍，深入分析算法机制机理，评估算法设计、部署和使用等应用环节的缺陷和漏洞，研判算法应用产生的意识形态、社会公平、道德伦理等安全风险，提出针对性应对措施。

(九)有序推进算法备案工作。建立算法备案制度，梳理算法备案基本情况，健全算法分级分类体系，明确算法备案范围，有序开展备案工作。积极做

好备案指导帮助，主动公布备案情况，接受社会监督。

(十)持续推进监管模式创新。持续研判算法领域技术发展新形势，推进监管模式与算法技术协同发展，不断完善、升级、创新监管的方式方法和治理举措，防范监管模式落后导致的算法安全风险。

(十一)严厉打击违法违规行为。着力解决网民反映强烈的算法安全问题，对算法监测、评估、备案等工作中发现的、以及网民举报并查实的涉算法违法违规行为，予以严厉打击，坚决维护互联网信息服务算法安全。

四、促进算法生态规范发展

(十二)树立算法正确导向。弘扬社会主义核心价值观，在算法应用中坚持正确政治方向、舆论导向、价值取向。提高正能量传播的精准性和有效性，规范信息分发行为和秩序，推动企业借助算法加强正能量传播，引导算法应用向上向善。

(十三)推动算法公开透明。规范企业算法应用行为，保护网民合理权益，秉持公平、公正原则，促进算法公开透明。督促企业及时、合理、有效地公开算法基本原理、优化目标、决策标准等信息，做好算法结果解释，畅通投诉通道，消除社会疑虑，推动算法健康发展。

(十四)鼓励算法创新发展。提升算法创新能力，积极开展算法研发工作，支持算法与社会、经济各领域深度结合。提高算法自主可控能力，加强知识产权保护，提高自研算法产品的推广和使用，增强算法核心竞争力。

(十五)防范算法滥用风险。维护网络空间传播秩序、市场秩序和社会秩序，防止利用算法干扰社会舆论、打压竞争对手、侵害网民权益等行为，防范算法滥用带来意识形态、经济发展和社会管理等方面的风险隐患。

中央网信办关于印发《国家网络安全事件应急预案》的通知

中网办发文〔2017〕4 号

各省、自治区、直辖市、新疆生产建设兵团党委网络安全和信息化领导小组，中央和国家机关各部委、各人民团体：

《国家网络安全事件应急预案》已经中央网络安全和信息化领导小组同意，现印发给你们，请认真组织实施。

中央网络安全和信息化领导小组办公室

2017 年 1 月 10 日

国家网络安全事件应急预案

目 录

1 总则

1.1 编制目的

建立健全国家网络安全事件应急工作机制，提高应对网络安全事件能力，预防和减少网络安全事件造成的损失和危害，保护公众利益，维护国家安全、公共安全和社会秩序。

1.2 编制依据

《中华人民共和国突发事件应对法》、《中华人民共和国网络安全法》、《国家突发公共事件总体应急预案》、《突发事件应急预案管理办法》和《信息安全技术 信息安全事件分类分级指南》(GB/Z 20986-2007)等相关规定。

1.3 适用范围

本预案所指网络安全事件是指由于人为原因、软硬件缺陷或故障、自然灾害等，对网络和信息系统或者其中的数据造成危害，对社会造成负面影响的事

件，可分为有害程序事件、网络攻击事件、信息破坏事件、信息内容安全事件、设备设施故障、灾害性事件和其他事件。

本预案适用于网络安全事件的应对工作。其中，有关信息内容安全事件的应对，另行制定专项预案。

1.4 事件分级

网络安全事件分为四级：特别重大网络安全事件、重大网络安全事件、较大网络安全事件、一般网络安全事件。

(1)符合下列情形之一的，为特别重大网络安全事件：

①重要网络和信息系统遭受特别严重的系统损失，造成系统大面积瘫痪，丧失业务处理能力。

②国家秘密信息、重要敏感信息和关键数据丢失或被窃取、篡改、假冒，对国家安全和社会稳定构成特别严重威胁。

③其他对国家安全、社会秩序、经济建设和公众利益构成特别严重威胁、造成特别严重影响的网络安全事件。

(2)符合下列情形之一且未达到特别重大网络安全事件的，为重大网络安全事件：

①重要网络和信息系统遭受严重的系统损失，造成系统长时间中断或局部瘫痪，业务处理能力受到极大影响。

②国家秘密信息、重要敏感信息和关键数据丢失或被窃取、篡改、假冒，对国家安全和社会稳定构成严重威胁。

③其他对国家安全、社会秩序、经济建设和公众利益构成严重威胁、造成严重影响的网络安全事件。

(3)符合下列情形之一且未达到重大网络安全事件的，为较大网络安全事件：

①重要网络和信息系统遭受较大的系统损失，造成系统中断，明显影响系统效率，业务处理能力受到影响。

②国家秘密信息、重要敏感信息和关键数据丢失或被窃取、篡改、假冒，对国家安全和社会稳定构成较严重威胁。

③其他对国家安全、社会秩序、经济建设和公众利益构成较严重威胁、造

成较严重影响的网络安全事件。

(4)除上述情形外，对国家安全、社会秩序、经济建设和公众利益构成一定威胁、造成一定影响的网络安全事件，为一般网络安全事件。

1.5 工作原则

坚持统一领导、分级负责；坚持统一指挥、密切协同、快速反应、科学处置；坚持预防为主，预防与应急相结合；坚持谁主管谁负责、谁运行谁负责，充分发挥各方面力量共同做好网络安全事件的预防和处置工作。

2 组织机构与职责

2.1 领导机构与职责

在中央网络安全和信息化领导小组(以下简称“领导小组”)的领导下，中央网络安全和信息化领导小组办公室(以下简称“中央网信办”)统筹协调组织国家网络安全事件应对工作，建立健全跨部门联动处置机制，工业和信息化部、公安部、国家保密局等相关部门按照职责分工负责相关网络安全事件应对工作。必要时成立国家网络安全事件应急指挥部(以下简称“指挥部”)，负责特别重大网络安全事件处置的组织指挥和协调。

2.2 办事机构与职责

国家网络安全应急办公室(以下简称“应急办”)设在中央网信办，具体工作由中央网信办网络安全协调局承担。应急办负责网络安全应急跨部门、跨地区协调工作和指挥部的事务性工作，组织指导国家网络安全应急技术支撑队伍做好应急处置的技术支撑工作。有关部门派负责相关工作的司局级同志为联络员，联络应急办工作。

2.3 各部门职责

中央和国家机关各部门按照职责和权限，负责本部门、本行业网络和信息系统网络安全事件的预防、监测、报告和应急处置工作。

2.4 各省(区、市)职责

各省(区、市)网信部门在本地区党委网络安全和信息化领导小组统一领导下，统筹协调组织本地区网络和信息系统网络安全事件的预防、监测、报告和应急处置工作。

3 监测与预警

3.1 预警分级

网络安全事件预警等级分为四级：由高到低依次用红色、橙色、黄色和蓝色表示，分别对应发生或可能发生特别重大、重大、较大和一般网络安全事件。

3.2 预警监测

各单位按照“谁主管谁负责、谁运行谁负责”的要求，组织对本单位建设运行的网络和信息系统开展网络安全监测工作。重点行业主管或监管部门组织指导做好本行业网络安全监测工作。各省(区、市)网信部门结合本地区实际，统筹组织开展对本地区网络和信息系统的安全监测工作。各省(区、市)、各部门将重要监测信息报应急办，应急办组织开展跨省(区、市)、跨部门的网络安全信息共享。

3.3 预警研判和发布

各省(区、市)、各部门组织对监测信息进行研判，认为需要立即采取防范措施的，应当及时通知有关部门和单位，对可能发生重大及以上网络安全事件的信息及时向应急办报告。各省(区、市)、各部门可根据监测研判情况，发布本地区、本行业的橙色及以下预警。

应急办组织研判，确定和发布红色预警和涉及多省(区、市)、多部门、多行业的预警。

预警信息包括事件的类别、预警级别、起始时间、可能影响范围、警示事项、应采取的措施和时限要求、发布机关等。

3.4 预警响应

3.4.1 红色预警响应

(1)应急办组织预警响应工作，联系专家和有关机构，组织对事态发展情况进行跟踪研判，研究制定防范措施和应急工作方案，协调组织资源调度和部门联动的各项准备工作。

(2)有关省(区、市)、部门网络安全事件应急指挥机构实行 24 小时值班，相关人员保持通信联络畅通。加强网络安全事件监测和事态发展信息搜集工作，组织指导应急支撑队伍、相关运行单位开展应急处置或准备、风险评估和控制工作，重要情况报应急办。

(3)国家网络安全应急技术支撑队伍进入待命状态，针对预警信息研究制定应对方案，检查应急车辆、设备、软件工具等，确保处于良好状态。

3.4.2 橙色预警响应

(1)有关省(区、市)、部门网络安全事件应急指挥机构启动相应应急预案，组织开展预警响应工作，做好风险评估、应急准备和风险控制工作。

(2)有关省(区、市)、部门及时将事态发展情况报应急办。应急办密切关注事态发展，有关重大事项及时通报相关省(区、市)和部门。

(3)国家网络安全应急技术支撑队伍保持联络畅通，检查应急车辆、设备、软件工具等，确保处于良好状态。

3.4.3 黄色、蓝色预警响应

有关地区、部门网络安全事件应急指挥机构启动相应应急预案，指导组织开展预警响应。

3.5 预警解除

预警发布部门或地区根据实际情况，确定是否解除预警，及时发布预警解除信息。

4 应急处置

4.1 事件报告

网络安全事件发生后，事发单位应立即启动应急预案，实施处置并及时报送信息。各有关地区、部门立即组织先期处置，控制事态，消除隐患，同时组织研判，注意保存证据，做好信息通报工作。对于初判为特别重大、重大网络安全事件的，立即报告应急办。

4.2 应急响应

网络安全事件应急响应分为四级，分别对应特别重大、重大、较大和一般网络安全事件。I 级为最高响应级别。

4.2.1 Ⅰ级响应

属特别重大网络安全事件的，及时启动 I 级响应，成立指挥部，履行应急处置工作的统一领导、指挥、协调职责。应急办 24 小时值班。

有关省(区、市)、部门应急指挥机构进入应急状态，在指挥部的统一领导、指挥、协调下，负责本省(区、市)、本部门应急处置工作或支援保障工

作，24 小时值班，并派员参加应急办工作。

有关省(区、市)、部门跟踪事态发展，检查影响范围，及时将事态发展变化情况、处置进展情况报应急办。指挥部对应对工作进行决策部署，有关省(区、市)和部门负责组织实施。

4.2.2 Ⅱ级响应

网络安全事件的Ⅱ级响应，由有关省(区、市)和部门根据事件的性质和情况确定。

(1)事件发生省(区、市)或部门的应急指挥机构进入应急状态，按照相关应急预案做好应急处置工作。

(2)事件发生省(区、市)或部门及时将事态发展变化情况报应急办。应急办将有关重大事项及时通报相关地区和部门。

(3)处置中需要其他有关省(区、市)、部门和国家网络安全应急技术支撑队伍配合和支持的，商应急办予以协调。相关省(区、市)、部门和国家网络安全应急技术支撑队伍应根据各自职责，积极配合、提供支持。

(4)有关省(区、市)和部门根据应急办的通报，结合各自实际有针对性地加强防范，防止造成更大范围影响和损失。

4.2.3 Ⅲ级、Ⅳ级响应

事件发生地区和部门按相关预案进行应急响应。

4.3 应急结束

4.3.1 Ⅰ级响应结束

应急办提出建议，报指挥部批准后，及时通报有关省(区、市)和部门。

4.3.2 Ⅱ级响应结束

由事件发生省(区、市)或部门决定，报应急办，应急办通报相关省(区、市)和部门。

5 调查与评估

特别重大网络安全事件由应急办组织有关部门和省(区、市)进行调查处理和总结评估，并按程序上报。重大及以下网络安全事件由事件发生地区或部门自行组织调查处理和总结评估，其中重大网络安全事件相关总结调查报告报应急办。总结调查报告应对事件的起因、性质、影响、责任等进行分析评估，提

出处理意见和改进措施。

事件的调查处理和总结评估工作原则上在应急响应结束后 30 天内完成。

6 预防工作

6.1 日常管理

各地区、各部门按职责做好网络安全事件日常预防工作，制定完善相关应急预案，做好网络安全检查、隐患排查、风险评估和容灾备份，健全网络安全信息通报机制，及时采取有效措施，减少和避免网络安全事件的发生及危害，提高应对网络安全事件的能力。

6.2 演练

中央网信办协调有关部门定期组织演练，检验和完善预案，提高实战能力。

各省(区、市)、各部门每年至少组织一次预案演练，并将演练情况报中央网信办。

6.3 宣传

各地区、各部门应充分利用各种传播媒介及其他有效的宣传形式，加强突发网络安全事件预防和处置的有关法律、法规和政策的宣传，开展网络安全基本知识和技能的宣传活动。

6.4 培训

各地区、各部门要将网络安全事件的应急知识列为领导干部和有关人员的培训内容，加强网络安全特别是网络安全应急预案的培训，提高防范意识及技能。

6.5 重要活动期间的预防措施

在国家重要活动、会议期间，各省(区、市)、各部门要加强网络安全事件的防范和应急响应，确保网络安全。应急办统筹协调网络安全保障工作，根据需要要求有关省(区、市)、部门启动红色预警响应。有关省(区、市)、部门加强网络安全监测和分析研判，及时预警可能造成重大影响的风险和隐患，重点部门、重点岗位保持 24 小时值班，及时发现和处置网络安全事件隐患。

7 保障措施

7.1 机构和人员

各地区、各部门、各单位要落实网络安全应急工作责任制，把责任落实到具体部门、具体岗位和个人，并建立健全应急工作机制。

7.2 技术支撑队伍

加强网络安全应急技术支撑队伍建设，做好网络安全事件的监测预警、预防防护、应急处置、应急技术支援工作。支持网络安全企业提升应急处置能力，提供应急技术支援。中央网信办制定评估认定标准，组织评估和认定国家网络安全应急技术支撑队伍。各省(区、市)、各部门应配备必要的网络安全专业技术人才，并加强与国家网络安全相关技术单位的沟通、协调，建立必要的网络安全信息共享机制。

7.3 专家队伍

建立国家网络安全应急专家组，为网络安全事件的预防和处置提供技术咨询和决策建议。各地区、各部门加强各自的专家队伍建设，充分发挥专家在应急处置工作中的作用。

7.4 社会资源

从教育科研机构、企事业单位、协会中选拔网络安全人才，汇集技术与数据资源，建立网络安全事件应急服务体系，提高应对特别重大、重大网络安全事件的能力。

7.5 基础平台

各地区、各部门加强网络安全应急基础平台和管理平台建设，做到早发现、早预警、早响应，提高应急处置能力。

7.6 技术研发和产业促进

有关部门加强网络安全防范技术研究，不断改进技术装备，为应急响应工作提供技术支撑。加强政策引导，重点支持网络安全监测预警、预防防护、处置救援、应急服务等方向，提升网络安全应急产业整体水平与核心竞争力，增强防范和处置网络安全事件的产业支撑能力。

7.7 国际合作

有关部门建立国际合作渠道，签订合作协定，必要时通过国际合作共同应对突发网络安全事件。

7.8 物资保障

加强对网络安全应急装备、工具的储备，及时调整、升级软件硬件工具，不断增强应急技术支撑能力。

7.9 经费保障

财政部门为网络安全事件应急处置提供必要的资金保障。有关部门利用现有政策和资金渠道，支持网络安全应急技术支撑队伍建设、专家队伍建设、基础平台建设、技术研发、预案演练、物资保障等工作开展。各地区、各部门为网络安全应急工作提供必要的经费保障。

7.10 责任与奖惩

网络安全事件应急处置工作实行责任追究制。

中央网信办及有关地区和部门对网络安全事件应急管理工作中作出突出贡献的先进集体和个人给予表彰和奖励。

中央网信办及有关地区和部门对不按照规定制定预案和组织开展演练，迟报、谎报、瞒报和漏报网络安全事件重要情况或者应急管理工作中有其他失职、渎职行为的，依照相关规定对有关责任人给予处分；构成犯罪的，依法追究刑事责任。

8 附则

8.1 预案管理

本预案原则上每年评估一次，根据实际情况适时修订。修订工作由中央网信办负责。

各省(区、市)、各部门、各单位要根据本预案制定或修订本地区、本部门、本行业、本单位网络安全事件应急预案。

8.2 预案解释

本预案由中央网信办负责解释。

8.3 预案实施时间

本预案自印发之日起实施。

附件：

1.网络安全事件分类

2.名词术语

3.网络和信息系统损失程度划分说明

附件 1

网络安全事件分类

网络安全事件分为有害程序事件、网络攻击事件、信息破坏事件、信息内容安全事件、设备设施故障、灾害性事件和其他网络安全事件等。

(1)有害程序事件分为计算机病毒事件、蠕虫事件、特洛伊木马事件、僵尸网络事件、混合程序攻击事件、网页内嵌恶意代码事件和其他有害程序事件。

(2)网络攻击事件分为拒绝服务攻击事件、后门攻击事件、漏洞攻击事件、网络扫描窃听事件、网络钓鱼事件、干扰事件和其他网络攻击事件。

(3)信息破坏事件分为信息篡改事件、信息假冒事件、信息泄露事件、信息窃取事件、信息丢失事件和其他信息破坏事件。

(4)信息内容安全事件是指通过网络传播法律法规禁止信息，组织非法串联、煽动集会游行或炒作敏感问题并危害国家安全、社会稳定和公众利益的事件。

(5)设备设施故障分为软硬件自身故障、外围保障设施故障、人为破坏事故和其他设备设施故障。

(6)灾害性事件是指由自然灾害等其他突发事件导致的网络安全事件。

(7)其他事件是指不能归为以上分类的网络安全事件。

附件 2

名词术语

一、重要网络与信息系统

所承载的业务与国家安全、社会秩序、经济建设、公众利益密切相关的网络和信息系统。

(参考依据：《信息安全技术 信息安全事件分类分级指南》(GB/Z 20986-2007))

二、重要敏感信息

不涉及国家秘密，但与国家安全、经济发展、社会稳定以及企业和公众利益密切相关的信息，这些信息一旦未经授权披露、丢失、滥用、篡改或销毁，可能造成以下后果：

a)损害国防、国际关系；

b)损害国家财产、公共利益以及个人财产或人身安全；

c)影响国家预防和打击经济与军事间谍、政治渗透、有组织犯罪等；

d)影响行政机关依法调查处理违法、渎职行为，或涉嫌违法、渎职行为；

e)干扰政府部门依法公正地开展监督、管理、检查、审计等行政活动，妨碍政府部门履行职责；

f)危害国家关键基础设施、政府信息系统安全；

g)影响市场秩序，造成不公平竞争，破坏市场规律；

h)可推论出国家秘密事项；

i)侵犯个人隐私、企业商业秘密和知识产权；

j)损害国家、企业、个人的其他利益和声誉。

（参考依据：《信息安全技术 云计算服务安全指南》(GB/T31167-2014)）

附件 3

网络和信息系统损失程度划分说明

网络和信息系统损失是指由于网络安全事件对系统的软硬件、功能及数据的破坏，导致系统业务中断，从而给事发组织所造成的损失，其大小主要考虑恢复系统正常运行和消除安全事件负面影响所需付出的代价，划分为特别严重的系统损失、严重的系统损失、较大的系统损失和较小的系统损失，说明如下：

a)特别严重的系统损失：造成系统大面积瘫痪，使其丧失业务处理能力，或系统关键数据的保密性、完整性、可用性遭到严重破坏，恢复系统正常运行和消除安全事件负面影响所需付出的代价十分巨大，对于事发组织是不可承受的；

b)严重的系统损失：造成系统长时间中断或局部瘫痪，使其业务处理能力受到极大影响，或系统关键数据的保密性、完整性、可用性遭到破坏，恢复系统正常运行和消除安全事件负面影响所需付出的代价巨大，但对于事发组织是可承受的；

c)较大的系统损失：造成系统中断，明显影响系统效率，使重要信息系统或一般信息系统业务处理能力受到影响，或系统重要数据的保密性、完整性、可用性遭到破坏，恢复系统正常运行和消除安全事件负面影响所需付出的代价

较大，但对于事发组织是完全可以承受的；

d)较小的系统损失：造成系统短暂中断，影响系统效率，使系统业务处理能力受到影响，或系统重要数据的保密性、完整性、可用性遭到影响，恢复系统正常运行和消除安全事件负面影响所需付出的代价较小。

中央网信办秘书局关于进一步加强娱乐明星网上信息规范相关工作的通知

各省、自治区、直辖市党委网信办，新疆生产建设兵团党委网信办：

近年来，网上泛娱乐化倾向、低俗炒作现象屡禁不止，流量至上、畸形审美、“饭圈”乱象等不良文化冲击主流价值观， 一些网上有关明星的宣传信息内容失范，绯闻八卦、隐私爆料占据网站平台头条版面、热搜榜单，占用大量公共平台资源，人民群众反映强烈。为进一步规范娱乐明星网上信息，营造积极健康向上的网络环境，现就有关工作措施通知如下：

一、严把内容导向

1.加强正面引导。强化娱乐明星网上信息导向管理，发布和传播娱乐明星网上信息要遵守法律法规，遵循公序良俗，坚持正确舆论导向和价值取向，弘扬社会主义核心价值观，坚持健康格调品位。

2.建立负面清单。娱乐明星网上信息不得含有法律、行政法规明确禁止的内容，不得宣扬流量至上、畸形审美、奢靡享乐、炫富拜金等不良价值观，不得为博眼球低俗炒作绯闻丑闻、渲染明星情感纠纷隐秘细节，不得未经授权曝光、买卖明星身份信息、家庭住址、行程信息等个人隐私，不得批量发布涉明星艺人及其作品，进行恶意营销或刷量控评，不得发布涉明星虚假不实信息，进行曲解诋毁、造谣抹黑，不得为违法失德明星艺人复出造势、洗地宣传，不得挑动粉丝群体互撕谩骂、攻击对立，或刺激诱导粉丝群体进行过度消费、非法集资、非理性打投等应援行为。

二、规范信息呈现

细化娱乐明星网上信息分类，强化重点环节管理，严格规范娱乐明星信息网上呈现。

3.演艺作品类信息，具体包括明星影视、音乐、综艺作品及相关宣传、片段、演绎、评述等，原则上自然传播，但不得在《网络信息内容生态治理规定》第十一条规定的重点环节扎堆呈现，含有明星个人标识的，在首页首屏、

热门推荐、热搜榜单等环节，同一明星同一时段原则上只能呈现一条。

4.个人动态类信息，具体包括明星日常生活、行程动态、兴趣偏好、家庭成员等，原则上不在《网络信息内容生态治理规定》第十一条规定的重点环节呈现。

5.商业活动类信息，具体包括明星广告代言、品牌合作、商业推广等，原则上仅在各网站平台广告位置呈现，且应在显著位置标明广告字样。

6.公告类信息，具体包括明星维权、回应、澄清、公告等，原则上自然传播，但同一明星同一事件的公告类信息，在《网络信息内容生态治理规定》第十一条规定的重点环节同一时段原则上只能呈现一条。

7.公益类信息，具体包括明星参与公益活动、救援救助、正能量宣传等，原则上自然传播，但不得恶意蹭炒热点进行营销炒作。

8.权威发布类信息，具体包括国家机关、主流媒体、行业协会等关于明星相关事件的表态、回应、公布和舆论监督等，原则上自然传播。

三、加强账号管理

9.规范账号名称、头像和简介。娱乐明星、经纪公司(工作室)、粉丝团(后援会)和娱乐类公众账号等名称、头像和简介中，不得含有明示或暗示爆料明星隐私等信息，不得含有煽动互撕谩骂、拉踩引战等信息，严禁在禁言期通过更改名称、头像和简介等方式变相发布信息。

10.分级监测管理明星账号。各平台要全面摸清明星账号注册底数，根据粉丝数量、传播能力、信用评价等情况，对明星账号进行分级管理，相关情况向网信部门定期报备。建立各平台重点关注目录清单，对达到一定粉丝数量和传播能力的明星账号，进行实时监测和动态预警。对于热点敏感社会话题中，发布带偏节奏、混淆视听、煽动极端情绪信息内容的明星账号，及时采取处置措施，并向有关主管部门报告。

11.严格违法失德明星艺人账号管理。对违法失德明星艺人采取联合惩戒措施，全网统一标准，严防违法失德明星艺人转移阵地、“曲线复出”。

12.严格明星经纪公司和粉丝团账号管理。加强明星经纪公司(工作室)账号认证审核，同一经纪公司(工作室)原则上在同一平台只能注册一个账号。粉丝团(后援会)账号须经明星经纪公司(工作室)授权或认证，由其承担日常维护和

监督管理的责任。未经授权的个人或组织一律不得注册明星粉丝团账号。

13.严厉处置娱乐营销账号及其所属 MCN 机构。对于有组织或批量发布涉明星不实爆料、恶意抹黑、拉踩引战等信息，或进行刷量控评、恶意营销炒作的娱乐类公众账号，从严处置处罚。根据情节严重程度，对违法违规账号所属 MCN 机构及旗下其他账号连责处置，采取禁言、限制搜索、限制商业推广收益等措施。

四、强化舆情监测处置

14.建立监测处置机制。网站平台要建立娱乐明星网上信息舆情监测机制，及时发现处置爆料明星情感纠纷、爆料明星涉嫌违法犯罪行为、涉及粉丝群体性冲突等热点舆情苗头，并向主管部门报告。涉及网络暴力、寻衅滋事等问题线索，及时通报公安部门。

15.强化舆情引导。针对涉娱乐明星网上热点舆情，网站平台要对相关账号主体身份进行复核，对账号主体真实身份无法验证的，进行明确标注。同时，根据舆情事件性质，督促明星通过官方账号发声，引导粉丝理性看待，防止舆情持续发酵。

各地要高度重视加强娱乐明星网上信息规范工作，结合“饭圈”乱象整治，制定细化实施方案，指导督促属地网站平台抓好各项措施落实，务求取得工作实效。

中央网信办秘书局

2021 年 10 月 26 日

关于发布互联网信息服务算法备案信息的公告

（国家互联网信息办公室 2022 年 8 月 12 日）

根据《互联网信息服务算法推荐管理规定》，现公开发布境内互联网信息服务算法名称及备案编号，相关信息可通过互联网信息服务算法备案系统(https://beian.cac.gov.cn)进行查询。任何单位或个人如有疑议，请发送邮件至 pingguchu@cac.gov.cn，提出疑议应以事实为依据，并提供相关证据材料。后续将在本页面持续更新算法备案清单。

附件：境内互联网信息服务算法备案清单(2022 年 8 月)

关于实施个人信息保护认证的公告

国家市场监督管理总局 国家互联网信息办公室公告 2022 年第 37 号

为贯彻落实《中华人民共和国个人信息保护法》有关规定，规范个人信息处理活动，促进个人信息合理利用，根据《中华人民共和国认证认可条例》，国家市场监督管理总局、国家互联网信息办公室决定实施个人信息保护认证，鼓励个人信息处理者通过认证方式提升个人信息保护能力。从事个人信息保护认证工作的认证机构应当经批准后开展有关认证活动，并按照《个人信息保护认证实施规则》(见附件)实施认证。

特此公告。

附件：个人信息保护认证实施规则

国家市场监督管理总局 国家互联网信息办公室

2022 年 11 月 4 日

个人信息保护认证实施规则

1 适用范围

本规则依据《中华人民共和国认证认可条例》制定，规定了对个人信息处理者开展个人信息收集、存储、使用、加工、传输、提供、公开、删除以及跨境等处理活动进行认证的基本原则和要求。

2 认证依据

个人信息处理者应当符合 GB/T 35273《信息安全技术 个人信息安全规范》的要求。

对于开展跨境处理活动的个人信息处理者，还应当符合 TC260-PG-20222A《个人信息跨境处理活动安全认证规范》的要求。

上述标准、规范原则上应当执行最新版本。

3 认证模式

个人信息保护认证的认证模式为：

技术验证 + 现场审核 + 获证后监督

4 认证实施程序

4.1 认证委托

认证机构应当明确认证委托资料要求，包括但不限于认证委托人基本材料、认证委托书、相关证明文档等。

认证委托人应当按认证机构要求提交认证委托资料，认证机构在对认证委托资料审查后及时反馈是否受理。

认证机构应当根据认证委托资料确定认证方案，包括个人信息类型和数量、涉及的个人信息处理活动范围、技术验证机构信息等，并通知认证委托人。

4.2 技术验证

技术验证机构应当按照认证方案实施技术验证，并向认证机构和认证委托人出具技术验证报告。

4.3 现场审核

认证机构实施现场审核，并向认证委托人出具现场审核报告。

4.4 认证结果评价和批准

认证机构根据认证委托资料、技术验证报告、现场审核报告和其他相关资料信息进行综合评价，作出认证决定。对符合认证要求的，颁发认证证书；对暂不符合认证要求的，可要求认证委托人限期整改，整改后仍不符合的，以书面形式通知认证委托人终止认证。

如发现认证委托人、个人信息处理者存在欺骗、隐瞒信息、故意违反认证要求等严重影响认证实施的行为时，认证不予通过。

4.5 获证后监督

4.5.1 监督的频次

认证机构应当在认证有效期内，对获得认证的个人信息处理者进行持续监督，并合理确定监督频次。

4.5.2 监督的内容

认证机构应当采取适当的方式实施获证后监督，确保获得认证的个人信息处理者持续符合认证要求。

4.5.3 获证后监督结果的评价

认证机构对获证后监督结论和其他相关资料信息进行综合评价，评价通过的，可继续保持认证证书；不通过的，认证机构应当根据相应情形作出暂停直至撤销认证证书的处理。

4.6 认证时限

认证机构应当对认证各环节的时限作出明确规定，并确保相关工作按时限要求完成。认证委托人应当对认证活动予以积极配合。

5 认证证书和认证标志

5.1 认证证书

5.1.1 认证证书的保持

认证证书有效期为 3 年。在有效期内，通过认证机构的获证后监督，保持认证证书的有效性。

证书到期需延续使用的，认证委托人应当在有效期届满前 6 个月内提出认证委托。认证机构应当采用获证后监督的方式，对符合认证要求的委托换发新证书。

5.1.2 认证证书的变更

认证证书有效期内，若获得认证的个人信息处理者名称、注册地址，或认证要求、认证范围等发生变化时，认证委托人应当向认证机构提出变更委托。认证机构根据变更的内容，对变更委托资料进行评价，确定是否可以批准变更。如需进行技术验证和/或现场审核，还应当在批准变更前进行技术验证和/或现场审核。

5.1.3 认证证书的注销、暂停和撤销

当获得认证的个人信息处理者不再符合认证要求时，认证机构应当及时对认证证书予以暂停直至撤销。认证委托人在认证证书有效期内可申请认证证书暂停、注销。

5.1.4 认证证书的公布

认证机构应当采用适当方式对外公布认证证书颁发、变更、暂停、注销和撤销等相关信息。

5.2 认证标志

不含跨境处理活动的个人信息保护认证标志如下：

包含跨境处理活动的个人信息保护认证标志如下：

“ABCD”代表认证机构识别信息。

5.3 认证证书和认证标志的使用

在认证证书有效期内，获得认证的个人信息处理者应当按照有关规定在广告等宣传中正确使用认证证书和认证标志，不得对公众产生误导。

6 认证实施细则

认证机构应当依据本规则有关要求，细化认证实施程序，制定科学、合理、可操作的认证实施细则，并对外公布实施。

7 认证责任

认证机构应当对现场审核结论、认证结论负责。

技术验证机构应当对技术验证结论负责。

认证委托人应当对认证委托资料的真实性、合法性负责。

关于调整网络安全专用产品安全管理有关事项的公告

2023 年第 1 号

为加强网络安全专用产品安全管理，推动安全认证和安全检测结果互认，避免重复认证、检测，依据《中华人民共和国网络安全法》、《关于发布〈网络关键设备和网络安全专用产品目录(第一批)〉的公告》(2017 年第 1 号)、《国家认监委 工业和信息化部 公安部 国家互联网信息办公室关于发布承担网络关键设备和网络安全专用产品安全认证和安全检测任务机构名录(第一批)的公告》(2018 年第 12 号)、《关于统一发布网络关键设备和网络安全专用产品安全认证和安全检测结果的公告》(2022 年第 1 号)，现将调整网络安全专用产品安全管理有关事项公告如下：

一、自 2023 年 7 月 1 日起，列入《网络关键设备和网络安全专用产品目录》的网络安全专用产品应当按照《信息安全技术 网络安全专用产品安全技术要求》等相关国家标准的强制性要求，由具备资格的机构安全认证合格或者安全检测符合要求后，方可销售或者提供。

具备资格的机构是指列入《承担网络关键设备和网络安全专用产品安全认证和安全检测任务机构名录》的机构。

国家互联网信息办公室、工业和信息化部、公安部、国家认证认可监督管理委员会发布更新《网络关键设备和网络安全专用产品目录》、《承担网络关键设备和网络安全专用产品安全认证和安全检测任务机构名录》。

二、自 2023 年 7 月 1 日起，停止颁发《计算机信息系统安全专用产品销售许可证》(简称销售许可证)，产品生产者无需申领。此前已经获得销售许可证的产品在有效期内可继续销售或者提供。

三、自 2023 年 7 月 1 日起，停止执行《关于调整信息安全产品强制性认证实施要求的公告》(原国家质检总局、财政部、国家认证认可监督管理委员会 2009 年第 33 号)和《财政部 工业和信息化部 质检总局 认监委关于信息安全产品实施政府采购的通知》(财库〔2010〕48 号)。

四、国家互联网信息办公室会同工业和信息化部、公安部、国家认证认可监督管理委员会统一公布和更新符合要求的网络关键设备和网络安全专用产品清单，供社会查询和使用。

特此公告。

国家互联网信息办公室

工业和信息化部

公安部

财政部

国家认证认可监督管理委员会

2023 年 4 月 12 日

关于调整《网络关键设备和网络安全专用产品目录》的公告

2023 年第 2 号

依据《中华人民共和国网络安全法》，国家互联网信息办公室会同工业和信息化部、公安部、国家认证认可监督管理委员会等部门更新了《网络关键设备和网络安全专用产品目录》，现予以公布，自印发之日起施行。

2017 年国家互联网信息办公室、工业和信息化部、公安部、国家认证认可监督管理委员会联合发布的《关于发布〈网络关键设备和网络安全专用产品目录(第一批)〉的公告》(2017 年第 1 号)中的网络关键设备和网络安全专用产品目录同步废止。

特此公告。

附件：网络关键设备和网络安全专用产品目录

国家互联网信息办公室

工业和信息化部

公安部

国家认证认可监督管理委员会

2023 年 7 月 3 日

网站平台受理处置涉企网络侵权信息举报工作规范

(中央网信办 2023 年 8 月 10 日)

第一条 为规范境内网站平台受理处置涉企网络侵权信息举报工作，更好维护企业和企业家网络合法权益，根据《民法典》《网络安全法》《网络信息内容生态治理规定》《互联网用户账号信息管理规定》等法律法规和国家有关规定，结合举报工作实际，制定本规范。

第二条 境内网站平台受理处置涉企网络侵权信息举报，适用本规范。

第三条 网站平台应当按照依法依约、分级分类、限时办结的原则，快速准确受理处置涉企网络侵权信息举报。

第四条 网站平台应当重点受理处置以下涉企网络侵权信息举报：

(一)混淆企业主体身份的仿冒性信息；

(二)影响公众公正评判的误导性信息；

(三)不符合企业客观实际的谣言性信息；

(四)贬损丑化企业或企业家的侮辱性信息；

(五)侵害企业家个人隐私的泄密性信息；

(六)其他恶意干扰企业正常经营发展的信息。

第五条 涉企网络侵权信息举报满足以下条件的，网站平台应当予以受理：

(一)提交能够充分陈述举报事项、阐明举报理由的文字举报；

(二)提交企业营业执照、组织机构代码证或企业家身份证明等权利主体资格证明材料；如委托举报的，需提供举报代理人身份证明和授权委托书；

(三)提交举报人姓名、联系方式；

(四)提交请求采取必要措施的具体网络地址或者足以准确定位侵权内容的相关信息；

(五)提交能够证明举报内容侵权的初步证据材料；

(六)提交申明举报真实性、合法性的文字保证。

第六条 网站平台应当及时处理以下仿冒性信息：

(一)在名称、头像、简介等网络账号名称信息中，违规使用与企业相同或相似的名称标识或企业家姓名肖像的；

(二)假借企业或企业家名义发布信息的；

(三)非法镜像企业官方网站、APP，或冒用盗用企业官方网站、APP 备案注册信息或其他显著要素特征的；

(四)其他引发公众混淆企业主体身份的信息。

第七条 网站平台审核仿冒性信息举报，除企业或企业家和举报代理人身份证明外，原则上不再要求其他证据材料。存在依据身份证明难以识别的特殊情形，应当允许企业提供的证据材料包括但不限于：

(一)官方网站备案查询证明；

(二)官方账号持有证明；

(三)有关部门颁发的权属证书；

(四)企业对外公告声明。

第八条 网站平台应当及时处理以下误导性信息：

(一)通过增删信息、改变顺序、调整结构等方式，曲解新闻原意的；

(二)有关部门、新闻媒体等纠正或撤销的过期信息；

(三)删减旧闻旧事发生时间、地点和处理结果，重新发布的；

(四)使用与内容严重不符的夸张标题的；

(五)强调不利事实，回避有利事实，以偏概全的；

(六)断章取义企业家或企业代表过往言论的；

(七)片面解读企业各类对外公告的；

(八)其他引发公众误解误读的信息。

第九条 网站平台审核误导性信息举报，应当允许企业提供的初步证据材料包括但不限于：

(一)源发新闻稿件；

(二)具有新闻采编资质的源发媒体的撤稿函；

(三)有关部门依职权制作的文书或出具的证明；

(四)有关部门公开实施的职权行为信息；

(五)有关部门网上信息公示查询结果；

(六)企业历史档案记录；

(七)企业对外公告全文。

第十条 网站平台应当及时处理以下谣言类信息：

(一)虚构企业家隐私生活的；

(二)编造企业违法犯罪或违规生产经营的；

(三)杜撰企业家或企业员工违法犯罪或道德失范的;

(四)夸大企业或企业家生产经营困难的;

(五)歪曲企业或企业家正常生产经营和投资活动的;

(六)诋毁企业产品服务质量的;

(七)抹黑企业科技创新能力的;

(八)其他与企业客观实际情况不符的信息。

第十一条 网站平台审核谣言性信息举报,应当允许企业提供的初步证据材料包括但不限于:

(一)权威辟谣信息;

(二)有关部门依职权制作的文书或出具的证明;

(三)有关部门公开实施的职权行为信息;

(四)有关部门网上信息公示查询结果;

(五)有关部门颁发的专业资质证明;

(六)具有特定资质的第三方机构出具的证明;

(七)国家标准、行业标准、团体标准;

(八)当事双方订立的合同协议。

第十二条 网站平台应当及时处理以下侮辱性信息:

(一)攻击谩骂企业或企业家的;

(二)涂抹恶搞企业家肖像照片的;

(三)与色情低俗话题恶意关联的;

(四)其他违反公序良俗丑化企业或企业家的信息。

第十三条 网站平台审核侮辱性信息举报,除企业或企业家和举报代理人身份证明外,原则上不再要求其他证据材料。

第十四条 网站平台应当及时处理以下泄密性信息:

(一)违规披露企业家身份证、护照、社保卡、户籍档案等个人身份信息的;

(二)违规披露企业家家庭住址、电话号码、电子邮箱等个人联系信息的;

(三)其他法律法规禁止披露的隐私信息。

第十五条 网站平台审核泄密性信息举报,除企业或企业家和举报代理人身

份证明外，原则上不要求其他证据材料。

第十六条 网站平台应当及时处理以下恶意干扰企业正常生产经营的信息，包括但不限于：

(一)以舆论监督名义进行敲诈勒索的；

(二)恶意集纳企业负面信息的；

(三)以谋取非法利益为目的，发布企业负面报道评论的；

(四)蹭炒涉企热点事件进行恶意营销的；

(五)操纵跨平台账号、关联账号或矩阵账号密集发帖恶意攻击企业或企业家的；

(六)利用自身信息发布便利，以及技术、流量、影响力优势，攻击抹黑竞争对手的；

(七)提供涉企业、企业家虚假不实信息推荐词的。

第十七条 网站平台审核恶意干扰企业正常生产经营信息举报，应当允许企业提供的初步证据材料包括但不限于：

(一)有关部门依职权制作的文书或出具的证明；

(二)有关部门公开实施的职权行为信息；

(三)企业自行收集的其他证明证据。

第十八条 伪造证明证据举报、灌水举报等恶意举报的，网站平台可以拒绝处理。

第十九条 网站平台应当综合考虑涉企网络侵权信息的严重程度、发布频次、舆论影响以及社会危害程度等因素，按照宽严相济、统一标准的原则，分级分类、规范准确处置涉企网络侵权信息举报。

第二十条 针对事实清楚、举证充分的涉企网络侵权信息举报，网站平台应当采取删除或同等效果的处置措施。

第二十一条 针对举报理由充分，但短时间内难以充分举证，且存在以下情形的涉企网络侵权信息举报，网站平台应当采取“限时加私”措施：

(一)被举报信息刊发于企业生产经营发展关键节点的；

(二)被举报信息涉及事项已被有关部门正式立案调查的；

(三)其他不及时处置可能给企业造成较大负面影响的。

第二十二条 针对举报理由充分，但短时间内难以充分举证，且存在以下情形的涉企网络侵权信息举报，网站平台应当设置争议标记或提供澄清回应服务：

(一)企业与被举报主体存在劳资、合同、股权、产权、债务、消费等纠纷的；

(二)企业与被举报主体属于利益相关方或存在竞争关系的；

(三)企业已就被举报信息涉及事项启动起诉、报案等司法行政程序的；

(四)被举报信息涉及事项无法得到有关部门证实的；

(五)其他不及时处置可能引发公众较大误解的。

第二十三条 针对事实清楚、举证充分，且存在以下情形的涉企网络侵权信息举报，网站平台应当依法依约对网络账号采取处置措施：

(一)假冒仿冒的；

(二)持续发布涉企侵权信息，屡罚屡犯的；

(三)恶意首发首转、多发多转涉企侵权信息的；

(四)恶意集纳企业负面信息或发布涉企负面信息，进行敲诈勒索的；

(五)其他情节严重的。

第二十四条 被举报主体对处置措施提出异议的，网站平台应当要求被举报主体提供不侵权的相关证明，并依据双方举证综合判断、视情处置。

第二十五条 网站平台受理涉股东、高管、子公司、业务合作伙伴等企业利益相关方的网络侵权信息举报，研判认为有必要采取相应处置措施的，应当报请省级网信部门审核。对重大事项，报中央网信办相关司局审核。

第二十六条 网站平台及相关从业人员不得滥用举报处置权利，严禁实施有偿删帖、人情删帖等违法违规行为，严禁利用举报处置权利谋取不正当利益。

第二十七条 网站平台应当建立健全规章制度，严格工作流程，规范层级把关，强化内部监督，确保依法依规受理处置涉企网络侵权信息举报。

第二十八条 网站平台应当建立工作台账，如实记录涉企网络侵权信息举报受理处置全过程，留存全量数据不少于六个月，并在网信部门依法查询时，予以提供。相关账号处置情况，定期报送中央网信办相关司局。

第二十九条 各级网信举报部门应当建立健全日常检查和专项检查相结合的

工作制度，依法依规对属地网站平台涉企网络侵权信息举报受理处置工作实施监督管理。

《数据出境安全评估申报指南(第二版)》和《个人信息出境标准合同备案指南(第二版)》

(2024 年 3 月 22 日)

为了指导和帮助数据处理者规范有序申报数据出境安全评估、备案个人信息出境标准合同，国家互联网信息办公室编制了《数据出境安全评估申报指南(第二版)》、《个人信息出境标准合同备案指南(第二版)》，对申报数据出境安全评估、备案个人信息出境标准合同的方式、流程和材料等具体要求作出了说明，对数据处理者需要提交的相关材料进行了优化简化。

数据处理者因业务需要向境外提供重要数据和个人信息，应当遵守《数据出境安全评估办法》、《个人信息出境标准合同办法》和《促进和规范数据跨境流动规定》有关规定。符合数据出境安全评估适用情形的，按照申报指南申报数据出境安全评估；通过与境外接收方订立个人信息出境标准合同的方式向境外提供个人信息的，按照备案指南向所在地省级网信部门备案。

国家互联网信息办公室开通了“数据出境申报系统”，网址：https://sjcj.cac.gov.cn。数据处理者可以通过该系统申报数据出境安全评估、备案个人信息出境标准合同，具体使用说明见系统首页《用户手册》。

附件：1.数据出境安全评估申报指南(第二版)

2.个人信息出境标准合同备案指南(第二版)

第五章 全国信息安全标准化技术委员会

关于印发《全国信息安全标准化技术委员会〈网络安全标准实践指南〉管理办法(暂行)》的通知

信安秘字〔2019〕052 号

各位委员、各工作组、各成员单位：

为规范《网络安全标准实践指南》的制定和管理工作，根据《全国信息安全标准化技术委员会章程》等有关规定，全国信息安全标准化技术委员会秘书处制定了《全国信息安全标准化技术委员会标准〈网络安全标准实践指南〉管

理办法(暂行)》，现印发给你们，请认真遵照执行。

附件：《全国信息安全标准化技术委员会〈网络安全标准实践指南〉管理办法(暂行)》

全国信息安全标准化技术委员会秘书处

2019 年 8 月 21 日

关于发布《网络安全实践指南—CPU 熔断和幽灵漏洞防范指引》的通知

各有关单位：

全国信息安全标准化技术委员会秘书处针对近期披露的 CPU 熔断(Meltdown)和幽灵(Spectre)漏洞，组织相关厂商和安全专家，编制发布了《网络安全实践指南—CPU 熔断和幽灵漏洞防范指引》（以下简称《防范指引》）。

《防范指引》就受熔断和幽灵漏洞威胁的四类典型用户，包括云服务提供商、服务器用户、云租户、个人用户等，给出了详细的防范指引，并提供了部分厂商安全公告和补丁链接。其中，云服务提供商和服务器用户应在参考 CPU 厂商和操作系统厂商建议的基础上，结合自身环境制定升级方案，综合考虑安全风险、性能损耗等因素，采取相关安全措施防范安全风险；云租户和个人用户应及时关注云服务提供商、操作系统厂商、浏览器厂商等提供的安全补丁，及时升级，避免受到漏洞的影响。《防范指引》全文请点击附件下载。

附件：网络安全实践指南—CPU 熔断和幽灵漏洞防范指引.pdf

全国信息安全标准化技术委员会秘书处

2018 年 1 月 16 日

关于发布《网络安全实践指南—应对截获短信验证码实施网络身份假冒攻击的技术指引》的通知

各有关单位：

全国信息安全标准化技术委员会秘书处针对近期出现的利用截获短信验证码实施网络身份假冒攻击的行为，组织相关厂商和安全专家，编制了《网络安全实践指南—应对截获短信验证码实施网络身份假冒攻击的技术指引》（以下简称《技术指引》）。

《技术指引》针对利用截获短信验证码实施网络身份假冒攻击的问题，为

移动应用和网站服务提供商提出了加强身份验证安全性的建议，包括采用短信上行验证、语音通话传输验证码、常用设备绑定、生物特征识别、动态选择身份验证方式等五种具体措施。下载《技术指引》全文请点击附件。

附件：《网络安全实践指南—应对截获短信验证码实施网络身份假冒攻击的技术指引》.pdf

全国信息安全标准化技术委员会秘书处

2018 年 2 月 11 日

关于发布《网络安全实践指南—欧盟 GDPR 关注点》的通知

各有关单位：

2018 年 5 月 25 日，欧盟通用数据保护条例(General Data Protection Regulation，GDPR)正式实施，在全球范围内产生广泛影响。全国信息安全标准化技术委员会秘书处针对欧盟 GDPR 的核心内容，组织相关机构和专家，编制发布了《网络安全实践指南—欧盟 GDPR 关注点》，供各方参考，并建议各方关注 GDPR 对自身的影响。下载全文请点击附件。

附件：TC260-PG-20183A《网络安全实践指南-欧盟 GDPR 关注点》.pdf

全国信息安全标准化技术委员会秘书处

2018 年 5 月 25 日

关于发布《网络安全实践指南—移动互联网应用基本业务功能必要信息规范》的通知

各有关单位：

为落实《网络安全法》第四十一条提出的“网络运营者收集、使用个人信息，应当遵循合法、正当、必要的原则，公开收集、使用规则，明示收集、使用信息的目的、方式和范围，并经被收集者同意”和“网络运营者不得收集与其提供的服务无关的个人信息”等要求，遵循相关国家标准提出的个人信息最少够用原则，针对当前用户数量大、社会关注度高的移动互联网应用中存在的超范围收集、强制授权、过度索权等个人信息收集安全问题，全国信息安全标准化技术委员会秘书处组织相关机构和专家，结合当前移动互联网技术及应用现状，编制发布了《网络安全实践指南—移动互联网应用基本业务功能必要信

息规范(V1.0)》，给出了地图导航、网络约车、即时通讯社交、社区社交、网络支付、新闻资讯、网上购物、短视频、快递配送、餐饮外卖、交通票务、婚恋相亲、求职招聘、金融借贷、房产交易、汽车交易 16 类基本业务功能正常运行所需的个人信息，供各单位参考。下载全文请点击附件。

附件：《网络安全实践指南—移动互联网应用基本业务功能必要信息规范(V1.0)》.pdf

全国信息安全标准化技术委员会秘书处

2019 年 6 月 1 日

关于发布《网络安全标准实践指南—远程办公安全防护》的通知

信安秘字〔2020〕 12 号

各有关单位：

全国信息安全标准化技术委员会秘书处针对远程办公安全问题，组织相关厂商和安全专家，编制了《网络安全标准实践指南—远程办公安全防护》（以下简称《实践指南》）。

《实践指南》给出了远程办公的典型应用场景，分析了远程办公可能面临的办公系统自身安全、数据安全、设备安全和个人信息保护等风险，针对远程办公系统的使用方和用户，分别给出了安全控制措施建议。其中，使用方应在管理和技术两方面开展安全防护，健全远程办公管理制度，加强运维管理，强化安全措施。用户应提高自身安全意识，重点针对设备、数据、环境等方面的安全风险进行防护。《实践指南》全文请点击附件下载。

附件：《网络安全标准实践指南—远程办公安全防护》.pdf

全国信息安全标准化技术委员会秘书处

2020 年 3 月 13 日

关于发布《网络安全标准实践指南—移动互联网应用程序(App)收集使用个人信息自评估指南》的通知

信安秘字〔2020〕40 号

各有关单位：

为落实《网络安全法》相关要求， 围绕中央网信办、工信部、公安部、市场

监管总局联合制定的《App 违法违规收集使用个人信息行为认定方法》，基于 App 专项治理工作组发布的《App 违法违规收集使用个人信息自评估指南》，秘书处组织编制了《网络安全标准实践指南—移动互联网应用程序(App)收集使用个人信息自评估指南》（以下简称《实践指南》）。

《实践指南》归纳总结了 App 收集使用个人信息的六项评估点，供 App 运营者自评估参考使用，小程序、快应用等运营者也可参考其中的适用条款进行自评估。《实践指南》全文请点击附件下载。

附件：网络安全标准实践指南—移动互联网应用程序(App)收集使用个人信息自评估指南.pdf

全国信息安全标准化技术委员会秘书处

2020 年 7 月 22 日

关于发布《网络安全标准实践指南—移动互联网应用程序(App)个人信息保护常见问题及处置指南》的通知

信安秘字〔2020〕58 号

各有关单位：

为帮助 App 运营者了解和重视个人信息保护常见问题，采取相应措施持续提升 App 个人信息保护水平，秘书处组织编制了《移动互联网应用程序(App)个人信息保护常见问题及处置指南》。

《实践指南》针对 App 存在的超范围收集、强制索权、频繁索权等问题，给出了当前 App 个人信息保护十大常见问题和处置指南，适用于 App 运营者防范和处置个人信息保护常见问题，也可为 App 开发者、移动互联网应用分发平台运营者和移动智能终端厂商提供参考。《实践指南》全文请点击附件下载。

附件：《网络安全标准实践指南—移动互联网应用程序(App)个人信息保护常见问题及处置指南》.pdf

全国信息安全标准化技术委员会秘书处

2020 年 9 月 18 日

关于发布《网络安全标准实践指南—移动互联网应用程序(App)系统权限申请使用指南》的通知

信安秘字〔2020〕59 号

各有关单位：

为帮助 App 运营者规范 App 申请使用系统权限行为，防范因系统权限不当使用造成的个人信息安全风险，秘书处组织编制了《网络安全标准实践指南—移动互联网应用程序(App)系统权限申请使用指南》。

《实践指南》给出了 App 申请使用系统权限的基本原则和安全要求，适用于 App 运营者规范系统权限申请和使用行为，也可为 App 开发者、移动互联网应用分发平台运营者和移动智能终端厂商提供参考。《实践指南》全文请点击附件下载。

附件：《网络安全标准实践指南—移动互联网应用程序(App)系统权限申请使用指南》.pdf

全国信息安全标准化技术委员会秘书处

2020 年 9 月 18 日

关于发布《网络安全标准实践指南—移动互联网应用程序(App)使用软件开发工具包(SDK)安全指引》的通知

信安秘字〔2020〕 85 号

各有关单位：

为帮助 App 提供者使用 SDK 时防范 SDK 安全和合规风险，帮助SDK 提供者保障 SDK 安全和用户个人信息，秘书处组织编制了《网络安全标准实践指南—移动互联网应用程序(App)使用软件开发工具包(SDK)安全指引》。

《实践指南》给出了 SDK 常见安全风险，针对当前 App 使用 SDK 过程中存在的 SDK 自身安全漏洞、SDK 恶意行为、SDK 违法违规收集 App 用户的个人信息问题，结合当前移动互联网技术及应用现状，给出了 App 提供者、SDK 提供者针对 SDK 安全问题的实践指引。《实践指南》全文请点击附件下载。

附件：网络安全标准实践指南——移动互联网应用程序(App)使用软件开发工具包(SDK)安全指引.pdf

全国信息安全标准化技术委员会秘书处

2020 年 11 月 27 日

关于发布《网络安全标准实践指南—人工智能伦理安全风险防范指引》的通知

信安秘字〔2021〕2 号

各有关单位：

为防范人工智能伦理安全风险，秘书处组织编制了《网络安全标准实践指南—人工智能伦理安全风险防范指引》，为组织或个人开展人工智能研究开发、设计制造、部署应用等相关活动提供指引。

《实践指南》全文请点击附件下载。

附件：《网络安全标准实践指南—人工智能伦理安全风险防范指引》.pdf

全国信息安全标准化技术委员会秘书处

2021 年 1 月 5 日

关于发布《网络安全标准实践指南——网络数据分类分级指引》的通知

信安秘字〔2021〕173 号

各有关单位：

为贯彻落实《数据安全法》提出的“国家建立数据分类分级保护制度”要求，指导数据处理者开展数据分类分级工作，秘书处组织编制了《网络安全标准实践指南——网络数据分类分级指引》。

本《实践指南》依据法律法规和政策标准相关要求，给出了网络数据分类分级的原则、框架和方法。全文请点击附件下载。

附件：《网络安全标准实践指南——网络数据分类分级指引》.pdf

全国信息安全标准化技术委员会秘书处

2021 年 12 月 31 日

关于发布《网络安全标准实践指南—健康码防伪技术指南》的通知

信安秘字〔2022〕173 号

各有关单位：

为落实疫情防控政策，针对健康码伪造现象给疫情防控工作带来严重安全挑战，秘书处组织编制了《网络安全标准实践指南—健康码防伪技术指南》。

本《实践指南》给出了现场核验场景下健康码防伪的技术指南，指导健康码服务的技术提供方提高防伪能力，提升整体安全水平。全文请点击附件下载。

附件：《网络安全标准实践指南—健康码防伪技术指南》.pdf

全国信息安全标准化技术委员会秘书处

2022 年 9 月 28 日

关于发布《网络安全标准实践指南—个人信息跨境处理活动安全认证规范 V2.0》的通知

信安秘字〔2022〕216 号

各有关单位：

为支撑个人信息保护认证实施，指导个人信息处理者规范开展个人信息跨境处理活动，秘书处组织编制了《网络安全标准实践指南—个人信息跨境处理活动安全认证规范 V2.0》。

本《实践指南》规定了跨境处理个人信息应遵循的基本原则、个人信息处理者和境外接收方在个人信息跨境处理活动的个人信息保护、个人信息主体权益保障等方面内容。全文请点击附件下载。

附件：《网络安全标准实践指南—个人信息跨境处理活动安全认证规范 V2.0》.pdf

全国信息安全标准化技术委员会秘书处

2022 年 12 月 16 日

关于发布《网络安全标准实践指南—网络数据安全风险评估实施指引》的通知

信安秘字〔2023〕70 号

各有关单位：

为贯彻落实《数据安全法》关于数据安全风险评估的要求，秘书处在组织编制国家标准的同时，编制了《网络安全标准实践指南——网络数据安全风险评估实施指引》，用于指导开展网络数据安全风险评估工作。

本《实践指南》给出了网络数据安全风险评估的评估思路、工作流程和评估内容，依据本《实践指南》开展评估工作形成的优秀经验也可为国家标准制定提供参考。

全文请点击附件下载。

附件：《网络安全标准实践指南—网络数据安全风险评估实施指引》.pdf

全国信息安全标准化技术委员会秘书处

2023 年 5 月 26 日

关于发布《网络安全标准实践指南——IPv6 地址分配和编码规则 接口标识符》的通知

信安秘字〔2023〕82 号

各有关单位：

为指导相关方通过 IPv6 网络动态分配 IPv6 地址接口标识符，秘书处在组织编制国家标准的同时，编制了《网络安全标准实践指南——IPv6 地址分配和编码规则 接口标识符》。

本《实践指南》提出了 IPv6 地址接口标识符的编码方法和实施要求，为互联网接入服务商等相关实体通过 IPv6 网络动态分配 IPv6 地址接口标识符的活动提供指导和依据。

附件：《网络安全标准实践指南——IPv6 地址分配和编码规则 接口标识符》

全国信息安全标准化技术委员会秘书处

2023 年 6 月 21 日

关于发布《网络安全标准实践指南——生成式人工智能服务内容标识方法》的通知

信安秘字〔2023〕124 号

各有关单位：

为贯彻落实《生成式人工智能服务管理暂行办法》中对生成内容进行标识的要求，指导生成式人工智能服务提供者等有关单位做好内容标识工作，秘书处组织编制了《网络安全标准实践指南——生成式人工智能服务内容标识方法》。

本《实践指南》围绕文本、图片、音频、视频四类生成内容给出了内容标识方法，可用于指导生成式人工智能服务提供者提高安全管理水平。

附件：《网络安全标准实践指南—生成式人工智能服务内容标识方法》.pdf

全国信息安全标准化技术委员会秘书处

2023 年 8 月 25 日

关于发布《网络安全标准实践指南——网络安全产品互联互通 告警信息格式》的通知

信安秘字〔2023〕172 号

各有关单位：

为促进网络安全产品互联互通告警信息有效互通和整合，秘书处组织编制了《网络安全标准实践指南——网络安全产品互联互通 告警信息格式》。

本《实践指南》给出了网络安全产品互联互通时告警信息的描述格式，可用于指导网络安全产品互联互通功能的设计、开发、应用和测试。

附件：网络安全标准实践指南——网络安全产品互联互通 告警信息格式.pdf

全国信息安全标准化技术委员会秘书处

2023 年 11 月 28 日

关于发布《网络安全标准实践指南——车外画面局部轮廓化处理效果验证》的通知

网安秘字〔2024〕7 号

各有关单位：

为指导汽车数据处理者对车外画面进行人脸、车牌局部轮廓化处理效果的自行验证，秘书处组织编制了《网络安全标准实践指南——车外画面局部轮廓化处理效果验证》。

本《实践指南》给出了验证车外画面进行人脸、车牌局部轮廓化处理效果的流程、方法及验证指标，可为汽车数据处理者及有关机构验证车外画面局部轮廓化处理效果提供参考。

附件：《网络安全标准实践指南--车外画面局部轮廓化处理效果验证》.pdf

全国网络安全标准化技术委员会秘书处

2024 年 3 月 6 日

关于发布《网络安全标准实践指南——网络安全产品互联互通 资产信息格

式》的通知

网安秘字〔2024〕21 号

各有关单位：

为促进网络安全产品互联互通资产信息有效互通和整合，秘书处组织编制了《网络安全标准实践指南——网络安全产品互联互通 资产信息格式》。

本《实践指南》给出了网络安全产品互联互通时资产信息的描述格式，可用于指导网络安全产品互联互通功能的设计、开发、应用和测试。

附件：网络安全标准实践指南——网络安全产品互联互通 资产信息格式.pdf

全国网络安全标准化技术委员会秘书处

2024 年 3 月 13 日

关于发布《网络安全标准实践指南——大型互联网平台网络安全评估指南》的通知

网安秘字〔2024〕82 号

各有关单位：

为指导大型互联网平台评估发现和防范影响或者可能影响社会稳定、公共利益的网络安全风险，提升平台安全水平，秘书处组织编制了《网络安全标准实践指南——大型互联网平台网络安全评估指南》。

本《实践指南》提出了对大型互联网平台开展网络安全评估的内容和方法，可用于指导大型互联网平台开展网络安全评估活动。

附件：《网络安全标准实践指南 大型互联网平台网络安全评估指南》.pdf

全国网络安全标准化技术委员会秘书处

2024 年 6 月 25 日

《汽车采集数据处理安全指南》

《汽车采集数据处理安全指南》(TC260-001)

《生成式人工智能服务安全基本要求》

TC260-003《生成式人工智能服务安全基本要求》.pdf

第六章　国家标准化管理委员会

信息安全技术 信息安全风险处理实施指南

信息安全技术 信息安全风险处理实施指南- GB/T 33132-2016

信息安全技术 移动智能终端个人信息保护技术要求

《信息安全技术 移动智能终端个人信息保护技术要求》-GB/T 34978-2017

信息安全技术　网络安全等级保护基本要求

《信息安全技术　网络安全等级保护基本要求》-GB/T 22239-2019

信息安全技术　网络安全等级保护实施指南

《信息安全技术　网络安全等级保护实施指南》-GB/T 25058-2019

信息安全技术　网络安全等级保护安全设计技术要求

《信息安全技术　网络安全等级保护安全设计技术要求》-GB/T 25070-2019

信息安全技术　网络安全等级保护测评要求

《信息安全技术　网络安全等级保护测评要求》-GB/T 28448-2019

信息安全技术 数据交易服务安全要求

《信息安全技术　数据交易服务安全要求》- GB/T 37932-2019

信息安全技术 个人信息去标识化指南

《信息安全技术　个人信息去标识化指南》- GB/T 37964-2019

信息安全技术 大数据安全管理指南

《信息安全技术　大数据安全管理指南》- GB/T 37973-2019

信息安全技术 数据安全能力成熟度模型

《信息安全技术　数据安全能力成熟度模型》- GB/T 37988-2019

信息安全技术　网络安全等级保护定级指南

《信息安全技术　网络安全等级保护定级指南》-GB/T 22240-2020

信息安全技术 网络安全漏洞分类分级指南

《信息安全技术 网络安全漏洞分类分级指南》-GB/T 30279-2020

信息安全技术 个人信息安全规范

《信息安全技术 个人信息安全规范》-GB/T 35273-2020

信息安全技术 网络安全事件应急演练指南

信息安全技术 网络安全事件应急演练指南- GB/T 38645-2020

信息安全技术 网络产品和服务安全通用要求

《信息安全技术 网络产品和服务安全通用要求》-GB/T 39276-2020

信息安全技术 个人信息安全影响评估指南

《信息安全技术 个人信息安全影响评估指南》-GB/T 39335-2020

信息安全技术 政务信息共享 数据安全技术要求

《信息安全技术 政务信息共享 数据安全技术要求》- GB/T 39477-2020

信息安全技术 健康医疗数据安全指南

《信息安全技术 健康医疗数据安全指南》- GB/T 39725-2020

信息安全技术 数据备份与恢复产品技术要求与测试评价方法

《信息安全技术 数据备份与恢复产品技术要求与测试评价方法》- GB/T 29765-2021

信息安全技术 网站数据恢复产品技术要求与测试评价方法

《信息安全技术 网站数据恢复产品技术要求与测试评价方法》- GB/T 29766-2021

信息安全技术 生物特征识别信息保护基本要求

《信息安全技术 生物特征识别信息保护基本要求》-GB/T 40660-2021

信息安全技术 信息安全风险评估方法

《信息安全技术 信息安全风险评估方法》-GB/T 20984-2022

信息安全技术 移动互联网应用程序(App)收集个人信息基本要求

《信息安全技术 移动互联网应用程序(App)收集个人信息基本要求》-GB/T 41391-2022

信息安全技术 网络数据处理安全要求

《信息安全技术 网络数据处理安全要求》-GB/T 41479-2022

信息安全技术 关键信息基础设施安全保护要求

《信息安全技术 关键信息基础设施安全保护要求》-GB/T 39204-2022

信息安全技术 网络安全专用产品安全技术要求

《信息安全技术 网络安全专用产品安全技术要求》- GB 42250-2022

信息安全技术 个人信息处理中告知和同意的实施指南

《信息安全技术 个人信息处理中告知和同意的实施指南》- GB/T 42574—2023

金融信息系统网络安全风险评估规范

《金融信息系统网络安全风险评估规范》-GB/T 42926-2023

14 项网络安全国家标准获批发布

(全国信安标委，2022 年 10 月 19 日)

根据 2022 年 10 月 14 日国家市场监督管理总局、国家标准化管理委员会发布的中华人民共和国国家标准公告(2022 年第 13 号)，全国信息安全标准化技术委员会归口的 14 项国家标准正式发布。具体清单如下：

序号	标准编号	标准名称	代替标准号	实施日期
1	GB/T 25068.3-2022	信息技术 安全技术 网络安全 第 3 部分：面向网络接入场景的威胁、设计技术和控制	GB/T 25068.4-2010	2023-05-01
2	GB/T 25068.4-2022	信息技术 安全技术 网络安全 第 4 部分：使用安全网关的网间通信安全保护	GB/T 25068.3-2010	2023-05-01

3	GB/T 41773-2022	信息安全技术 步态识别数据安全要求	-	2023-05-01
4	GB/T 41806-2022	信息安全技术 基因识别数据安全要求	-	2023-05-01
5	GB/T 41807-2022	信息安全技术 声纹识别数据安全要求	-	2023-05-01
6	GB/T 41817-2022	信息安全技术 个人信息安全工程指南	-	2023-05-01
7	GB/T 41819-2022	信息安全技术 人脸识别数据安全要求	-	2023-05-01
8	GB/T 41871-2022	信息安全技术 汽车数据处理安全要求	-	2023-05-01
9	GB/T 42012-2022	信息安全技术 即时通信服务数据安全要求	-	2023-05-01
10	GB/T 42013-2022	信息安全技术 快递物流服务数据安全要求	-	2023-05-01
11	GB/T 42014-2022	信息安全技术 网上购物服务数据安全要求	-	2023-05-01
12	GB/T 42015-2022	信息安全技术 网络支付服务数据安全要求	-	2023-05-01
13	GB/T 42016-2022	信息安全技术 网络音视频服务数据安全要求	-	2023-05-01
14	GB/T 42017-2022	信息安全技术 网络预约汽车服务数据安全要求	-	2023-05-01
注：	上述国家标准全文可登录“国家标准全文公开系统”查询。 查询网址：https://openstd.samr.gov.cn/			

12 项网络安全国家标准获批发布

（全国信安标委，2023 年 3 月 23 日）

根据 2023 年 3 月 17 日国家市场监督管理总局、国家标准化管理委员会发布的中华人民共和国国家标准公告(2023 年第 1 号)，全国信息安全标准化技术委员会归口的 12 项网络安全国家标准正式发布。具体清单如下：

序号	标准编号	标准名称	代替标准号	实施日期
1	GB/T 15843.3-2023	信息技术 安全技术 实体鉴别 第3部分：采用数字签名技术的机制	GB/T 15843.3-2016	2023-10-01
2	GB/T 17902.1-2023	信息技术 安全技术 带附录的数字签名 第1部分：概述	GB/T 17902.1-1999	2023-10-01
3	GB/T 20274.1-2023	信息安全技术 信息系统安全保障评估框架 第1部分：简介和一般模型	GB/T 20274.1-2006	2023-10-01
4	GB/T 21053-2023	信息安全技术 公钥基础设施 PKI系统安全技术要求	GB/T 21053-2007	2023-10-01
5	GB/T 21054-2023	信息安全技术 公钥基础设施 PKI系统安全测评方法	GB/T 21054-2007	2023-10-01
6	GB/T 32922-2023	信息安全技术 IPSec VPN安全接入基本要求与实施指南	GB/T 32922-2016	2023-10-01
7	GB/T 33134-2023	信息安全技术 公共域名服务系统安全要求	_	2023-10-01
8	GB/T 42446-2023	信息安全技术 网络安全从业人员能力基本要求	_	2023-10-01
9	GB/T 42447-2023	信息安全技术 电信领域数据安全指南	_	2023-10-01
10	GB/T 42453-2023	信息安全技术 网络安全态势感知通用技术要求	_	2023-10-01
11	GB/T 42460-2023	信息安全技术 个人信息去标识化效果评估指南	_	2023-10-01
12	GB/T 42461-2023	信息安全技术 网络安全服务成本度量指南	_	2023-10-01
注：	上述国家标准全文可登录“国家标准全文公开系统”查询。 查询网址：https://openstd.samr.gov.cn/			

19 项网络安全国家标准获批发布

（全国信安标委，2023 年 5 月 31 日）

根据 2023 年 5 月 23 日国家市场监督管理总局、国家标准化管理委员会发布的中华人民共和国国家标准公告(2023 年第 2 号)，全国信息安全标准化技术委员会归口的 19 项网络安全国家标准正式发布。具体清单如下：

序号	标准编号	标准名称	代替标准号	实施日期
1	GB/T 20945-2023	信息安全技术 网络安全审计产品技术规范	GB/T 20945-2013	2023-12-01
2	GB/T 20986-2023	信息安全技术 网络安全事件分类分级指南	GB/Z 20986-2007	2023-12-01
3	GB/T 24364-2023	信息安全技术 信息安全风险管理实施指南	GB/Z 24364-2009	2023-12-01
4	GB/T 28451-2023	信息安全技术 网络入侵防御产品技术规范	GB/T 28451-2012	2023-12-01
5	GB/T 30282-2023	信息安全技术 反垃圾邮件产品技术规范	GB/T 30282-2013	2023-12-01
6	GB/T 31167-2023	信息安全技术 云计算服务安全指南	GB/T 31167-2014	2023-12-01
7	GB/T 31168-2023	信息安全技术 云计算服务安全能力要求	GB/T 31168-2014	2023-12-01
8	GB/T 31496-2023	信息技术 安全技术 信息安全管理体系 指南	GB/T 31496-2015	2023-12-01
9	GB/T 32920-2023	信息安全技术 行业间和组织间通信的信息安全管理	GB/T 32920-2016	2023-12-01
10	GB/T 35282-2023	信息安全技术 电子政务移动办公系统安全技术规范	GB/T 35282-2017	2023-12-01
11	GB/T 42564-2023	信息安全技术 边缘计算安全技术要求	_	2023-12-01
12	GB/T 42570-2023	信息安全技术 区块链技术安全框架	_	2023-12-01
13	GB/T 42571-2023	信息安全技术 区块链信息	_	2023-12-01

		服务安全规范		
14	GB/T 42572-2023	信息安全技术 可信执行环境服务规范	_	2023-12-01
15	GB/T 42573-2023	信息安全技术 网络身份服务安全技术要求	_	2023-12-01
16	GB/T 42574-2023	信息安全技术 个人信息处理中告知和同意的实施指南	_	2023-12-01
17	GB/T 42582-2023	信息安全技术 移动互联网应用程序(App)个人信息安全测评规范	_	2023-12-01
18	GB/T 42583-2023	信息安全技术 政务网络安全监测平台技术规范	_	2023-12-01
19	GB/T 42589-2023	信息安全技术 电子凭据服务安全规范	_	2023-12-01
注：	上述国家标准全文可登录“国家标准全文公开系统”查询。 查询网址：https://openstd.samr.gov.cn/			

3 项网络安全国家标准获批发布

（全国信安标委 ，2023 年 12 月 1 日）

根据 2023 年 11 月 27 日国家市场监督管理总局、国家标准化管理委员会发布的中华人民共和国国家标准公告(2023 年第 13 号)，全国信息安全标准化技术委员会归口的 3 项国家标准正式发布。具体清单如下：

序号	标准编号	标准名称	实施日期
1	GB/T 43269-2023	信息安全技术 网络安全应急能力评估准则	2024-06-01
2	GB/T 43435-2023	信息安全技术 移动互联网应用程序(App)软件开发工具包(SDK)安全要求	2024-06-01
3	GB/T 43445-2023	信息安全技术 移动智能终端预置应用软件基本安全要求	2024-06-01
注：	上述国家标准全文可登录“国家标准全文公开系统”查询。 查询网址：https://openstd.samr.gov.cn/		

5 项网络安全国家标准获批发布

（全国信安标委 ，2024 年 1 月 5 日）

根据 2023 年 12 月 28 日国家市场监督管理总局、国家标准化管理委员会发布的中华人民共和国国家标准公告(2023 年第 20 号)，全国信息安全标准化技术委员会归口的 5 项网络安全国家标准正式发布。具体清单如下：

序号	标准编号	标准名称	代替标准号	实施日期
1	GB/T 29246-2023	信息安全技术 信息安全管理体系概述和词汇	GB/T 29246-2017	2024-07-01
2	GB/T 35290-2023	信息安全技术 射频识别(RFID)系统安全技术规范	GB/T 35290-2017	2024-07-01
3	GB/T 43557-2023	信息安全技术 网络安全信息报送指南		2024-07-01
4	GB/T 43577.1-2023	信息安全技术 电子发现 第 1 部分：概述和概念		2024-07-01
5	GB/T 43578-2023	信息安全技术 通用密码服务接口规范		2024-07-01
注：	上述国家标准全文可登录“国家标准全文公开系统”查询。 查询网址：https://openstd.samr.gov.cn/			

5 项网络安全国家标准获批发布

（全国网安标委 ，2024-03-21）

根据 2024 年 3 月 15 日国家市场监督管理总局、国家标准化管理委员会发布的中华人民共和国国家标准公告(2024 年第 1 号)，全国网络安全标准化技术委员会归口的 5 项网络安全国家标准正式发布。具体清单如下：

序号	标准编号	标准名称	代替标准号	实施日期
1	GB/T 43697-2024	数据安全技术 数据分类分级规则		2024-10-01
2	GB/T 17903.1-2024	信息技术 安全技术 抗抵赖 第 1 部分：概述	GB/T 17903.1-2008	2024-10-01
3	GB/T 17903.3-2024	信息技术 安全技术 抗抵赖	GB/T 17903.3-2008	2024-10-01

		第 3 部分：采用非对称技术的机制		
4	GB/T 15843.4-2024	信息技术 安全技术 实体鉴别 第 4 部分：采用密码校验函数的机制	GB/T 15843.4-2008	2024-10-01
5	GB/T 31497-2024	信息技术 安全技术 信息安全管理 监视、测量、分析和评价	GB/T 31497-2015	2024-10-01
注：	上述国家标准全文可登录“国家标准全文公开系统”查询。 查询网址：https://openstd.samr.gov.cn/			

第七章 全国金融标准化技术委员会

证券期货业数据分类分级指引

《证券期货业数据分类分级指引》- JRT 0158-2018

金融数据安全 数据安全分级指南

《金融数据安全 数据安全分级指南》-JR/T 0197-2020

金融数据安全 数据生命周期安全规范

《金融数据安全 数据生命周期安全规范》- JR/T 0223—2021

第八章 证监会

证券期货业网络和信息安全管理办法

中国证券监督管理委员会令第 218 号

《证券期货业网络和信息安全管理办法》已经 2023 年 1 月 17 日中国证券监督管理委员会 2023 年第 1 次委务会议审议通过，现予公布，自 2023 年 5 月 1 日起施行。

中国证券监督管理委员会主席：易会满

2023 年 2 月 27 日

证券期货业网络和信息安全管理办法

(2023 年 1 月 17 日中国证券监督管理委员会第 1 次委务会议审议通过)

第一章 总 则

第一条 为了保障证券期货业网络和信息安全，保护投资者合法权益，促进证券期货业稳定健康发展，根据《中华人民共和国证券法》（以下简称《证券法》）、《中华人民共和国期货和衍生品法》（以下简称《期货和衍生品法》）、《中华人民共和国证券投资基金法》（以下简称《证券投资基金法》）、《中华人民共和国网络安全法》（以下简称《网络安全法》）、《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》（以下简称《个人信息保护法》）、《关键信息基础设施安全保护条例》等法律法规，制定本办法。

第二条 核心机构和经营机构在中华人民共和国境内建设、运营、维护、使用网络及信息系统，信息技术系统服务机构为证券期货业务活动提供产品或者服务的网络和信息安全保障，以及证券期货业网络和信息安全的监督管理，适用本办法。

第三条 核心机构和经营机构应当遵循保障安全、促进发展的原则，建立健全网络和信息安全防护体系，提升安全保障水平，确保与信息化工作同步推进，促进本机构相关工作稳妥健康发展。

信息技术系统服务机构应当遵循技术安全、服务合规的原则，为证券期货业务活动提供产品或者服务，与核心机构、经营机构共同保障行业网络和信息安全，促进行业信息化发展。

第四条 核心机构和经营机构应当依法履行网络和信息安全保护义务，对本机构网络和信息安全负责，相关责任不因其他机构提供产品或者服务进行转移或者减轻。

信息技术系统服务机构应当勤勉尽责，对提供产品或者服务的安全性、合规性承担责任。

第五条 中国证监会依法履行以下监督管理职责：

（一）组织制定并推动落实证券期货业网络和信息安全发展规划、监管规则和行业标准；

（二）负责证券期货业网络和信息安全的监督管理，按规定做好证券期货业涉及的关键信息基础设施安全保护工作；

（三）负责证券期货业网络和信息安全重大技术路线、重大科技项目管理；

（四）组织开展证券期货业投资者个人信息保护工作；

(五)负责证券期货业网络安全应急演练、应急处置、事件报告与调查处理;

(六)指导证券期货业网络和信息安全促进与发展;

(七)支持、协助国家有关部门组织实施网络和信息安全相关法律、行政法规;

(八)法律法规规定的其他网络和信息安全监管职责。

第六条 中国证监会建立集中管理、分级负责的证券期货业网络和信息安全监督管理体制。中国证监会科技监管部门对证券期货业网络和信息安全实施监督管理。中国证监会履行监管职责的其他部门配合开展相关工作。

中国证监会派出机构对本辖区经营机构和信息技术系统服务机构网络和信息安全实施日常监管。

第七条 中国证券业协会、中国期货业协会、中国证券投资基金业协会等行业协会(以下统称行业协会)依法制定行业网络和信息安全自律规则,对经营机构网络和信息安全实施自律管理。

第八条 核心机构依法制定保障市场相关主体与本机构信息系统安全互联的技术规则,对与本机构信息系统和网络通信设施相关联主体加强指导,督促其强化网络和信息安全管理,保障相关信息系统和网络通信设施的安全平稳运行。

第二章 网络和信息安全运行

第九条 核心机构和经营机构应当具有完善的信息技术治理架构,健全网络和信息安全管理制度体系,建立内部决策、管理、执行和监督机制,确保网络和信息安全管理能力与业务活动规模、复杂程度相匹配。

信息技术系统服务机构应当建立网络和信息安全管理制度,配备相应的安全、合规管理人员,建立与提供产品或者服务相适应的网络和信息安全管理机制。

第十条 核心机构和经营机构应当明确主要负责人为本机构网络和信息安全工作的第一责任人,分管网络和信息安全工作的领导班子成员或者高级管理人员为直接责任人。

核心机构和经营机构应当建立网络和信息安全工作协调和决策机制,保障

第一责任人和直接责任人履行职责。

第十一条 核心机构和经营机构应当指定或者设立网络和信息安全工作牵头部门或者机构，负责管理重要信息系统和相关基础设施、制定网络安全应急预案、组织应急演练等工作。

第十二条 核心机构和经营机构应当保障人员和资金投入与业务活动规模、复杂程度相适应，确保网络和信息安全人员具备与履行职责相匹配的专业知识和职业技能。

第十三条 核心机构和经营机构应当确保信息系统和相关基础设施具备合理的架构，足够的性能、容量、可靠性、扩展性和安全性，并保证相关安全技术措施与信息化工作同步规划、同步建设、同步使用。

第十四条 核心机构和经营机构应当落实网络安全等级保护制度，依法履行网络安全等级保护义务，按照国家和证券期货业网络安全等级保护相关要求，开展网络和信息系统定级备案、等级测评和安全建设等工作。

核心机构和经营机构应当按照相关要求，将网络安全等级保护工作开展情况报送中国证监会及其派出机构。

第十五条 核心机构和经营机构新建上线、运行变更、下线移除重要信息系统的，应当充分评估技术和业务风险，制定风险防控措施、应急处置和回退方案，并对相关结果进行复核验证；可能对证券期货市场安全平稳运行产生较大影响的，应当提前向中国证监会及其派出机构报告。

核心机构和经营机构不得在交易时段对重要信息系统进行变更，重要信息系统存在故障、缺陷，经评估须进行紧急修复的情形除外。

第十六条 核心机构和经营机构在重要信息系统上线、变更前应当制定全面的测试方案，持续完善测试用例和测试数据，并保障测试的有效执行。

除必须使用敏感数据的情形外，核心机构和经营机构应当对测试环境涉及的敏感数据进行脱敏，对未脱敏数据须采取与生产环境同等的安全控制措施。

核心机构交易、行情、开户、结算、通信等重要信息系统上线或者进行重大升级变更时，应当组织市场相关主体进行联网测试。

第十七条 核心机构和经营机构暂停或者终止借助网络向投资者提供服务前，应当履行告知义务，合理选取公告、定向通知等方式告知投资者相关业务

影响情况、替代方式及应对措施。

第十八条 核心机构和经营机构应当建立健全网络和信息安全监测预警机制，设定监测指标，持续监测信息系统和相关基础设施的运行状况，及时处置异常情形，对监测机制执行效果进行定期评估并持续优化。

核心机构和经营机构应当全面、准确记录并妥善保存生产运营过程中的业务日志和系统日志，确保满足故障分析、内部控制、调查取证等工作的需要。重要信息系统业务日志应当保存五年以上，系统日志应当保存六个月以上。

第十九条 核心机构和经营机构应当构建网络和信息安全防护体系，综合采取网络隔离、用户认证、访问控制、策略管理、数据加密、网站防篡改、病毒木马防范、非法入侵检测和网络安全态势感知等安全保障措施，提升网络和信息安全防护能力，及时识别、阻断相关网络攻击，保护重要信息系统和相关基础设施，防范信息泄露与损毁。

第二十条 核心机构和经营机构应当建立本地、同城和异地数据备份设施，重要信息系统应当每天至少备份数据一次，每季度至少对数据备份进行一次有效性验证。

核心机构和经营机构应当建立重要信息系统的故障备份设施和灾难备份设施，根据信息系统的重要程度和业务影响情况，确定恢复目标，保证业务连续运行。灾难备份设施应当通过同城或者异地灾难备份中心的形式体现。核心机构和经营机构采取双活或者多活架构部署重要信息系统的，在确保业务连续运行的前提下，任一数据中心可视为其他数据中心的灾难备份设施。

第二十一条 核心机构和经营机构应当每年至少开展一次重要信息系统压力测试；发现市场较大波动，重要信息系统的性能容量可能无法保障安全平稳运行的，应当及时对相关信息系统开展压力测试。

核心机构和经营机构应当依照有关行业标准，根据系统技术特点和承载业务类型，制定压力测试方案，设定测试场景，从系统性能、网络负载、灾备建设等方面设置测试指标，有序组织测试工作，测试完成后形成压力测试报告存档备查，并保存五年以上。

核心机构和经营机构重要信息系统的性能容量应当在历史峰值的两倍以上。核心机构交易时段相关网络近一年使用峰值应当在当前带宽的百分之五十

以下，经营机构交易时段相关网络近一年使用峰值应当在当前带宽的百分之八十以下。

第二十二条 核心机构和经营机构应当建立健全供应商管理机制，明确信息技术产品和服务准入标准，审慎采购并持续评估相关产品和服务的质量，及时改进风险管理措施，健全应急处置机制，确保重要信息系统运行安全可控。

核心机构和经营机构应当与供应商签订合同及保密协议，明确约定各方保障网络和信息安全的权利和义务；在使用供应商提供产品或者服务时引发网络安全事件的，相关供应商有义务配合中国证监会及其派出机构查明网络安全事件原因，认定网络安全事件责任。

第二十三条 供应商为核心机构和经营机构提供重要信息系统相关产品或者服务的，应当依法作为信息技术系统服务机构向中国证监会备案。

核心机构和经营机构应当督促相关信息技术系统服务机构依法履行备案义务。

第二十四条 任何机构和个人不得违规开展证券期货业信息系统认证、检测、风险评估等活动，不得违规发布证券期货业信息安全漏洞、计算机病毒、网络攻击、网络侵入等信息。

第二十五条 核心机构和经营机构应当建立信息发布审核机制，加强对本机构和本机构运营平台发布信息的管理，发现违反法律法规和有关监管规定的，应当立即停止发布传输，采取必要的处置措施，防止信息扩散，积极消除负面影响，并及时向中国证监会及其派出机构报告。

第二十六条 核心机构应当对交易、行情、开户、结算、风控、通信等重要信息系统具有自主开发能力，掌握执行程序和源代码并安全可靠存放。

经营机构应当根据自身发展需要，加强自主研发能力建设，持续提升自主可控能力。

核心机构和经营机构应当按照国家及中国证监会有关要求，开展信息技术应用创新以及商用密码应用相关工作。

第二十七条 中国证监会可以委托相关机构建设证券期货业备份数据中心，开展行业数据的集中备份和管理工作，并采取有效安全防护手段，防范数据损毁泄露风险，持续提升证券期货业重大灾难应对能力。

鼓励证券期货业关键信息基础设施运营者及时向证券期货业备份数据中心备份数据。其他核心机构和经营机构可以结合经营需要，自主选择证券期货业备份数据中心，开展数据级灾难备份工作。

第二十八条 核心机构和经营机构应当按照知识产权相关法律法规，制定知识产权保护策略和制度，不侵犯他人的知识产权，并采取有效措施保护本机构自主知识产权。

第三章 投资者个人信息保护

第二十九条 核心机构和经营机构应当遵循合法、正当、必要和诚信原则，处理投资者个人信息，规范投资者个人信息处理行为，履行投资者个人信息保护义务，不得损害投资者合法权益。

第三十条 核心机构和经营机构处理投资者个人信息，应当建立健全投资者个人信息保护体系，明确相关岗位及职责要求，建立健全投资者个人信息处理、安全防护、应急处置、审计监督等管理机制，加强投资者个人信息保护。

第三十一条 核心机构和经营机构应当按照法律法规的规定及合同的约定处理投资者个人信息，明确告知投资者处理个人信息的目的、方式、范围和隐私保护政策，不得超范围收集和使用投资者个人信息，不得收集提供服务非必要的投资者个人信息。合同约定事项应当基于从事证券期货业务活动的必要限度。

核心机构和经营机构不得以投资者不同意处理其个人信息或者撤回同意为由，拒绝向投资者提供服务，为投资者提供服务所必需、履行法定职责或者法定义务等情形除外。

第三十二条 核心机构和经营机构处理投资者个人信息时，应当确保个人信息在收集、存储、使用、加工、传输、提供、公开、删除等处理过程中的合规、安全，防止个人信息的泄露、篡改、丢失。

第三十三条 核心机构和经营机构应当依法依规向第三方机构提供投资者个人信息，明确告知投资者个人信息处理目的、处理方式、个人信息种类、保存期限、保护措施以及相关方的权利和义务等，并取得投资者个人单独同意，履行法定职责或者法定义务的情形除外。

第三十四条 核心机构和经营机构在本机构网络安全防护边界以外处理投资

者个人信息的，应当采取数据脱敏、数据加密等措施，防范化解投资者个人信息在处理过程中的泄露风险。

核心机构和经营机构通过短信、邮件等非自主运营渠道发送投资者敏感个人信息的，应当将投资者账号信息、身份证号码等敏感个人信息进行脱敏处理。

第三十五条 核心机构和经营机构利用生物特征进行客户身份认证的，应当对其必要性、安全性进行风险评估，不得将人脸、步态、指纹、虹膜、声纹等生物特征作为唯一的客户身份认证方式，强制客户同意收集其个人生物特征信息。

第四章 网络和信息安全应急处置

第三十六条 核心机构、经营机构和信息技术系统服务机构发现网络和信息安全产品或者服务存在安全缺陷、安全漏洞等风险隐患的，应当及时核实并加固整改；可能对证券期货业网络和信息安全平稳运行产生较大影响的，应当向中国证监会及其派出机构报告。

第三十七条 核心机构和经营机构应当根据业务影响分析情况，建立健全网络安全应急预案，明确应急目标、应急组织和处置流程，应急场景应当覆盖网络安全事件、自然灾害和公共卫生事件、本机构网络和信息安全相关重大人事变动、主要信息技术系统服务机构退出等情形。

第三十八条 核心机构应当组织与本机构信息系统和网络通信设施相关联主体开展网络安全应急演练，每年至少开展一次，并于演练后 15 个工作日内将相关情况报告中国证监会。

核心机构和经营机构应当定期开展网络安全应急演练，并形成应急演练报告存档备查。

第三十九条 核心机构和经营机构应当建立应急处置机制，及时处置网络安全事件，尽快恢复信息系统正常运行，保护事件现场和相关证据，向中国证监会及其派出机构进行应急报告，不得瞒报、谎报、迟报、漏报。

信息技术系统服务机构应当协助开展信息系统故障排查、修复等工作，并及时告知使用同类产品或者服务的核心机构和经营机构，配合开展风险排查和整改工作。

第四十条 核心机构和经营机构应当配合中国证监会及其派出机构对网络安全事件进行调查处理，及时组织内部调查，完成问题整改，认定追究事件责任，并按照有关规定报告中国证监会及其派出机构。

第四十一条 核心机构和经营机构发生网络安全事件，对投资者造成影响的，应当及时通过官方网站、客户交易终端、电话或者邮件等有效渠道通知相关方可以采取的替代方式或者应急措施，提示相关方防范和应对可能出现的风险。

第五章 关键信息基础设施安全保护

第四十二条 证券期货业关键信息基础设施运营者应当按照法律法规及中国证监会有关规定，强化安全管理措施、技术防护及其他必要手段，保障经费投入，确保关键信息基础设施安全稳定运行，维护数据的完整性、保密性和可用性。

第四十三条 证券期货业关键信息基础设施运营者应当将关键信息基础设施安全保护情况纳入网络和信息安全工作第一责任人、直接责任人和相关人员的责任考核机制。

第四十四条 证券期货业关键信息基础设施运营者应当指定专门机构或者部门负责关键信息基础设施安全保护管理工作，为每个关键信息基础设施指定网络和信息安全管理责任人，依法认定网络安全关键岗位，配备充足的网络和信息安全人员，并对专门安全管理机构负责人和关键岗位人员进行安全背景审查。

第四十五条 证券期货业关键信息基础设施运营者新建承载关键业务的重要网络设施、信息系统等，投入使用前应当按照关键信息基础设施安全保护相关要求开展安全检测和风险评估，检测评估通过后上线运行。

证券期货业关键信息基础设施运营者对关键信息基础设施实施运行变更或者下线移除，可能对证券期货市场安全平稳运行产生较大影响的，应当在遵守本办法第十五条的前提下，组织开展专家评审；未通过评审的，原则上不得实施运行变更、下线移除等操作。

证券期货业关键信息基础设施停止运营或者发生较大变化，可能影响认定结果的，相关运营者应当及时将相关情况报告中国证监会及其派出机构。

第四十六条 证券期货业关键信息基础设施运营者应当每年至少进行一次网络和信息安全检测和风险评估，对发现的安全问题及时整改，网络和信息安全检测和风险评估的内容包括但不限于：关键信息基础设施的运行情况、面临的主要威胁、风险管理情况、应急处置情况等。

第四十七条 证券期货业关键信息基础设施运营者采购网络产品或者服务的，应当按照国家网络安全审查制度要求开展风险预判工作；采购网络产品或者服务与关键信息基础设施密切相关，投入使用后可能影响国家安全的，应当及时申报网络安全审查。

第四十八条 证券期货业关键信息基础设施运营者应当对关键信息基础设施的安全运行进行持续监测，定期开展压力测试，发现系统性能和网络容量不足的，应当及时采取系统升级、扩容等处置措施，确保系统性能容量在历史峰值的三倍以上，交易时段相关网络带宽应当在近一年使用峰值的两倍以上。

第四十九条 证券期货业关键信息基础设施运营者应当在符

合本办法第二十条规定的基础上，建设同城和异地灾难备份中心，实现数据同步保存。

第六章 网络和信息安全促进与发展

第五十条 鼓励核心机构、经营机构和信息技术系统服务机构在依法合规的前提下，积极开展网络和信息安全技术应用工作，运用新技术提升网络和信息安全保障水平。

第五十一条 核心机构和经营机构组织开展行业信息基础设施建设的，应当在保障本机构网络和信息安全的前提下，为行业统筹提供服务，提升信息技术资源利用和服务水平。

第五十二条 核心机构和经营机构参加资本市场金融科技创新机制的，应当遵守有关规定，在依法合规、风险可控的前提下，有序开展金融科技创新与应用，借助新型信息技术手段，提升本机构证券期货业务活动的运行质量和效能。

信息技术系统服务机构参加资本市场金融科技创新机制的，应当遵守有关规定，持续优化技术服务水平，增强安全合规管理能力。

第五十三条 核心机构可以申请开展证券期货业网络和信息安全相关认证、

检测、测试和风险评估等监管支撑工作。相关核心机构应当保障充足的资源投入，完善内部管理制度和工作流程，保证工作专业性、独立性和公信力。

中国证监会定期对核心机构前款工作情况开展评估，评估通过的，可以将其作为证券期货业网络和信息安全监管支撑单位，相关工作情况可以作为中国证监会及其派出机构实施监督管理的参考依据。

第五十四条 核心机构和经营机构应当加强网络和信息安全人才队伍建设，建立与网络和信息安全工作特点相适应的人才培养机制，确保人才资质、经验、专业素质及职业道德符合岗位要求。

行业协会应当制定网络和信息安全培训计划，定期组织培训交流，提高证券期货从业人员网络和信息安全意识和专业素养。

第五十五条 核心机构和经营机构应当加强本机构网络和信息安全宣传与教育，每年至少开展一次全员网络和信息安全教育活动，提升员工网络和信息安全意识。

经营机构应当定期组织开展面向投资者的网络和信息安全宣传教育活动，结合网上证券期货业务活动的特点，揭示网络和信息安全风险，增强投资者风险防范能力。

第五十六条 行业协会应当鼓励、引导网络和信息安全技术创新与应用，增强自主可控能力，组织开展科技奖励，促进行业科技进步。

行业协会应当引导信息技术系统服务机构规范参与行业网络和信息安全和信息化工作，提升服务的安全合规水平，促进市场有序竞争。

第七章 监督管理与法律责任

第五十七条 核心机构、经营机构和信息技术系统服务机构应当向中国证监会及其派出机构报送或者提供证券期货业网络和信息安全管理相关信息和数据，确保有关信息和数据的真实、准确、完整。

第五十八条 中国证监会负责建立健全行业网络和信息安全态势感知工作机制，并就相关安全缺陷、安全漏洞等风险隐患开展行业通报预警。核心机构、经营机构和信息技术系统服务机构应当及时排查并采取风险防范措施。

第五十九条 核心机构和经营机构应当于每年 4 月 30 日前，完成对上一年网络和信息安全工作的专项评估，编制网络和信息安全管理年报，报送中国证

监会及其派出机构，年报内容包括但不限于网络和信息安全治理情况、人员情况、投入情况、风险情况、处置情况和下一年度工作计划等。

核心机构和经营机构报送网络和信息安全管理年报时，可以与中国证监会要求的信息科技管理专项报告等其他年度信息科技类报告合并报送，关键信息基础设施安全保护年度计划除外。

证券期货业关键信息基础设施运营者应当将关键信息基础设施网络和信息安全检测和风险评估情况纳入网络和信息安全管理年报。

第六十条 中国证监会及其派出机构可以委托国家、行业有关专业机构采用漏洞扫描、风险评估等方式，协助对核心机构、经营机构和信息技术系统服务机构开展监督、检查。

第六十一条 中国证监会可以根据国家有关要求或者行业工作需要，组织开展证券期货业重要时期网络和信息安全保障。中国证监会派出机构负责督促本辖区经营机构和信息技术系统服务机构落实相关工作要求。

证券期货业重要时期网络和信息安全保障期间，核心机构和经营机构应当遵循安全优先的原则，加强安全生产值守，严格落实信息报送要求。

第六十二条 核心机构违反本办法规定的，中国证监会可以对其采取责令改正、监管谈话等监管措施；对有关高级管理人员给予警告、记过、记大过、降级、撤职、开除等行政处分，并责令核心机构对其他责任人给予纪律处分。

经营机构和信息技术系统服务机构违反本办法规定的，中国证监会及其派出机构可以对其采取责令改正、监管谈话、出具警示函、责令公开说明、责令定期报告、责令增加内部合规检查次数等监管措施；对直接责任人和其他责任人员采取责令改正、监管谈话、出具警示函等监管措施；情节严重的，对相关机构及责任人员单处或者并处警告、十万元以下罚款，涉及金融安全且有危害后果的，并处二十万元以下罚款。

第六十三条 经营机构违反本办法规定，反映机构治理混乱、内控失效或者不符合持续性经营规则的，中国证监会及其派出机构可以依照《证券法》《期货和衍生品法》《证券投资基金法》相关规定，采取责令暂停借助网络开展部分业务或者全部业务、责令更换董事、监事、高级管理人员或者限制其权利等监管措施。

信息技术系统服务机构违反本办法规定，未履行备案义务的，中国证监会及其派出机构可以依照《证券法》《期货和衍生品法》相关规定予以处罚。

第六十四条 核心机构、经营机构和信息技术系统服务机构违反本办法第九条、第十条、第十八条、第十九条、第二十条、第三十七条、第三十九条规定，未履行网络和信息安全保护义务，或者应急管理存在重大过失的，中国证监会及其派出机构可以依照《网络安全法》相关规定予以处罚。

证券期货业关键信息基础设施运营者未履行本办法第九条、第十条、第十八条、第十九条、第二十条、第二十二条、第三十七条、第三十八条、第四十二条、第四十四条、第四十六条、第四十九条、第五十五条规定的网络安全保护义务的，中国证监会及其派出机构可以依照《网络安全法》《关键信息基础设施安全保护条例》相关规定予以处罚。

第六十五条 核心机构和经营机构违反本办法第十七条、第三十六条规定，擅自暂停或者终止借助网络向投资者提供服务，对其产品、服务存在安全缺陷、漏洞等风险未立即采取补救措施，或者未按照规定及时报告的，中国证监会及其派出机构可以依照《网络安全法》相关规定予以处罚。

第六十六条 违反本办法第二十四条规定，开展证券期货业信息系统认证、检测、风险评估等活动，或者向社会发布证券期货业信息安全漏洞、计算机病毒、网络攻击、网络侵入等信息的，中国证监会及其派出机构可以依照《网络安全法》相关规定予以处罚。

第六十七条 核心机构和经营机构违反本办法第二十五条规定，对法律、行政法规禁止发布或者传输的信息未停止传输、采取消除等处置措施、保存有关记录的，中国证监会及其派出机构可以依照《网络安全法》相关规定予以处罚。

第六十八条 核心机构和经营机构违反本办法第三十一条第一款、第三十二条、第三十三条规定，违规处理个人信息，或者处理个人信息未履行个人信息保护义务的，中国证监会及其派出机构可以依照《网络安全法》《个人信息保护法》相关规定予以处罚。

第六十九条 核心机构、经营机构和信息技术系统服务机构拒绝、阻碍中国证监会及其派出机构行使监督检查、调查职权的，中国证监会及其派出机构可

以依法予以处罚。

第七十条 核心机构和经营机构参加资本市场金融科技创新机制或者信息技术应用创新机制，相关项目发生网络安全事件，相关机构处置得当，积极消除不良影响的，中国证监会及其派出机构可以予以从轻或者减轻处罚，未对证券期货市场产生不良影响的，可以免于处罚。

第八章 附 则

第七十一条 本办法中下列用语的含义：

(一)核心机构，包括证券期货交易场所、证券登记结算机构等承担证券期货市场公共职能、承担证券期货业信息技术公共基础设施运营的证券期货市场核心机构及其承担上述相关职能的下属机构。

(二)经营机构，是指证券公司、期货公司和基金管理公司等证券期货经营机构。

(三)信息技术系统服务机构，是指为证券期货业务活动提供重要信息系统的开发、测试、集成、测评、运维及日常安全管理等产品或者服务的机构。

(四)双活或者多活架构，是指在同城或者异地的两个或者多个数据中心同时对外提供服务，当其中一个或者多个数据中心发生灾难性事故时，可以将原先由其承载的服务请求划拨至其他正常运作的数据中心，保障业务连续运行。

(五)重要信息系统，是指承载证券期货业关键业务活动，如出现系统服务异常、数据泄露等情形，将对证券期货市场和投资者产生重大影响的信息系统。

(六)可能对证券期货市场安全平稳运行产生较大影响，是指依据网络安全事件调查处理有关办法，可能引发较大或者以上级别网络安全事件的情形。

(七)“以上”含本数，“以下”不含本数。

第七十二条 本办法规定的核心机构、经营机构和信息技术系统服务机构相关报告事项，是指依照监管职责，核心机构应当向中国证监会报告；除中国证监会另有要求的，经营机构和信息技术系统服务机构原则上应当向属地中国证监会派出机构报告。

第七十三条 国家对存储、处理涉及国家秘密信息的网络和信息安全管理另有规定的，从其规定。

第七十四条 境内开展证券公司客户交易结算资金第三方存管业务、期货保证金存管业务的商业银行，证券投资咨询机构，基金托管机构和从事公开募集基金的销售、销售支付、份额登记、估值、投资顾问、评价等基金服务业务的机构，从事证券期货业务活动的经营机构子公司，借助自身运维管理的信息系统从事证券投资活动且存续产品涉及基金份额持有人账户合计一千人以上的私募证券投资基金管理人，应当根据相关信息系统网络和信息安全管理的特点，参照适用本办法。

核心机构和经营机构设立信息科技专业子公司，为母公司提供信息科技服务的，信息科技专业子公司应当按照本办法落实网络和信息安全相关要求。

第七十五条 本办法自 2023 年 5 月 1 日起施行。2012 年 11 月 1 日公布的《证券期货业信息安全保障管理办法》(证监会令第 82 号)同时废止。

证券期货业网络安全事件报告与调查处理办法

证监会公告〔2021〕12 号

现公布《证券期货业网络安全事件报告与调查处理办法》，自公布之日起施行。

证监会

2021 年 6 月 4 日

证券期货业网络安全事件报告与调查处理办法

第一章 总 则

第一条 为了规范证券期货业网络安全事件的报告和调查处理，减少网络安全事件的发生，根据《证券法》、《证券投资基金法》、《证券公司监督管理条例》、《期货交易管理条例》、《证券期货业信息安全保障管理办法》、《证券基金经营机构信息技术管理办法》等法律、行政法规和规章，制定本办法。

第二条 证券期货业网络安全事件是指由于人为原因、软硬件缺陷或故障、自然灾害等，对证券期货业网络和信息系统或者数据造成影响，发生网络和信息系统服务能力异常或者数据损毁、泄露，对国家金融安全、社会秩序、投资者合法权益造成损害的事件。

第三条 证券期货业网络安全保障责任主体发生网络安全事件后，应当按本办法规定进行报告和调查处理。

前款所称责任主体，包括证券期货交易场所、证券登记结算机构等承担证券期货市场公共职能、承担证券期货业信息技术公共基础设施运营的证券期货市场核心机构及其承担上述相关职能的下属机构(以下简称核心机构)，证券公司、期货公司、基金管理公司及其提供证券期货相关服务的下属机构、证券期货服务机构等证券期货经营机构(以下简称经营机构)。

第四条 核心机构、经营机构发生网络安全事件后，应当及时、准确、完整报告，不得迟报、漏报、谎报或者瞒报。

第五条 网络安全事件调查处理应当坚持实事求是、尊重科学、客观公正、及时稳妥的原则。

第二章 系统分类与事件分级

第六条 根据网络和信息系统发生网络安全事件后，直接对国家金融安全、社会秩序、投资者合法权益造成的损害程度，网络和信息系统由高到低分为五类系统、四类系统、三类系统、二类系统和一类系统。各类系统的分类原则及典型系统见《网络和信息系统分类表》和《典型系统》(见附件 1)。

未列在《典型系统》中的网络和信息系统，如发生网络安全事件，在应急处置和调查处理时，应依据《网络和信息系统分类表》进行分类。

第七条 核心机构和经营机构结算系统等中后台业务系统发生网络安全事件后，按照受其影响的前台业务系统的类别和受影响程度，或按照其导致的投资者数据和结算金额差错、直接资金损失等，进行网络安全事件的分类分级。

第八条 根据服务能力异常程度，网络和信息系统服务能力异常分为严重异常、中度异常、轻度异常。具体如下：

(一)严重异常，是指网络和信息系统发生故障，服务能力异常80%以上的情形；

(二)中度异常，是指网络和信息系统发生故障，服务能力异常 30%以上且未构成严重异常的情形；

(三)轻度异常，是指网络和信息系统发生故障，服务能力异常但未构成严重异常、中度异常的情形。

不同业务类型网络和信息系统服务能力异常的计算方法见《服务能力异常计算方法》(见附件 2)。

第九条 综合考虑网络和信息系统类别、服务能力异常程度、事件持续时间、数据损毁程度、结算金额差错数额、直接资金损失以及对国家金融安全、社会秩序、投资者合法权益造成损害的程度，网络安全事件分为特别重大事件、重大事件、较大事件、一般事件。

同时符合两类或两类以上分级情形的，应当以孰高原则分级。

第十条 特别重大事件是指对国家金融安全、社会秩序、投资者合法权益造成特别严重损害的网络安全事件。符合下列情形之一的为特别重大事件：

(一)五类系统服务能力严重异常且故障持续时间 30 分钟以上的；

(二)四类系统服务能力严重异常且故障持续时间 2 小时以上的；

(三)100 万人以上的投资者数据发生损毁、泄露或篡改的；

(四)结算金额差错 100 亿元人民币以上，或者给投资者造成直接资金损失 10 亿元人民币以上的；

(五)其他对国家金融安全、社会秩序、投资者合法权益造成特别严重损害的事件。

第十一条 重大事件是指对国家金融安全、社会秩序、投资者合法权益造成严重损害的网络安全事件。符合下列情形之一，且未达到特别重大事件的为重大事件：

(一)五类系统服务能力严重异常且故障持续时间 15 分钟以上，或者服务能力中度异常且故障持续时间 30 分钟以上的；

(二)四类系统服务能力严重异常且故障持续时间 30 分钟以上，或者服务能力中度异常且故障持续时间 2 小时以上的；

(三)三类系统服务能力严重异常且故障持续时间 2 小时以上的；

(四)10 万人以上的投资者数据发生损毁、泄露、篡改的；

(五)结算金额差错 10 亿元人民币以上，或者给投资者造成直接资金损失 1 亿元人民币以上的；

(六)其他对国家金融安全、社会秩序、投资者合法权益造成严重损害的事件。

第十二条 较大事件是指对国家金融安全、社会秩序、投资者合法权益造成较大损害的网络安全事件。符合下列情形之一，且未达到重大事件的为较大事

件：

(一)五类系统服务能力严重异常且故障持续时间 5 分钟以上，或者服务能力中度异常且故障持续时间 15 分钟以上，或者服务能力轻度异常且故障持续时间 30 分钟以上的；

(二)四类系统服务能力严重异常且故障持续时间 10 分钟以上，或者服务能力中度异常且故障持续时间 30 分钟以上，或者服务能力轻度异常且故障持续时间 2 小时以上的；

(三)三类系统服务能力严重异常且故障持续时间 30 分钟以上，或者服务能力中度异常且故障持续时间 2 小时以上的；

(四)二类系统服务能力严重异常且故障持续时间 2 小时以上的；

(五)1 万人以上的投资者数据发生损毁、泄露、篡改的；

(六)因审核不严或系统被非法入侵，相关信息平台发送违法和不良信息造成恶劣的社会影响或者直接向 10 万人以上发送相关信息的；

(七)结算金额差错达到 1 亿元人民币以上，或者给投资者造成直接资金损失达到 1000 万元人民币以上的；

(八)其他对国家金融安全、社会秩序、投资者合法权益造成较大损害的事件。

第十三条 一般事件是指对国家金融安全、社会秩序、投资者合法权益造成损害的网络安全事件。符合下列情形之一，且未达到较大事件的为一般事件：

(一)一类、二类、三类、四类、五类系统出现服务能力严重异常、中度异常、轻度异常等情形的；

(二)1 万人以下的投资者数据发生损毁、泄露、篡改的；

(三)因审核不严或网络和信息系统被非法入侵，相关信息平台发送违法和不良信息造成社会影响的；

(四)结算金额差错 1 亿元人民币以下且未能及时完成差错处理，或者给投资者造成直接资金损失 1000 万元人民币以下；

(五)其他对国家金融安全、社会秩序、投资者合法权益造成损害的事件。

第十四条 存在明显过错、疏忽且社会影响较大的网络安全事件，中国证监会及其派出机构可酌情提高事件定级。

第十五条 符合以下情形之一的，未发现明显过错、疏忽且不良影响较小的，可酌情从轻分级，或不认定为网络安全事件：

(一)自主研发的系统上线一年内发生网络安全事件的；

(二)基金销售、会计核算、注册登记系统发生网络安全事件后及时修复，未对行业及投资者权益造成影响的；

(三)具有冗余架构的系统或基础设施，在合理的切换时间内完成切换不影响系统提供正常服务的；

(四)经营机构面向 50 名以下投资者提供服务或者网络安全事件发生前 20 个交易日日均成交笔数不足 50 笔的系统、分支机构系统发生故障，处置得当，受影响客户得到妥善安抚的；

(五)其他未发现明显过错、疏忽且不良影响较小的网络安全事件。

第十六条 本章所称的“以上”包括本数，所称的“以下”、“不足”不包括本数。

第三章 事件报告

第十七条 核心机构和经营机构应当建立网络安全风险监测预警体系，发现风险隐患应当尽快加以核实，采取必要的防范措施，如有重大情况应当及时进行预警报告。

预警报告应当包括：事件基本情况(包括预警发生的时间、地点、经过等)，可能造成的影响范围和后果，已采取的防范措施及相关建议、需要有关部门和单位协调处置的有关事宜。

第十八条 核心机构和经营机构应当建立网络安全应急处置机制，及时处置网络安全事件，尽快恢复系统的正常运行，保护事件现场和相关证据，并按照下列要求进行应急报告：

(一)网络和信息系统发生故障，可能构成网络安全事件的，应当立即报告。可能构成特别重大、重大网络安全事件的，应当每隔 30 分钟至少上报一次事件处置情况，直至系统恢复正常运行；对较大和一般网络安全事件，第一次上报后，无须持续上报事件处置情况；如有重要情况应当立即报告。

(二)发生涉及犯罪的网络安全事件，应当立即报告。在事件解决前，如有重要情况应当立即报告。

第十九条 核心机构和经营机构进行应急报告时应当先通过电话或事件报送平台进行报告，随后书面报送《网络安全事件情况报告书》（见附件 3），内容包括：事件初步定级、事件发生时间、地点、简要经过、影响范围初步评估、影响程度初步评估、影响人数初步评估、经济损失初步评估、后果初步判断、原因初步判断、事件性质初步判断、已采取的措施及效果、需要有关部门和单位协助处置的有关事宜、报告单位、签发人和报告时间、联系人与联系方式、与本事件有关的其他内容。

第二十条 核心机构和经营机构应当在网络安全事件应急处置结束、系统恢复正常运行后 7 个工作日内，组织内部调查，准确查清事件经过、原因和损失，查明事件性质，认定并追究事件责任，提出整改措施，并进行事件总结报告。事件总结报告内容应当包括：

（一）事件基本情况，包括事件发生时间、地点、经过、影响范围、影响程度、损失情况等；

（二）应急处置情况，包括事件报告的情况、采取的措施及效果；

（三）事件调查情况，包括事件原因、事件级别、责任认定和结论；

（四）事件处理情况，包括事件暴露出的问题及采取的整改措施，责任追究情况。

暂时无法确定事件原因、责任和结论的，应当提交事件的初步分析报告，同时尽快查找原因，认定并追究事件责任，采取整改措施，并在事件应急处置结束、系统恢复正常运行后 30 个工作日内提交事件补充报告。

第二十一条 核心机构和经营机构接到中国证监会及其派出机构关于系统漏洞、安全隐患、产品缺陷的网络安全通报书后，应当立即核实情况，采取必要的处置措施，并根据要求进行事件总结报告。

事件总结报告内容应当包括：事件基本情况，可能或者已经造成的影响范围和后果，已采取的防范措施及相关建议。

第二十二条 核心机构或者经营机构应当按照下列规定向有关机构进行报告：

（一）核心机构应当向中国证监会进行预警报告、应急报告和事件总结报告。

(二)核心机构发生网络安全事件影响到其他机构的，应当及时向有关机构进行应急通报。

(三)经营机构应当向住所地中国证监会派出机构进行预警报告、应急报告和事件总结报告，经营机构分支机构应当向所在地中国证监会派出机构进行预警报告、应急报告和事件总结报告。事件总结报告应当抄送中国证券业协会、中国期货业协会或者中国证券投资基金业协会。

(四)经营机构发生网络安全事件影响到证券期货交易业务时，应当向相关证券期货交易场所进行应急报告和事件总结报告；影响到证券登记结算业务时，应当向中国证券登记结算有限责任公司进行应急报告和事件总结报告；影响到转融通业务时，应当向中国证券金融股份有限公司进行应急报告和事件总结报告；影响到其他机构的，应当及时向有关机构进行应急通报。

(五)核心机构或者经营机构发生涉及犯罪的网络安全事件，核心机构和经营机构应当向公安机关进行应急报告。

第四章 调查处理

第二十三条 中国证监会及其派出机构依据本办法规定对核心机构、经营机构的网络安全事件进行调查处理。网络安全事件相关的核心机构、经营机构应当配合中国证监会及其派出机构和发生事件的机构对事件进行调查和处理。

第二十四条 调查人员有权向网络安全事件相关的核心机构、经营机构和个人了解事件有关的情况，可采取听取报告、询问当事人、调阅文件资料、调阅系统日志、实地核查等工作方式。

在事件调查期间，发生网络安全事件的机构相关人员应当积极配合接受询问，如实介绍情况，提供证据和所需的文件、资料，并签名确认。

第二十五条 调查人员应当诚信公正，认真履职，遵守工作纪律，做好笔录，严格保守事件调查的秘密，以及在调查过程中了解到的商业秘密、技术秘密。未经允许，不得泄露或者擅自发布事件调查中知悉的有关信息。

第二十六条 中国证监会或者其派出机构督促发生网络安全事件的机构落实整改措施，并对整改措施落实情况进行监督。

发生网络安全事件的机构应当认真吸取事件教训，尽快落实整改措施，消除风险隐患。

第二十七条 中国证监会视情况将网络安全事件有关情况向全行业通报，中国证监会派出机构视情况向本辖区证券期货经营机构通报。

第二十八条 核心机构、经营机构在研发、测试、上线及运维等系统管理过程中未能严格执行相关法律法规和行业相关技术管理规定、技术规则、技术指引和技术标准，造成网络安全事件的，中国证监会及其派出机构依照有关法律、行政法规和规章，对事件相关机构及其负责人员采取监督管理措施或者实施行政处罚。事件相关机构应当对相关责任人员进行内部责任追究。

第二十九条 妨碍网络安全事件报告与调查处理的，中国证监会或者其派出机构依照有关法律、行政法规和规章，对相关机构和负责人员采取监督管理措施或者实施行政处罚。

第五章 附 则

第三十条 本办法自公布之日起施行。《证券期货业信息安全事件报告与调查处理办法》（证监会公告〔2012〕46 号）同时废止。

附件：1. 网络和信息系统分类表、典型系统

2. 服务能力异常计算方法

3. 网络安全事件情况报告书

《上市公司公告电子化规范》等 9 项金融行业标准

证监会公告〔2023〕56 号

现公布金融行业推荐性标准《上市公司公告电子化规范 第 1 部分：公告分类》（JR/T 0021.1—2023）、《上市公司公告电子化规范 第 2 部分：首次披露》（JR/T 0021.2—2023）、《上市公司公告电子化规范 第 3 部分：交易类临时公告》（JR/T 0021.3—2023）、《上市公司公告电子化规范 第 4 部分：公司治理类临时公告》（JR/T 0021.4—2023）、《上市公司公告电子化规范 第 5 部分：权益变动类临时公告》（JR/T 0021.5—2023）、《上市公司公告电子化规范 第 6 部分：融资类临时公告》（JR/T 0021.6—2023）、《上市公司公告电子化规范 第 7 部分：其他临时公告》（JR/T 0021.7—2023）、《上市公司公告电子化规范 第 8 部分：定期报告》（JR/T 0021.8—2023）、《证券期货业信息安全运营管理指南》（JR/T 0295—2023），自公布之日起施行。

附件 9：证券期货业信息安全运营管理指南.pdf

中国证监会

2023 年 10 月 23 日

第九章 公安部

公安机关互联网安全监督检查规定

中华人民共和国公安部令第 151 号

《公安机关互联网安全监督检查规定》已经 2018 年 9 月 5 日公安部部长办公会议通过，现予发布，自 2018 年 11 月 1 日起施行。

部长 赵克志

2018 年 9 月 15 日

公安机关互联网安全监督检查规定

第一章 总 则

第一条 为规范公安机关互联网安全监督检查工作，预防网络违法犯罪，维护网络安全，保护公民、法人和其他组织合法权益，根据《中华人民共和国人民警察法》《中华人民共和国网络安全法》等有关法律、行政法规，制定本规定。

第二条 本规定适用于公安机关依法对互联网服务提供者和联网使用单位履行法律、行政法规规定的网络安全义务情况进行的安全监督检查。

第三条 互联网安全监督检查工作由县级以上地方人民政府公安机关网络安全保卫部门组织实施。

上级公安机关应当对下级公安机关开展互联网安全监督检查工作情况进行指导和监督。

第四条 公安机关开展互联网安全监督检查，应当遵循依法科学管理、保障和促进发展的方针，严格遵守法定权限和程序，不断改进执法方式，全面落实执法责任。

第五条 公安机关及其工作人员对履行互联网安全监督检查职责中知悉的个人信息、隐私、商业秘密和国家秘密，应当严格保密，不得泄露、出售或者非法向他人提供。

公安机关及其工作人员在履行互联网安全监督检查职责中获取的信息，只

能用于维护网络安全的需要，不得用于其他用途。

第六条 公安机关对互联网安全监督检查工作中发现的可能危害国家安全、公共安全、社会秩序的网络安全风险，应当及时通报有关主管部门和单位。

第七条 公安机关应当建立并落实互联网安全监督检查工作制度，自觉接受检查对象和人民群众的监督。

第二章 监督检查对象和内容

第八条 互联网安全监督检查由互联网服务提供者的网络服务运营机构和联网使用单位的网络管理机构所在地公安机关实施。互联网服务提供者为个人的，可以由其经常居住地公安机关实施。

第九条 公安机关应当根据网络安全防范需要和网络安全风险隐患的具体情况，对下列互联网服务提供者和联网使用单位开展监督检查：

(一)提供互联网接入、互联网数据中心、内容分发、域名服务的；

(二)提供互联网信息服务的；

(三)提供公共上网服务的；

(四)提供其他互联网服务的；

对开展前款规定的服务未满一年的，两年内曾发生过网络安全事件、违法犯罪案件的，或者因未履行法定网络安全义务被公安机关予以行政处罚的，应当开展重点监督检查。

第十条 公安机关应当根据互联网服务提供者和联网使用单位履行法定网络安全义务的实际情况，依照国家有关规定和标准，对下列内容进行监督检查：

(一)是否办理联网单位备案手续，并报送接入单位和用户基本信息及其变更情况；

(二)是否制定并落实网络安全管理制度和操作规程，确定网络安全负责人；

(三)是否依法采取记录并留存用户注册信息和上网日志信息的技术措施；

(四)是否采取防范计算机病毒和网络攻击、网络侵入等技术措施；

(五)是否在公共信息服务中对法律、行政法规禁止发布或者传输的信息依法采取相关防范措施；

(六)是否按照法律规定的要求为公安机关依法维护国家安全、防范调查恐

怖活动、侦查犯罪提供技术支持和协助；

(七)是否履行法律、行政法规规定的网络安全等级保护等义务。

第十一条 除本规定第十条所列内容外，公安机关还应当根据提供互联网服务的类型，对下列内容进行监督检查：

(一)对提供互联网接入服务的，监督检查是否记录并留存网络地址及分配使用情况；

(二)对提供互联网数据中心服务的，监督检查是否记录所提供的主机托管、主机租用和虚拟空间租用的用户信息；

(三)对提供互联网域名服务的，监督检查是否记录网络域名申请、变动信息，是否对违法域名依法采取处置措施；

(四)对提供互联网信息服务的，监督检查是否依法采取用户发布信息管理措施，是否对已发布或者传输的法律、行政法规禁止发布或者传输的信息依法采取处置措施，并保存相关记录；

(五)对提供互联网内容分发服务的，监督检查是否记录内容分发网络与内容源网络链接对应情况；

(六)对提供互联网公共上网服务的，监督检查是否采取符合国家标准的网络与信息安全保护技术措施。

第十二条 在国家重大网络安全保卫任务期间，对与国家重大网络安全保卫任务相关的互联网服务提供者和联网使用单位，公安机关可以对下列内容开展专项安全监督检查：

(一)是否制定重大网络安全保卫任务所要求的工作方案、明确网络安全责任分工并确定网络安全管理人员；

(二)是否组织开展网络安全风险评估，并采取相应风险管控措施堵塞网络安全漏洞隐患；

(三)是否制定网络安全应急处置预案并组织开展应急演练，应急处置相关设施是否完备有效；

(四)是否依法采取重大网络安全保卫任务所需要的其他网络安全防范措施；

(五)是否按照要求向公安机关报告网络安全防范措施及落实情况。

对防范恐怖袭击的重点目标的互联网安全监督检查，按照前款规定的内容执行。

第三章 监督检查程序

第十三条 公安机关开展互联网安全监督检查，可以采取现场监督检查或者远程检测的方式进行。

第十四条 公安机关开展互联网安全现场监督检查时，人民警察不得少于二人，并应当出示人民警察证和县级以上地方人民政府公安机关出具的监督检查通知书。

第十五条 公安机关开展互联网安全现场监督检查可以根据需要采取以下措施：

(一)进入营业场所、机房、工作场所；

(二)要求监督检查对象的负责人或者网络安全管理人员对监督检查事项作出说明；

(三)查阅、复制与互联网安全监督检查事项相关的信息；

(四)查看网络与信息安全保护技术措施运行情况。

第十六条 公安机关对互联网服务提供者和联网使用单位是否存在网络安全漏洞，可以开展远程检测。

公安机关开展远程检测，应当事先告知监督检查对象检查时间、检查范围等事项或者公开相关检查事项，不得干扰、破坏监督检查对象网络的正常运行。

第十七条 公安机关开展现场监督检查或者远程检测，可以委托具有相应技术能力的网络安全服务机构提供技术支持。

网络安全服务机构及其工作人员对工作中知悉的个人信息、隐私、商业秘密和国家秘密，应当严格保密，不得泄露、出售或者非法向他人提供。公安机关应当严格监督网络安全服务机构落实网络安全管理与保密责任。

第十八条 公安机关开展现场监督检查，应当制作监督检查记录，并由开展监督检查的人民警察和监督检查对象的负责人或者网络安全管理人员签名。监督检查对象负责人或者网络安全管理人员对监督检查记录有异议的，应当允许其作出说明；拒绝签名的，人民警察应当在监督检查记录中注明。

公安机关开展远程检测，应当制作监督检查记录，并由二名以上开展监督检查的人民警察在监督检查记录上签名。

委托网络安全服务机构提供技术支持的，技术支持人员应当一并在监督检查记录上签名。

第十九条 公安机关在互联网安全监督检查中，发现互联网服务提供者和联网使用单位存在网络安全风险隐患，应当督促指导其采取措施消除风险隐患，并在监督检查记录上注明；发现有违法行为，但情节轻微或者未造成后果的，应当责令其限期整改。

监督检查对象在整改期限届满前认为已经整改完毕的，可以向公安机关书面提出提前复查申请。

公安机关应当自整改期限届满或者收到监督检查对象提前复查申请之日起三个工作日内，对整改情况进行复查，并在复查结束后三个工作日内反馈复查结果。

第二十条 监督检查过程中收集的资料、制作的各类文书等材料，应当按照规定立卷存档。

第四章 法 律 责 任

第二十一条 公安机关在互联网安全监督检查中，发现互联网服务提供者和联网使用单位有下列违法行为的，依法予以行政处罚：

(一)未制定并落实网络安全管理制度和操作规程，未确定网络安全负责人的，依照《中华人民共和国网络安全法》第五十九条第一款的规定予以处罚；

(二)未采取防范计算机病毒和网络攻击、网络侵入等危害网络安全行为的技术措施的，依照《中华人民共和国网络安全法》第五十九条第一款的规定予以处罚；

(三)未采取记录并留存用户注册信息和上网日志信息措施的，依照《中华人民共和国网络安全法》第五十九条第一款的规定予以处罚；

(四)在提供互联网信息发布、即时通讯等服务中，未要求用户提供真实身份信息，或者对不提供真实身份信息的用户提供相关服务的，依照《中华人民共和国网络安全法》第六十一条的规定予以处罚；

(五)在公共信息服务中对法律、行政法规禁止发布或者传输的信息未依法

或者不按照公安机关的要求采取停止传输、消除等处置措施、保存有关记录的，依照《中华人民共和国网络安全法》第六十八条或者第六十九条第一项的规定予以处罚；

(六)拒不为公安机关依法维护国家安全和侦查犯罪的活动提供技术支持和协助的，依照《中华人民共和国网络安全法》第六十九条第三项的规定予以处罚。

有前款第四至六项行为违反《中华人民共和国反恐怖主义法》规定的，依照《中华人民共和国反恐怖主义法》第八十四条或者第八十六条第一款的规定予以处罚。

第二十二条 公安机关在互联网安全监督检查中，发现互联网服务提供者和联网使用单位，窃取或者以其他非法方式获取、非法出售或者非法向他人提供个人信息，尚不构成犯罪的，依照《中华人民共和国网络安全法》第六十四条第二款的规定予以处罚。

第二十三条 公安机关在互联网安全监督检查中，发现互联网服务提供者和联网使用单位在提供的互联网服务中设置恶意程序的，依照《中华人民共和国网络安全法》第六十条第一项的规定予以处罚。

第二十四条 互联网服务提供者和联网使用单位拒绝、阻碍公安机关实施互联网安全监督检查的，依照《中华人民共和国网络安全法》第六十九条第二项的规定予以处罚；拒不配合反恐怖主义工作的，依照《中华人民共和国反恐怖主义法》第九十一条或者第九十二条的规定予以处罚。

第二十五条 受公安机关委托提供技术支持的网络安全服务机构及其工作人员，从事非法侵入监督检查对象网络、干扰监督检查对象网络正常功能、窃取网络数据等危害网络安全的活动的，依照《中华人民共和国网络安全法》第六十三条的规定予以处罚；窃取或者以其他非法方式获取、非法出售或者非法向他人提供在工作中获悉的个人信息的，依照《中华人民共和国网络安全法》第六十四条第二款的规定予以处罚，构成犯罪的，依法追究刑事责任。

前款规定的机构及人员侵犯监督检查对象的商业秘密，构成犯罪的，依法追究刑事责任。

第二十六条 公安机关及其工作人员在互联网安全监督检查工作中，玩忽职

守、滥用职权、徇私舞弊的，对直接负责的主管人员和其他直接责任人员依法予以处分；构成犯罪的，依法追究刑事责任。

第二十七条 互联网服务提供者和联网使用单位违反本规定，构成违反治安管理行为的，依法予以治安管理处罚；构成犯罪的，依法追究刑事责任。

第五章 附 则

第二十八条 对互联网上网服务营业场所的监督检查，按照《互联网上网服务营业场所管理条例》的有关规定执行。

第二十九条 本规定自 2018 年 11 月 1 日起施行。

互联网个人信息安全保护指南

（2019 年 4 月 10 日 公安部网络安全保卫局、北京网络行业协会、公安部第三研究所联合发布）

为深入贯彻落实《网络安全法》，指导个人信息持有者建立健全公民个人信息安全保护管理制度和技术措施，有效防范侵犯公民个人信息违法行为，保障网络数据安全和公民合法权益，公安机关结合侦办侵犯公民个人信息网络犯罪案件和安全监督管理工作中掌握的情况，会同北京网络行业协会和公安部第三研究所等单位，研究制定了《互联网个人信息安全保护指南》。

现正式发布，供互联网企业、联网单位在个人信息安全保护工作中参考借鉴。

目 次

引 言

为有效防范侵犯公民个人信息违法行为，保障网络数据安全和公民合法权益，公安机关结合侦办侵犯公民个人信息网络犯罪案件和安全监督管理工作中掌握的情况，组织北京市网络行业协会和公安部第三研究所等单位相关专家，研究起草了《互联网个人信息安全保护指南》，供互联网服务单位在个人信息保护工作中参考借鉴。

互联网个人信息安全保护指南

1 范围

本文件制定了个人信息安全保护的管理机制、安全技术措施和业务流程。

适用于个人信息持有者在个人信息生命周期处理过程中开展安全保护工作参考使用。本文件适用于通过互联网提供服务的企业， 也适用于使用专网或非联网环境控制和处理个人信息的组织或个人。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件， 仅注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本(包括所有的修改单)适用于本文件。

GB/T25069—2010 信息安全技术 术语

GB/T35273—2017 信息安全技术 个人信息安全规范

GB/T22239 信息安全技术 网络安全等级保护基本要求(信息系统安全等级保护基本要求)

3 术语和定义

3.1 个人信息

以电子或者其他方式记录的能够单独或者与其他信息结合识别自然人个人身份的各种信息，包括但不限于自然人的姓名、出生日期、身份证件号码、个人生物识别信息、住址、电话号码等。

[中华人民共和国网络安全法，第七十六条(五)]

注：个人信息还包括通信通讯联系方式、通信记录和内容、账号密码、财产信息、征信信息、行踪轨迹、住宿信息、健康生理信息、交易信息等。

3.2 个人信息主体

个人信息所标识的自然人。

[GB/T35273-2017，定义 3.3]

3.3 个人信息持有

对个人信息及相关资源、环境、管理体系等进行计划、组织、协调、控制的相关活动或行为。

3.4 个人信息持有者

对个人信息进行控制和处理的组织或个人。

3.5 个人信息收集

获得对个人信息的控制权的行为，包括由个人信息主体主动提供、通过与个人信息主体交互或记录个人信息主体行为等自动采集，以及通过共享、转让、搜集公开信息间接获取等方式。

[GB/T35273-2017，定义 3.5]

3.6 个人信息使用

通过自动或非自动方式对个人信息进行操作，例如记录、组织、排列、存储、改编或变更、检索、咨询、披露、传播或以其他方式提供、调整或组合、限制、删除等。

3.7 个人信息删除

在实现日常业务功能所涉及的系统中去除个人信息的行为，使其保持不可被检索、访问的状态。

[GB/T 35273-2017，定义 3.9]

3.8 个人信息生命周期

包括个人信息持有者收集、保存、应用、委托处理、共享、转让和公开披露、删除个人信息在内的全部生命历程。

3.9 个人信息处理系统

处理个人信息的计算机信息系统，涉及个人信息生命周期一个或多个阶段(收集、保存、应用、委托处理、共享、转让和公开披露、删除)。

4 管理机制

4.1 基本要求

个人信息处理系统的安全管理要求应满足 GB/T22239 相应等级的要求。

4.2 管理制度

4.2.1 管理制度内容

a)应制定个人信息保护的总体方针和安全策略等相关规章制度和文件，其中包括本机构的个人信息保护工作的目标、范围、原则和安全框架等相关说明；

b)应制定工作人员对个人信息日常管理的操作规程；

c)应建立个人信息管理制度体系，其中包括安全策略、管理制度、操作规程和记录表单；

d)应制定个人信息安全事件应急预案。

4.2.2 管理制度制定发布

a)应指定专门的部门或人员负责安全管理制度的制定；

b)应明确安全管理制度的制定程序和发布方式，对制定的安全管理制度进行论证和审定，并形成论证和评审记录；

c)应明确管理制度的发布范围，并对发文及确认情况进行登记记录。

4.2.3 管理制度执行落实

a)应对相关制度执行情况进行审批登记；

b)应保存记录文件，确保实际工作流程与相关的管理制度内容相同；

c)应定期汇报总结管理制度执行情况。

4.2.4 管理制度评审改进

a)应定期对安全管理制度进行评审，存在不足或需要改进的予以修订；

b)安全管理制度评审应形成记录，如果对制度做过修订，应更新所有下发的相关安全管理制度。

4.3 管理机构

4.3.1 管理机构的岗位设置

a)应设置指导和管理个人信息保护的工作机构，明确定义机构的职责；

b)应由最高管理者或授权专人负责个人信息保护的工作；

c)应明确设置安全主管、安全管理各个方面的负责人， 设立审计管理员和安全管理员等岗位，清晰、明确定义其职责范围。

4.3.2 管理机构的人员配置

a)应明确安全管理岗位人员的配备，包括数量、专职还是兼职情况等； 配备负责数据保护的专门人员；

b)应建立安全管理岗位人员信息表，登记机房管理员、系统管理员、数据库管理员、网络管理员、审计管理员、安全管理员等重要岗位人员的信息， 审计管理员和安全管理员不应兼任网络管理员、系统管理员、数据库管理员、数据操作员等岗位。

4.4 管理人员

4.4.1 管理人员的录用

a)应设立专门的部门或人员负责人员的录用工作；

b)应明确人员录用时对人员的条件要求，对被录用人的身份、背景和专业资格进行审查，对技术人员的技术技能进行考核；

c)录用后应签署相应的针对个人信息的保密协议；

d)应建立管理文档，说明录用人员应具备的条件(如学历、学位要求，技术人员应具备的专业技术水平，管理人员应具备的安全管理知识等)；

e)应记录录用人身份、背景和专业资格等，记录审查内容和审查结果等；

f)应记录录用人录用时的技能考核文档或记录，记录考核内容和考核结果等；

g)应签订保密协议，其中包括保密范围、保密责任、违约责任、协议的有效期限和责任人签字等内容。

4.4.2 管理人员的离岗

a)人员离岗时应办理调离手续，签署调离后个人信息保密义务的承诺书，防范内部员工、管理员因工作原因非法持有、披露和使用个人信息；

b)应对即将离岗人员具有控制方法，及时终止离岗人员的所有访问权限，取回其身份认证的配件，诸如身份证件、钥匙、徽章以及机构提供的软硬件设备；采用生理特征进行访问控制的，需要及时删除生理特征录入的相关信息；

c)应形成对离岗人员的安全处理记录(如交还身份证件、设备等的登记记录)；

d)应具有按照离职程序办理调离手续的记录。

4.4.3 管理人员的考核

a)应设立专人负责定期对接触个人信息数据工作的工作人员进行全面、严格的安全审查、意识考核和技能考核；

b)应按照考核周期形成考核文档，被考核人员应包括各个岗位的人员；

c)应对违反违背制定的安全策略和规定的人员进行惩戒；

d)应定期考查安全管理员、系统管理员和网络管理员其对工作相关的信息安全基础知识、安全责任和惩戒措施、相关法律法规等的理解程度， 并对考核记录进行记录存档。

4.4.4 管理人员的教育培训

a)应制定培训计划并按计划对各岗位员工进行基本的安全意识教育培训和岗位技能培训；

b)应制定安全教育和培训计划文档，明确培训方式、培训对象、培训内容、培训时间和地点等，培训内容包含信息安全基础知识、岗位操作规程等；

c)应形成安全教育和培训记录，记录包含培训人员、培训内容、培训结果等。

4.4.5 外部人员访问

a)应建立关于物理环境的外部人员访问的安全措施：

1)制定外部人员允许访问的设备、区域和信息的规定；

2)外部人员访问前需要提出书面申请并获得批准；

3)外部人员访问被批准后应有专人全程陪同或监督，并进行全程监控录像；

4)外部人员访问情况应登记备案。

b)应建立关于网络通道的外部人员访问的安全措施：

1)制定外部人员允许接入受控网络访问系统的规定；

2)外部人员访问前需要提出书面申请并获得批准；

3)外部人员访问时应进行身份认证；

4)应根据外部访问人员的身份划分不同的访问权限和访问内容；

5)应对外部访问人员的访问时间进行限制；

6)对外部访问人员对个人信息的操作进行记录。

5 技术措施

5.1 基本要求

个人信息处理系统其安全技术措施应满足 GB/T22239 相应等级的要求，按照网络安全等级保护制度的要求，履行安全保护义务，保障网络免受干扰、破坏或者未经授权的访问，防止网络数据泄露或者被窃取、篡改。

5.2 通用要求

5.2.1 通信网络安全

5.2.1.1 网络架构

a)应为个人信息处理系统所处网络划分不同的网络区域，并按照方便管理和控制的原则为各网络区域分配地址；

b)个人信息处理系统应作为重点区域部署，并设有边界防护措施。

5.2.1.2 通信传输

a)应采用校验技术或密码技术保证通信过程中个人信息的完整性；

b)应采用密码技术保证通信过程中个人信息字段或整个报文的保密性。

5.2.2 区域边界安全

5.2.2.1 边界防护

a)应对跨越边界访问通信信息进行有效防护；

b)应对非授权设备跨越边界行为进行检查或限制。

5.2.2.2 访问控制

应在个人信息处理系统边界根据访问控制策略设置访问控制规则。

5.2.2.3 入侵防范

应在个人信息处理系统边界部署入侵防护措施，检测、防止或限制从外部、内部发起的网络攻击行为。

5.2.2.4 恶意代码防范

应在个人信息处理系统的网络边界处对恶意代码进行检测和清除，并维护恶意代码防护机制的升级和更新。

5.2.2.5 安全审计

a)应在个人信息处理系统的网络边界、重要网络节点进行安全审计， 审计应覆盖到每个用户、用户行为和安全事件；

b)审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功， 以及个人信息的范围、类型、操作方式、操作人、流转双方及其他与审计相关的信息；

c)应对审计记录进行保护，定期备份并避免受到未预期的删除、修改或覆盖等；

d)审计记录的留存时间应符合法律法规的要求；

e)应能够对远程访问的用户行为、访问互联网的用户行为等单独进行行为审计和数据分析。

5.2.3 计算环境安全

5.2.3.1 身份鉴别

a)应对登录个人信息处理系统的用户进行身份标识和鉴别，身份鉴别标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；

b)个人信息处理系统应启用登录失败处理功能，采取诸如结束会话、限制非法登录次数和自动退出等措施；

c)个人信息处理系统进行远程管理时，应采取措施防止身份鉴别信息在网络传输过程中被窃听；

d)个人信息处理系统应采用口令、密码技术、生物技术等两种或两种以上组合的鉴别技术对用户进行身份鉴别，且其中一种鉴别技术至少应使用密码技术来实现，密码技术应符合国家密码主管部门规范。

5.2.3.2 访问控制

a)应对登录个人信息处理系统的用户分配账户和权限；

b)个人信息处理系统应重命名或删除默认账户，修改默认账户的默认口令；

c)个人信息处理系统应及时删除或停用多余的、过期的账户， 避免共享账户

的存在；

d)个人信息处理系统应进行角色划分，并授予管理用户所需的最小权限，实现管理用户的权限分离；

e)个人信息处理系统应由授权主体配置访问控制策略，访问控制策略应规定主体对客体的访问规则；

f)个人信息处理系统的访问控制的粒度应达到主体为用户级或进程级，客体为文件、数据库表级；

g)个人信息处理系统应对个人信息设置安全标记，并控制主体对有安全标记资源的访问。

5.2.3.3 安全审计

a)个人信息处理系统应启用安全审计功能，并且审计覆盖到每个用户，应对重要的用户行为和重要的安全事件进行审计；

b)审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；

c)应对审计记录进行保护，进行定期备份并避免受到未预期的删除、修改或覆盖等；

d)审计记录的留存时间应符合法律法规的要求；

e)应对审计进程进行保护，防止未经授权的中断。

5.2.3.4 入侵防范

a)个人信息处理系统应遵循最小安装的原则，只安装需要的组件和应用程序；

b)个人信息处理系统应关闭不需要的系统服务、默认共享和高危端口；

c)个人信息处理系统应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；

d)个人信息处理系统应能够发现存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞；

e)个人信息处理系统应能够检测到对重要节点的入侵行为并进行防御，并在发生严重入侵事件时提供报警；

5.2.3.5 恶意代码防范和程序可信执行

应采取免受恶意代码攻击的技术措施或可信验证机制对系统程序、应用程序

和重要配置文件/参数进行可信执行验证，并在检测到其完整性受到破坏时采取恢复措施。

5.2.3.6 资源控制

a)应限制单个用户或进程对个人信息处理和存储设备系统资源的最大使用限度；

b)应提供重要节点设备的硬件冗余，保证系统的可用性；

c)应对重要节点进行监视，包括监视 CPU、硬盘、内存等资源的使用情况；

d)应能够对重要节点的服务水平降低到预先规定的最小值进行检测和报警。

5.2.4 应用和数据安全

5.2.4.1 身份鉴别

a)个人信息处理系统应对登录的用户进行身份标识和鉴别，该身份标识应具有唯一性，鉴别信息应具有复杂度并要求定期更换；

b)个人信息处理系统应提供并启用登录失败处理功能，并在多次登录后采取必要的保护措施；

c)个人信息处理系统应强制用户首次登录时修改初始口令，当确定信息被泄露后，应提供提示全部用户强制修改密码的功能，在验证确认用户后修改密码；

d)用户身份鉴别信息丢失或失效时，应采取技术措施保证鉴别信息重置过程的安全；

e)应采取静态口令、动态口令、密码技术、生物技术等两种或两种以上的组合鉴别技术对用户进行身份鉴别，且其中一种鉴别技术使用密码技术来实现。

5.2.4.2 访问控制

a)个人信息处理系统应提供访问控制功能，并对登录的用户分配账户和权限；

b)应重命名或删除默认账户，修改默认账户的默认口令；

c)应及时删除或停用多余的、过期的账户，避免共享账户的存在；

d)应授予不同账户为完成各自承担任务所需的最小权限，在它们之间形成相互制约的关系；

e)应由授权主体配置访问控制策略，访问控制策略规定主体对客体的访问规则；

f)访问控制的粒度应达到主体为用户级，客体为文件、数据库表级、记录或

字段级；

g)个人信息应设置安全标记，控制主体对有安全标记资源的访问。

5.2.4.3 安全审计

a)个人信息处理系统应提供安全审计功能，审计应覆盖到每个用户，应对重要的用户行为和重要的安全事件进行审计；

b)审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；

c)应对审计记录进行保护，定期备份，并避免受到未预期的删除、修改或覆盖等；

d)审计记录的留存时间应符合法律法规的要求；

e)应对审计进程进行保护，防止未经授权的中断。

5.2.4.4 软件容错

a)应提供个人信息的有效性校验功能，保证通过人机接口输入或通过通信接口输入的内容符合个人信息处理系统设定要求；

b)应能够发现个人信息处理系统软件组件可能存在的已知漏洞，并能够在充分测试评估后及时修补漏洞；

c)应能够在故障发生时，继续提供一部分功能，并能够实施必要的措施。

5.2.4.5 资源控制

a)在通信双方中的一方在一段时间内未做任何响应时，另一方应能够自动结束会话；

b)应对个人信息处理系统的最大并发会话连接数进行限制；

c)应能够对单个用户的多重并发会话进行限制。

5.2.4.6 数据完整性

a)应采取校验技术或密码技术保证重要数据在传输过程中的完整性，包括但不限于鉴别数据和个人信息；

b)应采用校验技术或密码技术保证重要数据在存储过程中的完整性，包括但不限于鉴别数据和个人信息。

5.2.4.7 数据保密性

a)应采用密码技术保证重要数据在传输过程中的保密性，包括但不限于鉴别

数据和个人信息；

b)应采用密码技术保证重要数据在存储过程中的保密性，包括但不限于鉴别数据和个人信息。

5.2.4.8 数据备份恢复

a)应提供个人信息的本地数据备份与恢复功能，定期对备份数据进行恢复测试，保证数据可用性；

b)应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地；

c)应提供重要数据处理系统的热冗余，保证系统的高可用性。

5.2.4.9 剩余信息保护

a)应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除；

b)应保证存有个人信息的存储空间被释放或重新分配前得到完全清除。

5.3 扩展要求

5.3.1 云计算安全扩展要求

a)应确保个人信息在云计算平台中存储于中国境内，如需出境应遵循国家相关规定；

b)应使用校验技术或密码技术保证虚拟机迁移过程中，个人信息的完整性，并在检测到完整性受到破坏时采取必要的恢复措施；

c)应使用密码技术保证虚拟机迁移过程中，个人信息的保密性，防止在迁移过程中的个人信息泄露。

5.3.2 物联网安全扩展要求

物联网感知节点设备采集信息回传应采用密码技术保证通信过程中个人信息的保密性。

6 业务流程

6.1 收集

个人信息的收集行为应满足以下要求：

a)个人信息收集前，应当遵循合法、正当、必要的原则向被收集的个人信息主体公开收集、使用规则，明示收集、使用信息的目的、方式和范围等信息；

b)个人信息收集应获得个人信息主体的同意和授权，不应收集与其提供的服务无关的个人信息，不应通过捆绑产品或服务各项业务功能等方式强迫收集个人

信息；

c)个人信息收集应执行收集前签署的约定和协议，不应超范围收集；

d)不应大规模收集或处理我国公民的种族、民族、政治观点、宗教信仰等敏感数据；

e)个人生物识别信息应仅收集和使用摘要信息，避免收集其原始信息；

f)应确保收集个人信息过程的安全性：

1)收集个人信息之前，应有对被收集人进行身份认证的机制，该身份认证机制应具有相应安全性；

2)收集个人信息时，信息在传输过程中应进行加密等保护处理；

3)收集个人信息的系统应落实网络安全等级保护要求；

4)收集个人信息时应有对收集内容进行安全检测和过滤的机制，防止非法内容提交。

6.2 保存

个人信息的保存行为应满足以下要求：

a)在境内运营中收集和产生的个人信息应在境内存储，如需出境应遵循国家相关规定；

b)收集到的个人信息应采取相应的安全加密存储等安全措施进行处理；

c)应对保存的个人信息根据收集、使用目的、被收集人授权设置相应的保存时限；

d)应对保存的个人信息在超出设置的时限后予以删除；

e)保存信息的主要设备，应对个人信息数据提供备份和恢复功能，确保数据备份的频率和时间间隔，并使用不少于以下一种备份手段：

1)具有本地数据备份功能；

2)将备份介质进行场外存放；

3)具有异地数据备份功能。

6.3 应用

个人信息的应用应满足以下要求：

a)对个人信息的应用，应符合与个人信息主体签署的相关协议和规定，不应超范围应用个人信息；

注：经过处理无法识别特定个人且不能复原的个人信息数据，可以超出与信息主体签署的相关使用协议和约定，但应提供适当的保护措施进行保护。

b)个人信息主体应拥有控制本人信息的权限，包括：

1)允许对本人信息的访问；

2)允许通过适当方法对本人信息的修改或删除，包括纠正不准确和不完整的数据，并保证修改后的本人信息具备真实性和有效性；

c)完全依靠自动化处理的用户画像技术应用于精准营销、搜索结果排序、个性化推送新闻、定向投放广告等增值应用， 可事先不经用户明确授权，但应确保用户有反对或者拒绝的权利；如应用于征信服务、行政司法决策等可能对用户带来法律后果的增值应用，或跨网络运营者使用，应经用户明确授权方可使用其数据；

d)应对个人信息的接触者设置相应的访问控制措施，包括：

1)对被授权访问个人信息数据的工作人员按照最小授权的原则，只能访问最少够用的信息，只具有完成职责所需的最少的数据操作权限；

2)对个人信息的重要操作设置内部审批流程，如批量修改、拷贝、下载等；

3)对特定人员超限制处理个人信息时配置相应的责任人或负责机构进行审批，并对这种行为进行记录。

e)应对必须要通过界面(如显示屏幕、纸面)展示的个人信息进行去标识化的处理。

6.4 删除

a)个人信息在超过保存时限之后应进行删除，经过处理无法识别特定个人且不能复原的除外；

b)个人信息持有者如有违反法律、行政法规的规定或者双方的约定收集、使用其个人信息时，个人信息主体要求删除其个人信息的，应采取措施予以删除；

c)个人信息相关存储设备，将存储的个人信息数据进行删除之后应采取措施防止通过技术手段恢复；

d)对存储过个人信息的设备在进行新信息的存储时，应将之前的内容全部进行删除；

e)废弃存储设备，应在进行删除后再进行处理。

6.5 第三方委托处理

a)在对个人信息委托处理时，不应超出该信息主体授权同意的范围；

b)在对个人信息的相关处理进行委托时，应对委托行为进行个人信息安全影响评估；

c)对个人信息进行委托处理时，应签订相关协议要求受托方符合本文件；

d)应向受托方进行对个人信息数据的使用和访问的授权；

e)受托方对个人信息的相关数据进行处理完成之后，应对存储的个人信息数据的内容进行删除。

6.6 共享和转让

个人信息原则上不得共享、转让。如存在个人信息共享和转让行为时， 应满足以下要求：

a)共享和转让行为应经过合法性、必要性评估；

b)在对个人信息进行共享和转让时应进行个人信息安全影响评估，应对受让方的数据安全能力进行评估确保受让方具备足够的数据安全能力，并按照评估结果采取有效的保护个人信息主体的措施；

c)在共享、转让前应向个人信息主体告知转让该信息的目的、规模、公开范围数据接收方的类型等信息；

d)在共享、转让前应得到个人信息主体的授权同意，与国家安全、国防安全、公共安全、公共卫生、重大公共利益或与犯罪侦查、起诉、审判和判决执行等直接相关的情形除外；

e)应记录共享、转让信息内容，将共享、转让情况中包括共享、转让的日期、数据量、目的和数据接收方的基本情况在内的信息进行登记；

f)在共享、转让后应了解接收方对个人信息的保存、使用情况和个人信息主体的权利，例如访问、更正、删除、注销等；

g)当个人信息持有者发生收购、兼并、重组、破产等变更时， 个人信息持有者应向个人信息主体告知有关情况，并继续履行原个人信息持有者的责任和义务，如变更个人信息使用目的时，应重新取得个人信息主体的明示同意。

6.7 公开披露

个人信息原则上不得公开披露。如经法律授权或具备合理事由确需公开披露

时，应充分重视风险，遵守以下要求：

a)事先开展个人信息安全影响评估，并依评估结果采取有效的保护个人信息主体的措施；

b)向个人信息主体告知公开披露个人信息的目的、类型， 并事先征得个人信息主体明示同意，与国家安全、国防安全、公共安全、公共卫生、重大公共利益或与犯罪侦查、起诉、审判和判决执行等直接相关的情形除外；

c)公开披露个人敏感信息前，除 6.7b)中告知的内容外，还应向个人信息主体告知涉及的个人敏感信息的内容；

d)准确记录和保存个人信息的公开披露的情况，包括公开披露的日期、规模、目的、公开范围等；

e)承担因公开披露个人信息对个人信息主体合法权益造成损害的相应责任；

f)不得公开披露个人生物识别信息和基因、疾病等个人生理信息；

g)不得公开披露我国公民的种族、民族、政治观点、宗教信仰等敏感数据分析结果。

7 应急处置

7.1 应急机制和预案

a)应建立健全网络安全风险评估和应急工作机制，在个人信息处理过程中发生应急事件时具有上报有关主管部门的机制；

b)应制定个人信息安全事件应急预案，包括应急处理流程、事件上报流程等内容；

c)应定期(至少每半年一次)组织内部相关人员进行应急响应培训和应急演练，使其掌握岗位职责和应急处置策略和规程，留存应急培训和应急演练记录；

d)应定期对原有的应急预案重新评估，修订完善。

7.2 处置和响应

a)发现网络存在较大安全风险，应采取措施，进行整改，消除隐患；发生安全事件时应及时向公安机关报告，协助开展调查和取证工作，尽快消除隐患；

b)发生个人信息安全事件后，应记录事件内容，包括但不限于：发现事件的人员、时间、地点， 涉及的个人信息及人数，发生事件的系统名称，对其他互联系统的影响，是否已联系执法机关或有关部门；

c)应对安全事件造成的影响进行调查和评估，采取技术措施和其他必要措施，消除安全隐患，防止危害扩大；

d)应按《国家网络安全事件应急预案》等相关规定及时上报安全事件， 报告内容包括但不限于：涉及个人信息主体的类型、数量、内容、性质等总体情况，事件可能造成的影响，已采取或将要采取的处置措施，事件处置相关人员的联系方式；

e)应将事件的情况告知受影响的个人信息主体，并及时向社会发布与公众有关的警示信息。

关于印发《信息安全等级保护管理办法》的通知

公通字〔2007〕43 号)

各省、自治区、直辖市公安厅(局)、保密局、国家密码管理局(国家密码管理委员会办公室)、信息化领导小组办公室，新疆生产建设兵团公安局、保密局、国家密码管理局、信息化领导小组办公室， 中央和国家机关各部委保密委员会办公室、密码工作领导小组办公室、信息化领导小组办公室， 各人民团体保密委员会办公室：

为加快推进信息安全等级保护，规范信息安全等级保护管理，提高信息安全保障能力和水平，维护国家安全、社会稳定和公共利益，保障和促进信息化建设，公安部、国家保密局、国家密码管理局、国务院信息化工作办公室制定了《信息安全等级保护管理办法》。现印发给你们，请认真贯彻执行。

公安部

国家保密局

国家密码管理局

国务院信息工作办公室

二〇〇七年六月二十二日

信息安全等级保护管理办法

第一章 总 则

第一条 为规范信息安全等级保护管理，提高信息安全保障能力和水平，维护国家安全、社会稳定和公共利益， 保障和促进信息化建设，根据《中华人民共和国计算机信息系统安全保护条例》等有关法律法规，制定本办法。

第二条 国家通过制定统一的信息安全等级保护管理规范和技术标准，组织公民、法人和其他组织对信息系统分等级实行安全保护， 对等级保护工作的实施进行监督、管理。

第三条 公安机关负责信息安全等级保护工作的监督、检查、指导。国家保密工作部门负责等级保护工作中有关保密工作的监督、检查、指导。国家密码管理部门负责等级保护工作中有关密码工作的监督、检查、指导。涉及其他职能部门管辖范围的事项，由有关职能部门依照国家法律法规的规定进行管理。国务院信息化工作办公室及地方信息化领导小组办事机构负责等级保护工作的部门间协调。

第四条 信息系统主管部门应当依照本办法及相关标准规范，督促、检查、指导本行业、本部门或者本地区信息系统运营、使用单位的信息安全等级保护工作。

第五条 信息系统的运营、使用单位应当依照本办法及其相关标准规范，履行信息安全等级保护的义务和责任。

第二章 等级划分与保护

第六条 国家信息安全等级保护坚持自主定级、自主保护的原则。信息系统的安全保护等级应当根据信息系统在国家安全、经济建设、社会生活中的重要程度，信息系统遭到破坏后对国家安全、社会秩序、公共利益以及公民、法人和其他组织的合法权益的危害程度等因素确定。

第七条 信息系统的安全保护等级分为以下五级：

第一级，信息系统受到破坏后，会对公民、法人和其他组织的合法权益造成损害，但不损害国家安全、社会秩序和公共利益。

第二级，信息系统受到破坏后，会对公民、法人和其他组织的合法权益产生严重损害，或者对社会秩序和公共利益造成损害，但不损害国家安全。

第三级，信息系统受到破坏后，会对社会秩序和公共利益造成严重损害，或者对国家安全造成损害。

第四级，信息系统受到破坏后，会对社会秩序和公共利益造成特别严重损害，或者对国家安全造成严重损害。

第五级，信息系统受到破坏后，会对国家安全造成特别严重损害。

第八条 信息系统运营、使用单位依据本办法和相关技术标准对信息系统进行保护，国家有关信息安全监管部门对其信息安全等级保护工作进行监督管理。

第一级信息系统运营、使用单位应当依据国家有关管理规范和技术标准进行保护。

第二级信息系统运营、使用单位应当依据国家有关管理规范和技术标准进行保护。国家信息安全监管部门对该级信息系统信息安全等级保护工作进行指导。

第三级信息系统运营、使用单位应当依据国家有关管理规范和技术标准进行保护。国家信息安全监管部门对该级信息系统信息安全等级保护工作进行监督、检查。

第四级信息系统运营、使用单位应当依据国家有关管理规范、技术标准和业务专门需求进行保护。国家信息安全监管部门对该级信息系统信息安全等级保护工作进行强制监督、检查。

第五级信息系统运营、使用单位应当依据国家管理规范、技术标准和业务特殊安全需求进行保护。国家指定专门部门对该级信息系统信息安全等级保护工作进行专门监督、检查。

第三章 等级保护的实施与管理

第九条 信息系统运营、使用单位应当按照《信息系统安全等级保护实施指南》具体实施等级保护工作。

第十条 信息系统运营、使用单位应当依据本办法和《信息系统安全等级保护定级指南》确定信息系统的安全保护等级。有主管部门的， 应当经主管部门审核批准。

跨省或者全国统一联网运行的信息系统可以由主管部门统一确定安全保护等级。

对拟确定为第四级以上信息系统的，运营、使用单位或者主管部门应当请国家信息安全保护等级专家评审委员会评审。

第十一条 信息系统的安全保护等级确定后，运营、使用单位应当按照国家信息安全等级保护管理规范和技术标准，使用符合国家有关规定，满足信息系统安全保护等级需求的信息技术产品，开展信息系统安全建设或者改建工作。

第十二条 在信息系统建设过程中，运营、使用单位应当按照《计算机信息

系统安全保护等级划分准则》(GB17859-1999)、《信息系统安全等级保护基本要求》等技术标准，参照《信息安全技术 信息系统通用安全技术要求》(GB/T20271-2006)、《信息安全技术 网络基础安全技术要求》(GB/T20270-2006)、《信息安全技术 操作系统安全技术要求》(GB/T20272-2006)、《信息安全技术 数据库管理系统安全技术要求》(GB/T20273-2006)、《信息安全技术 服务器技术要求》、《信息安全技术 终端计算机系统安全等级技术要求》(GA/T671-2006)等技术标准同步建设符合该等级要求的信息安全设施。

第十三条 运营、使用单位应当参照《信息安全技术 信息系统安全管理要求》(GB/T20269-2006)、《信息安全技术 信息系统安全工程管理要求》(GB/T20282-2006)、《信息系统安全等级保护基本要求》等管理规范，制定并落实符合本系统安全保护等级要求的安全管理制度。

第十四条 信息系统建设完成后，运营、使用单位或者其主管部门应当选择符合本办法规定条件的测评机构，依据《信息系统安全等级保护测评要求》等技术标准，定期对信息系统安全等级状况开展等级测评。第三级信息系统应当每年至少进行一次等级测评，第四级信息系统应当每半年至少进行一次等级测评，第五级信息系统应当依据特殊安全需求进行等级测评。

信息系统运营、使用单位及其主管部门应当定期对信息系统安全状况、安全保护制度及措施的落实情况进行自查。第三级信息系统应当每年至少进行一次自查，第四级信息系统应当每半年至少进行一次自查，第五级信息系统应当依据特殊安全需求进行自查。

经测评或者自查，信息系统安全状况未达到安全保护等级要求的，运营、使用单位应当制定方案进行整改。

第十五条 已运营(运行)的第二级以上信息系统，应当在安全保护等级确定后 30 日内，由其运营、使用单位到所在地设区的市级以上公安机关办理备案手续。

新建第二级以上信息系统，应当在投入运行后 30 日内，由其运营、使用单位到所在地设区的市级以上公安机关办理备案手续。

隶属于中央的在京单位，其跨省或者全国统一联网运行并由主管部门统一定级的信息系统，由主管部门向公安部办理备案手续。跨省或者全国统一联网运行

的信息系统在各地运行、应用的分支系统，应当向当地设区的市级以上公安机关备案。

第十六条 办理信息系统安全保护等级备案手续时，应当填写《信息系统安全等级保护备案表》，第三级以上信息系统应当同时提供以下材料：

(一)系统拓扑结构及说明；

(二)系统安全组织机构和管理制度；

(三)系统安全保护设施设计实施方案或者改建实施方案；

(四)系统使用的信息安全产品清单及其认证、销售许可证明；

(五)测评后符合系统安全保护等级的技术检测评估报告；

(六)信息系统安全保护等级专家评审意见；

(七)主管部门审核批准信息系统安全保护等级的意见。

第十七条 信息系统备案后，公安机关应当对信息系统的备案情况进行审核，对符合等级保护要求的，应当在收到备案材料之日起的 10 个工作日内颁发信息系统安全等级保护备案证明；发现不符合本办法及有关标准的，应当在收到备案材料之日起的 10 个工作日内通知备案单位予以纠正；发现定级不准的，应当在收到备案材料之日起的 10 个工作日内通知备案单位重新审核确定。

运营、使用单位或者主管部门重新确定信息系统等级后，应当按照本办法向公安机关重新备案。

第十八条 受理备案的公安机关应当对第三级、第四级信息系统的运营、使用单位的信息安全等级保护工作情况进行检查。对第三级信息系统每年至少检查一次，对第四级信息系统每半年至少检查一次。对跨省或者全国统一联网运行的信息系统的检查，应当会同其主管部门进行。

对第五级信息系统，应当由国家指定的专门部门进行检查。

公安机关、国家指定的专门部门应当对下列事项进行检查：

(一)信息系统安全需求是否发生变化，原定保护等级是否准确；

(二)运营、使用单位安全管理制度、措施的落实情况；

(三)运营、使用单位及其主管部门对信息系统安全状况的检查情况；

(四)系统安全等级测评是否符合要求；

(五)信息安全产品使用是否符合要求；

(六)信息系统安全整改情况;

(七)备案材料与运营、使用单位、信息系统的符合情况;

(八)其他应当进行监督检查的事项。

第十九条 信息系统运营、使用单位应当接受公安机关、国家指定的专门部门的安全监督、检查、指导, 如实向公安机关、国家指定的专门部门提供下列有关信息安全保护的信息资料及数据文件:

(一)信息系统备案事项变更情况;

(二)安全组织、人员的变动情况;

(三)信息安全管理制度、措施变更情况;

(四)信息系统运行状况记录;

(五)运营、使用单位及主管部门定期对信息系统安全状况的检查记录;

(六)对信息系统开展等级测评的技术测评报告;

(七)信息安全产品使用的变更情况;

(八)信息安全事件应急预案,信息安全事件应急处置结果报告;

(九)信息系统安全建设、整改结果报告。

第二十条 公安机关检查发现信息系统安全保护状况不符合信息安全等级保护有关管理规范和技术标准的,应当向运营、使用单位发出整改通知。运营、使用单位应当根据整改通知要求,按照管理规范和技术标准进行整改。整改完成后,应当将整改报告向公安机关备案。必要时,公安机关可以对整改情况组织检查。

第二十一条 第三级以上信息系统应当选择使用符合以下条件的信息安全产品:

(一)产品研制、生产单位是由中国公民、法人投资或者国家投资或者控股的,在中华人民共和国境内具有独立的法人资格;

(二)产品的核心技术、关键部件具有我国自主知识产权;

(三)产品研制、生产单位及其主要业务、技术人员无犯罪记录;

(四)产品研制、生产单位声明没有故意留有或者设置漏洞、后门、木马等程序和功能;

(五)对国家安全、社会秩序、公共利益不构成危害;

(六)对已列入信息安全产品认证目录的,应当取得国家信息安全产品认证机

构颁发的认证证书。

第二十二条 第三级以上信息系统应当选择符合下列条件的等级保护测评机构进行测评：

(一)在中华人民共和国境内注册成立(港澳台地区除外)；

(二)由中国公民投资、中国法人投资或者国家投资的企事业单位(港澳台地区除外)；

(三)从事相关检测评估工作两年以上，无违法记录；

(四)工作人员仅限于中国公民；

(五)法人及主要业务、技术人员无犯罪记录；

(六)使用的技术装备、设施应当符合本办法对信息安全产品的要求；

(七)具有完备的保密管理、项目管理、质量管理、人员管理和培训教育等安全管理制度；

(八)对国家安全、社会秩序、公共利益不构成威胁。

第二十三条 从事信息系统安全等级测评的机构，应当履行下列义务：

(一)遵守国家有关法律法规和技术标准，提供安全、客观、公正的检测评估服务，保证测评的质量和效果；

(二)保守在测评活动中知悉的国家秘密、商业秘密和个人隐私， 防范测评风险；

(三)对测评人员进行安全保密教育，与其签订安全保密责任书，规定应当履行的安全保密义务和承担的法律责任，并负责检查落实。

第四章 涉及国家秘密信息系统的分级保护管理

第二十四条 涉密信息系统应当依据国家信息安全等级保护的基本要求，按照国家保密工作部门有关涉密信息系统分级保护的管理规定和技术标准，结合系统实际情况进行保护。

非涉密信息系统不得处理国家秘密信息。

第二十五条 涉密信息系统按照所处理信息的最高密级，由低到高分为秘密、机密、绝密三个等级。

涉密信息系统建设使用单位应当在信息规范定密的基础上，依据涉密信息系统分级保护管理办法和国家保密标准 BMB17-2006《涉及国家秘密的计算机信息

系统分级保护技术要求》确定系统等级。对于包含多个安全域的涉密信息系统，各安全域可以分别确定保护等级。

保密工作部门和机构应当监督指导涉密信息系统建设使用单位准确、合理地进行系统定级。

第二十六条 涉密信息系统建设使用单位应当将涉密信息系统定级和建设使用情况，及时上报业务主管部门的保密工作机构和负责系统审批的保密工作部门备案，并接受保密部门的监督、检查、指导。

第二十七条 涉密信息系统建设使用单位应当选择具有涉密集成资质的单位承担或者参与涉密信息系统的设计与实施。

涉密信息系统建设使用单位应当依据涉密信息系统分级保护管理规范和技术标准，按照秘密、机密、绝密三级的不同要求，结合系统实际进行方案设计，实施分级保护，其保护水平总体上不低于国家信息安全等级保护第三级、第四级、第五级的水平。

第二十八条 涉密信息系统使用的信息安全保密产品原则上应当选用国产品，并应当通过国家保密局授权的检测机构依据有关国家保密标准进行的检测，通过检测的产品由国家保密局审核发布目录。

第二十九条 涉密信息系统建设使用单位在系统工程实施结束后，应当向保密工作部门提出申请，由国家保密局授权的系统测评机构依据国家保密标准BMB22-2007《涉及国家秘密的计算机信息系统分级保护测评指南》，对涉密信息系统进行安全保密测评。

涉密信息系统建设使用单位在系统投入使用前，应当按照《涉及国家秘密的信息系统审批管理规定》，向设区的市级以上保密工作部门申请进行系统审批，涉密信息系统通过审批后方可投入使用。已投入使用的涉密信息系统， 其建设使用单位在按照分级保护要求完成系统整改后，应当向保密工作部门备案。

第三十条 涉密信息系统建设使用单位在申请系统审批或者备案时，应当提交以下材料：

(一)系统设计、实施方案及审查论证意见；

(二)系统承建单位资质证明材料；

(三)系统建设和工程监理情况报告；

(四)系统安全保密检测评估报告;

(五)系统安全保密组织机构和管理制度情况;

(六)其他有关材料。

第三十一条 涉密信息系统发生涉密等级、连接范围、环境设施、主要应用、安全保密管理责任单位变更时，其建设使用单位应当及时向负责审批的保密工作部门报告。保密工作部门应当根据实际情况，决定是否对其重新进行测评和审批。

第三十二条 涉密信息系统建设使用单位应当依据国家保密标准 BMB20-2007《涉及国家秘密的信息系统分级保护管理规范》，加强涉密信息系统运行中的保密管理，定期进行风险评估，消除泄密隐患和漏洞。

第三十三条 国家和地方各级保密工作部门依法对各地区、各部门涉密信息系统分级保护工作实施监督管理，并做好以下工作:

(一)指导、监督和检查分级保护工作的开展;

(二)指导涉密信息系统建设使用单位规范信息定密，合理确定系统保护等级;

(三)参与涉密信息系统分级保护方案论证，指导建设使用单位做好保密设施的同步规划设计;

(四)依法对涉密信息系统集成资质单位进行监督管理;

(五)严格进行系统测评和审批工作，监督检查涉密信息系统建设使用单位分级保护管理制度和技术措施的落实情况;

(六)加强涉密信息系统运行中的保密监督检查。对秘密级、机密级信息系统每两年至少进行一次保密检查或者系统测评，对绝密级信息系统每年至少进行一次保密检查或者系统测评;

(七)了解掌握各级各类涉密信息系统的管理使用情况，及时发现和查处各种违规违法行为和泄密事件。

第五章 信息安全等级保护的密码管理

第三十四条 国家密码管理部门对信息安全等级保护的密码实行分类分级管理。根据被保护对象在国家安全、社会稳定、经济建设中的作用和重要程度， 被保护对象的安全防护要求和涉密程度，被保护对象被破坏后的危害程度以及密码使用部门的性质等，确定密码的等级保护准则。

信息系统运营、使用单位采用密码进行等级保护的， 应当遵照《信息安全等

级保护密码管理办法》、《信息安全等级保护商用密码技术要求》等密码管理规定和相关标准。

第三十五条 信息系统安全等级保护中密码的配备、使用和管理等，应当严格执行国家密码管理的有关规定。

第三十六条 信息系统运营、使用单位应当充分运用密码技术对信息系统进行保护。采用密码对涉及国家秘密的信息和信息系统进行保护的，应报经国家密码管理局审批，密码的设计、实施、使用、运行维护和日常管理等，应当按照国家密码管理有关规定和相关标准执行；采用密码对不涉及国家秘密的信息和信息系统进行保护的，须遵守《商用密码管理条例》和密码分类分级保护有关规定与相关标准，其密码的配备使用情况应当向国家密码管理机构备案。

第三十七条 运用密码技术对信息系统进行系统等级保护建设和整改的，必须采用经国家密码管理部门批准使用或者准于销售的密码产品进行安全保护，不得采用国外引进或者擅自研制的密码产品；未经批准不得采用含有加密功能的进口信息技术产品。

第三十八条 信息系统中的密码及密码设备的测评工作由国家密码管理局认可的测评机构承担，其他任何部门、单位和个人不得对密码进行评测和监控。

第三十九条 各级密码管理部门可以定期或者不定期对信息系统等级保护工作中密码配备、使用和管理的情况进行检查和测评，对重要涉密信息系统的密码配备、使用和管理情况每两年至少进行一次检查和测评。在监督检查过程中，发现存在安全隐患或者违反密码管理相关规定或者未达到密码相关标准要求的，应当按照国家密码管理的相关规定进行处置。

第六章 法律责任

第四十条 第三级以上信息系统运营、使用单位违反本办法规定，有下列行为之一的，由公安机关、国家保密工作部门和国家密码工作管理部门按照职责分工责令其限期改正；逾期不改正的，给予警告，并向其上级主管部门通报情况，建议对其直接负责的主管人员和其他直接责任人员予以处理，并及时反馈处理结果：

(一)未按本办法规定备案、审批的；

(二)未按本办法规定落实安全管理制度、措施的；

(三)未按本办法规定开展系统安全状况检查的;

(四)未按本办法规定开展系统安全技术测评的;

(五)接到整改通知后,拒不整改的;

(六)未按本办法规定选择使用信息安全产品和测评机构的;

(七)未按本办法规定如实提供有关文件和证明材料的;

(八)违反保密管理规定的;

(九)违反密码管理规定的;

(十)违反本办法其他规定的。

违反前款规定,造成严重损害的,由相关部门依照有关法律、法规予以处理。

第四十一条 信息安全监管部门及其工作人员在履行监督管理职责中,玩忽职守、滥用职权、徇私舞弊的, 依法给予行政处分;构成犯罪的,依法追究刑事责任。

第七章 附 则

第四十二条 已运行信息系统的运营、使用单位自本办法施行之日起 180 日内确定信息系统的安全保护等级;新建信息系统在设计、规划阶段确定安全保护等级。

第四十三条 本办法所称“以上”包含本数(级)。

第四十四条 本办法自发布之日起施行,《信息安全等级保护管理办法(试行)》(公通字〔2006〕7 号)同时废止。

关于印发《互联网危险物品信息发布管理规定》的通知

公通字〔2015〕5 号

各省、自治区、直辖市公安厅(局)、互联网信息办、工业和信息化厅、通信管理局、环境保护厅(局)、工商行政管理局、安全生产监督管理局, 新疆生产建设兵团公安局、互联网信息办、工业和信息化局、环境保护局、工商行政管理局、安全生产监督管理局:

为进一步加强对互联网危险物品信息的管理,规范危险物品从业单位信息发布行为,依法查处、打击涉及危险物品违法犯罪活动, 净化网络环境,保障公共安全,公安部、国家互联网信息办公室、工业和信息化部、环境保护部、国家工商行政管理总局、国家安全生产监督管理总局联合制定了《互联网危险物品信息

发布管理规定》，现印发给你们，请结合本地实际，认真贯彻执行。

公安部

国家互联网信息办公室

工业和信息化部

环境保护部

国家工商行政管理总局

国家安全生产监督管理总局

2015 年 2 月 5 日

互联网危险物品信息发布管理规定

第一条 为进一步加强对互联网危险物品信息的管理，规范危险物品从业单位信息发布行为，依法查处、打击涉及危险物品的违法犯罪活动，净化网络环境，保障公共安全，根据《全国人大常委会关于加强网络信息保护的决定》、《全国人大常委会关于维护互联网安全的决定》、《广告法》、《枪支管理法》、《放射性污染防治法》和《民用爆炸物品安全管理条例》、《烟花爆竹安全管理条例》、《危险化学品安全管理条例》、《放射性同位素与射线装置安全和防护条例》、《核材料管制条例》、《互联网信息服务管理办法》等法律、法规和规章，制定本规定。

第二条 本规定所称危险物品，是指枪支弹药、爆炸物品、剧毒化学品、易制爆危险化学品和其他危险化学品、放射性物品、核材料、管制器具等能够危及人身安全和财产安全的物品。

第三条 本规定所称危险物品从业单位，是指依法取得危险物品生产、经营、使用资质的单位以及从事危险物品相关工作的教学、科研、社会团体、中介机构等单位。具体包括：

(一)经公安机关核发《民用枪支(弹药)制造许可证》、《民用枪支(弹药)配售许可证》的民用枪支、弹药制造、配售企业；

(二)经民用爆炸物品行业主管部门核发《民用爆炸物品生产许可证》、《民用爆炸物品销售许可证》的民用爆炸物品生产、销售企业， 经公安机关核发《爆破作业单位许可证》的爆破作业单位；

(三)经安全生产监督管理部门核发《烟花爆竹安全生产许可证》、《烟花爆竹经营(批发)许可证》、《烟花爆竹经营(零售)许可证》的烟花爆竹生产、经营单位；

(四)经安全生产监督管理部门核发《危险化学品安全生产许可证》、《危险化学品经营许可证》、《危险化学品安全使用许可证》的危险化学品生产、经营、使用单位;

(五)经环境保护主管部门核发《辐射安全许可证》的生产、销售、使用放射性同位素和射线装置单位;

(六)经国务院核材料管理部门核发《核材料许可证》的核材料持有、使用、生产、储存、运输和处置单位;

(七)经公安机关批准的弩制造企业、营业性射击场， 经公安机关登记备案的管制刀具制造、销售单位;

(八)从事危险物品教学、科研、服务的高等院校、科研院所、社会团体、中介机构和技术服务企业;

(九)法律、法规规定的其他危险物品从业单位。

第四条 本规定所称危险物品信息，是指在互联网上发布的危险物品生产、经营、储存、使用信息， 包括危险物品种类、性能、用途和危险物品专业服务等相关信息。

第五条 危险物品从业单位从事互联网信息服务的，应当按照《互联网信息服务管理办法》规定， 向电信主管部门申请办理互联网信息服务增值电信业务经营许可或者办理非经营性互联网信息服务备案手续，并按照《计算机信息网络国际联网安全保护管理办法》规定， 持从事危险物品活动的合法资质材料到所在地县级以上人民政府公安机关接受网站安全检查。

第六条 危险物品从业单位依法取得互联网信息服务增值电信业务经营许可或者办理非经营性互联网信息服务备案手续后，可以在本单位网站发布危险物品信息。

禁止个人在互联网上发布危险物品信息。

第七条 接入服务提供者应当与危险物品从业单位签订协议或者确认提供服务，不得为未取得增值电信业务许可或者未办理非经营性互联网信息服务备案手续的危险物品从业单位提供接入服务。

接入服务提供者不得为危险物品从业单位以外的任何单位或者个人提供危险物品信息发布网站接入服务。

第八条 危险物品从业单位应当在本单位网站主页显著位置标明可供查询的互联网信息服务经营许可证编号或者备案编号、从事危险物品活动的合法资质和营业执照等材料。

第九条 危险物品从业单位应当在本单位网站网页显著位置标明单位、个人购买相关危险物品应当具备的资质、资格条件：

(一)购买民用枪支、弹药应当持有省级或者设区的市级人民政府公安机关核发的《民用枪支(弹药)配购证》。

(二)购买民用爆炸物品应当持有国务院民用爆炸物品行业主管部门核发的《民用爆炸物品生产许可证》，或者省级人民政府民用爆炸物品行业主管部门核发的《民用爆炸物品销售许可证》，或者所在地县级人民政府公安机关核发的《民用爆炸物品购买许可证》。

(三)购买烟花爆竹的，批发企业应当持有安全生产监督管理部门核发的《烟花爆竹经营(批发)许可证》；零售单位应当持有安全生产监督管理部门核发的《烟花爆竹经营(零售)许可证》；举办焰火晚会以及其他大型焰火燃放活动的应当持有公安机关核发的《焰火燃放许可证》；个人消费者应当向持有安全生产监督管理部门核发的《烟花爆竹经营(零售)许可证》的零售单位购买。批发企业向烟花爆竹生产企业采购烟花爆竹；零售经营者向烟花爆竹批发企业采购烟花爆竹。严禁零售单位和个人购买专业燃放类烟花爆竹。

(四)购买剧毒化学品应当持有安全生产监督管理部门核发的《危险化学品安全生产许可证》，或者设区的市级人民政府安全生产监督管理部门核发的《危险化学品经营许可证》或者《危险化学品安全使用许可证》，或者县级人民政府公安机关核发的《剧毒化学品购买许可证》。

购买易制爆危险化学品应当持有安全生产监督管理部门核发的《危险化学品安全生产许可证》，或者工业和信息化部核发的《民用爆炸物品生产许可证》，或者设区的市级人民政府安全生产监督管理部门核发的《危险化学品经营许可证》或者《危险化学品安全使用许可证》，或者本单位出具的合法用途证明。

(五)购买放射性同位素的单位应当持有环境保护主管部门核发的《辐射安全许可证》。

(六)购买核材料的单位应当持有国务院核材料管理部门核发的《核材料许可

证》。

(七)购买弩应当持有省级人民政府公安机关批准使用的许可文件。

(八)购买匕首、三棱刮刀应当持有所在单位的批准文件或者证明，且匕首仅限于军人、警察、专业狩猎人员和地质、勘探等野外作业人员购买，三棱刮刀仅限于机械加工单位购买。

(九)法律、法规和相关管理部门的其他规定。

第十条 禁止危险物品从业单位在本单位网站以外的互联网应用服务中发布危险物品信息及建立相关链接。

危险物品从业单位发布的危险物品信息不得包含诱导非法购销危险物品行为的内容。

第十一条 禁止任何单位和个人在互联网上发布危险物品制造方法的信息。

第十二条 网络服务提供者应当加强对接入网站及用户发布信息的管理，定期对发布信息进行巡查，对法律、法规和本规定禁止发布或者传输的危险物品信息，应当立即停止传输，采取消除等处置措施，保存有关记录，并向公安机关等主管部门报告。

第十三条 各级公安、网信、工业和信息化、电信主管、环境保护、工商行政管理、安全监管等部门在各自的职责范围内依法履行职责，完善危险物品从业单位许可、登记备案、信息情况通报和信息发布机制，加强协作配合，共同防范危险物品信息发布的违法犯罪行为。

第十四条 违反规定制作、复制、发布、传播含有危险物品内容的信息，或者故意为制作、复制、发布、传播违法违规危险物品信息提供服务的，依法给予停止联网、停机整顿、吊销许可证或者取消备案、暂时关闭网站直至关闭网站等处罚；构成违反治安管理行为的，依法给予治安管理处罚；构成犯罪的，依法追究刑事责任。

第十五条 任何组织和个人对在互联网上违法违规发布危险物品信息和利用互联网从事走私、贩卖危险物品的违法犯罪行为，有权向有关主管部门举报。接到举报的部门应当依法及时处理，并对举报有功人员予以奖励。

第十六条 本规定自 2015 年 3 月 1 日起执行。

公安部关于印送《贯彻落实网络安全等级保护制度和关键信息基础设施安全保

护制度的指导意见》的函

公网安〔2020〕1960 号

中央和国家机关各部委，国务院各直属机构、办事机构、事业单位，各中央企业：

为深入贯彻党中央有关文件精神和《网络安全法》，指导重点行业、部门全面落实网络安全等级保护制度和关键信息基础设施安全保护制度，健全完善国家网络安全综合防控体系，有效防范网络安全威胁，有力处置重大网络安全事件，配合公安机关加强网络安全监管，严厉打击危害网络安全的违法犯罪活动，切实保障关键信息基础设施、重要网络和数据安全，公安部研究制定了《贯彻落实网络安全等级保护制度和关键信息基础设施安全保护制度的指导意见》。现印送给你们，请结合本行业、本部门工作实际，认真参照执行。

中华人民共和国公安部

2020 年 7 月 22 日

贯彻落实网络安全等级保护制度和关键信息基础设施安全保护制度的指导意见

网络安全等级保护制度和关键信息基础设施安全保护制度是党中央有关文件和《网络安全法》确定的基本制度。近年来，各单位、各部门按照中央网络安全政策要求和《网络安全法》等法律法规规定，全面加强网络安全工作，有力保障了国家关键信息基础设施、重要网络和数据安全。但随着信息技术飞速发展，网络安全工作仍面临一些新形势、新任务和新挑战。为深入贯彻落实网络安全等级保护制度和关键信息基础设施安全保护制度，健全完善国家网络安全综合防控体系，有效防范网络安全威胁，有力处置网络安全事件，严厉打击危害网络安全的违法犯罪活动，切实保障国家网络安全，特制定以下指导意见。

一、指导思想、基本原则和工作目标

(一)指导思想

以习近平新时代中国特色社会主义思想为指导，按照党中央、国务院决策部署，以总体国家安全观为统领，认真贯彻实施网络强国战略，全面加强网络安全工作统筹规划，以贯彻落实网络安全等级保护制度和关键信息基础设施安全保护制度为基础，以保护关键信息基础设施、重要网络和数据安全为重点，

全面加强网络安全防范管理、监测预警、应急处置、侦查打击、情报信息等各项工作，及时监测、处置网络安全风险、威胁和网络安全突发事件，保护关键信息基础设施、重要网络和数据免受攻击、侵入、干扰和破坏，依法惩治网络违法犯罪活动，切实提高网络安全保护能力，积极构建国家网络安全综合防控体系，切实维护国家网络空间主权、国家安全和社会公共利益，保护人民群众的合法权益，保障和促进经济社会信息化健康发展。

(二)基本原则

——坚持分等级保护、突出重点。根据网络(包含网络设施、信息系统、数据资源等)在国家安全、经济建设、社会生活中的重要程度，以及其遭到破坏后的危害程度等因素，科学确定网络的安全保护等级，实施分等级保护、分等级监管，重点保障关键信息基础设施和第三级(含第三级、下同)以上网络的安全。

——坚持积极防御、综合防护。按照法律法规和有关国家标准规范，充分利用人工智能、大数据分析等技术，积极落实网络安全管理和技术防范措施，强化网络安全监测、态势感知、通报预警和应急处置等重点工作，综合采取网络安全保护、保卫、保障措施，防范和遏制重大网络安全风险、事件发生，保护云计算、物联网、新型互联网、大数据、智能制造等新技术应用和新业态安全。

——坚持依法保护、形成合力。依据《网络安全法》等法律法规规定，公安机关依法履行网络安全保卫和监督管理职责，网络安全行业主管部门(含监管部门，下同)依法履行网络安全主管、监管责任，强化和落实网络运营者主体防护责任，充分发挥和调动社会各方力量，协调配合、群策群力，形成网络安全保护工作合力。

(三)工作目标

——网络安全等级保护制度深入贯彻实施。网络安全等级保护定级备案、等级测评、安全建设和检查等基础工作深入推进。网络安全保护“实战化、体系化、常态化”和“动态防御、主动防御、纵深防御、精准防护、整体防控、联防联控”的“三化六防”措施得到有效落实，网络安全保护良好生态基本建立，国家网络安全综合防护能力和水平显著提升。

——关键信息基础设施安全保护制度建立实施。关键信息基础设施底数清晰，安全保护机构健全、职责明确、保障有力。在贯彻落实网络安全等级保护制度的基础上，关键信息基础设施涉及的关键岗位人员管理、供应链安全、数据安全、应急处置等重点安全保护措施得到有效落实，关键信息基础设施安全防护能力明显增强。

——网络安全监测预警和应急处置能力显著提升。跨行业、跨部门、跨地区的立体化网络安全监测体系和网络安全保护平台基本建成，网络安全态势感知、通报预警和事件发现处置能力明显提高。网络安全预案科学齐备，应急处置机制完善，应急演练常态化开展，网络安全重大事件得到有效防范、遏制和处置。

——网络安全综合防控体系基本形成。网络安全保护工作机制健全完善，党委统筹领导、各部门分工负责、社会力量多方参与的网络安全工作格局进一步完善。网络安全责任制得到有效落实，网络安全管理防范、监督指导和侦查打击等能力显著提升，“打防管控”一体化的网络安全综合防控体系基本形成。

二、深入贯彻实施国家网络安全等级保护制度

按照国家网络安全等级保护制度要求，各单位、各部门在公安机关指导监督下，认真组织、深入开展网络安全等级保护工作，建立良好的网络安全保护生态，切实履行主体责任，全面提升网络安全保护能力。

(一)深化网络定级备案工作。网络运营者应全面梳理本单位各类网络，特别是云计算、物联网、新型互联网、大数据、智能制造等新技术应用的基本情况，并根据网络的功能、服务范围、服务对象和处理数据等情况，科学确定网络的安全保护等级，对第二级以上网络依法向公安机关备案，并向行业主管部门报备。对新建网络，应在规划设计阶段确定安全保护等级。公安机关对网络运营者提交的备案材料和网络的安全保护等级进行审核，对定级结果合理、备案材料符合要求的，及时出具网络安全等级保护备案证明。行业主管部门可以依据《网络安全等级保护定级指南》国家标准，结合行业特点制定行业网络安全等级保护定级指导意见。

(二)定期开展网络安全等级测评。网络运营者应依据有关标准规范，对已定级备案网络的安全性进行检测评估，查找可能存在的网络安全问题和隐患。

第三级以上网络运营者应委托符合国家有关规定的等级测评机构，每年开展一次网络安全等级测评，并及时将等级测评报告提交受理备案的公安机关和行业主管部门。新建第三级以上网络应在通过等级测评后投入运行。网络运营者在开展测评服务过程中要与测评机构签署安全保密协议，并对测评过程进行监督管理。公安机关要加强对本地等级测评机构的监督管理，建立测评人员背景审查和人员审核制度，确保等级测评过程客观、公正、安全。

(三)科学开展安全建设整改。网络运营者应在网络建设和运营过程中，同步规划、同步建设、同步使用有关网络安全保护措施。应依据《网络安全等级保护基本要求》《网络安全等级保护安全设计技术要求》等国家标准，在现有安全保护措施的基础上，全面梳理分析安全保护需求，并结合等级测评过程中发现的问题隐患，按照“一个中心(安全管理中心)、三重防护(安全通信网络、安全区域边界、安全计算环境)”的要求，认真开展网络安全建设和整改加固，全面落实安全保护技术措施。网络运营者可将网络迁移上云，或将网络安全服务外包，充分利用云服务商和网络安全服务商提升网络安全保护能力和水平。应全面加强网络安全管理，建立完善人员管理、教育培训、系统安全建设和运维等管理制度，加强机房、设备和介质安全管理，强化重要数据和个人信息保护，制定操作规范和工作流程，加强日常监督和考核，确保各项管理措施有效落实。

(四)强化安全责任落实。行业主管部门、网络运营者应依据《网络安全法》等法律法规和有关政策要求，按照“谁主管谁负责、谁运营谁负责”的原则，厘清网络安全保护边界，明确安全保护工作责任，建立网络安全等级保护工作责任制，落实责任追究制度，作到“守土有责、守土尽责”。网络运营者要定期组织专门力量开展网络安全自查和检测评估，行业主管部门要组织风险评估，及时发现网络安全隐患和薄弱环节并予以整改，不断提高网络安全保护能力和水平。

(五)加强供应链安全管理。网络运营者应加强网络关键人员的安全管理，第三级以上网络运营者应对为其提供设计、建设、运维、技术服务的机构和人员加强管理，评估服务过程中可能存在的安全风险，并采取相应的管控措施。网络运营者应加强网络运维管理，因业务需要确需通过互联网远程运维的，应

进行评估论证，并采取相应的管控措施。网络运营者应采购、使用符合国家法律法规和有关标准规范要求的网络产品及服务，第三级以上网络运营者应积极应用安全可信的网络产品及服务。

(六)落实密码安全防护要求。网络运营者应贯彻落实《密码法》等有关法律法规规定和密码应用相关标准规范。第三级以上网络应正确、有效采用密码技术进行保护，并使用符合相关要求的密码产品和服务。第三级以上网络运营者应在网络规划、建设和运行阶段，按照密码应用安全性评估管理办法和相关标准，在网络安全等级测评中同步开展密码应用安全性评估。

三、建立并实施关键信息基础设施安全保护制度

公安机关指导监督关键信息基础设施安全保护工作。各单位、各部门应加强关键信息基础设施安全的法律体系、政策体系、标准体系、保护体系、保卫体系和保障体系建设，建立并实施关键信息基础设施安全保护制度，在落实网络安全等级保护制度基础上，突出保护重点，强化保护措施，切实维护关键信息基础设施安全。

(一)组织认定关键信息基础设施。根据党中央和公安部有关规定，公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务、国防科技工业等重要行业和领域的主管、监管部门(以下统称保护工作部门)应制定本行业、本领域关键信息基础设施认定规则并报公安部备案。保护工作部门根据认定规则负责组织认定本行业、本领域关键信息基础设施，及时将认定结果通知相关设施运营者并报公安部。应将符合认定条件的基础网络、大型专网、核心业务系统、云平台、大数据平台、物联网、工业控制系统、智能制造系统、新型互联网、新兴通讯设施等重点保护对象纳入关键信息基础设施。关键信息基础设施清单实行动态调整机制，有关网络设施、信息系统发生较大变化，可能影响其认定结果的，运营者应及时将相关情况报告保护工作部门，保护工作部门应组织重新认定，将认定结果通知运营者，并报公安部。

(二)明确关键信息基础设施安全保护工作职能分工。公安部负责关键信息基础设施安全保护工作的顶层设计和规划部署，会同相关部门健全完善关键信息基础设施安全保护制度体系。保护工作部门负责对本行业、本领域关键信息基础设施安全保护工作的组织领导，根据国家网络安全法律法规和有关标准规

范要求，制定并实施本行业、本领域关键信息基础设施安全总体规划和安全防护策略，落实本行业、本领域网络安全指导监督责任。关键信息基础设施运营者负责设置专门安全管理机构，组织开展关键信息基础设施安全保护工作，主要负责人对本单位关键信息基础设施安全保护负总责。

(三)落实关键信息基础设施重点防护措施。关键信息基础设施运营者应依据网络安全等级保护标准开展安全建设并进行等级测评，发现问题和风险隐患要及时整改；依据关键信息基础设施安全保护标准，加强安全保护和保障，并进行安全检测评估。要梳理网络资产，建立资产档案，强化核心岗位人员管理、整体防护、监测预警、应急处置、数据保护等重点保护措施，合理分区分域，收敛互联网暴露面，加强网络攻击威胁管控，强化纵深防御，积极利用新技术开展网络安全保护，构建以密码技术、可信计算、人工智能、大数据分析等为核心的网络安全保护体系，不断提升关键信息基础设施内生安全、主动免疫和主动防御能力。有条件的运营者应组建自己的安全服务机构，承担关键信息基础设施安全保护任务，也可通过迁移上云或购买安全服务等方式，提高网络安全专业化、集约化保障能力。

(四)加强重要数据和个人信息保护。运营者应建立并落实重要数据和个人信息安全保护制度，对关键信息基础设施中的重要网络和数据库进行容灾备份，采取身份鉴别、访问控制、密码保护、安全审计、安全隔离、可信验证等关键技术措施，切实保护重要数据全生命周期安全。运营者在境内运营中收集和产生的个人信息和重要数据应当在境内存储，因业务需要，确需向境外提供的，应当遵守有关规定并进行安全评估。

(五)强化核心岗位人员和产品服务的安全管理。要对专门安全管理机构的负责人和关键岗位人员进行安全背景审查，加强管理。要对关键信息基础设施设计、建设、运行、维护等服务实施安全管理，采购安全可信的网络产品和服务，确保供应链安全。当采购产品和服务可能影响国家安全的，应按照国家有关规定通过安全审查。公安机关加强对关键信息基础设施安全服务机构的安全管理，为运营者开展安全保护工作提供支持。

四、加强网络安全保护工作协作配合

行业主管部门、网络运营者与公安机关要密切协同，大力开展安全监测、

通报预警、应急处置、威胁情报等工作，落实常态化措施，提升应对、处置网络安全突发事件和重大风险防控能力。

(一)加强网络安全立体化监测体系建设。各单位、各部门要全面加强网络安全监测，对关键信息基础设施、重要网络等开展实时监测，发现网络攻击和安全威胁，立即报告公安机关和有关部门并采取有效措施处置。要加强网络新技术研究和应用，研究绘制网络空间地理信息图谱(网络地图)，实现挂图作战。行业主管部门、网络运营要建设本行业、本单位的网络安全保护业务平台，建设平台智慧大脑，依托平台和大数据开展实时监测、通报预警、应急处置、安全防护、指挥调度等工作，并与公安机关有关安全保卫平台对接，形成条块结合、纵横联通、协同联动的综合防控大格局。重点行业、网络运营者和公安机关要建设网络安全监控指挥中心，落实 7×24 小时值班值守制度，建立常态化、实战化的网络安全工作机制。

(二)加强网络安全信息共享和通报预警。行业主管部门、网络运营者要依托国家网络与信息安全信息通报机制，加强本行业、本领域网络安全信息通报预警力量建设，及时收集、汇总、分析各方网络安全信息，加强威胁情报工作，组织开展网络安全威胁分析和态势研判，及时通报预警和处置。第三级以上网络运营者和关键信息基础设施运营者要开展网络安全监测预警和信息通报工作，及时接收、处置来自国家、行业和地方网络安全预警通报信息，按规定向行业主管部门、备案公安机关报送网络安全监测预警信息和网络安全事件。公安机关要加强网络与信息安全信息通报预警机制建设和力量建设，不断提高网络安全通报预警能力。

(三)加强网络安全应急处置机制建设。行业主管部门、网络运营者要按照国家有关要求制定网络安全应急预案，加强网络安全应急力量建设和应急资源储备，与公安机关密切配合，建立网络安全事件报告制度和应急处置机制。关键信息基础设施运营者和第三级以上网络运营者应定期开展应急演练，有效处置网络安全事件，并针对应急演练中发现的突出问题和漏洞隐患，及时整改加固，完善保护措施。行业主管部门、网络运营者应配合公安机关每年组织开展的网络安全监督检查、比武演习等工作，不断提升安全保护能力和对抗能力。

(四)加强网络安全事件处置和案件侦办。关键信息基础设施、第三级以上

网络发生重大网络安全威胁和事件时，行业主管部门、网络运营者和公安机关应联合开展处置。电信业务经营者、网络服务提供者应提供支持及协助。网络运营者应配合公安机关打击网络违法犯罪行为；发现违法犯罪线索、重大网络安全威胁和事件时，应及时报告公安机关和有关部门并提供必要协助。

(五)加强网络安全问题隐患整改督办。公安机关建立挂牌督办制度，针对网络运营者网络安全工作不力、重大安全问题隐患久拖不改，或存在较大网络安全风险、发生重大网络安全案事件的，按照规定的权限和程序，会同行业主管部门对相关负责人进行约谈，挂牌督办，并加大监督检查和行政执法力度，依法依规进行行政处罚。网络运营者应按照有关要求采取措施，及时进行整改，消除重大风险隐患。发生重大网络安全案事件的，行业主管部门应组织全行业开展整改整顿。

五、加强网络安全工作各项保障

(一)加强组织领导。各单位、各部门要高度重视网络安全等级保护和关键信息基础设施安全保护工作，将其列入重要议事日程，加强统筹领导和规划设计，认真研究解决网络安全机构设置、人员配备、经费投入、安全保护措施建设等重大问题。行业主管部门和网络运营者要明确本单位主要负责人是网络安全的第一责任人，并确定一名领导班子成员分管网络安全工作，成立网络安全专门机构，明确任务分工，一级抓一级，层层抓落实。

(二)加强经费政策保障。各单位、各部门要通过现有经费渠道，保障关键信息基础设施、第三级以上网络等开展等级测评、风险评估、密码应用安全性检测、演练竞赛、安全建设整改、安全保护平台建设、密码保障系统建设、运行维护、监督检查、教育培训等经费投入。关键信息基础设施运营者应保障足额的网络安全投入，作出网络安全和信息化有关决策时应有网络安全管理机构人员参与。有关部门要扶持重点网络安全技术产业和项目，支持网络安全技术研究开发和创新应用，推动网络安全产业健康发展。公安机关要会同相关部门组织实施“一带一路”网络安全战略，支持网络安全企业“走出去”，与有关国家共享中国网络安全保护经验。

(三)加强考核评价。各单位、各部门要进一步健全完善网络安全考核评价制度，明确考核指标，组织开展考核。公安机关将网络安全工作纳入社会治安

综合治理考核评价体系，每年组织对各地区网络安全工作进行考核评价，每年评选网络安全等级保护、关键信息基础设施安全保护工作先进单位，并将结果报告党委政府，通报网信部门。

(四)加强技术攻关。各单位、各部门要充分调动网络安全企业、科研机构、专家等社会力量积极参与网络安全核心技术攻关，加强网络安全协同协作、互动互补、共治共享和群防群治。公安机关要会同有关部门加强网络安全等级保护和关键信息基础设施安全保护标准制定工作，出台标准应用指南，加强标准宣贯和应用实施，建设试点示范基地，促进我国网络安全产业和企业的健康发展。

(五)加强人才培养。各单位、各部门要加强网络安全等级保护和关键信息基础设施安全保护业务交流，通过组织开展比武竞赛等形式，发现选拔高精尖技术人才，建设人才库，建立健全人才发现、培养、选拔和使用机制，为做好网络安全工作提供人才保障。

第十章 国家市场监督管理总局

网络交易监督管理办法

(2021 年 3 月 15 日国家市场监督管理总局令第 37 号公布)

第一章 总 则

第一条 为了规范网络交易活动，维护网络交易秩序，保障网络交易各方主体合法权益，促进数字经济持续健康发展，根据有关法律、行政法规，制定本办法。

第二条 在中华人民共和国境内，通过互联网等信息网络(以下简称通过网络)销售商品或者提供服务的经营活动以及市场监督管理部门对其进行监督管理，适用本办法。

在网络社交、网络直播等信息网络活动中销售商品或者提供服务的经营活动，适用本办法。

第三条 网络交易经营者从事经营活动，应当遵循自愿、平等、公平、诚信原则，遵守法律、法规、规章和商业道德、公序良俗，公平参与市场竞争，认真履行法定义务，积极承担主体责任，接受社会各界监督。

第四条 网络交易监督管理坚持鼓励创新、包容审慎、严守底线、线上线下一体化监管的原则。

第五条 国家市场监督管理总局负责组织指导全国网络交易监督管理工作。

县级以上地方市场监督管理部门负责本行政区域内的网络交易监督管理工作。

第六条 市场监督管理部门引导网络交易经营者、网络交易行业组织、消费者组织、消费者共同参与网络交易市场治理，推动完善多元参与、有效协同、规范有序的网络交易市场治理体系。

第二章 网络交易经营者

第一节 一般规定

第七条 本办法所称网络交易经营者，是指组织、开展网络交易活动的自然人、法人和非法人组织，包括网络交易平台经营者、平台内经营者、自建网站经营者以及通过其他网络服务开展网络交易活动的网络交易经营者。

本办法所称网络交易平台经营者，是指在网络交易活动中为交易双方或者多方提供网络经营场所、交易撮合、信息发布等服务，供交易双方或者多方独立开展网络交易活动的法人或者非法人组织。

本办法所称平台内经营者，是指通过网络交易平台开展网络交易活动的网络交易经营者。

网络社交、网络直播等网络服务提供者为经营者提供网络经营场所、商品浏览、订单生成、在线支付等网络交易平台服务的，应当依法履行网络交易平台经营者的义务。通过上述网络交易平台服务开展网络交易活动的经营者，应当依法履行平台内经营者的义务。

第八条 网络交易经营者不得违反法律、法规、国务院决定的规定，从事无证无照经营。除《中华人民共和国电子商务法》第十条规定的不需要进行登记的情形外，网络交易经营者应当依法办理市场主体登记。

个人通过网络从事保洁、洗涤、缝纫、理发、搬家、配制钥匙、管道疏通、家电家具修理修配等依法无须取得许可的便民劳务活动，依照《中华人民共和国电子商务法》第十条的规定不需要进行登记。

个人从事网络交易活动，年交易额累计不超过 10 万元的，依照《中华人民

共和国电子商务法》第十条的规定不需要进行登记。同一经营者在同一平台或者不同平台开设多家网店的，各网店交易额合并计算。个人从事的零星小额交易须依法取得行政许可的，应当依法办理市场主体登记。

第九条 仅通过网络开展经营活动的平台内经营者申请登记为个体工商户的，可以将网络经营场所登记为经营场所，将经常居住地登记为住所，其住所所在地的县、自治县、不设区的市、市辖区市场监督管理部门为其登记机关。同一经营者有两个以上网络经营场所的，应当一并登记。

第十条 平台内经营者申请将网络经营场所登记为经营场所的，由其入驻的网络交易平台为其出具符合登记机关要求的网络经营场所相关材料。

第十一条 网络交易经营者销售的商品或者提供的服务应当符合保障人身、财产安全的要求和环境保护要求，不得销售或者提供法律、行政法规禁止交易，损害国家利益和社会公共利益，违背公序良俗的商品或者服务。

第十二条 网络交易经营者应当在其网站首页或者从事经营活动的主页面显著位置，持续公示经营者主体信息或者该信息的链接标识。鼓励网络交易经营者链接到国家市场监督管理总局电子营业执照亮照系统，公示其营业执照信息。

已经办理市场主体登记的网络交易经营者应当如实公示下列营业执照信息以及与其经营业务有关的行政许可等信息，或者该信息的链接标识：

(一)企业应当公示其营业执照登载的统一社会信用代码、名称、企业类型、法定代表人(负责人)、住所、注册资本(出资额)等信息；

(二)个体工商户应当公示其营业执照登载的统一社会信用代码、名称、经营者姓名、经营场所、组成形式等信息；

(三)农民专业合作社、农民专业合作社联合社应当公示其营业执照登载的统一社会信用代码、名称、法定代表人、住所、成员出资总额等信息。

依照《中华人民共和国电子商务法》第十条规定不需要进行登记的经营者应当根据自身实际经营活动类型，如实公示以下自我声明以及实际经营地址、联系方式等信息，或者该信息的链接标识：

(一)“个人销售自产农副产品，依法不需要办理市场主体登记”；

(二)“个人销售家庭手工业产品，依法不需要办理市场主体登记”；

(三)“个人利用自己的技能从事依法无须取得许可的便民劳务活动，依法不需要办理市场主体登记”；

(四)“个人从事零星小额交易活动，依法不需要办理市场主体登记”。

网络交易经营者公示的信息发生变更的，应当在十个工作日内完成更新公示。

第十三条 网络交易经营者收集、使用消费者个人信息，应当遵循合法、正当、必要的原则，明示收集、使用信息的目的、方式和范围，并经消费者同意。网络交易经营者收集、使用消费者个人信息，应当公开其收集、使用规则，不得违反法律、法规的规定和双方的约定收集、使用信息。

网络交易经营者不得采用一次概括授权、默认授权、与其他授权捆绑、停止安装使用等方式，强迫或者变相强迫消费者同意收集、使用与经营活动无直接关系的信息。收集、使用个人生物特征、医疗健康、金融账户、个人行踪等敏感信息的，应当逐项取得消费者同意。

网络交易经营者及其工作人员应当对收集的个人信息严格保密，除依法配合监管执法活动外，未经被收集者授权同意，不得向包括关联方在内的任何第三方提供。

第十四条 网络交易经营者不得违反《中华人民共和国反不正当竞争法》等规定，实施扰乱市场竞争秩序，损害其他经营者或者消费者合法权益的不正当竞争行为。

网络交易经营者不得以下列方式，作虚假或者引人误解的商业宣传，欺骗、误导消费者：

(一)虚构交易、编造用户评价；

(二)采用误导性展示等方式，将好评前置、差评后置，或者不显著区分不同商品或者服务的评价等；

(三)采用谎称现货、虚构预订、虚假抢购等方式进行虚假营销；

(四)虚构点击量、关注度等流量数据，以及虚构点赞、打赏等交易互动数据。

网络交易经营者不得实施混淆行为，引人误认为是他人商品、服务或者与他人存在特定联系。

网络交易经营者不得编造、传播虚假信息或者误导性信息，损害竞争对手的商业信誉、商品声誉。

第十五条 消费者评价中包含法律、行政法规、规章禁止发布或者传输的信息的，网络交易经营者可以依法予以技术处理。

第十六条 网络交易经营者未经消费者同意或者请求，不得向其发送商业性信息。

网络交易经营者发送商业性信息时，应当明示其真实身份和联系方式，并向消费者提供显著、简便、免费的拒绝继续接收的方式。消费者明确表示拒绝的，应当立即停止发送，不得更换名义后再次发送。

第十七条 网络交易经营者以直接捆绑或者提供多种可选项方式向消费者搭售商品或者服务的，应当以显著方式提醒消费者注意。提供多种可选项方式的，不得将搭售商品或者服务的任何选项设定为消费者默认同意，不得将消费者以往交易中选择的选项在后续独立交易中设定为消费者默认选择。

第十八条 网络交易经营者采取自动展期、自动续费等方式提供服务的，应当在消费者接受服务前和自动展期、自动续费等日期前五日，以显著方式提请消费者注意，由消费者自主选择；在服务期间内，应当为消费者提供显著、简便的随时取消或者变更的选项，并不得收取不合理费用。

第十九条 网络交易经营者应当全面、真实、准确、及时地披露商品或者服务信息，保障消费者的知情权和选择权。

第二十条 通过网络社交、网络直播等网络服务开展网络交易活动的网络交易经营者，应当以显著方式展示商品或者服务及其实际经营主体、售后服务等信息，或者上述信息的链接标识。

网络直播服务提供者对网络交易活动的直播视频保存时间自直播结束之日起不少于三年。

第二十一条 网络交易经营者向消费者提供商品或者服务使用格式条款、通知、声明等的，应当以显著方式提请消费者注意与消费者有重大利害关系的内容，并按照消费者的要求予以说明，不得作出含有下列内容的规定：

(一)免除或者部分免除网络交易经营者对其所提供的商品或者服务应当承担的修理、重作、更换、退货、补足商品数量、退还货款和服务费用、赔偿损

失等责任；

(二)排除或者限制消费者提出修理、更换、退货、赔偿损失以及获得违约金和其他合理赔偿的权利；

(三)排除或者限制消费者依法投诉、举报、请求调解、申请仲裁、提起诉讼的权利；

(四)排除或者限制消费者依法变更或者解除合同的权利；

(五)规定网络交易经营者单方享有解释权或者最终解释权；

(六)其他对消费者不公平、不合理的规定。

第二十二条 网络交易经营者应当按照国家市场监督管理总局及其授权的省级市场监督管理部门的要求，提供特定时段、特定品类、特定区域的商品或者服务的价格、销量、销售额等数据信息。

第二十三条 网络交易经营者自行终止从事网络交易活动的，应当提前三十日在其网站首页或者从事经营活动的主页面显著位置，持续公示终止网络交易活动公告等有关信息，并采取合理、必要、及时的措施保障消费者和相关经营者的合法权益。

第二节 网络交易平台经营者

第二十四条 网络交易平台经营者应当要求申请进入平台销售商品或者提供服务的经营者提交其身份、地址、联系方式、行政许可等真实信息，进行核验、登记，建立登记档案，并至少每六个月核验更新一次。

网络交易平台经营者应当对未办理市场主体登记的平台内经营者进行动态监测，对超过本办法第八条第三款规定额度的，及时提醒其依法办理市场主体登记。

第二十五条 网络交易平台经营者应当依照法律、行政法规的规定，向市场监督管理部门报送有关信息。

网络交易平台经营者应当分别于每年 1 月和 7 月向住所地省级市场监督管理部门报送平台内经营者的下列身份信息：

(一)已办理市场主体登记的平台内经营者的名称(姓名)、统一社会信用代码、实际经营地址、联系方式、网店名称以及网址链接等信息；

(二)未办理市场主体登记的平台内经营者的姓名、身份证件号码、实际经

营地址、联系方式、网店名称以及网址链接、属于依法不需要办理市场主体登记的具体情形的自我声明等信息；其中，对超过本办法第八条第三款规定额度的平台内经营者进行特别标示。

鼓励网络交易平台经营者与市场监督管理部门建立开放数据接口等形式的自动化信息报送机制。

第二十六条 网络交易平台经营者应当为平台内经营者依法履行信息公示义务提供技术支持。平台内经营者公示的信息发生变更的，应当在三个工作日内将变更情况报送平台，平台应当在七个工作日内进行核验，完成更新公示。

第二十七条 网络交易平台经营者应当以显著方式区分标记已办理市场主体登记的经营者和未办理市场主体登记的经营者，确保消费者能够清晰辨认。

第二十八条 网络交易平台经营者修改平台服务协议和交易规则的，应当完整保存修改后的版本生效之日前三年的全部历史版本，并保证经营者和消费者能够便利、完整地阅览和下载。

第二十九条 网络交易平台经营者应当对平台内经营者及其发布的商品或者服务信息建立检查监控制度。网络交易平台经营者发现平台内的商品或者服务信息有违反市场监督管理法律、法规、规章，损害国家利益和社会公共利益，违背公序良俗的，应当依法采取必要的处置措施，保存有关记录，并向平台住所地县级以上市场监督管理部门报告。

第三十条 网络交易平台经营者依据法律、法规、规章的规定或者平台服务协议和交易规则对平台内经营者违法行为采取警示、暂停或者终止服务等处理措施的，应当自决定作出处理措施之日起一个工作日内予以公示，载明平台内经营者的网店名称、违法行为、处理措施等信息。警示、暂停服务等短期处理措施的相关信息应当持续公示至处理措施实施期满之日止。

第三十一条 网络交易平台经营者对平台内经营者身份信息的保存时间自其退出平台之日起不少于三年；对商品或者服务信息，支付记录、物流快递、退换货以及售后等交易信息的保存时间自交易完成之日起不少于三年。法律、行政法规另有规定的，依照其规定。

第三十二条 网络交易平台经营者不得违反《中华人民共和国电子商务法》第三十五条的规定，对平台内经营者在平台内的交易、交易价格以及与其他经

营者的交易等进行不合理限制或者附加不合理条件，干涉平台内经营者的自主经营。具体包括：

(一)通过搜索降权、下架商品、限制经营、屏蔽店铺、提高服务收费等方式，禁止或者限制平台内经营者自主选择在多个平台开展经营活动，或者利用不正当手段限制其仅在特定平台开展经营活动；

(二)禁止或者限制平台内经营者自主选择快递物流等交易辅助服务提供者；

(三)其他干涉平台内经营者自主经营的行为。

第三章 监督管理

第三十三条 县级以上地方市场监督管理部门应当在日常管理和执法活动中加强协同配合。

网络交易平台经营者住所地省级市场监督管理部门应当根据工作需要，及时将掌握的平台内经营者身份信息与其实际经营地的省级市场监督管理部门共享。

第三十四条 市场监督管理部门在依法开展监督检查、案件调查、事故处置、缺陷消费品召回、消费争议处理等监管执法活动时，可以要求网络交易平台经营者提供有关的平台内经营者身份信息，商品或者服务信息，支付记录、物流快递、退换货以及售后等交易信息。网络交易平台经营者应当提供，并在技术方面积极配合市场监督管理部门开展网络交易违法行为监测工作。

为网络交易经营者提供宣传推广、支付结算、物流快递、网络接入、服务器托管、虚拟主机、云服务、网站网页设计制作等服务的经营者(以下简称其他服务提供者)，应当及时协助市场监督管理部门依法查处网络交易违法行为，提供其掌握的有关数据信息。法律、行政法规另有规定的，依照其规定。

市场监督管理部门发现网络交易经营者有违法行为，依法要求网络交易平台经营者、其他服务提供者采取措施制止的，网络交易平台经营者、其他服务提供者应当予以配合。

第三十五条 市场监督管理部门对涉嫌违法的网络交易行为进行查处时，可以依法采取下列措施：

(一)对与涉嫌违法的网络交易行为有关的场所进行现场检查；

(二)查阅、复制与涉嫌违法的网络交易行为有关的合同、票据、账簿等有关资料;

(三)收集、调取、复制与涉嫌违法的网络交易行为有关的电子数据;

(四)询问涉嫌从事违法的网络交易行为的当事人;

(五)向与涉嫌违法的网络交易行为有关的自然人、法人和非法人组织调查了解有关情况;

(六)法律、法规规定可以采取的其他措施。

采取前款规定的措施,依法需要报经批准的,应当办理批准手续。

市场监督管理部门对网络交易违法行为的技术监测记录资料,可以作为实施行政处罚或者采取行政措施的电子数据证据。

第三十六条 市场监督管理部门应当采取必要措施保护网络交易经营者提供的数据信息的安全,并对其中的个人信息、隐私和商业秘密严格保密。

第三十七条 市场监督管理部门依法对网络交易经营者实施信用监管,将网络交易经营者的注册登记、备案、行政许可、抽查检查结果、行政处罚、列入经营异常名录和严重违法失信企业名单等信息,通过国家企业信用信息公示系统统一归集并公示。对存在严重违法失信行为的,依法实施联合惩戒。

前款规定的信息还可以通过市场监督管理部门官方网站、网络搜索引擎、经营者从事经营活动的主页面显著位置等途径公示。

第三十八条 网络交易经营者未依法履行法定责任和义务,扰乱或者可能扰乱网络交易秩序,影响消费者合法权益的,市场监督管理部门可以依职责对其法定代表人或者主要负责人进行约谈,要求其采取措施进行整改。

第四章 法律责任

第三十九条 法律、行政法规对网络交易违法行为的处罚已有规定的,依照其规定。

第四十条 网络交易平台经营者违反本办法第十条,拒不为入驻的平台内经营者出具网络经营场所相关材料的,由市场监督管理部门责令限期改正;逾期不改正的,处一万元以上三万元以下罚款。

第四十一条 网络交易经营者违反本办法第十一条、第十三条、第十六条、第十八条,法律、行政法规有规定的,依照其规定;法律、行政法规没有规定

的，由市场监督管理部门依职责责令限期改正，可以处五千元以上三万元以下罚款。

第四十二条 网络交易经营者违反本办法第十二条、第二十三条，未履行法定信息公示义务的，依照《中华人民共和国电子商务法》第七十六条的规定进行处罚。对其中的网络交易平台经营者，依照《中华人民共和国电子商务法》第八十一条第一款的规定进行处罚。

第四十三条 网络交易经营者违反本办法第十四条的，依照《中华人民共和国反不正当竞争法》的相关规定进行处罚。

第四十四条 网络交易经营者违反本办法第十七条的，依照《中华人民共和国电子商务法》第七十七条的规定进行处罚。

第四十五条 网络交易经营者违反本办法第二十条，法律、行政法规有规定的，依照其规定；法律、行政法规没有规定的，由市场监督管理部门责令限期改正；逾期不改正的，处一万元以下罚款。

第四十六条 网络交易经营者违反本办法第二十二条的，由市场监督管理部门责令限期改正；逾期不改正的，处五千元以上三万元以下罚款。

第四十七条 网络交易平台经营者违反本办法第二十四条第一款、第二十五条第二款、第三十一条，不履行法定核验、登记义务，有关信息报送义务，商品和服务信息、交易信息保存义务的，依照《中华人民共和国电子商务法》第八十条的规定进行处罚。

第四十八条 网络交易平台经营者违反本办法第二十七条、第二十八条、第三十条的，由市场监督管理部门责令限期改正；逾期不改正的，处一万元以上三万元以下罚款。

第四十九条 网络交易平台经营者违反本办法第二十九条，法律、行政法规有规定的，依照其规定；法律、行政法规没有规定的，由市场监督管理部门依职责责令限期改正，可以处一万元以上三万元以下罚款。

第五十条 网络交易平台经营者违反本办法第三十二条的，依照《中华人民共和国电子商务法》第八十二条的规定进行处罚。

第五十一条 网络交易经营者销售商品或者提供服务，不履行合同义务或者履行合同义务不符合约定，或者造成他人损害的，依法承担民事责任。

第五十二条 网络交易平台经营者知道或者应当知道平台内经营者销售的商品或者提供的服务不符合保障人身、财产安全的要求，或者有其他侵害消费者合法权益行为，未采取必要措施的，依法与该平台内经营者承担连带责任。

对关系消费者生命健康的商品或者服务，网络交易平台经营者对平台内经营者的资质资格未尽到审核义务，或者对消费者未尽到安全保障义务，造成消费者损害的，依法承担相应的责任。

第五十三条 对市场监督管理部门依法开展的监管执法活动，拒绝依照本办法规定提供有关材料、信息，或者提供虚假材料、信息，或者隐匿、销毁、转移证据，或者有其他拒绝、阻碍监管执法行为，法律、行政法规、其他市场监督管理部门规章有规定的，依照其规定；法律、行政法规、其他市场监督管理部门规章没有规定的，由市场监督管理部门责令改正，可以处五千元以上三万元以下罚款。

第五十四条 市场监督管理部门的工作人员，玩忽职守、滥用职权、徇私舞弊，或者泄露、出售或者非法向他人提供在履行职责中所知悉的个人信息、隐私和商业秘密的，依法追究法律责任。

第五十五条 违反本办法规定，构成犯罪的，依法追究刑事责任。

第五章 附 则

第五十六条 本办法自 2021 年 5 月 1 日起施行。2014 年 1 月 26 日原国家工商行政管理总局令第 60 号公布的《网络交易管理办法》同时废止。

关于开展 App 安全认证工作的公告

市场监管总局、中央网信办公告 2019 年第 11 号

为规范移动互联网应用程序(以下称 App)收集、使用用户信息特别是个人信息的行为，加强个人信息安全保护，根据《中华人民共和国网络安全法》《中华人民共和国认证认可条例》，市场监管总局、中央网信办决定开展 App 安全认证工作。现将有关事项公告如下：

一、App 安全认证活动依据《移动互联网应用程序(App)安全认证实施规则》(见附件)开展。

二、从事 App 安全认证的认证机构为中国网络安全审查技术与认证中心，检测机构由认证机构根据认证业务需要和技术能力确定。

三、认证机构和检测机构应按有关规定，客观、公正地开展认证和检测活动，并对认证和检测结果负责。

四、国家鼓励 App 运营者自愿通过 App 安全认证，鼓励搜索引擎、应用商店等明确标识并优先推荐通过认证的 App。

附件：移动互联网应用程序(App)安全认证实施规则

市场监管总局

中央网信办

2019 年 3 月 13 日

关于开展网络安全服务认证工作的实施意见

国市监认证规〔2023〕3 号

各省、自治区、直辖市和新疆生产建设兵团市场监管局(厅、委)、党委网信办、工业和信息化主管部门、公安厅(局)，各省、自治区、直辖市通信管理局，各有关单位：

为推进网络安全服务认证体系建设，提升网络安全服务机构能力水平和服务质量，根据《网络安全法》《认证认可条例》，市场监管总局、中央网信办、工业和信息化部、公安部就开展国家统一推行的网络安全服务认证工作提出以下意见。

一、网络安全服务认证工作坚持“统一管理、共同实施、统一标准、规范有序”的基本原则。市场监管总局、中央网信办、工业和信息化部、公安部根据职责，加强认证工作的组织实施和监督管理，鼓励网络运营者等广泛采信网络安全服务认证结果，促进网络安全服务产业健康有序发展。

二、网络安全服务认证目录由市场监管总局会同中央网信办、工业和信息化部、公安部根据市场需求和产业发展状况确定并适时调整，现阶段包括检测评估、安全运维、安全咨询和等级保护测评等服务类别。认证规则和认证标志由市场监管总局征求中央网信办、工业和信息化部、公安部意见后另行制定发布。

三、市场监管总局、中央网信办、工业和信息化部、公安部联合组建由政府部门、科研机构、认证机构、标准化机构、网络安全服务机构和用户等相关方参与的网络安全服务认证技术委员会，协调解决认证体系建设和实施过程中

出现的技术问题，研究提出认证目录、认证规则编写修订工作建议等。

四、从事网络安全服务认证活动的认证机构应当依法设立，符合《认证认可条例》《认证机构管理办法》规定的基本条件，具备从事网络安全服务认证活动的专业能力，并经市场监管总局根据各部门职责征求中央网信办、工业和信息化部、公安部意见后批准取得资质。

五、网络安全服务认证机构应当根据认证委托人提出的认证委托，按照网络安全服务认证基本规范、认证规则开展认证工作，建立可追溯工作机制对认证全过程完整记录。

六、网络安全服务认证机构应当公开认证收费标准和认证证书有效、暂停、注销或者撤销等状态，并按照有关规定报送网络安全服务认证实施情况及认证证书信息。

七、通过认证的网络安全服务机构应当按照有关法律法规、标准规范等开展网络安全服务工作，确保持续符合认证要求。

八、市场监管部门负责对网络安全服务认证机构、认证活动和认证结果进行监督管理，依法查处认证违法行为。

九、网信部门、工业和信息化部门、公安部门依据各自职责，推动认证结果采信应用，加强网络安全服务监督管理，促进网络安全服务产业发展，依法查处有关违法行为。

国家市场监督管理总局

中央网络安全和信息化委员会办公室

工业和信息化部

公安部

2023 年 3 月 15 日

第十一章 国家金融监督管理总局(银保监会)

银行保险机构消费者权益保护管理办法

(2022 年 12 月 26 日中国银行保险监督管理委员会令 2022 年第 9 号公布 自 2023 年 3 月 1 日起施行)

第一章 总 则

第一条 为维护公平公正的金融市场环境，切实保护银行业保险业消费者合法权益，促进行业高质量健康发展，根据《中华人民共和国银行业监督管理法》《中华人民共和国商业银行法》《中华人民共和国保险法》《中华人民共和国消费者权益保护法》等法律法规，制定本办法。

第二条 本办法所称银行保险机构，是指在中华人民共和国境内依法设立的向消费者提供金融产品或服务的银行业金融机构和保险机构。

第三条 银行保险机构承担保护消费者合法权益的主体责任。银行保险机构应当通过适当程序和措施，在业务经营全过程公平、公正和诚信对待消费者。

第四条 消费者应当诚实守信，理性消费，审慎投资，依法维护自身合法权益。

第五条 中国银行保险监督管理委员会(以下简称银保监会)及其派出机构依法对银行保险机构消费者权益保护行为实施监督管理。

第六条 银行保险机构消费者权益保护应当遵循依法合规、平等自愿、诚实守信的原则。

第二章 工作机制与管理要求

第七条 银行保险机构应当将消费者权益保护纳入公司治理、企业文化建设和经营发展战略，建立健全消费者权益保护体制机制，将消费者权益保护要求贯穿业务流程各环节。

第八条 银行保险机构董事会承担消费者权益保护工作的最终责任，对消费者权益保护工作进行总体规划和指导，董事会应当设立消费者权益保护委员会。高级管理层应当建立健全消费者权益保护管理体系，确保消费者权益保护目标和政策得到有效执行。监事会应当对董事会、高级管理层消费者权益保护工作履职情况进行监督。

银行保险机构应当明确履行消费者权益保护职责的部门，由其牵头组织并督促指导各部门开展消费者权益保护工作。

第九条 银行保险机构应当建立消费者权益保护审查机制，健全审查工作制度，对面向消费者提供的产品和服务在设计开发、定价管理、协议制定、营销宣传等环节进行消费者权益保护审查，从源头上防范侵害消费者合法权益行为发生。推出新产品和服务或者现有产品和服务涉及消费者利益的条款发生重大

变化时，应当开展审查。

第十条 银行保险机构应当建立完善消费者权益保护信息披露机制，遵循真实性、准确性、完整性和及时性原则，在售前、售中、售后全流程披露产品和服务关键信息。

银行保险机构应当通过年报等适当方式，将消费者权益保护工作开展情况定期向公众披露。

第十一条 银行保险机构应当建立消费者适当性管理机制，对产品的风险进行评估并实施分级、动态管理，开展消费者风险认知、风险偏好和风险承受能力测评，将合适的产品提供给合适的消费者。

第十二条 银行保险机构应当按照相关规定建立销售行为可回溯管理机制，对产品和服务销售过程进行记录和保存，利用现代信息技术，提升可回溯管理便捷性，实现关键环节可回溯、重要信息可查询、问题责任可确认。

第十三条 银行保险机构应当建立消费者个人信息保护机制，完善内部管理制度、分级授权审批和内部控制措施，对消费者个人信息实施全流程分级分类管控，有效保障消费者个人信息安全。

第十四条 银行保险机构应当建立合作机构名单管理机制，对涉及消费者权益的合作事项，设定合作机构准入和退出标准，并加强对合作机构的持续管理。在合作协议中应当明确双方关于消费者权益保护的责任和义务，包括但不限于信息安全管控、服务价格管理、服务连续性、信息披露、纠纷解决机制、违约责任承担和应急处置等内容。

第十五条 银行保险机构应当建立健全投诉处理工作机制，畅通投诉渠道，规范投诉处理流程，加强投诉统计分析，不断溯源整改，切实履行投诉处理主体责任。

第十六条 银行保险机构应当健全矛盾纠纷多元化解配套机制，积极主动与消费者协商解决矛盾纠纷，在协商不成的情况下，通过调解、仲裁、诉讼等方式促进矛盾纠纷化解。

消费者向银行业保险业纠纷调解组织请求调解的，银行保险机构无正当理由不得拒绝参加调解。

第十七条 银行保险机构应当建立消费者权益保护内部培训机制，对从业人

员开展消费者权益保护培训，提升培训效能，强化员工消费者权益保护意识。

第十八条 银行保险机构应当完善消费者权益保护内部考核机制，建立消费者权益保护内部考核制度，对相关部门和分支机构的工作进行评估和考核。

银行保险机构应当将消费者权益保护内部考核纳入综合绩效考核体系，合理分配权重，并纳入人力资源管理体系和问责体系，充分发挥激励约束作用。

第十九条 银行保险机构应当建立常态化、规范化的消费者权益保护内部审计机制，制定消费者权益保护审计方案，将消费者权益保护工作纳入年度审计范围，以 5 年为一个周期全面覆盖本机构相关部门和一级分支机构。

第三章 保护消费者知情权、自主选择权和公平交易权

第二十条 银行保险机构应当优化产品设计，对新产品履行风险评估和审批程序，充分评估客户可能承担的风险，准确评定产品风险等级。

第二十一条 银行保险机构应当保障消费者的知情权，使用通俗易懂的语言和有利于消费者接收、理解的方式进行产品和服务信息披露。对产品和服务信息的专业术语进行解释说明，及时、真实、准确揭示风险。

第二十二条 银行保险机构应当以显著方式向消费者披露产品和服务的性质、利息、收益、费用、费率、主要风险、违约责任、免责条款等可能影响消费者重大决策的关键信息。贷款类产品应当明示年化利率。

第二十三条 银行保险机构不得进行欺诈、隐瞒或者误导性的宣传，不得作夸大产品收益或者服务权益、掩饰产品风险等虚假或者引人误解的宣传。

第二十四条 银行业金融机构应当根据业务性质，完善服务价格管理体系，按照服务价格管理相关规定，在营业场所、网站主页等醒目位置公示服务项目、服务内容和服务价格等信息。新设收费服务项目或者提高服务价格的，应当提前公示。

第二十五条 银行保险机构不得允许第三方合作机构在营业网点或者自营网络平台以银行保险机构的名义向消费者推介或者销售产品和服务。

第二十六条 银行保险机构销售产品或者提供服务的过程中，应当保障消费者自主选择权，不得存在下列情形：

(一)强制捆绑、强制搭售产品或者服务；

(二)未经消费者同意，单方为消费者开通收费服务；

(三)利用业务便利，强制指定第三方合作机构为消费者提供收费服务；

(四)采用不正当手段诱使消费者购买其他产品；

(五)其他侵害消费者自主选择权的情形。

第二十七条 银行保险机构向消费者提供产品和服务时，应当确保风险收益匹配、定价合理、计量正确。

在提供相同产品和服务时，不得对具有同等交易条件或者风险状况的消费者实行不公平定价。

第二十八条 银行保险机构应当保障消费者公平交易权，不得存在下列情形：

(一)在格式合同中不合理地加重消费者责任、限制或者排除消费者合法权利；

(二)在格式合同中不合理地减轻或者免除本机构义务或者损害消费者合法权益应当承担的责任；

(三)从贷款本金中预先扣除利息；

(四)在协议约定的产品和服务收费外，以向第三方支付咨询费、佣金等名义变相向消费者额外收费；

(五)限制消费者寻求法律救济；

(六)其他侵害消费者公平交易权的情形。

第四章 保护消费者财产安全权和依法求偿权

第二十九条 银行保险机构应当审慎经营，保障消费者财产安全权，采取有效的内控措施和监控手段，严格区分自身资产与消费者资产，不得挪用、占用消费者资金。

第三十条 银行保险机构应当合理设计业务流程和操作规范，在办理业务过程中落实消费者身份识别和验证，不得为伪造、冒用他人身份的客户开立账户。

第三十一条 银行保险机构应当严格区分公募和私募资产管理产品，严格审核投资者资质，不得组织、诱导多个消费者采取归集资金的方式满足购买私募资产管理产品的条件。

资产管理产品管理人应当强化受托管理责任，诚信、谨慎履行管理义务。

第三十二条 保险公司应当勤勉尽责，收到投保人的保险要求后，及时审慎审核投保人提供的保险标的或者被保险人的有关情况。

保险公司应当对核保、理赔的规则和标准实行版本管理，不得在保险事故发生后以不同于核保时的标准重新对保险标的或者被保险人的有关情况进行审核。

第三十三条 保险公司收到被保险人或者受益人的赔偿或者给付保险金的请求后，应当依照法律法规和合同约定及时作出处理，不得拖延理赔、无理拒赔。

第五章 保护消费者受教育权和受尊重权

第三十四条 银行保险机构应当开展金融知识教育宣传，加强教育宣传的针对性，通过消费者日常教育与集中教育活动，帮助消费者了解金融常识和金融风险，提升消费者金融素养。

第三十五条 金融知识教育宣传应当坚持公益性，不得以营销、推介行为替代金融知识普及与消费者教育。银行保险机构应当建立多元化金融知识教育宣传渠道，在官方网站、移动互联网应用程序、营业场所设立公益性金融知识普及和教育专区。

第三十六条 银行保险机构应当加强诚信教育与诚信文化建设，构建诚信建设长效机制，培育行业的信用意识，营造诚实、公平、守信的信用环境。

第三十七条 银行保险机构应当不断提升服务质量，融合线上线下，积极提供高品质、便民化金融服务。提供服务过程中，应当尊重消费者的人格尊严和民族风俗习惯，不得进行歧视性差别对待。

第三十八条 银行保险机构应当积极融入老年友好型社会建设，优化网点布局，尊重老年人使用习惯，保留和改进人工服务，不断丰富适老化产品和服务。

第三十九条 银行保险机构应当充分保障残障人士公平获得金融服务的权利，加快线上渠道无障碍建设，提供更加细致和人性化的服务。有条件的营业网点应当提供无障碍设施和服务，更好满足残障人士日常金融服务需求。

第四十条 银行保险机构应当规范营销行为，通过电话呼叫、信息群发、网络推送等方式向消费者发送营销信息的，应当向消费者提供拒收或者退订选

择。消费者拒收或者退订的，不得以同样方式再次发送营销信息。

第四十一条 银行保险机构应当规范催收行为，依法依规督促债务人清偿债务。加强催收外包业务管理，委托外部机构实施催收前，应当采取适当方式告知债务人。

银行保险机构自行或者委托外部机构催收过程中不得存在下列情形：

(一)冒用行政机关、司法机关等名义实施催收；

(二)采取暴力、恐吓、欺诈等不正当手段实施催收；

(三)采用其他违法违规和违背公序良俗的手段实施催收。

第六章 保护消费者信息安全权

第四十二条 银行保险机构处理消费者个人信息，应当坚持合法、正当、必要、诚信原则，切实保护消费者信息安全权。

第四十三条 银行保险机构收集消费者个人信息应当向消费者告知收集使用的目的、方式和范围等规则，并经消费者同意，法律法规另有规定的除外。消费者不同意的，银行保险机构不得因此拒绝提供不依赖于其所拒绝授权信息的金融产品或服务。

银行保险机构不得采取变相强制、违规购买等不正当方式收集使用消费者个人信息。

第四十四条 对于使用书面形式征求个人信息处理同意的，银行保险机构应当以醒目的方式、清晰易懂的语言明示与消费者存在重大利害关系的内容。

银行保险机构通过线上渠道使用格式条款获取个人信息授权的，不得设置默认同意的选项。

第四十五条 银行保险机构应当在消费者授权同意等基础上与合作方处理消费者个人信息，在合作协议中应当约定数据保护责任、保密义务、违约责任、合同终止和突发情况下的处置条款。

合作过程中，银行保险机构应当严格控制合作方行为与权限，通过加密传输、安全隔离、权限管控、监测报警、去标识化等方式，防范数据滥用或者泄露风险。

第四十六条 银行保险机构应当督促和规范与其合作的互联网平台企业有效保护消费者个人信息，未经消费者同意，不得在不同平台间传递消费者个人信

息，法律法规另有规定的除外。

第四十七条 银行保险机构处理和使用个人信息的业务和信息系统，遵循权责对应、最小必要原则设置访问、操作权限，落实授权审批流程，实现异常操作行为的有效监控和干预。

第四十八条 银行保险机构应当加强从业人员行为管理，禁止违规查询、下载、复制、存储、篡改消费者个人信息。从业人员不得超出自身职责和权限非法处理和使用消费者个人信息。

第七章 监督管理

第四十九条 银保监会及其派出机构依法履行消费者权益保护监管职责，通过采取监管措施和手段，督促银行保险机构切实保护消费者合法权益。严格行为监管要求，对经营活动中的同类业务、同类主体统一标准、统一裁量，依法打击侵害消费者权益乱象和行为，营造公平有序的市场环境。

第五十条 银行保险机构发生涉及消费者权益问题的重大事件，应当根据属地监管原则，及时向银保监会或其派出机构消费者权益保护部门报告。

重大事件是指银行保险机构因消费者权益保护工作不到位或者发生侵害消费者权益行为导致大量集中投诉、引发群体性事件或者造成重大负面舆情等。

第五十一条 各类银行业保险业行业协会以及各地方行业社团组织应当通过行业自律、维权、协调及宣传等方式，指导会员单位提高消费者权益保护水平，妥善化解矛盾纠纷，维护行业良好形象。

第五十二条 银保监会及其派出机构指导设立银行业保险业纠纷调解组织，监督银行业保险业消费纠纷调解机制的有效运行。

银行业保险业纠纷调解组织应当优化治理结构，建章立制，提升调解效能，通过线上、现场、电话等途径，及时高效化解纠纷。

第五十三条 银保监会及其派出机构对银行保险机构消费者权益保护工作中存在的问题，视情节轻重依法采取相应监管措施，包括但不限于：

(一)监管谈话；

(二)责令限期整改；

(三)下发风险提示函、监管意见书等；

(四)责令对直接负责的董事、高级管理人员和其他直接责任人员进行内部

问责；

(五)责令暂停部分业务，停止批准开办新业务；

(六)将相关问题在行业内通报或者向社会公布；

(七)职责范围内依法可以采取的其他措施。

第五十四条 银行保险机构以及从业人员违反本办法规定的，由银保监会及其派出机构依据《中华人民共和国银行业监督管理法》《中华人民共和国商业银行法》《中华人民共和国保险法》《中华人民共和国消费者权益保护法》等法律法规实施行政处罚。法律、行政法规没有规定，但违反本办法的，由银保监会及其派出机构责令改正；情节严重或者逾期不改正的，区分不同情形，给予以下行政处罚：

(一)通报批评；

(二)警告；

(三)处以 10 万元以下罚款。

银行保险机构存在严重侵害消费者合法权益行为，且涉及人数多、涉案金额大、持续时间长、社会影响恶劣的，银保监会及其派出机构除按前款规定处理外，可对相关董事会成员及高级管理人员给予警告，并处以 10 万元以下罚款。

银行保险机构以及从业人员涉嫌犯罪的，依法移交司法机关追究其刑事责任。

第八章 附 则

第五十五条 本办法所称银行业金融机构是指商业银行、农村信用合作社等吸收公众存款的金融机构以及信托公司、消费金融公司、汽车金融公司、理财公司等非银行金融机构。保险机构是指保险集团(控股)公司、保险公司(不含再保险公司)和保险专业中介机构。

银保监会负责监管的其他金融机构参照适用本办法。邮政企业代理邮政储蓄银行办理商业银行有关业务的，适用本办法有关规定。

第五十六条 本办法由银保监会负责解释。

第五十七条 本办法自 2023 年 3 月 1 日起施行。

中国银行保险监督管理委员会关于印发银行业金融机构数据治理指引的通知

银保监发〔2018〕22 号

各银监局，机关各部门，各政策性银行、大型银行、股份制银行，邮储银行，外资银行，金融资产管理公司，其他会管金融机构：

现将《银行业金融机构数据治理指引》印发给你们，请遵照执行。

2018 年 5 月 21 日

银行业金融机构数据治理指引

第一章 总 则

第一条 为指导银行业金融机构加强数据治理，提高数据质量，发挥数据价值，提升经营管理能力，根据《中华人民共和国银行业监督管理法》等法律法规，制定本指引。

第二条 本指引适用于中华人民共和国境内经银行业监督管理机构批准设立的银行业金融机构。

本指引所称银行业金融机构，是指在中华人民共和国境内设立的商业银行、农村信用合作社等吸收公众存款的金融机构、政策性银行以及国家开发银行。

第三条 数据治理是指银行业金融机构通过建立组织架构，明确董事会、监事会、高级管理层及内设部门等职责要求，制定和实施系统化的制度、流程和方法，确保数据统一管理、高效运行，并在经营管理中充分发挥价值的动态过程。

第四条 银行业金融机构应当将数据治理纳入公司治理范畴，建立自上而下、协调一致的数据治理体系。

第五条 银行业金融机构数据治理应当遵循以下基本原则：

(一)全覆盖原则。数据治理应当覆盖数据的全生命周期，覆盖业务经营、风险管理和内部控制流程中的全部数据，覆盖内部数据和外部数据，覆盖监管数据，覆盖所有分支机构和附属机构。

(二)匹配性原则。数据治理应当与管理模式、业务规模、风险状况等相适应，并根据情况变化进行调整。

(三)持续性原则。数据治理应当持续开展，建立长效机制。

(四)有效性原则。数据治理应当推动数据真实准确客观反映银行业金融机

构实际情况，并有效应用于经营管理。

第六条 银行业金融机构应当将监管数据纳入数据治理，建立工作机制和流程，确保监管数据报送工作有效组织开展，监管数据质量持续提升。

法定代表人或主要负责人对监管数据质量承担最终责任。

第七条 银行业监督管理机构依据本指引对银行业金融机构数据治理情况实施监管。

第二章 数据治理架构

第八条 银行业金融机构应当建立组织架构健全、职责边界清晰的数据治理架构，明确董事会、监事会、高级管理层和相关部门的职责分工，建立多层次、相互衔接的运行机制。

第九条 银行业金融机构董事会应当制定数据战略，审批或授权审批与数据治理相关的重大事项，督促高级管理层提升数据治理有效性，对数据治理承担最终责任。

第十条 银行业金融机构监事会负责对董事会和高级管理层在数据治理方面的履职尽责情况进行监督评价。

第十一条 银行业金融机构高级管理层负责建立数据治理体系，确保数据治理资源配置，制定和实施问责和激励机制，建立数据质量控制机制，组织评估数据治理的有效性和执行情况，并定期向董事会报告。

银行业金融机构可根据实际情况设立首席数据官。首席数据官是否纳入高级管理人员由银行业金融机构根据经营状况确定；纳入高级管理人员管理的，应当符合相关行政许可事项的要求。

第十二条 银行业金融机构应当确定并授权归口管理部门牵头负责实施数据治理体系建设，协调落实数据管理运行机制，组织推动数据在经营管理流程中发挥作用，负责监管数据相关工作，设置监管数据相关工作专职岗位。

第十三条 业务部门应当负责本业务领域的数据治理，管理业务条线数据源，确保准确记录和及时维护，落实数据质量控制机制，执行监管数据相关工作要求，加强数据应用，实现数据价值。

第十四条 银行业金融机构应当在数据治理归口管理部门设立满足工作需要的专职岗位，在其他相关业务部门设置专职或兼职岗位。

第十五条 银行业金融机构应当建立一支满足数据治理工作需要的专业队伍，至少按年度对人员进行系统培训，科学规划职业成长通道，确定合理薪酬水平。

第十六条 银行业金融机构应当建立良好的数据文化，树立数据是重要资产和数据应真实客观的理念与准则，强化用数意识，遵循依规用数、科学用数的职业操守。

第三章 数据管理

第十七条 银行业金融机构应当结合自身发展战略、监管要求等，制定数据战略并确保有效执行和修订。

第十八条 银行业金融机构应当制定全面科学有效的数据管理制度，包括但不限于组织管理、部门职责、协调机制、安全管控、系统保障、监督检查和数据质量控制等方面。

银行业金融机构应当根据监管要求和实际需要，持续评价更新数据管理制度。

第十九条 银行业金融机构应当制定与监管数据相关的监管统计管理制度和业务制度，及时发布并定期评价和更新，报银行业监督管理机构备案。制度出现重大变化的，应当及时向银行业监督管理机构报告。

第二十条 银行业金融机构应当建立覆盖全部数据的标准化规划，遵循统一的业务规范和技术标准。数据标准应当符合国家标准化政策及监管规定，并确保被有效执行。

第二十一条 银行业金融机构应当持续完善信息系统，覆盖各项业务和管理数据。信息系统应当有完备的数据字典和维护流程，并具有可拓展性。

第二十二条 银行业金融机构应当建立适应监管数据报送工作需要的信息系统，实现流程控制的程序化，提高监管数据加工的自动化程度。

第二十三条 银行业金融机构应当加强数据采集的统一管理，明确系统间数据交换流程和标准，实现各类数据有效共享。

第二十四条 银行业金融机构应当建立数据安全策略与标准，依法合规采集、应用数据，依法保护客户隐私，划分数据安全等级，明确访问和拷贝等权限，监控访问和拷贝等行为，完善数据安全技术，定期审计数据安全。

银行业金融机构采集、应用数据涉及到个人信息的，应遵循国家个人信息保护法律法规要求，符合与个人信息安全相关的国家标准。

第二十五条 银行业金融机构应当加强数据资料统一管理，建立全面严密的管理流程、归档制度，明确存档交接、口径梳理等要求，保证数据可比性。

第二十六条 银行业金融机构应当建立数据应急预案，根据业务影响分析，组织开展应急演练，完善处置流程，保证在系统服务异常以及危机等情景下数据的完整、准确和连续。

第二十七条 银行业金融机构应当建立数据治理自我评估机制，明确评估周期、流程、结果应用、组织保障等要素的相关要求。

评估内容应覆盖数据治理架构、数据管理、数据安全、数据质量和数据价值实现等方面，并按年度向银行业监督管理机构报送。

第二十八条 银行业金融机构应当建立问责机制，定期排查数据管理、数据质量控制、数据价值实现等方面问题，依据有关规定对高级管理层和相关部门及责任人进行问责。

银行业金融机构应结合实际情况，建立激励机制，保障数据治理工作有效推进。

第四章 数据质量控制

第二十九条 银行业金融机构应当确立数据质量管理目标，建立控制机制，确保数据的真实性、准确性、连续性、完整性和及时性。

第三十条 银行业金融机构各项业务制度应当充分考虑数据质量管理需要，涉及指标含义清晰明确，取数规则统一，并根据业务变化及时更新。

第三十一条 银行业金融机构应当加强数据源头管理，确保将业务信息全面准确及时录入信息系统。信息系统应当能自动提示异常变动及错误情况。

第三十二条 银行业金融机构应当建立数据质量监控体系，覆盖数据全生命周期，对数据质量持续监测、分析、反馈和纠正。

第三十三条 银行业金融机构应当建立数据质量现场检查制度，定期组织实施，原则上不低于每年一次，对重大问题要按照既定的报告路径提交，并按流程实施整改。

第三十四条 银行业金融机构应当建立数据质量考核评价体系，考核结果纳

入本机构绩效考核体系，实现数据质量持续提升。

第三十五条 银行业金融机构应当建立数据质量整改机制，对日常监控、检查和考核评价过程中发现的问题，及时组织整改，并对整改情况跟踪评价，确保整改落实到位。

第三十六条 银行业金融机构应当按照监管要求报送法人和集团的相关数据，保证同一监管指标在监管报送与对外披露之间的一致性。如有重大差异，应当及时向银行业监督管理机构解释说明。

第三十七条 银行业金融机构应当建立监管数据质量管控制度，包括但不限于：关键监管指标数据质量承诺、数据异常变动分析和报告、重大差错通报以及问责等。

第五章 数据价值实现

第三十八条 银行业金融机构应当在风险管理、业务经营与内部控制中加强数据应用，实现数据驱动，提高管理精细化程度，发挥数据价值。

第三十九条 银行业金融机构应当充分运用数据分析，合理制定风险管理策略、风险偏好、风险限额以及风险管理政策和程序，监控执行情况并适时优化调整，提升风险管理体系的有效性。

全球系统重要性银行应遵循更高的标准，对照有效风险数据加总与风险报告评估要点的相关要求，强化风险管理。

第四十条 银行业金融机构应当加强数据应用，持续改善风险管理方法，有效识别、计量、评估、监测、报告和控制各类风险。

第四十一条 银行业金融机构应当提高数据加总能力，明确数据加总范围、方法、流程和加总结果要求等，满足在正常经营、压力情景以及危机状况下风险管理的数据需要。

加总内容包括但不限于交易对手、产品、地域、行业、客户以及其他相关的分类。加总技术应当主要采取自动化方式。

第四十二条 银行业金融机构应当加强数据分析应用能力，提高风险报告质量，明确风险报告数据准确性保障措施，覆盖重要风险领域和新风险，提供风险处置的决策与建议以及未来风险发展趋势。

第四十三条 银行业金融机构应当加强数据积累，优化风险计量，持续完善

风险定价模型，优化风险定价体系。

第四十四条 银行业金融机构应当充分评估兼并收购、资产剥离等业务对自身数据治理能力的影响。有重大影响的，应当明确整改计划和时间表，满足银行集团风险管理要求。

第四十五条 银行业金融机构应当明确新产品新服务的数据管理相关要求，确保清晰评估成本、风险和收益，并作为准入标准。

第四十六条 银行业金融机构应当通过数据分析挖掘，准确理解客户需求，提供精准产品服务，提升客户服务质量和服务水平。

第四十七条 银行业金融机构应当通过量化分析业务流程，减少管理冗余，提高经营效率，降低经营成本。

第四十八条 银行业金融机构应当充分运用大数据技术，实现业务创新、产品创新和服务创新。

第四十九条 银行业金融机构应当按照可量化导向，完善内部控制评价制度和内部控制评价质量控制机制，前瞻性识别内部控制流程的缺陷，评估影响程度并及时处理，持续提升内部控制的有效性。

第六章 监督管理

第五十条 银行业监督管理机构应当通过非现场监管和现场检查对银行业金融机构数据治理情况进行持续监管。

第五十一条 银行业监督管理机构可根据需要，要求银行业金融机构通过内部审计机构或委托外部审计机构对其数据治理情况进行审计，并及时报送审计报告。

第五十二条 对数据治理不满足《中华人民共和国银行业监督管理法》等法律法规及国务院银行业监督管理机构审慎经营规则要求的银行业金融机构，银行业监督管理机构可采取相应措施：

(一)要求其制定整改方案，责令限期改正；

(二)与公司治理评价结果或监管评级挂钩；

(三)依法采取监管措施及实施行政处罚。

第七章 附 则

第五十三条 外国银行分行以及银行业监督管理机构负责监管的其他金融机

构参照执行本指引。

第五十四条 本指引由国务院银行业监督管理机构负责解释。

第五十五条 本指引自印发之日起施行。《银行监管统计数据质量管理良好标准(试行)》(银监发〔2011〕63 号)同时废止。

中国银保监会关于印发监管数据安全管理办法(试行)的通知

各银保监局，机关各部门，各会管单位：

为切实加强监管数据安全管理，防范监管数据安全风险，我会制定了《中国银保监会监管数据安全管理办法(试行)》，现予以印发，请遵照执行。

2020 年 9 月 23 日

中国银保监会监管数据安全管理办法(试行)

第一章 总 则

第一条 为规范银保监会监管数据安全管理工作，提高监管数据安全保护能力，防范监管数据安全风险，依据《中华人民共和国网络安全法》《中华人民共和国银行业监督管理法》《中华人民共和国保险法》《工作秘密管理暂行办法》等法律法规及有关规定，制定本办法。

第二条 本办法所称监管数据是指银保监会在履行监管职责过程中，依法定期采集，经监管信息系统记录、生成和存储的，或经银保监会各业务部门认定的数字、指标、报表、文字等各类信息。

本办法所称监管信息系统是指以满足监管需求为目的开发建设的，具有数据采集、处理、存储等功能的信息系统。

第三条 本办法所称监管数据安全是指监管数据在采集、处理、存储、使用等活动(以下简称监管数据活动)中，处于可用、完整和可审计状态，未发生泄露、篡改、损毁、丢失或非法使用等情况。

第四条 银保监会及受托机构开展监管数据活动，适用本办法。

本办法所称受托机构是指受银保监会委托或委派，为银保监会提供监管数据采集、处理或存储服务的企事业单位。

第五条 开展监管数据活动，必须遵守相关法律和行政法规。任何单位和个人对在监管数据活动中知悉的国家秘密、工作秘密、商业秘密和个人信息，应当依照相关规定予以保密。

第六条 银保监会建立健全监管数据安全协同管理体系，推动银保监会有关业务部门、各级派出机构、受托机构等共同参与监管数据安全保护工作，加强培训教育，形成共同维护监管数据安全的良好环境。

第二章 工 作 职 责

第七条 监管数据安全管理实行归口管理，建立统筹协调、分工负责的管理机制。

银保监会统计信息部门是归口管理部门，负责统筹监管数据安全管理工作。银保监会各业务部门负责本部门监管数据安全管理工作。

第八条 归口管理部门具体职责包括：

(一)制定监管数据安全工作规则和管理流程；

(二)制定监管数据安全技术防护措施；

(三)组织实施监管数据安全评估和监督检查。

第九条 各业务部门具体职责包括：

(一)规范本部门监管数据安全使用，明确具体工作要求，落实相关责任；

(二)组织开展本部门监管数据安全管理工作；

(三)协助归口管理部门实施监管数据安全监督检查。

第三章 监管数据采集、存储和加工处理

第十条 监管数据的采集应按照安全、准确、完整和依法合规的原则进行，避免重复、过度采集。

第十一条 监管数据应通过监管工作网或金融专网进行传输。因客观条件限制需要通过物理介质、互联网或其它网络传输的，应经归口管理部门评估同意。

第十二条 监管数据应存储在银保监会机房，并具有完备的备份措施。确有必要存储在受托机构机房的，应经归口管理部门评估同意。

第十三条 监管数据存储期限、存储介质管理应按照国家和银保监会有关规定执行。

第十四条 监管数据的加工处理应在监管工作权限或受托范围内进行。未经归口管理部门同意，任何单位和个人不得将代码、接口、算法模型和开发工具等接入监管信息系统。

第十五条 监管数据采集、传输、存储、加工处理、转移交换、销毁，以及用于系统开发测试等活动，应根据监管数据类型和管理要求采取分级分类安全技术防护措施。

第四章 监管数据使用

第十六条 监管数据仅限于银保监会履行监管工作职责使用。纪检监察、司法、审计等党政机关为履行工作职责需要使用监管数据时，按照有关规定办理。

第十七条 监管数据的使用行为应通过管理和技术手段确保可追溯。监管数据用于信息系统开发测试以及对外展示时，应经过脱敏处理。

第十八条 使用未公开披露的监管数据，原则上应在不可连接互联网的台式机或笔记本等银保监会工作机中进行。因客观条件限制需采取虚拟专用网络等方式使用监管数据时，应经归口管理部门评估同意。

第十九条 因工作需要下载的监管数据，仅可存储于银保监会的工作机中。承载监管数据的使用介质应妥善保管，防止数据泄露。

第二十条 在使用监管数据过程中产生的加工数据、汇总结果等信息应视同监管数据进行安全管理。

第二十一条 监管数据对外披露应由指定业务部门按照有关规定和流程实施。

第二十二条 各业务部门因工作需要向非党政机关单位、个人提供监管数据时，应充分评估数据安全风险，经本部门主要负责人同意后实施，必要时与对方签订备忘录和保密协议并报归口管理部门备案。

与境外监管机构或国际组织共享监管数据时，应由国际事务部门依照银保监会签署的监管合作谅解备忘录、合作协议等约定或其他有关工作安排进行管理。

法律法规另有规定的，从其规定。

第二十三条 各业务部门因工作需要和系统下线停用监管数据时，应及时对其采取封存或销毁措施。

第五章 监管数据委托服务管理

第二十四条 各业务部门监管数据采集涉及受托机构提供服务时，应事先与

归口管理部门沟通并会签同意。受托机构的技术服务方案，应通过归口管理部门的安全评估。技术服务方案发生变更的，应事先报归口管理部门进行安全评估。

安全评估不通过的，不得开展委托服务或建立委派关系。

第二十五条 为银保监会提供监管数据服务的受托机构，应满足以下基本条件：

(一)具备从事监管数据工作所需系统的自主研发及运维能力；

(二)具备相关信息安全管理资质认证；

(三)拥有自主产权或已签订长期租赁合同的机房；

(四)网络和信息系统具备有效的安全保护和稳定运行措施，三年内未发生网络安全重大事件；

(五)具备有效的监管数据安全管理措施，能够保障银保监会各部门对监管数据的访问和控制；

(六)具有监管数据备份体系、应急组织体系和业务连续性计划。

第二十六条 银保监会通过与受托机构签订协议，确立监管数据委托服务关系。协议应明确服务项目、期限、安全管理责任和终止事由等内容。

银保监会通过委派方式确立监管数据服务关系的，应下达委派任务书。

第二十七条 因有关政策调整导致原委托或委派事项无需继续履行，或发现受托机构监管数据服务出现重大安全问题的，银保监会有权终止委托或委派关系。

委托或委派关系终止时，受托机构应及时、完整地移交监管数据，并销毁因委托或委派事项而获取的监管数据，不得保留相关数据备份等内容。

第六章 监 督 管 理

第二十八条 各业务部门及受托机构应按照监管数据安全工作规则定期开展自查，发现监管数据安全缺陷、漏洞等风险时，应立即采取补救措施。

第二十九条 归口管理部门应定期对各业务部门及受托机构开展监管数据安全管理评估检查工作。

各业务部门及受托机构对于评估和检查中发现的问题应制定整改措施，及时整改，并向归口管理部门报送整改报告。

第三十条 各业务部门及受托机构发生以下监管数据重大安全风险事项时，应立即采取应急处置措施，及时消除安全隐患，防止危害扩大，并于 48 小时内向归口管理部门报告。

(一)监管数据发生泄露或非法使用；

(二)监管数据发生损毁或丢失；

(三)承载监管数据的信息系统或网络发生系统性故障造成服务中断4 小时以上；

(四)承载监管数据的信息系统或网络遭受非法入侵、发生有害信息或计算机病毒的大规模传播等破坏；

(五)监管数据安全事件引发舆情；

(六)《网络安全重大事件判定指南》列明的其他影响监管数据安全的网络安全重大事件。

辖区发生以上监管数据重大安全风险事项时，各银保监局应立即采取补救措施，并于 48 小时内向银保监会归口管理部门报告。

第三十一条 归口管理部门应建立监管数据安全事件通报工作机制，及时通报监管数据安全事件。

第七章 附 则

第三十二条 涉密监管数据按照国家和银保监会保密管理有关规定进行管理。

第三十三条 各银保监局承担辖区监管数据安全管理责任，参照本办法制定辖区监管数据安全管理办法，明确职责和管理要求，强化监管数据安全保护。

第三十四条 本办法自印发之日起施行。

国家发展改革委办公厅 银保监会办公厅关于加强信用信息共享应用推进融资信用服务平台网络建设的通知

发改办财金〔2022〕299 号

各省、自治区、直辖市、新疆生产建设兵团社会信用体系建设牵头部门、各银保监局，国家公共信用信息中心，各政策性银行、大型银行、股份制银行：

为贯彻落实《国务院办公厅关于印发加强信用信息共享应用促进中小微企业融资实施方案的通知》（国办发〔2021〕52 号，以下简称《实施方案》），加

快构建全国一体化融资信用服务平台网络，加强信用信息共享应用促进中小微企业融资，现将有关工作通知如下。

一、建立健全融资信用服务平台网络

国家公共信用信息中心要按照《实施方案》要求，加快与有关部门系统对接，实现“总对总”信息的机制化、高质量共享，并及时与地方共享。各省级社会信用体系建设牵头部门、各银保监局要积极统筹协调辖区内资源，高标准推动地方融资信用服务平台(以下简称地方平台)建设工作，加快实现与全国中小企业融资综合信用服务平台(以下简称国家平台)互联互通。各地要依托省级信用信息共享平台建立国家平台省级节点，充分发挥信用信息“上传下达”枢纽作用。

国家公共信用信息中心要制定省级节点管理办法和相关标准规范。各省级社会信用体系建设牵头部门要按照有关要求，在 4 月底前实现省级节点与国家平台、辖区内符合条件的地方平台联通。对于已经与国家平台直连的地方平台，按照先立后破原则，待省级节点运行后逐步调整规范到位。

各银保监局要发挥监管部门了解银行的优势，及时收集并反映银行服务中小微企业的实际需求，推动各地更加精准、更加全面地归集共享信息，优化数据交换方式，提升信用信息的可用性，为银行提高中小微企业服务能力做好数据支撑。

二、加快推进涉企信用信息归集共享

各级社会信用体系建设牵头部门要对照《实施方案》中的信用信息共享清单，推进本辖区内纳税信息、生态环境领域信息、不动产信息、行政强制信息、水电气费缴纳信息和科技研发信息等由地方政府负责的信息归集共享，并由省级节点统一共享至国家平台。其中，行政强制信息要按照国家公共信用信息中心制定的数据归集标准及时报送至全国信用信息共享平台，并于年底前实现全量报送。要压实部门责任，分解工作任务，加大协调督促力度，确保按照《实施方案》明确的时限要求完成信息归集共享任务。

《实施方案》中已明确属于全国集中管理但“总对总”共享方式尚未实现或共享内容不充分的信用信息，各地可先行推进共享。鼓励各地结合实际需求和工作实际，在《实施方案》规定的信用信息共享清单的基础上，依法依规扩

大信息归集共享范围，拓展数据共享的广度和深度。

三、着力提升融资信用服务平台服务质量

国家公共信用信息中心要强化国家平台功能和服务能力建设，扩大公共信用综合评价覆盖面。各省级社会信用体系建设牵头部门要着力提升信用信息服务质量，加强数据治理，建立数据质量监测、反馈、修正机制，持续改善数据质量，不断提高数据准确性、完整性、连续性和时效性。接入省级节点的地方平台要依法依规向金融机构充分开放信息，要根据不同数据特点，分类采取授权查询、核验比对等方式与金融机构共享，经企业明确授权允许金融机构查询的，应尽可能提供原始明细数据，便于使用。鼓励各级平台采用联合建模、隐私计算等方式与金融机构深化合作，更好服务金融机构产品研发、信用评估和风险管理，推动扩大中小微企业贷款规模。鼓励省级节点和地方平台与信用服务机构合作，提升数据清洗加工能力，创新开发信用报告、信用评价等标准化产品供金融机构使用。

各省级社会信用体系建设牵头部门要与有关部门、金融机构等合作，加大政策宣传解读力度，广泛动员辖区内中小微企业和个体工商户在地方平台进行实名注册，并主动完善相关信息，扩大市场主体覆盖面。

各银行业金融机构要积极对接各级平台，把握好信用信息共享深化的有利时机，强化自身数据能力建设，充分利用信用信息资源和银行内部金融数据，综合运用大数据等金融科技手段，扎实推进小微企业、涉农贷款业务的数字化转型，提高授信审批、风险预警管理的能力，创新信贷产品，努力提高信用贷和首贷占比，并反馈通过地方平台发放贷款的统计数据。

四、切实加强信息安全和主体权益保护

各省级社会信用体系建设牵头部门要指导辖区内各级地方平台加强信息安全和主体权益保护，督促平台主管部门和建设运营单位落实主体责任，强化对银行等接入机构信息管理要求，获取的信息不得用于为企业提供融资支持以外的活动。银行与第三方机构合作处理信息时，要依据“最小、必要”原则进行脱敏处理，防范数据泄露风险。未经脱敏处理或信息主体明确授权，各级地方平台不得对外提供涉及商业秘密或个人隐私的信息，不得违法传播、泄露、出售有关信用信息。

各省级社会信用体系建设牵头部门要组织做好省级节点管理工作，严格按照相关标准和程序对接国家平台和地方平台，加强地方平台接入前安全评估和接入后安全管理。对不符合信息安全条件的地方平台，一律不得接入；对接入后违反信息安全管理规定的地方平台，要督促整改甚至取消接入。对发生信息安全责任事故的，要依法依规严肃追究有关单位和人员的责任。

五、强化政策支持

各省级社会信用体系建设牵头部门要将加强信用信息共享应用促进中小微企业融资工作作为支撑企业纾困解难转型发展的重要措施和推动社会信用体系建设高质量发展的重点任务，积极争取人员和经费保障，建立健全跨部门协调机制，主动与有关部门和金融机构沟通衔接，勇于创新，狠抓落实，确保《实施方案》落地见效。

各省级社会信用体系建设牵头部门和各银保监局要积极推动地方政府因地制宜建立中小微企业信用贷款市场化风险分担补偿机制，出台贷款贴息和融资担保补贴等优惠政策，并通过地方平台落实落地。

六、加强工作通报

各省级社会信用体系建设牵头部门要依托省级节点定期向国家平台反馈工作进展和成效，主要包括本辖区内信息共享工作推进情况、地方平台接入省级节点情况、接入平台注册企业和入驻金融机构情况以及平台支持融资服务情况等。

国家发展改革委(财金司)将按月通报重点工作进展情况，定期开展督查，对进度缓慢的地方开展约谈，对先进经验做法加大宣传推广力度。

国家发展改革委办公厅 银保监会办公厅

2022 年 4 月 7 日

第十二章 中国人民银行

中国人民银行金融消费者权益保护实施办法

中国人民银行令〔2020〕第 5 号

《中国人民银行金融消费者权益保护实施办法》已经 2020 年 9 月 1 日中国人民银行 2020 年第 6 次行务会议审议通过，现予发布，自 2020 年 11 月 1 日起

施行。

行 长 易 纲

2020 年 9 月 15 日

中国人民银行金融消费者权益保护实施办法

第一章 总 则

第一条 为了保护金融消费者合法权益，规范金融机构提供金融产品和服务的行为，维护公平、公正的市场环境，促进金融市场健康稳定运行，根据《中华人民共和国中国人民银行法》《中华人民共和国商业银行法》《中华人民共和国消费者权益保护法》和《国务院办公厅关于加强金融消费者权益保护工作的指导意见》（国办发〔2015〕81 号)等，制定本办法。

第二条 在中华人民共和国境内依法设立的为金融消费者提供金融产品或者服务的银行业金融机构(以下简称银行)，开展与下列业务相关的金融消费者权益保护工作，适用本办法：

(一)与利率管理相关的。

(二)与人民币管理相关的。

(三)与外汇管理相关的。

(四)与黄金市场管理相关的。

(五)与国库管理相关的。

(六)与支付、清算管理相关的。

(七)与反洗钱管理相关的。

(八)与征信管理相关的。

(九)与上述第一项至第八项业务相关的金融营销宣传和消费者金融信息保护。

(十)其他法律、行政法规规定的中国人民银行职责范围内的金融消费者权益保护工作。

在中华人民共和国境内依法设立的非银行支付机构(以下简称支付机构)提供支付服务的，适用本办法。

本办法所称金融消费者是指购买、使用银行、支付机构提供的金融产品或者服务的自然人。

第三条 银行、支付机构向金融消费者提供金融产品或者服务，应当遵循自愿、平等、公平、诚实信用的原则，切实承担金融消费者合法权益保护的主体责任，履行金融消费者权益保护的法定义务。

第四条 金融消费者应当文明、理性进行金融消费，提高自我保护意识，诚实守信，依法维护自身的合法权益。

第五条 中国人民银行及其分支机构坚持公平、公正原则，依法开展职责范围内的金融消费者权益保护工作，依法保护金融消费者合法权益。

中国人民银行及其分支机构会同有关部门推动建立和完善金融机构自治、行业自律、金融监管和社会监督相结合的金融消费者权益保护共同治理体系。

第六条 鼓励金融消费者和银行、支付机构充分运用调解、仲裁等方式解决金融消费纠纷。

第二章 金融机构行为规范

第七条 银行、支付机构应当将金融消费者权益保护纳入公司治理、企业文化建设和经营发展战略，制定本机构金融消费者权益保护工作的总体规划和具体工作措施。建立金融消费者权益保护专职部门或者指定牵头部门，明确部门及人员职责，确保部门有足够的人力、物力能够独立开展工作，并定期向高级管理层、董(理)事会汇报工作开展情况。

第八条 银行、支付机构应当落实法律法规和相关监管规定关于金融消费者权益保护的相关要求，建立健全金融消费者权益保护的各项内控制度：

(一)金融消费者权益保护工作考核评价制度。

(二)金融消费者风险等级评估制度。

(三)消费者金融信息保护制度。

(四)金融产品和服务信息披露、查询制度。

(五)金融营销宣传管理制度。

(六)金融知识普及和金融消费者教育制度。

(七)金融消费者投诉处理制度。

(八)金融消费者权益保护工作内部监督和责任追究制度。

(九)金融消费者权益保护重大事件应急制度。

(十)中国人民银行明确规定应当建立的其他金融消费者权益保护工作制

度。

第九条 银行、支付机构应当建立健全涉及金融消费者权益保护工作的全流程管控机制，确保在金融产品或者服务的设计开发、营销推介及售后管理等各个业务环节有效落实金融消费者权益保护工作的相关规定和要求。全流程管控机制包括但不限于下列内容：

(一)事前审查机制。银行、支付机构应当实行金融消费者权益保护事前审查，及时发现并更正金融产品或者服务中可能损害金融消费者合法权益的问题，有效督办落实金融消费者权益保护审查意见。

(二)事中管控机制。银行、支付机构应当履行金融产品或者服务营销宣传中须遵循的基本程序和标准，加强对营销宣传行为的监测与管控。

(三)事后监督机制。银行、支付机构应当做好金融产品和服务的售后管理，及时调整存在问题或者隐患的金融产品和服务规则。

第十条 银行、支付机构应当开展金融消费者权益保护工作人员培训，增强工作人员的金融消费者权益保护意识和能力。

银行、支付机构应当每年至少开展一次金融消费者权益保护专题培训，培训对象应当全面覆盖中高级管理人员、基层业务人员及新入职人员。对金融消费者投诉多发、风险较高的业务岗位，应当适当提高培训的频次。

第十一条 银行、支付机构开展考核评价时，应当将金融消费者权益保护工作作为重要内容，并合理分配相关指标的占比和权重，综合考虑业务合规性、客户满意度、投诉处理及时率与合格率等，不得简单以投诉数量作为考核指标。

第十二条 银行、支付机构应当根据金融产品或者服务的特性评估其对金融消费者的适合度，合理划分金融产品和服务风险等级以及金融消费者风险承受等级，将合适的金融产品或者服务提供给适当的金融消费者。

第十三条 银行、支付机构应当依法保障金融消费者在购买、使用金融产品和服务时的财产安全，不得挪用、非法占用金融消费者资金及其他金融资产。

第十四条 银行、支付机构应当尊重社会公德，尊重金融消费者的人格尊严和民族风俗习惯，不得因金融消费者性别、年龄、种族、民族或者国籍等不同实行歧视性差别对待，不得使用歧视性或者违背公序良俗的表述。

第十五条 银行、支付机构应当尊重金融消费者购买金融产品或者服务的真实意愿，不得擅自代理金融消费者办理业务，不得擅自修改金融消费者的业务指令，不得强制搭售其他产品或者服务。

第十六条 银行、支付机构应当依据金融产品或者服务的特性，及时、真实、准确、全面地向金融消费者披露下列重要内容：

(一)金融消费者对该金融产品或者服务的权利和义务，订立、变更、中止和解除合同的方式及限制。

(二)银行、支付机构对该金融产品或者服务的权利、义务及法律责任。

(三)贷款产品的年化利率。

(四)金融消费者应当负担的费用及违约金，包括金额的确定方式，交易时间和交易方式。

(五)因金融产品或者服务产生纠纷的处理及投诉途径。

(六)银行、支付机构对该金融产品或者服务所执行的强制性标准、推荐性标准、团体标准或者企业标准的编号和名称。

(七)在金融产品说明书或者服务协议中，实际承担合同义务的经营主体完整的中文名称。

(八)其他可能影响金融消费者决策的信息。

第十七条 银行、支付机构对金融产品和服务进行信息披露时，应当使用有利于金融消费者接收、理解的方式。对利率、费用、收益及风险等与金融消费者切身利益相关的重要信息，应当根据金融产品或者服务的复杂程度及风险等级，对其中关键的专业术语进行解释说明，并以适当方式供金融消费者确认其已接收完整信息。

第十八条 银行、支付机构向金融消费者说明重要内容和披露风险时，应当依照法律法规和监管规定留存相关资料，自业务关系终止之日起留存时间不得少于 3 年。法律、行政法规另有规定的，从其规定。

留存的资料包括但不限于：

(一)金融消费者确认的金融产品说明书或者服务协议。

(二)金融消费者确认的风险提示书。

(三)记录向金融消费者说明重要内容的录音、录像资料或者系统日志等相

关数据电文资料。

第十九条 银行、支付机构不得利用技术手段、优势地位，强制或者变相强制金融消费者接受金融产品或者服务，或者排除、限制金融消费者接受同业机构提供的金融产品或者服务。

第二十条 银行、支付机构在提供金融产品或者服务的过程中，不得通过附加限制性条件的方式要求金融消费者购买、使用协议中未作明确要求的产品或者服务。

第二十一条 银行、支付机构向金融消费者提供金融产品或者服务时使用格式条款的，应当以足以引起金融消费者注意的字体、字号、颜色、符号、标识等显著方式，提请金融消费者注意金融产品或者服务的数量、利率、费用、履行期限和方式、注意事项、风险提示、纠纷解决等与金融消费者有重大利害关系的内容，并按照金融消费者的要求予以说明。格式条款采用电子形式的，应当可被识别且易于获取。

银行、支付机构不得以通知、声明、告示等格式条款的方式作出含有下列内容的规定：

(一)减轻或者免除银行、支付机构造成金融消费者财产损失的赔偿责任。

(二)规定金融消费者承担超过法定限额的违约金或者损害赔偿金。

(三)排除或者限制金融消费者依法对其金融信息进行查询、删除、修改的权利；

(四)排除或者限制金融消费者选择同业机构提供的金融产品或者服务的权利。

(五)其他对金融消费者不公平、不合理的规定。

银行、支付机构应当对存在侵害金融消费者合法权益问题或者隐患的格式条款和服务协议文本及时进行修订或者清理。

第二十二条 银行、支付机构应当对营销宣传内容的真实性负责。银行、支付机构实际承担的义务不得低于在营销宣传活动中通过广告、资料或者说明等形式对金融消费者所承诺的标准。

前款“广告、资料或者说明”是指以营销为目的，利用各种传播媒体、宣传工具或者方式，就银行、支付机构的金融产品或者服务进行直接或者间接的

宣传、推广等。

第二十三条 银行、支付机构在进行营销宣传活动时，不得有下列行为：

(一)虚假、欺诈、隐瞒或者引人误解的宣传。

(二)引用不真实、不准确的数据和资料或者隐瞒限制条件等，对过往业绩或者产品收益进行夸大表述。

(三)利用金融管理部门对金融产品或者服务的审核或者备案程序，误导金融消费者认为金融管理部门已对该金融产品或者服务提供保证。

(四)明示或者暗示保本、无风险或者保收益等，对非保本投资型金融产品的未来效果、收益或者相关情况作出保证性承诺。

(五)其他违反金融消费者权益保护相关法律法规和监管规定的行为。

第二十四条 银行、支付机构应当切实承担金融知识普及和金融消费者教育的主体责任，提高金融消费者对金融产品和服务的认知能力，提升金融消费者金融素养和诚实守信意识。

银行、支付机构应当制定年度金融知识普及与金融消费者教育工作计划，结合自身特点开展日常性金融知识普及与金融消费者教育活动，积极参与中国人民银行及其分支机构组织的金融知识普及活动。银行、支付机构不得以营销金融产品或者服务替代金融知识普及与金融消费者教育。

第二十五条 银行、支付机构应当重视金融消费者需求的多元性与差异性，积极支持普惠金融重点目标群体获得必要、及时的基本金融产品和服务。

第二十六条 出现侵害金融消费者合法权益重大事件的，银行、支付机构应当根据重大事项报告的相关规定及时向中国人民银行或其分支机构报告。

第二十七条 银行、支付机构应当配合中国人民银行及其分支机构开展金融消费者权益保护领域的相关工作，按照规定报送相关资料。

第三章 消费者金融信息保护

第二十八条 本办法所称消费者金融信息，是指银行、支付机构通过开展业务或者其他合法渠道处理的消费者信息，包括个人身份信息、财产信息、账户信息、信用信息、金融交易信息及其他与特定消费者购买、使用金融产品或者服务相关的信息。

消费者金融信息的处理包括消费者金融信息的收集、存储、使用、加工、

传输、提供、公开等。

第二十九条 银行、支付机构处理消费者金融信息，应当遵循合法、正当、必要原则，经金融消费者或者其监护人明示同意，但是法律、行政法规另有规定的除外。银行、支付机构不得收集与业务无关的消费者金融信息，不得采取不正当方式收集消费者金融信息，不得变相强制收集消费者金融信息。银行、支付机构不得以金融消费者不同意处理其金融信息为由拒绝提供金融产品或者服务，但处理其金融信息属于提供金融产品或者服务所必需的除外。

金融消费者不能或者拒绝提供必要信息，致使银行、支付机构无法履行反洗钱义务的，银行、支付机构可以根据《中华人民共和国反洗钱法》的相关规定对其金融活动采取限制性措施；确有必要时，银行、支付机构可以依法拒绝提供金融产品或者服务。

第三十条 银行、支付机构收集消费者金融信息用于营销、用户体验改进或者市场调查的，应当以适当方式供金融消费者自主选择是否同意银行、支付机构将其金融信息用于上述目的；金融消费者不同意的，银行、支付机构不得因此拒绝提供金融产品或者服务。银行、支付机构向金融消费者发送金融营销信息的，应当向其提供拒绝继续接收金融营销信息的方式。

第三十一条 银行、支付机构应当履行《中华人民共和国消费者权益保护法》第二十九条规定的明示义务，公开收集、使用消费者金融信息的规则，明示收集、使用消费者金融信息的目的、方式和范围，并留存有关证明资料。

银行、支付机构通过格式条款取得消费者金融信息收集、使用同意的，应当在格式条款中明确收集消费者金融信息的目的、方式、内容和使用范围，并在协议中以显著方式尽可能通俗易懂地向金融消费者提示该同意的可能后果。

第三十二条 银行、支付机构应当按照法律法规的规定和双方约定的用途使用消费者金融信息，不得超出范围使用。

第三十三条 银行、支付机构应当建立以分级授权为核心的消费者金融信息使用管理制度，根据消费者金融信息的重要性、敏感度及业务开展需要，在不影响本机构履行反洗钱等法定义务的前提下，合理确定本机构工作人员调取信息的范围、权限，严格落实信息使用授权审批程序。

第三十四条 银行、支付机构应当按照国家档案管理和电子数据管理等规

定，采取技术措施和其他必要措施，妥善保管和存储所收集的消费者金融信息，防止信息遗失、毁损、泄露或者被篡改。

银行、支付机构及其工作人员应当对消费者金融信息严格保密，不得泄露或者非法向他人提供。在确认信息发生泄露、毁损、丢失时，银行、支付机构应当立即采取补救措施；信息泄露、毁损、丢失可能危及金融消费者人身、财产安全的，应当立即向银行、支付机构住所地的中国人民银行分支机构报告并告知金融消费者；信息泄露、毁损、丢失可能对金融消费者产生其他不利影响的，应当及时告知金融消费者，并在 72 小时以内报告银行、支付机构住所地的中国人民银行分支机构。中国人民银行分支机构接到报告后，视情况按照本办法第五十五条规定处理。

第四章 金融消费争议解决

第三十五条 金融消费者与银行、支付机构发生金融消费争议的，鼓励金融消费者先向银行、支付机构投诉，鼓励当事人平等协商，自行和解。

金融消费者应当依法通过正当途径客观、理性反映诉求，不扰乱正常的金融秩序和社会公共秩序。

本办法所称金融消费争议，是指金融消费者与银行、支付机构因购买、使用金融产品或者服务所产生的民事争议。

第三十六条 银行、支付机构应当切实履行金融消费投诉处理的主体责任，银行、支付机构的法人机构应当按年度向社会发布金融消费者投诉数据和相关分析报告。

第三十七条 银行、支付机构应当通过金融消费者方便获取的渠道公示本机构的投诉受理方式，包括但不限于营业场所、官方网站首页、移动应用程序的醒目位置及客服电话主要菜单语音提示等。

第三十八条 银行、支付机构应当按照中国人民银行要求，加强对金融消费者投诉处理信息系统的建设与管理，对投诉进行正确分类并按时报送相关信息，不得迟报、漏报、谎报、错报或者瞒报投诉数据。

第三十九条 银行、支付机构收到金融消费者投诉后，依照相关法律法规和合同约定进行处理，并告知投诉人处理情况，但因投诉人原因导致无法告知的除外。

第四十条 中国人民银行分支机构设立投诉转办服务渠道。金融消费者对银行、支付机构作出的投诉处理不接受的，可以通过银行、支付机构住所地、合同签订地或者经营行为发生地中国人民银行分支机构进行投诉。

通过电子商务、网络交易购买、使用金融产品或者服务的，金融消费者通过银行、支付机构住所地的中国人民银行分支机构进行投诉。

第四十一条 金融消费者通过中国人民银行分支机构进行投诉，应当提供以下信息：姓名，有效身份证件信息，联系方式，明确的投诉对象及其住所地，具体的投诉请求、事实和理由。

金融消费者可以本人提出投诉，也可以委托他人代为提出投诉。以来信来访方式进行委托投诉的，应当向中国人民银行分支机构提交前款规定的投诉材料、授权委托书原件、委托人和受托人的身份证明。授权委托书应当载明受托人、委托事项、权限和期限，并由委托人本人签名。

第四十二条 中国人民银行分支机构对下列投诉不予接收：

(一)投诉人投诉的机构、产品或者服务不属于中国人民银行监管范围的。

(二)投诉人未提供真实身份，或者没有明确的被投诉人、没有具体的投诉请求和事实依据的。

(三)投诉人并非金融消费者本人，也未经金融消费者本人委托的。

(四)人民法院、仲裁机构、其他金融管理部门、行政部门或者依法设立的调解组织已经受理、接收或者处理的。

(五)双方达成和解协议并已经执行，没有新情况、新理由的。

(六)被投诉机构已提供公平合理的解决方案，投诉人就同一事项再次向中国人民银行分支机构投诉的。

(七)其他不符合法律、行政法规、规章有关规定的。

第四十三条 中国人民银行分支机构收到金融消费者投诉的，应当自收到投诉之日起 7 个工作日内作出下列处理：

(一)对投诉人和被投诉机构信息、投诉请求、事实和理由等进行登记。

(二)作出是否接收投诉的决定。决定不予接收的，应当告知投诉人。

(三)决定接收投诉的，应当将投诉转交被投诉机构处理或者转交金融消费纠纷调解组织提供调解服务。

需要投诉人对投诉内容进行补正的，处理时限于补正完成之日起计算。

银行、支付机构应当自收到中国人民银行分支机构转交的投诉之日起 15 日内答复投诉人。情况复杂的，经本机构投诉处理工作负责人批准，可以延长处理期限，并告知投诉人延长处理期限的理由，但最长处理期限不得超过 60 日。

第四十四条 银行、支付机构收到中国人民银行分支机构转交的投诉，应当按要求向中国人民银行分支机构反馈投诉处理情况。

反馈的内容包括投诉基本情况、争议焦点、调查结果及证据、处理依据、与金融消费者的沟通情况、延期处理情况及投诉人满意度等。

银行、支付机构应当妥善保存投诉资料，投诉资料留存时间自投诉办结之日起不得少于 3 年。法律、行政法规另有规定的，从其规定。

第四十五条 银行、支付机构、金融消费者可以向调解组织申请调解、中立评估。调解组织受理调解、中立评估申请后，可在合理、必要范围内请求当事人协助或者提供相关文件、资料。

本办法所称中立评估，是指调解组织聘请独立专家就争议解决提出参考性建议的行为。

第四十六条 金融消费纠纷调解组织应当依照法律、行政法规、规章及其章程的规定，组织开展金融消费纠纷调解、中立评估等工作，对银行、支付机构和金融消费者进行金融知识普及和教育宣传引导。

第五章 监督与管理机制

第四十七条 中国人民银行综合研究金融消费者保护重大问题，负责拟定发展规划和业务标准，建立健全金融消费者保护基本制度。

第四十八条 中国人民银行及其分支机构与其他金融管理部门、地方政府有关部门建立健全金融消费者权益保护工作协调机制，加强跨市场跨业态跨区域金融消费者权益保护的监管，强化信息共享和部门间沟通协作。

第四十九条 中国人民银行及其分支机构统筹开展金融消费者教育，引导、督促银行、支付机构开展金融知识普及宣传活动，协调推进金融知识纳入国民教育体系，组织开展消费者金融素养调查。

第五十条 中国人民银行及其分支机构会同有关部门构建监管执法合作机制，探索合作开展金融消费者权益保护监督检查、评估等具体工作。

第五十一条 中国人民银行及其分支机构牵头构建非诉第三方解决机制，鼓励、支持金融消费者权益保护社会组织依法履行职责，推动构建公正、高效、便捷的多元化金融消费纠纷解决体系。

第五十二条 中国人民银行及其分支机构协调推进相关普惠金融工作，建立健全普惠金融工作机制，指导、督促银行、支付机构落实普惠金融发展战略，组织开展职责范围内的普惠金融具体工作。

第五十三条 中国人民银行及其分支机构对金融消费者投诉信息进行汇总和分析，根据汇总和分析结果适时优化金融消费者权益保护监督管理方式、金融机构行为规范等。

第五十四条 中国人民银行及其分支机构可以采取下列措施，依法在职责范围内开展对银行、支付机构金融消费者权益保护工作的监督检查：

(一)进入被监管机构进行检查。

(二)询问被监管机构的工作人员，要求其对有关检查事项作出说明。

(三)查阅、复制被监管机构与检查事项有关的文件、资料，对可能被转移、隐匿或者毁损的文件、资料予以登记保存。

(四)检查被监管机构的计算机网络与信息系统。

进行现场检查时，检查人员不得少于二人，并应当出示合法证件和检查通知书。

银行、支付机构应当积极配合中国人民银行及其分支机构的现场检查和非现场检查，如实提供有关资料，不得拒绝、阻挠、逃避检查，不得谎报、隐匿、销毁相关证据材料。

第五十五条 银行、支付机构有侵害金融消费者合法权益行为的，中国人民银行及其分支机构可以对其采取下列措施：

(一)要求提交书面说明或者承诺。

(二)约见谈话。

(三)责令限期整改。

(四)视情将相关信息向其上级机构、行业监管部门反馈，在行业范围内发布，或者向社会公布。

(五)建议银行、支付机构对直接负责的董事、高级管理人员和其他直接责

任人员给予处分。

(六)依法查处或者建议其他行政管理部门依法查处。

(七)中国人民银行职责范围内依法可以采取的其他措施。

第五十六条 中国人民银行及其分支机构组织开展银行、支付机构履行金融消费者权益保护义务情况的评估工作。

评估工作以银行、支付机构自评估为基础。银行、支付机构应当按年度进行自评估，并于次年 1 月 31 日前向中国人民银行或其分支机构报送自评估报告。

中国人民银行及其分支机构根据日常监督管理、投诉管理以及银行、支付机构自评估等情况进行非现场评估，必要时可以进行现场评估。

第五十七条 中国人民银行及其分支机构可以根据具体情况开展金融消费者权益保护环境评估工作。

第五十八条 中国人民银行及其分支机构建立金融消费者权益保护案例库制度，按照预防为先、教育为主的原则向银行、支付机构和金融消费者进行风险提示。

第五十九条 中国人民银行及其分支机构对于涉及金融消费者权益保护的重大突发事件，应当按照有关规定做好相关应急处置工作。

第六章 法律责任

第六十条 银行、支付机构有下列情形之一，侵害消费者金融信息依法得到保护的权利的，中国人民银行或其分支机构应当在职责范围内依照《中华人民共和国消费者权益保护法》第五十六条的规定予以处罚：

(一)未经金融消费者明示同意，收集、使用其金融信息的。

(二)收集与业务无关的消费者金融信息，或者采取不正当方式收集消费者金融信息的。

(三)未公开收集、使用消费者金融信息的规则，未明示收集、使用消费者金融信息的目的、方式和范围的。

(四)超出法律法规规定和双方约定的用途使用消费者金融信息的。

(五)未建立以分级授权为核心的消费者金融信息使用管理制度，或者未严格落实信息使用授权审批程序的。

(六)未采取技术措施和其他必要措施，导致消费者金融信息遗失、毁损、泄露或者被篡改，或者非法向他人提供的。

第六十一条 银行、支付机构有下列情形之一，对金融产品或者服务作出虚假或者引人误解的宣传的，中国人民银行或其分支机构应当在职责范围内依照《中华人民共和国消费者权益保护法》第五十六条的规定予以处罚：

(一)实际承担的义务低于在营销宣传活动中通过广告、资料或者说明等形式对金融消费者所承诺的标准的。

(二)引用不真实、不准确的数据和资料或者隐瞒限制条件等，对过往业绩或者产品收益进行夸大表述的。

(三)利用金融管理部门对金融产品或者服务的审核或者备案程序，误导金融消费者认为金融管理部门已对该金融产品或者服务提供保证的。

(四)明示或者暗示保本、无风险或者保收益等，对非保本投资型金融产品的未来效果、收益或者相关情况作出保证性承诺的。

第六十二条 银行、支付机构违反本办法规定，有下列情形之一，有关法律、行政法规有处罚规定的，依照其规定给予处罚；有关法律、行政法规未作处罚规定的，中国人民银行或其分支机构应当根据情形单处或者并处警告、处以五千元以上三万元以下罚款：

(一)未建立金融消费者权益保护专职部门或者指定牵头部门，或者金融消费者权益保护部门没有足够的人力、物力独立开展工作的。

(二)擅自代理金融消费者办理业务，擅自修改金融消费者的业务指令，或者强制搭售其他产品或者服务的。

(三)未按要求向金融消费者披露与金融产品和服务有关的重要内容的。

(四)利用技术手段、优势地位，强制或者变相强制金融消费者接受金融产品或者服务，或者排除、限制金融消费者接受同业机构提供的金融产品或者服务的。

(五)通过附加限制性条件的方式要求金融消费者购买、使用协议中未作明确要求的产品或者服务的。

(六)未按要求使用格式条款的。

(七)出现侵害金融消费者合法权益重大事件未及时向中国人民银行或其分

支机构报告的。

(八)不配合中国人民银行及其分支机构开展金融消费者权益保护领域相关工作，或者未按照规定报送相关资料的。

(九)未按要求对金融消费者投诉进行正确分类，或者迟报、漏报、谎报、错报、瞒报投诉数据的。

(十)收到中国人民银行分支机构转交的投诉后，未在规定期限内答复投诉人，或者未按要求向中国人民银行分支机构反馈投诉处理情况的。

(十一)拒绝、阻挠、逃避检查，或者谎报、隐匿、销毁相关证据材料的。

第六十三条 对银行、支付机构侵害金融消费者权益重大案件负有直接责任的董事、高级管理人员和其他直接责任人员，有关法律、行政法规有处罚规定的，依照其规定给予处罚；有关法律、行政法规未作处罚规定的，中国人民银行或其分支机构应当根据情形单处或者并处警告、处以五千元以上三万元以下罚款。

第六十四条 中国人民银行及其分支机构的工作人员在开展金融消费者权益保护工作过程中有下列情形之一的，依法给予处分；涉嫌构成犯罪的，移送司法机关依法追究刑事责任：

(一)违反规定对银行、支付机构进行检查的。

(二)泄露知悉的国家秘密或者商业秘密的。

(三)滥用职权、玩忽职守的其他行为。

第七章 附 则

第六十五条 商业银行理财子公司、金融资产管理公司、信托公司、汽车金融公司、消费金融公司以及征信机构、个人本外币兑换特许业务经营机构参照适用本办法。法律、行政法规另有规定的，从其规定。

第六十六条 本办法中除“工作日”以外的“日”为自然日。

第六十七条 本办法由中国人民银行负责解释。

第六十八条 本办法自2020年11月1日起施行。《中国人民银行金融消费权益保护工作管理办法(试行)》(银办发〔2013〕107号文印发)与《中国人民银行金融消费者权益保护实施办法》(银发〔2016〕314号文印发)同时废止。

征信业务管理办法

中国人民银行令〔2021〕第 4 号

《征信业务管理办法》已经 2021 年 9 月 17 日中国人民银行 2021 年第 9 次行务会议审议通过，现予发布，自 2022 年 1 月 1 日起施行。

行长 易纲

2021 年 9 月 27 日

征信业务管理办法

第一章 总 则

第一条 为了规范征信业务及其相关活动，保护信息主体合法权益，促进征信业健康发展，推进社会信用体系建设，根据《中华人民共和国中国人民银行法》《中华人民共和国个人信息保护法》《征信业管理条例》等法律法规，制定本办法。

第二条 在中华人民共和国境内，对法人和非法人组织(以下统称企业)、个人开展征信业务及其相关活动的，适用本办法。

第三条 本办法所称征信业务，是指对企业和个人的信用信息进行采集、整理、保存、加工，并向信息使用者提供的活动。

本办法所称信用信息，是指依法采集，为金融等活动提供服务，用于识别判断企业和个人信用状况的基本信息、借贷信息、其他相关信息， 以及基于前述信息形成的分析评价信息。

第四条 从事个人征信业务的，应当依法取得中国人民银行个人征信机构许可；从事企业征信业务的，应当依法办理企业征信机构备案；从事信用评级业务的，应当依法办理信用评级机构备案。

第五条 金融机构不得与未取得合法征信业务资质的市场机构开展商业合作获取征信服务。

本办法所称金融机构，是指国务院金融管理部门监督管理的从事金融业务的机构。

地方金融监管部门负责监督管理的地方金融组织适用本办法关于金融机构的规定。

第六条 从事征信业务及其相关活动，应当保护信息主体合法权益，保障信息安全，防范信用信息泄露、丢失、毁损或者被滥用， 不得危害国家秘密，不得

侵犯个人隐私和商业秘密。

从事征信业务及其相关活动，应当遵循独立、客观、公正的原则， 不得违反法律法规的规定，不得违反社会公序良俗。

第二章 信用信息采集

第七条 采集个人信用信息，应当采取合法、正当的方式，遵循最小、必要的原则，不得过度采集。

第八条 征信机构不得以下列方式采集信用信息：

(一)欺骗、胁迫、诱导；

(二)向信息主体收费；

(三)从非法渠道采集；

(四)以其他侵害信息主体合法权益的方式。

第九条 信息提供者向征信机构提供信用信息的，征信机构应当制定相关制度，对信息提供者的信息来源、信息质量、信息安全、信息主体授权等进行必要的审查。

第十条 征信机构与信息提供者在开办业务及合作中应当遵守《中华人民共和国个人信息保护法》等法律法规， 通过协议等形式明确信息采集的原则以及各自在获得客户同意、信息采集、加工处理、信息更正、异议处理、信息安全等方面的权利义务和责任。

第十一条 征信机构经营个人征信业务，应当制定采集个人信用信息的方案，并就采集的数据项、信息来源、采集方式、信息主体合法权益保护制度等事项及其变化向中国人民银行报告。

第十二条 征信机构采集个人信用信息应当经信息主体本人同意，并且明确告知信息主体采集信用信息的目的。依照法律法规公开的信息除外。

第十三条 征信机构通过信息提供者取得个人同意的，信息提供者应当向信息主体履行告知义务。

第十四条 个人征信机构应当将与其合作，进行个人信用信息采集、整理、加工和分析的信息提供者，向中国人民银行报告。

个人征信机构应当规范与信息提供者的合作协议内容。信息提供者应当就个人信用信息处理事项接受个人征信机构的风险评估和中国人民银行的情况核实。

第十五条 采集企业信用信息，应当基于合法的目的，不得侵犯商业秘密。

第三章 信用信息整理、保存、加工

第十六条 征信机构整理、保存、加工信用信息，应当遵循客观性原则，不得篡改原始信息。

第十七条 征信机构应当采取措施，提高征信系统信息的准确性，保障信息质量。

第十八条 征信机构在整理、保存、加工信用信息过程中发现信息错误的，如属于信息提供者报送错误的，应当及时通知信息提供者更正；如属于内部处理错误的，应当及时更正，并优化信用信息内部处理流程。

第十九条 征信机构应当对来自不同信息提供者的信息进行比对，发现信息不一致的，及时进行核查和处理。

第二十条 征信机构采集的个人不良信息的保存期限，自不良行为或者事件终止之日起为 5 年。

个人不良信息保存期限届满，征信机构应当将个人不良信息在对外服务和应用中删除；作为样本数据的，应当进行匿名化处理。

第四章 信用信息提供、使用

第二十一条 征信机构对外提供征信产品和服务，应当遵循公平性原则，不得设置不合理的商业条件限制不同的信息使用者使用，不得利用优势地位提供歧视性或者排他性的产品和服务。

第二十二条 征信机构应当采取适当的措施，对信息使用者的身份、业务资质、使用目的等进行必要的审查。

征信机构应当对信息使用者接入征信系统的网络和系统安全、合规性管理措施进行评估，对查询行为进行监测。发现安全隐患或者异常行为的，及时核查；发现违法违规行为的，停止提供服务。

第二十三条 信息使用者应当采取必要的措施，保障查询个人信用信息时取得信息主体的同意，并且按照约定用途使用个人信用信息。

第二十四条 信息使用者使用征信机构提供的信用信息，应当基于合法、正当的目的，不得滥用信用信息。

第二十五条 个人信息主体有权每年两次免费获取本人的信用报告，征信机

构可以通过互联网查询、营业场所查询等多种方式为个人信息主体提供信用报告查询服务。

第二十六条 信息主体认为信息存在错误、遗漏的，有权向征信机构或者信息提供者提出异议；认为侵害自身合法权益的，可以向所在地中国人民银行分支机构投诉。对异议和投诉按照《征信业管理条例》及相关规定办理。

第二十七条 征信机构不得以删除不良信息或者不采集不良信息为由，向信息主体收取费用。

第二十八条 征信机构提供信用报告等信用信息查询产品和服务的，应当客观展示查询的信用信息内容，并对查询的信用信息内容及专业名词进行解释说明。

信息主体有权要求征信机构在信用报告中添加异议标注和声明。

第二十九条 征信机构提供画像、评分、评级等信用评价类产品和服务的，应当建立评价标准，不得将与信息主体信用无关的要素作为评价标准。

征信机构正式对外提供信用评价类产品和服务前，应当履行必要的内部测试和评估验证程序，使评价规则可解释、信息来源可追溯。

征信机构提供经济主体或者债务融资工具信用评级产品和服务的，应当按照《信用评级业管理暂行办法》（中国人民银行 发展改革委 财政部 证监会令〔2019〕第 5 号发布)等相关规定开展业务。

第三十条 征信机构提供信用反欺诈产品和服务的，应当建立欺诈信用信息的认定标准。

第三十一条 征信机构提供信用信息查询、信用评价类、信用反欺诈产品和服务，应当向中国人民银行或其省会(首府)城市中心支行以上分支机构报告下列事项：

(一)信用报告的模板及内容；

(二)信用评价类产品和服务的评价方法、模型、主要维度要素；

(三)信用反欺诈产品和服务的数据来源、欺诈信用信息认定标准。

第三十二条 征信机构不得从事下列活动：

(一)对信用评价结果进行承诺；

(二)使用对信用评价结果有暗示性的内容宣传产品和服务；

(三)未经政府部门或者行业协会同意，假借其名义进行市场推广；

(四)以胁迫、欺骗、诱导的方式向信息主体或者信息使用者提供征信产品和服务;

(五)对征信产品和服务进行虚假宣传;

(六)提供其他影响征信业务客观公正性的征信产品和服务。

第五章 信用信息安全

第三十三条 征信机构应当落实网络安全等级保护制度，制定涉及业务活动和设备设施的安全管理制度，采取有效保护措施，保障征信系统的安全。

第三十四条 个人征信机构、保存或者处理 100 万户以上企业信用信息的企业征信机构，应当符合下列要求：

(一)核心业务信息系统网络安全保护等级具备三级或者三级以上安全保护能力;

(二)设立信息安全负责人和个人信息保护负责人，由公司章程规定的高级管理人员担任;

(三)设立专职部门，负责信息安全和个人信息保护工作，定期检查征信业务、系统安全、个人信息保护制度措施执行情况。

第三十五条 征信机构应当保障征信系统运行设施设备、安全控制设施设备以及互联网应用程序的安全，做好征信系统日常运维管理，保障系统物理安全、通信网络安全、区域边界安全、计算环境安全、管理中心安全等， 防范征信系统受到非法入侵和破坏。

第三十六条 征信机构应当在人员录用、离岗、考核、安全教育、培训和外部人员访问管理等方面做好人员安全管理工作。

第三十七条 征信机构应当严格限定公司内部查询和获取信用信息的工作人员的权限和范围。

征信机构应当留存工作人员查询、获取信用信息的操作记录， 明确记载工作人员查询和获取信用信息的时间、方式、内容及用途。

第三十八条 征信机构应当建立应急处置制度，在发生或者有可能发生信用信息泄露等事件时，立即采取必要措施降低危害，并及时向中国人民银行及其省会(首府)城市中心支行以上分支机构报告。

第三十九条 征信机构在中华人民共和国境内开展征信业务及其相关活动，

采集的企业信用信息和个人信用信息应当存储在中华人民共和国境内。

第四十条 征信机构向境外提供个人信用信息，应当符合法律法规的规定。

征信机构向境外信息使用者提供企业信用信息查询产品和服务，应当对信息使用者的身份、信用信息用途进行必要的审查， 确保信用信息用于跨境贸易、投融资等合理用途，不得危害国家安全。

第四十一条 征信机构与境外征信机构合作的，应当在合作协议签署后、业务开展前将合作协议报告中国人民银行。

第六章 监督管理

第四十二条 征信机构应当将下列事项向社会公开，接受社会监督：

(一)采集的信用信息类别；

(二)信用报告的基本格式内容；

(三)异议处理流程；

(四)中国人民银行认为需要公开的其他事项。

第四十三条 个人征信机构应当每年对自身个人征信业务遵守《中华人民共和国个人信息保护法》《征信业管理条例》的情况进行合规审计，并将合规审计报告及时报告中国人民银行。

第四十四条 中国人民银行及其省会(首府)城市中心支行以上分支机构对征信机构的下列事项进行监督检查：

(一)征信内控制度建设，包括各项制度和相关规程的齐备性、合规性和可操作性等；

(二)征信业务合规经营情况，包括采集信用信息、对外提供和使用信用信息、异议与投诉处理、用户管理、其他事项合规性等；

(三)征信系统安全情况，包括信息技术制度、安全管理、系统开发等；

(四)与征信业务活动相关的其他事项。

第四十五条 信息提供者和信息使用者违反《征信业管理条例》规定，侵犯信息主体合法权益的，由中国人民银行及其省会(首府)城市中心支行以上分支机构依法对其检查和处理。

第七章 法律责任

第四十六条 违反本办法第四条规定，擅自从事个人征信业务的，由中国人

民银行按照《征信业管理条例》第三十六条进行处罚；擅自从事企业征信业务的，由中国人民银行省会(首府)城市中心支行以上分支机构按照《征信业管理条例》第三十七条进行处罚。

金融机构违反本办法第五条规定，与未取得合法征信业务资质的市场机构开展商业合作获取征信服务的，由中国人民银行及其分支机构责令改正，对单位处3万元以下罚款，对直接负责的主管人员处1000元以下罚款。

第四十七条 征信机构违反本办法第八条、第十六条、第二十条、第二十七条、第三十二条规定的， 由中国人民银行及其省会(首府)城市中心支行以上分支机构按照《征信业管理条例》第三十八条进行处罚。

第四十八条 征信机构违反本办法第十四条、第二十一条、第三十一条、第三十四条、第三十九条、第四十二条规定的， 由中国人民银行及其省会(首府)城市中心支行以上分支机构责令改正，没收违法所得，对单位处3万元以下罚款，对直接负责的主管人员处1000元以下罚款。法律、行政法规另有规定的，依照其规定。

第八章 附 则

第四十九条 金融信用信息基础数据库从事征信业务、从事信贷业务的机构向金融信用信息基础数据库报送或者查询信用信息参照本办法执行。

第五十条 以“信用信息服务”“信用服务”“信用评分”“信用评级”“信用修复”等名义对外实质提供征信服务的，适用本办法。

第五十一条 本办法施行前未取得个人征信业务经营许可或者未进行企业征信机构备案但实质从事征信业务的机构，应当自本办法施行之日起18个月内完成合规整改。

第五十二条 本办法由中国人民银行负责解释。

第五十三条 本办法自2022年1月1日起施行。

中国人民银行关于发布金融行业标准做好个人金融信息保护技术管理工作的通知

银发〔2020〕45号

《个人金融信息保护技术规范》(JR/T0171-2020，以下简称《规范》)金融行业标准已经全国金融标准化技术委员会审查通过，现予以发布，并就有关事

项通知如下：

一、金融业机构可结合实际按照《规范》加强个人金融信息全生命周期技术管理，强化风险识别和监控，建立健全风险事件处置机制，保障个人金融信息主体合法权益。

二、行业协会可根据工作需要按照《规范》加强个人金融信息保护行业自律管理，建立健全自律检查、违规约束、投诉处理等机制，定期向人民银行报送相关情况

请人民银行副省级城市中心支行以上分支机构将本通知告知辖区内分支机构和金融业机构。

附件：个人金融信息保护技术规范

中国人民银行

2020 年 03 月 04 日

第十三章 国家卫生健康委员会

国家卫生计生委关于印发《人口健康信息管理办法(试行)》的通知

国卫规划发〔2014〕24 号

各省、自治区、直辖市卫生计生委(卫生厅局、人口计生委)，新疆生产建设兵团卫生局、人口计生委，委机关各司局，委直属和联系单位：

为规范人口健康信息的管理工作，促进人口健康信息的互联互通和共享利用，推动卫生计生事业科学发展，我委按照相关法律法规，研究制定了《人口健康信息管理办法(试行)》。现印发你们，请遵照执行。

国家卫生计生委

2014 年 5 月 5 日

人口健康信息管理办法(试行)

第一条 为规范人口健康信息的管理工作，促进人口健康信息的互联互通和共享利用，推动卫生计生事业科学发展，制定本办法。

第二条 本办法适用于各级各类医疗卫生计生服务机构所涉及的人口健康信息的采集、管理、利用、安全和隐私保护工作。

第三条 本办法所称人口健康信息，是指依据国家法律法规和工作职责，各

级各类医疗卫生计生服务机构在服务和管理过程中产生的人口基本信息、医疗卫生服务信息等人口健康信息。

符合《中华人民共和国电子签名法》等有关法律法规规定的人口健康电子信息，与纸质文本具有同等法律效力。

第四条 人口健康信息管理工作应当统筹规划、统一标准，属地管理、责权一致，保障安全、便民高效。

第五条县级以上人民政府卫生计生行政部门(含中医药行政部门，下同)是人口健康信息主管部门。国家卫生计生委负责制订全国人口健康信息发展规划和管理规范，统筹指导全国人口健康信息管理工作；县级以上地方人民政府卫生计生行政部门负责推进、指导、监督本行政区域人口健康信息管理工作。

各级各类医疗卫生计生服务机构(含中医药服务机构，下同)负责人口健康信息的采集、利用、管理、安全和隐私保护，是人口健康信息管理中的责任单位。

第六条 责任单位采集、利用、管理人口健康信息应当按照法律法规的规定，遵循医学伦理原则，保证信息安全，保护个人隐私。

第七条责任单位应当根据本单位人口健康信息采集、利用和管理的情况， 设立相应的人口健康信息管理部门和岗位职责，建立完善的人口健康信息质量控制管理制度，建立或利用相应的信息系统。严格执行相关标准和程序， 做到标准统一、术语规范、内容准确。

第八条 责任单位应当按照“一数一源、最少够用”的原则采集人口健康信息，所采集的信息应当符合业务应用和管理要求，保证服务和管理对象在本单位信息系统中身份标识的唯一性，基本数据项的一致性，所采集的信息应当严格实行信息复核程序，避免重复采集、多头采集。

第九条 人口健康信息实行分级存储。责任单位按照国家统一规划，负责存储、管理工作中产生的人口健康信息， 应当具备符合国家有关规定要求的数据存储、容灾备份和管理条件， 建立可靠的人口健康信息容灾备份工作机制，定期进行备份和恢复检测，确保数据能够及时、完整、准确恢复， 实现长期保存和历史数据的归档管理。

第十条 责任单位应当结合服务和管理工作需要，及时更新与维护人口健康信息，确保信息处于最新、连续、有效状态。

不得将人口健康信息在境外的服务器中存储，不得托管、租赁在境外的服务器。

第十一条委托其他机构存储、运维人口健康信息的， 委托单位承担人口健康信息的管理和安全责任。

受委托的存储、运维机构应当严格按照委托协议做好人口健康信息管理的技术支持，禁止超权限采集、开发和利用人口健康信息。

第十二条责任单位发生变更时，应当将所管理的人口健康信息完整、安全地移交给主管部门或承接延续其职能的机构管理，不得造成人口健康信息的损毁、丢失。

第十三条人口健康信息的利用实行分类管理，逐步实现互联共享。

人口健康信息的利用应当以提高医学研究、科学决策和便民服务水平为目的。

依法应当向社会公开的信息应当及时主动公开；涉及保密信息和个人隐私信息，不得对外提供。

第十四条责任单位应当建立人口健康信息综合利用工作制度，授权利用有关信息。

利用单位或者个人不得超出授权范围利用和发布人口健康信息。

第十五条责任单位应当为服务和管理对象提供其人口健康个案信息的查询和复制服务，并提供安全的信息查询和复制渠道。

第十六条责任单位应当做好人口健康信息安全和隐私保护工作，按照国家信息安全等级保护制度要求，加强建设人口健康信息相关系统安全保障体系，制定安全管理制度、操作规程和技术规范，保障人口健康信息安全。

利用单位和个人应当按照授权要求，做好所涉及的人口健康信息安全和隐私保护工作。

第十七条涉及国家秘密的人口健康信息系统应当按照国家涉密信息管理的要求进行分级保护，杜绝泄密。

第十八条责任单位应当建立痕迹管理制度，任何建立、修改和访问人口健康信息的用户，都应当通过严格的实名身份鉴别和授权控制，做到其行为可管理、可控制、可追溯。

第十九条人口健康信息相关系统的信息技术产品和服务提供者应当遵守国

家有关信息安全审查制度，不得中断或者以其他方式中断合理的技术支持与服务，并应当为人口健康信息在不同系统间的迁移、交互、共享提供安全与便利条件。

第二十条 卫生计生行政部门应当加强对本行政区域内各责任单位人口健康信息管理工作的日常监督检查，对本行政区域内各责任单位人口健康信息综合利用工作的指导监督，提高精细化人口健康服务和管理能力。

第二十一条卫生计生行政部门建立通报制度。相关单位和个人在人口健康信息利用、人口健康信息系统建设维护和技术支持等过程中， 违反本办法规定造成不良后果的，主管部门或责任单位应当对其予以通报；情节严重、违反国家法律法规的，依照国家有关法律法规追究其法律责任。

第二十二条 卫生计生行政部门建立人口健康信息管理工作责任追究制度。对于违反本办法规定的主管部门和责任单位，上级主管部门应当视情节轻重予以督导整改、通报批评、提出给予行政处分的建议； 构成犯罪的，依法追究刑事责任。

第二十三条本办法自印发之日起施行。

国家卫生健康委员会关于印发国家健康医疗大数据标准、安全和服务管理办法(试行)的通知

国卫规划发〔2018〕23 号

各省、自治区、直辖市及新疆生产建设兵团卫生计生委， 委机关各司局，委直属和联系单位，国家中医药局：

为加强健康医疗大数据服务管理，促进“互联网+医疗健康”发展，充分发挥健康医疗大数据作为国家重要基础性战略资源的作用，根据相关法律法规，我委研究制定了《国家健康医疗大数据标准、安全和服务管理办法(试行)》（可从国家卫生健康委员会官网下载)。现印发你们，请遵照执行。

国家卫生健康委员会

2018 年 7 月 12 日

国家健康医疗大数据标准、安全和服务管理办法(试行)

第一章 总 则

第一条 为加强健康医疗大数据服务管理，促进“互联网+医疗健康”发展，充分发挥健康医疗大数据作为国家重要基础性战略资源的作用，根据《中华人民

共和国网络安全法》等法律法规和《国务院促进大数据发展行动纲要》《国务院办公厅关于促进和规范健康医疗大数据应用发展的指导意见》《国务院办公厅关于促进“互联网+医疗健康”发展的意见》等文件精神，就健康医疗大数据标准、安全和服务管理，制定本办法。

第二条 我国公民在中华人民共和国境内所产生的健康和医疗数据，国家在保障公民知情权、使用权和个人隐私的基础上， 根据国家战略安全和人民群众生命安全需要，加以规范管理和开发利用。

第三条 坚持以人为本、创新驱动，规范有序、安全可控，开放融合、共建共享的原则，加强健康医疗大数据的标准管理、安全管理和服务管理， 推动健康医疗大数据惠民应用，促进健康医疗大数据产业发展。

第四条 本办法所称健康医疗大数据，是指在人们疾病防治、健康管理等过程中产生的与健康医疗相关的数据。

第五条 本办法适用于县级以上卫生健康行政部门（含中医药主管部门，下同）、各级各类医疗卫生机构、相关单位及个人所涉及的健康医疗大数据的管理。

第六条 国家卫生健康委员会(含国家中医药管理局，下同)会同相关部门负责统筹规划、指导、评估、监督全国健康医疗大数据的标准管理、安全管理和服务管理工作。县级以上卫生健康行政部门会同相关部门负责本行政区域内健康医疗大数据管理工作，是本行政区域内健康医疗大数据安全和应用管理的监管单位。

各级各类医疗卫生机构和相关企事业单位是健康医疗大数据安全和应用管理的责任单位。

第二章 标准管理

第七条 健康医疗大数据标准管理工作遵循政策引领、强化监督、分类指导、分级管理的原则。

第八条 国家卫生健康委员会负责统筹规划、组织制定全国健康医疗大数据标准，监督指导评估标准的应用工作，在已有的基础性通用性大数据标准基础上组织制定健康医疗大数据标准体系规划，负责制定、组织实施年度健康医疗大数据标准工作计划。省级卫生健康行政部门（含省级中医药主管部门）负责监督指导评估本地区健康医疗大数据标准的应用工作，依据国家健康医疗大数据标准体系规划，结合本地实际，负责指导和监督健康医疗大数据标准体系在本省域内落地

执行。

第九条 国家卫生健康委员会鼓励医疗卫生机构、科研教育单位、相关企业或行业协会、社会团体等参与健康医疗大数据标准制定工作。公民、法人或者其他组织可提出制修订健康医疗大数据标准的立项建议，并提交相应标准项目建议书。

第十条 国家卫生健康委员会负责统一组织实施，择优确定健康医疗大数据标准起草单位和负责人，提倡多方参与协作机制，由各相关单位组成协作组参与标准起草工作。

第十一条 健康医疗大数据标准起草、审查及发布的程序和要求，按照国家和行业有关规定执行。

第十二条 卫生健康行政部门应当对健康医疗大数据标准的实施加强引导和监督，充分发挥各级各类医疗卫生机构、相关企业等市场主体在标准应用实施中的积极性和主动性，建立激励和促进标准应用实施的长效管理机制。

第十三条 卫生健康行政部门应当建立相应的健康医疗大数据标准化产品生产和采购的激励约束机制，卫生健康行政部门要积极推进健康医疗大数据标准规范和测评工作，并将测评结果与医疗卫生机构评审评价挂钩。

第十四条 国家卫生健康委员会加强健康医疗大数据技术产品和服务模式的标准体系及制度建设，组织对健康医疗大数据标准应用效果评估工作，并根据评估情况，对相关标准进行组织修订或废止等。

第十五条 国家卫生健康委员会基于卫生标准管理平台，动态管理健康医疗大数据标准的开发与应用，对各级各类医疗卫生机构和企事业单位的标准应用情况进行动态监测。

第三章 安全管理

第十六条 健康医疗大数据安全管理是指在数据采集、存储、挖掘、应用、运营、传输等多个环节中的安全和管理， 包括国家战略安全、群众生命安全、个人信息安全的权责管理工作。

第十七条 责任单位应当建立健全相关安全管理制度、操作规程和技术规范，落实“一把手”责任制，加强安全保障体系建设，强化统筹管理和协调监督，保障健康医疗大数据安全。

涉及国家秘密的健康医疗大数据的安全、管理和使用等，按照国家有关保密规定执行。责任单位应当建立健全涉及国家秘密的健康医疗大数据管理与使用制度，对制作、审核、登记、拷贝、传输、销毁等环节进行严格管理。

第十八条 责任单位应当采取数据分类、重要数据备份、加密认证等措施保障健康医疗大数据安全。责任单位应当建立可靠的数据容灾备份工作机制，定期进行备份和恢复检测，确保数据能够及时、完整、准确恢复，实现长期保存和历史数据的归档管理。

第十九条 责任单位应当按照国家网络安全等级保护制度要求，构建可信的网络安全环境，加强健康医疗大数据相关系统安全保障体系建设，提升关键信息基础设施和重要信息系统的安全防护能力，确保健康医疗大数据关键信息基础设施和核心系统安全可控。健康医疗大数据中心、相关信息系统等均应开展定级、备案、测评等工作。

第二十条 健康医疗大数据相关系统的产品和服务提供者应当遵守国家有关网络安全审查制度，不得中断或者变相中断合理的技术支持与服务，并应当为健康医疗大数据在不同系统间的交互、共享和运营提供安全与便利条件。

第二十一条 责任单位应当依法依规使用健康医疗大数据有关信息，提供安全的信息查询和复制渠道，确保公民隐私保护和数据安全。

第二十二条 责任单位应当按照《中华人民共和国网络安全法》的要求，严格规范不同等级用户的数据接入和使用权限，并确保数据在授权范围内使用。任何单位和个人不得擅自利用和发布未经授权或超出授权范围的健康医疗大数据，不得使用非法手段获取数据。

第二十三条 责任单位应当建立严格的电子实名认证和数据访问控制，规范数据接入、使用和销毁过程的痕迹管理，确保健康医疗大数据访问行为可管、可控及服务管理全程留痕，可查询、可追溯，对任何数据泄密泄露事故及风险可追溯到相关责任单位和责任人。

第二十四条 建立健全健康医疗大数据安全管理人才培养机制，确保相关从业人员具备健康医疗大数据安全管理所要求的知识和技能。

第二十五条 责任单位应当建立健康医疗大数据安全监测和预警系统，建立网络安全通报和应急处置联动机制，开展数据安全规范和技术规范的研究工作，

不断丰富网络安全相关的标准规范体系，重点防范数据资源的集聚性风险和新技术应用的潜在性风险。发生网络安全重大事件， 应当按照相关法律法规和有关要求进行报告并处置。

第四章 服务管理

第二十六条 国家卫生健康委员会负责制定健康医疗大数据应用领域相关规范、标准， 建立健康医疗大数据应用诚信机制和退出机制，制定健康医疗大数据挖掘、应用的安全和管理规范。

第二十七条 责任单位实施健康医疗大数据管理和服务，应当按照法律法规和相关文件规定，遵循医学伦理原则，保护个人隐私。

第二十八条 责任单位应当根据本单位健康医疗大数据管理的需求，明确相应的管理部门和岗位，按照国家授权，实行“统一分级授权、分类应用管理、权责一致”的管理制度，并建设相应的健康医疗大数据信息系统作为技术和管理支撑。

第二十九条 责任单位采集健康医疗大数据，应当严格执行国家和行业相关标准和程序，符合业务应用技术标准和管理规范，做到标准统一、术语规范、内容准确，保证服务和管理对象在本单位信息系统中身份标识唯一、基本数据项一致，所采集的信息应当严格实行信息复核终审程序，做好数据质量管理。

第三十条 责任单位应当具备符合国家有关规定要求的数据存储、容灾备份和安全管理条件，加强对健康医疗大数据的存储管理。健康医疗大数据应当存储在境内安全可信的服务器上，因业务需要确需向境外提供的，应当按照相关法律法规及有关要求进行安全评估审核。

第三十一条 责任单位选择健康医疗大数据服务提供商时，应当确保其符合国家和行业规定及要求，具备履行相关法规制度、落实相关标准、确保数据安全的能力，建立数据安全管理、个人隐私保护、应急响应管理等方面管理制度。

第三十二条 责任单位委托有关机构存储、运营健康医疗大数据，委托单位与受托单位共同承担健康医疗大数据的管理和安全责任。受托单位应当严格按照相关法律法规和委托协议做好健康医疗大数据的存储、管理与运营工作。

第三十三条 责任单位应当结合服务和管理工作需要，及时更新、甄别、优化和维护健康医疗大数据，确保信息处于最新、连续、有效、优质和安全状态。

第三十四条 责任单位发生变更时，应当将所管理的健康医疗大数据完整、安全地移交给承接延续其职能的机构或本行政区域内的卫生健康行政部门，不得造成健康医疗大数据的损毁、丢失和泄露。

第三十五条 责任单位向社会公开健康医疗大数据时，应当遵循国家有关规定，不得泄露国家秘密、商业秘密和个人隐私， 不得侵害国家利益、社会公共利益和公民、法人及其他组织的合法权益。

第三十六条 责任单位应当加强健康医疗大数据的使用和服务，创造条件规范使用健康医疗大数据，推动部分健康医疗大数据在线查询。

第三十七条 国家卫生健康委员会负责按照国家信息资源开放共享有关规定，建立健康医疗大数据开放共享的工作机制，加强健康医疗大数据的共享和交换，统筹建设健康医疗大数据上报系统平台、信息资源目录体系和共享交换体系。

第五章 管理监督

第三十八条 卫生健康行政部门应当加强监督管理，对本行政区域内各责任单位健康医疗大数据安全管理工作开展日常检查，指导监督本行政区域内各责任单位数据综合利用工作，提高数据服务质量和确保安全。各级各类医疗卫生机构应当接入相应区域全民健康信息平台，传输和备份医疗健康服务产生的数据，并向卫生健康行政部门开放监管端口。

第三十九条 卫生健康行政部门应当加强监测评估，定期开展健康医疗大数据平台和服务商的稳定和安全测评及健康医疗大数据应用的安全监测评估，建立网络安全防护、系统互联共享、公民隐私保护等软件评价和安全审查保密制度。

第四十条 卫生健康行政部门会同相关部门建立健康医疗大数据安全管理工作责任追究制度。对于违反本办法规定的单位和个人， 由主管部门视情节轻重予以约谈、督导整改、诫勉、通报批评、处分或提出给予处分的建议；构成违法的，移送司法部门依法追究法律责任。

第六章 附 则

第四十一条 本办法自印发之日起施行。

国家卫生健康委员会、国家中医药管理局关于印发互联网诊疗管理办法(试行)等 3 个文件的通知

国卫医发〔2018〕25 号

各省、自治区、直辖市及新疆生产建设兵团卫生计生委、中医药管理局：

为贯彻落实《国务院办公厅关于促进“互联网＋医疗健康”发展的意见》有关要求，进一步规范互联网诊疗行为，发挥远程医疗服务积极作用，提高医疗服务效率，保证医疗质量和医疗安全，国家卫生健康委员会和国家中医药管理局组织制定了《互联网诊疗管理办法(试行)》、《互联网医院管理办法(试行)》、《远程医疗服务管理规范(试行)》，现印发给你们，请遵照执行。

附件：1.互联网诊疗管理办法(试行)

2.互联网医院管理办法(试行)

3.远程医疗服务管理规范(试行)

国家卫生健康委员会

国家中医药管理局

2018 年 7 月 17 日

附件 1：

互联网诊疗管理办法(试行)

第一章 总 则

第一条 为落实《国务院办公厅关于促进“互联网＋医疗健康”发展的意见》，规范互联网诊疗活动，推动互联网医疗服务健康快速发展，保障医疗质量和医疗安全，根据《执业医师法》、《医疗机构管理条例》等法律法规，制定本办法。

第二条 本办法所称互联网诊疗是指医疗机构利用在本机构注册的医师，通过互联网等信息技术开展部分常见病、慢性病复诊和“互联网＋”家庭医生签约服务。

第三条 国家对互联网诊疗活动实行准入管理。

第四条 国务院卫生健康行政部门和中医药主管部门负责全国互联网诊疗活动的监督管理。地方各级卫生健康行政部门(含中医药主管部门，下同)负责辖区内互联网诊疗活动的监督管理。

第二章 互联网诊疗活动准入

第五条 互联网诊疗活动应当由取得《医疗机构执业许可证》的医疗机构提供。

第六条 新申请设置的医疗机构拟开展互联网诊疗活动，应当在设置申请书

注明，并在设置可行性研究报告中写明开展互联网诊疗活动的有关情况。如果与第三方机构合作建立互联网诊疗服务信息系统，应当提交合作协议。

第七条 卫生健康行政部门受理申请后，依据《医疗机构管理条例》、《医疗机构管理条例实施细则》的有关规定进行审核，在规定时间内作出同意或者不同意的书面答复。批准设置并同意其开展互联网诊疗的，在《设置医疗机构批准书》中注明同意其开展互联网诊疗活动。医疗机构按照有关法律法规和规章申请执业登记。

第八条 已经取得《医疗机构执业许可证》的医疗机构拟开展互联网诊疗活动，应当向其《医疗机构执业许可证》发证机关提出开展互联网诊疗活动的执业登记申请，并提交下列材料：

(一)医疗机构法定代表人或主要负责人签署同意的申请书，提出申请开展互联网诊疗活动的原因和理由；

(二)如果与第三方机构合作建立互联网诊疗服务信息系统，应当提交合作协议；

(三)登记机关规定提交的其他材料。

第九条 执业登记机关按照有关法律法规和规章对医疗机构登记申请材料进行审核。审核合格的，予以登记，在《医疗机构执业许可证》副本服务方式中增加“互联网诊疗”。审核不合格的，将审核结果以书面形式通知申请人。

第十条 医疗机构与第三方机构的合作协议应当明确各方在医疗服务、信息安全、隐私保护等方面的责权利。

第十一条 医疗机构开展互联网诊疗活动应当与其诊疗科目相一致。未经卫生健康行政部门核准的诊疗科目，医疗机构不得开展相应的互联网诊疗活动。

第三章 执业规则

第十二条 医疗机构开展互联网诊疗活动应当符合医疗管理要求，建立医疗质量和医疗安全规章制度。

第十三条 医疗机构开展互联网诊疗活动，应当具备满足互联网技术要求的设备设施、信息系统、技术人员以及信息安全系统，并实施第三级信息安全等级保护。

第十四条 开展互联网诊疗活动的医师、护士应当能够在国家医师、护士电

子注册系统中查询。医疗机构应当对开展互联网诊疗活动的医务人员进行电子实名认证，鼓励有条件的医疗机构通过人脸识别等人体特征识别技术加强医务人员管理。

第十五条 基层医疗卫生机构实施“互联网＋”家庭医生签约服务，在协议中告知患者服务内容、流程、双方责任和权利以及可能出现的风险等， 签订知情同意书。

第十六条 医疗机构在线开展部分常见病、慢性病复诊时，医师应当掌握患者病历资料，确定患者在实体医疗机构明确诊断为某种或某几种常见病、慢性病后，可以针对相同诊断进行复诊。当患者出现病情变化需要医务人员亲自诊查时，医疗机构及其医务人员应当立即终止互联网诊疗活动，引导患者到实体医疗机构就诊。

不得对首诊患者开展互联网诊疗活动。

第十七条 医疗机构开展互联网诊疗活动应当按照《医疗机构病历管理规定》和《电子病历基本规范(试行)》等相关文件要求， 为患者建立电子病历，并按照规定进行管理。

第十八条 医疗机构开展互联网诊疗活动应当严格遵守《处方管理办法》等处方管理规定。医师掌握患者病历资料后， 可以为部分常见病、慢性病患者在线开具处方。在线开具的处方必须有医师电子签名， 经药师审核后，医疗机构、药品经营企业可委托符合条件的第三方机构配送。

第十九条 医疗机构开展互联网诊疗活动时，不得开具麻醉药品、精神药品等特殊管理药品的处方。为低龄儿童(6 岁以下)开具互联网儿童用药处方时，应当确认患儿有监护人和相关专业医师陪伴。

第二十条 医疗机构应当严格执行信息安全和医疗数据保密的有关法律法规，妥善保管患者信息，不得非法买卖、泄露患者信息。发生患者信息和医疗数据泄露后，医疗机构应当及时向主管的卫生健康行政部门报告，并立即采取有效应对措施。

第二十一条 医疗机构开展互联网诊疗活动应当符合分级诊疗相关规定，与其功能定位相适应。

第二十二条 鼓励医联体内利用互联网技术，加快实现医疗资源上下贯通，

提高基层医疗服务能力和效率，推动构建有序的分级诊疗格局。鼓励三级医院在医联体内通过互联网诊疗信息系统向下转诊患者。

第二十三条 三级医院应当优先发展与二级医院、基层医疗卫生机构之间的互联网医疗服务，为基层医疗卫生机构开展的互联网诊疗活动提供技术支持。

第四章 监督管理

第二十四条 医疗机构应当加强互联网诊疗活动管理，建立完善相关管理制度、服务流程， 保证互联网诊疗活动全程留痕、可追溯， 并向监管部门开放数据接口。

第二十五条 医师开展互联网诊疗活动应当依法取得相应执业资质，具有 3 年以上独立临床工作经验，并经其执业注册的医疗机构同意。

第二十六条 医疗机构开展互联网诊疗活动按照属地化管理的原则，由县级及以上地方卫生健康行政部门进行监督管理。

第二十七条 县级及以上地方卫生健康行政部门应当向社会公布允许开展互联网诊疗活动的医疗机构名单，公布监督电话或者其他监督方式，及时受理和处置违法违规互联网诊疗服务举报。发现不符合本办法规定的， 应当及时告知有关主管部门。

第二十八条 下级卫生健康行政部门未按照《医疗机构管理条例》和本办法规定管理互联网诊疗活动的，上级卫生健康行政部门应当及时予以纠正。

第二十九条 县级及以上地方卫生健康行政部门应当充分发挥社会组织作用，加强互联网诊疗活动的行业监督和自律。

第五章 附 则

第三十条 本办法施行前已经开展互联网诊疗活动的医疗机构，自本办法施行之日起 30 日内，按照本办法要求重新提出执业登记申请。

第三十一条 远程医疗服务按照《远程医疗服务管理规范(试行)》等相关文件管理。

互联网医院按照《互联网医院管理办法(试行)》管理。

第三十二条 本办法自发布之日起施行。

附件 2：

互联网医院管理办法(试行)

第一章 总 则

第一条 为落实《国务院办公厅关于促进“互联网＋医疗健康”发展的意见》，推动互联网医院持续健康发展，规范互联网医院管理，提高医疗服务效率，保证医疗质量和医疗安全，根据《执业医师法》、《医疗机构管理条例》等法律法规，制定本办法。

第二条 本办法所称互联网医院包括作为实体医疗机构第二名称的互联网医院，以及依托实体医疗机构独立设置的互联网医院(互联网医院基本标准见附录)。

第三条 国家按照《医疗机构管理条例》、《医疗机构管理条例实施细则》对互联网医院实行准入管理。

第四条 国务院卫生健康行政部门和中医药主管部门负责全国互联网医院的监督管理。地方各级卫生健康行政部门(含中医药主管部门，下同)负责辖区内互联网医院的监督管理。

第二章 互联网医院准入

第五条 实体医疗机构自行或者与第三方机构合作搭建信息平台，使用在本机构和其他医疗机构注册的医师开展互联网诊疗活动的，应当申请将互联网医院作为第二名称。

实体医疗机构仅使用在本机构注册的医师开展互联网诊疗活动的，可以申请将互联网医院作为第二名称。

第六条 实施互联网医院准入前，省级卫生健康行政部门应当建立省级互联网医疗服务监管平台，与互联网医院信息平台对接，实现实时监管。

第七条 申请设置互联网医院，应当向其依托的实体医疗机构执业登记机关提出设置申请，并提交以下材料：

(一)设置申请书；

(二)设置可行性研究报告，可根据情况适当简化报告内容；

(三)所依托实体医疗机构的地址；

(四)申请设置方与实体医疗机构共同签署的合作建立互联网医院的协议书。

第八条 新申请设置的实体医疗机构拟将互联网医院作为第二名称的，应当在设置申请书中注明，并在设置可行性研究报告中写明建立互联网医院的有关情况。如果与第三方机构合作建立互联网医院信息平台，应当提交合作协议。

第九条 卫生健康行政部门受理设置申请后，依据《医疗机构管理条例》、《医疗机构管理条例实施细则》的有关规定进行审核，在规定时间内作出同意或者不同意的书面答复。批准设置并同意其将互联网医院作为第二名称的，在《设置医疗机构批准书》中注明；批准第三方机构申请设置互联网医院的，发给《设置医疗机构批准书》。医疗机构按照有关法律法规和规章申请执业登记。

第十条 已经取得《医疗机构执业许可证》的实体医疗机构拟建立互联网医院，将互联网医院作为第二名称的，应当向其《医疗机构执业许可证》发证机关提出增加互联网医院作为第二名称的申请，并提交下列材料：

(一)医疗机构法定代表人或主要负责人签署同意的申请书，提出申请增加互联网医院作为第二名称的原因和理由；

(二)与省级互联网医疗服务监管平台对接情况；

(三)如果与第三方机构合作建立互联网医院，应当提交合作协议；

(四)登记机关规定提交的其他材料。

第十一条 执业登记机关按照有关法律法规和规章对互联网医院登记申请材料进行审核。审核合格的，予以登记。审核不合格的，将审核结果以书面形式通知申请人。

第十二条 互联网医院的命名应当符合有关规定，并满足以下要求：

(一)实体医疗机构独立申请互联网医院作为第二名称，应当包括“本机构名称＋互联网医院”；

(二)实体医疗机构与第三方机构合作申请互联网医院作为第二名称，应当包括“本机构名称＋合作方识别名称＋互联网医院”；

(三)独立设置的互联网医院，名称应当包括“申请设置方识别名称＋互联网医院”。

第十三条 合作建立的互联网医院，合作方发生变更或出现其他合作协议失效的情况时，需要重新申请设置互联网医院。

第三章 执业规则

第十四条 互联网医院执行由国家或行业学协会制定的诊疗技术规范和操作规程。

第十五条 互联网医院信息系统按照国家有关法律法规和规定，实施第三级

信息安全等级保护。

第十六条 在互联网医院提供医疗服务的医师、护士应当能够在国家医师、护士电子注册系统中进行查询。互联网医院应当对医务人员进行电子实名认证。鼓励有条件的互联网医院通过人脸识别等人体特征识别技术加强医务人员管理。

第十七条 第三方机构依托实体医疗机构共同建立互联网医院的，应当为实体医疗机构提供医师、药师等专业人员服务和信息技术支持服务， 通过协议、合同等方式明确各方在医疗服务、信息安全、隐私保护等方面的责权利。

第十八条 互联网医院必须对患者进行风险提示，获得患者的知情同意。

第十九条 患者在实体医疗机构就诊， 由接诊的医师通过互联网医院邀请其他医师进行会诊时，会诊医师可以出具诊断意见并开具处方；患者未在实体医疗机构就诊，医师只能通过互联网医院为部分常见病、慢性病患者提供复诊服务。互联网医院可以提供家庭医生签约服务。

当患者病情出现变化或存在其他不适宜在线诊疗服务的，医师应当引导患者到实体医疗机构就诊。

第二十条 互联网医院应当严格遵守《处方管理办法》等处方管理规定。在线开具处方前，医师应当掌握患者病历资料，确定患者在实体医疗机构明确诊断为某种或某几种常见病、慢性病后，可以针对相同诊断的疾病在线开具处方。

所有在线诊断、处方必须有医师电子签名。处方经药师审核合格后方可生效，医疗机构、药品经营企业可委托符合条件的第三方机构配送。不得在互联网上开具麻醉药品、精神类药品处方以及其他用药风险较高、有其他特殊管理规定的药品处方。为低龄儿童(6 岁以下)开具互联网儿童用药处方时，应当确定患儿有监护人和相关专业医师陪伴。

第二十一条 互联网医院开展互联网诊疗活动应当按照《医疗机构病历管理规定》和《电子病历基本规范(试行)》等相关文件要求，为患者建立电子病历，并按照规定进行管理。患者可以在线查询检查检验结果和资料、诊断治疗方案、处方和医嘱等病历资料。

第二十二条 互联网医院发生的医疗服务不良事件和药品不良事件按照国家有关规定上报。

第二十三条 互联网医院应当严格执行信息安全和医疗数据保密的有关法律

法规，妥善保管患者信息，不得非法买卖、泄露患者信息。发生患者信息和医疗数据泄露时，医疗机构应当及时向主管的卫生健康行政部门报告，并立即采取有效应对措施。

第二十四条 实体医疗机构或者与实体医疗机构共同申请互联网医院的第三方，应当为医师购买医疗责任保险。

第二十五条 互联网医院提供医疗服务应当符合分级诊疗相关规定，与依托的实体医疗机构功能定位相适应。

第二十六条 鼓励城市三级医院通过互联网医院与偏远地区医疗机构、基层医疗卫生机构、全科医生与专科医生的数据资源共享和业务协同， 促进优质医疗资源下沉。

第四章 监督管理

第二十七条 互联网医院应当严格按照国家法律法规加强内部各项管理。

第二十八条 互联网医院应当建立互联网医疗服务不良事件防范和处置流程，落实个人隐私信息保护措施，加强互联网医院信息平台内容审核管理，保证互联网医疗服务安全、有效、有序开展。

第二十九条 互联网医院提供诊疗服务的医师，应当依法取得相应执业资质，在依托的实体医疗机构或其他医疗机构注册，具有 3 年以上独立临床工作经验。互联网医院提供服务的医师，应当确保完成主要执业机构规定的诊疗工作。

第三十条 省级卫生健康行政部门与互联网医院登记机关，通过省级互联网医疗服务监管平台，对互联网医院共同实施监管，重点监管互联网医院的人员、处方、诊疗行为、患者隐私保护和信息安全等内容。将互联网医院纳入当地医疗质量控制体系，相关服务纳入行政部门对实体医疗机构的绩效考核和医疗机构评审，开展线上线下一体化监管，确保医疗质量和医疗安全。

第三十一条 县级及以上地方卫生健康行政部门应当向社会公布互联网医院名单及监督电话或者其他监督方式，及时受理和处置违法违规互联网医疗服务的举报。发现不符合本办法规定的，应当及时告知相关主管部门。

第三十二条 取得《医疗机构执业许可证》的互联网医院，独立作为法律责任主体；实体医疗机构以互联网医院作为第二名称时，实体医疗机构为法律责任主体。互联网医院合作各方按照合作协议书承担相应法律责任。

患者与互联网医院发生医疗纠纷时，应当向互联网医院登记机关提出处理申请，按照有关法律、法规和规定追偿法律责任。

第三十三条 医疗机构和医务人员在开展互联网医疗服务过程中，有违反《执业医师法》、《医疗机构管理条例》、《医疗事故处理条例》和《护士条例》等法律、法规行为的，按照有关法律、法规规定处理。

第三十四条 下级卫生健康行政部门未按照《医疗机构管理条例》和本办法规定管理互联网医院的，上级卫生健康行政部门应当及时予以纠正。

第五章 附 则

第三十五条 本办法施行前已经批准设置或备案的互联网医院，自本办法施行之日起 30 日内，按照本办法要求重新提出设置和执业登记申请。

第三十六条 本办法自发布之日起施行。

附录

互联网医院基本标准(试行)

申请设置互联网医院或者以互联网医院作为第二名称的，应当符合本标准。

一、诊疗科目

互联网医院根据开展业务内容确定诊疗科目，不得超出所依托的实体医疗机构诊疗科目范围。

二、科室设置

互联网医院根据开展业务内容设置相应临床科室，并与所依托的实体医疗机构临床科室保持一致。必须设置医疗质量管理部门、信息技术服务与管理部门、药学服务部门。

三、人员

(一)互联网医院开设的临床科室，其对应的实体医疗机构临床科室至少有 1 名正高级、1 名副高级职称的执业医师注册在本机构(可多点执业)。

(二)互联网医院有专人负责互联网医院的医疗质量、医疗安全、电子病历的管理，提供互联网医院信息系统维护等技术服务，确保互联网医院系统稳定运行。

(三)有专职药师负责在线处方审核工作，确保业务时间至少有 1 名药师在岗审核处方。药师人力资源不足时， 可通过合作方式，由具备资格的第三方机构药师进行处方审核。

(四)相关人员必须经过医疗卫生法律法规、医疗服务相关政策、各项规章制度、岗位职责、流程规范和应急预案的培训， 确保其掌握服务流程，明确可能存在的风险。

四、房屋和设备设施

(一)用于互联网医院运行的服务器不少于 2 套，数据库服务器与应用系统服务器需划分。存放服务器的机房应当具备双路供电或紧急发电设施。存储医疗数据的服务器不得存放在境外。

(二)拥有至少 2 套开展互联网医院业务的音视频通讯系统(含必要的软件系统和硬件设备)。

(三)具备高速率高可靠的网络接入，业务使用的网络带宽不低于 10Mbps，且至少由两家宽带网络供应商提供服务。鼓励有条件的互联网医院接入互联网专线、虚拟专用网 (VPN)，保障医疗相关数据传输服务质量。

(四)建立数据访问控制信息系统，确保系统稳定和服务全程留痕，并与实体医疗机构的 HIS、PACS/RIS、LIS 系统实现数据交换与共享。

(五)具备远程会诊、远程门诊、远程病理诊断、远程医学影像诊断和远程心电诊断等功能。

(六)信息系统实施第三级信息安全等级保护。

五、规章制度

建立互联网医疗服务管理体系和相关管理制度、人员岗位职责、服务流程。规章制度应当包括互联网医疗服务管理制度、互联网医院信息系统使用管理制度、互联网医疗质量控制和评价制度、在线处方管理制度、患者知情同意与登记制度、在线医疗文书管理制度、在线复诊患者风险评估与突发状况预防处置制度、人员培训考核制度，停电、断网、设备故障、网络信息安全等突发事件的应急预案。

附件 3：

远程医疗服务管理规范(试行)

为贯彻落实《国务院办公厅关于促进“互联网＋医疗健康”发展的意见》(国办发〔2018〕26 号)，进一步推动远程医疗服务持续健康发展，优化医疗资源配置，促进优质医疗资源下沉，推进区域医疗资源整合共享，提高医疗服务能力和水平，制定本规范。

一、管理范围

本规范所称远程医疗服务包括以下情形：

(一)某医疗机构(以下简称邀请方)直接向其他医疗机构(以下简称受邀方)发出邀请，受邀方运用通讯、计算机及网络技术等信息化技术， 为邀请方患者诊疗提供技术支持的医疗活动，双方通过协议明确责权利。

(二)邀请方或第三方机构搭建远程医疗服务平台，受邀方以机构身份在该平台注册，邀请方通过该平台发布需求，由平台匹配受邀方或其他医疗机构主动对需求做出应答，运用通讯、计算机及网络技术等信息化技术， 为邀请方患者诊疗提供技术支持的医疗活动。邀请方、平台建设运营方、受邀方通过协议明确责权利。

邀请方通过信息平台直接邀请医务人员提供在线医疗服务的，必须申请设置互联网医院，按照《互联网医院管理办法(试行)》管理。

二、开展远程医疗服务的基本条件

(一)医疗机构基本条件。

1.有卫生健康行政部门(含中医药主管部门，下同)批准、与所开展远程医疗服务相应的诊疗科目。

2.有在本机构注册、符合远程医疗服务要求的专业技术人员。

3.有完善的远程医疗服务管理制度、医疗质量与医疗安全、信息化技术保障措施。

(二)人员基本条件。

邀请方与受邀方应当根据患者病情安排相应医务人员参与远程医疗服务。邀请方至少有 1 名执业医师(可多点执业)陪同，若邀请方为基层医疗卫生机构，可以由执业助理医师或乡村医生陪同；受邀方至少有 1 名具有相应诊疗服务能力、独立开展临床工作 3 年以上的执业医师(可多点执业)为患者提供远程医疗服务。根据患者病情，可提供远程多学科联合诊疗服务。

有专职人员负责仪器、设备、设施、信息系统的定期检测、登记、维护、改造、升级， 符合远程医疗相关卫生信息标准和信息安全的规定，保障远程医疗服务信息系统(硬件和软件)处于正常运行状态，满足医疗机构开展远程医疗服务的需要。

(三)设备设施基本条件。

1.远程医疗信息系统应当满足图像、声音、文字以及诊疗所需其他医疗信息的安全、实时传输， 图像清晰，数据准确，符合《远程医疗信息系统建设技术指南》，满足临床诊疗要求。

2.重要设备和网络应当有不间断电源。

3.远程医疗服务网络应当至少有 2 家网络供应商提供的网络，保障远程医疗服务信息传输通畅。有条件的可以建设远程医疗专网。

三、远程医疗服务流程及有关要求

(一)签订合作协议。医疗机构间直接或通过第三方平台开展远程医疗服务的，要签订远程医疗合作协议，约定合作目的、合作条件、合作内容、远程医疗流程、各方责任权利义务、医疗损害风险和责任分担等事项。合作协议可以以电子文件形式签订。

(二)知情同意。邀请方应当根据患者的病情和意愿组织远程医疗服务， 并向患者说明远程医疗服务内容、费用等情况， 征得患者书面同意，签署远程医疗服务知情同意书。不宜向患者说明病情的，应当征得其监护人或者近亲属书面同意。

(三)远程会诊。医疗机构之间通过远程进行会诊，受邀方提供诊断治疗意见，邀请方明确诊断治疗方案。

1.发出邀请。邀请方需要与受邀方通过远程医疗服务开展个案病例讨论的，需向受邀方直接或通过第三方平台提出邀请，邀请至少应当包括邀请事由、目的、时间安排、患者相关病历摘要及拟邀请医师的专业和技术职务任职资格等。医疗联合体内可以协商建立稳定的远程心电诊断、远程影像诊断、远程病理诊断等机制，加强上级医院对基层医疗机构的技术支持。

2.接受邀请。受邀方接到邀请方或第三方平台发出的远程医疗服务邀请后，要及时作出是否接受邀请的决定。接受邀请的， 须告知邀请方，并做好相关准备工作；不接受邀请的，及时告知邀请方并说明理由。第三方平台参与匹配的， 还要同时将是否接受邀请告知第三方平台运营方。

3.实施服务。受邀方应当认真负责地安排具备相应资质和技术能力的医务人员，按照相关法律、法规和诊疗规范的要求， 提供远程医疗服务，及时将诊疗意见告知邀请方，并出具由相关医师签名的诊疗意见报告。邀请方根据患者临床资

料，参考受邀方的诊疗意见，决定诊断与治疗方案。

(四)远程诊断。邀请方和受邀方建立对口支援或者形成医疗联合体等合作关系，由邀请方实施医学影像、病理、心电、超声等辅助检查，由受邀的上级医疗机构进行诊断，具体流程由邀请方和受邀方通过协议明确。

(五)妥善保存资料。邀请方和受邀方要按照病历书写及保管有关规定共同完成病历资料，原件由邀请方和受邀方分别归档保存。远程医疗服务相关文书可通过传真、扫描文件及电子签名的电子文件等方式发送。医务人员为患者提供咨询服务后，应当记录咨询信息。

四、管理要求

(一)机构管理。开展远程医疗服务的医疗机构应当按照以下要求开展工作：

1.制定并落实管理规章制度，执行国家发布或者认可的技术规范和操作规程，建立应急预案，保障医疗质量与安全。

2.设置专门的医疗质量安全管理部门或配备专职人员，负责远程医疗服务质量管理与控制工作，履行以下职责：

①对规章制度、技术规范、操作规程的落实情况进行检查；

②对医疗质量、器械和设备管理等方面进行检查；

③对重点环节和影响医疗质量与安全的高危因素进行监测、分析和反馈， 提出预防与控制措施；

④对病历书写、资料保存进行指导和检查等。

3.医疗质量安全管理人员应当具备相关专业知识和工作经验。

4.参与远程医疗运行各方应当加强信息安全和患者隐私保护，防止违法传输、修改，防止数据丢失，建立数据安全管理规程，确保网络安全、操作安全、数据安全、隐私安全。

5.与第三方机构合作发展远程医疗服务的，要通过协议明确各方权利、义务和法律责任，落实财务管理各项制度。

(二)人员管理。

1.医疗机构应当制定并落实远程医疗服务相关医务人员的培训计划，使其具备与本职工作相关的专业知识。建立对技术人员的专业知识更新、专业技能维持与培养等管理的相关制度和记录。落实相关管理制度和工作规范。

2.医务人员对患者进行远程医疗服务时应当遵守医疗护理常规和诊疗规范。

(三)质量管理。开展远程医疗服务的医疗机构应当按照以下要求开展医疗质量管理工作:

1.按照国家发布或认可的诊疗技术规范和操作规程有关要求，建立并实施医疗质量管理体系，遵守相关技术规范和标准，实行患者实名制管理，持续改进医疗质量。

2.积极参与省级以上远程医疗服务质控中心组织的医疗质量管理与控制相关工作，接受卫生健康行政部门和质控中心的业务指导与监管。

3.医疗质量安全管理人员督促落实各项规章制度和日常管理工作，并对本机构远程医疗服务行为进行定期巡视。

4.信息技术专业人员做好远程医疗设备的日常维护，保证其正常运转。

5.受邀方参与远程医疗服务的医务人员应当具有应急处理能力。

6.提供医学检查检验等服务的远程医疗服务中心，应当配备具有相应资质的卫生专业技术人员，按照相应的规范开展工作。

7.建立良好的医患沟通机制，保障患者知情同意权，维护患者合法权益。

8.严格按照有关规定与要求，规范使用和管理医疗设备、医疗耗材、消毒药械和医疗用品等。

五、加强监管

(一)地方各级卫生健康行政部门应当加强对辖区内医疗机构提供远程医疗服务的监督管理，将远程医疗服务纳入当地医疗质量控制体系，确保远程医疗服务质量和安全。

(二)在远程医疗服务过程中发生医疗争议时，患者向邀请方所在地卫生健康行政部门提出处理申请。远程会诊由邀请方承担相应法律责任， 远程诊断由邀请方和受邀方共同承担相应法律责任。

(三)医疗机构与第三方机构合作开展远程医疗服务发生争议时，由邀请方、受邀方、第三方机构按照相关法律、法规和各方达成的协议进行处理， 并承担相应的责任。

(四)医疗机构和医务人员在开展远程医疗服务过程中，有违反《执业医师法》、《医疗机构管理条例》、《医疗事故处理条例》和《护士条例》等法律、法规行为

的，由卫生健康行政部门按照有关法律、法规规定处理。

国家卫生健康委办公厅 国家中医药局办公室关于印发互联网诊疗监管细则(试行)的通知

国卫办医发〔2022〕2 号

各省、自治区、直辖市及新疆生产建设兵团卫生健康委、中医药管理局：

为进一步规范互联网诊疗活动，加强互联网诊疗体系建设，国家卫生健康委办公厅和国家中医药局办公室联合制定了《互联网诊疗监管细则(试行)》，现印发给你们，请认真贯彻落实。

国家卫生健康委办公厅 国家中医药局办公室

2022 年 2 月 8 日

互联网诊疗监管细则(试行)

第一章 总 则

第一条 为进一步规范互联网诊疗活动，加强互联网诊疗监管，根据《基本医疗卫生与健康促进法》《医师法》《中医药法》《医疗机构管理条例》《互联网诊疗管理办法(试行)》《互联网医院管理办法(试行)》等法律法规和规定，制定本细则。

第二条 本细则适用于对医疗机构根据《互联网诊疗管理办法(试行)》《互联网医院管理办法(试行)》开展互联网诊疗活动的监管。

第三条 国务院卫生健康主管部门和中医药主管部门负责指导全国互联网诊疗监管工作。地方各级卫生健康主管部门(含中医药主管部门，下同)落实属地化监管责任。

第二章 医疗机构监管

第四条 省级卫生健康主管部门应当建立省级互联网医疗服务监管平台(以下简称“省级监管平台”)，对开展互联网诊疗活动的医疗机构(以下简称“医疗机构”)进行监管。

第五条 医疗机构应当主动与所在地省级监管平台对接，及时上传、更新《医疗机构执业许可证》等相关执业信息，主动接受监督。

第六条 医疗机构应当有专门部门管理互联网诊疗的医疗质量、医疗安全、药学服务、信息技术等，建立相应的管理制度，包括但不限于医疗机构依法执

业自查制度、互联网诊疗相关的医疗质量和安全管理制度、医疗质量(安全)不良事件报告制度、医务人员培训考核制度、患者知情同意制度、处方管理制度、电子病历管理制度、信息系统使用管理制度等。

第七条 作为实体医疗机构第二名称的互联网医院，与该实体医疗机构同时校验；依托实体医疗机构单独获得《医疗机构执业许可证》的互联网医院，每年校验 1 次。

第八条 医疗机构应当在互联网诊疗平台显著位置公布本机构提供互联网诊疗服务医务人员的电子证照等信息，方便患者查询。

第九条 医疗机构应当充分告知患者互联网诊疗相关的规则、要求、风险，取得患者知情同意后方可开展互联网诊疗活动。

第十条 地方各级卫生健康主管部门应当向社会公布辖区内批准开展互联网诊疗的医疗机构名单、监督电话及其他监督方式，设置投诉受理渠道，及时处置违法违规行为。

第十一条 地方各级卫生健康主管部门应当按照《医疗机构管理条例》及其实施细则，对互联网诊疗活动建立评价和退出机制。

第三章 人员监管

第十二条 医疗机构应当对开展互联网诊疗活动的医务人员进行实名认证，确保医务人员具备合法资质。

第十三条 医师接诊前需进行实名认证，确保由本人提供诊疗服务。其他人员、人工智能软件等不得冒用、替代医师本人提供诊疗服务。各级卫生健康主管部门应当负责对在该医疗机构开展互联网诊疗的人员进行监管。

第十四条 医疗机构应当将开展互联网诊疗活动的医务人员信息上传至省级监管平台，包括身份证号码、照片、相关资质、执业地点、执业机构、执业范围、临床工作年限等必要信息。省级监管平台应当与医师、护士电子化注册系统对接，药师信息应当上传监管平台且可查询，有条件的同时与卫生健康监督信息系统对接。

医疗机构应当对开展互联网诊疗活动的医务人员建立考核机制，根据依法执业、医疗质量、医疗安全、医德医风、满意度等内容进行考核并建立准入、退出机制。

第十五条 医疗机构应当对开展互联网诊疗活动以及从事相关管理服务的人员开展定期培训，内容包括卫生健康相关的法律法规、医疗管理相关政策、岗位职责、互联网诊疗流程、平台使用与应急处置等。

第十六条 医务人员如在主执业机构以外的其他互联网医院开展互联网诊疗活动，应当根据该互联网医院所在地多机构执业相关要求进行执业注册或备案。

第四章 业务监管

第十七条 互联网诊疗实行实名制，患者有义务向医疗机构提供真实的身份证明及基本信息，不得假冒他人就诊。

第十八条 患者就诊时应当提供具有明确诊断的病历资料，如门诊病历、住院病历、出院小结、诊断证明等，由接诊医师留存相关资料，并判断是否符合复诊条件。

医疗机构应当明确互联网诊疗的终止条件。当患者病情出现变化、本次就诊经医师判断为首诊或存在其他不适宜互联网诊疗的情况时，接诊医师应当立即终止互联网诊疗活动，并引导患者到实体医疗机构就诊。

第十九条 医疗机构开展互联网诊疗过程中所产生的电子病历信息，应当与依托的实体医疗机构电子病历格式一致、系统共享，由依托的实体医疗机构开展线上线下一体化质控。

互联网诊疗病历记录按照门诊电子病历的有关规定进行管理，保存时间不得少于 15 年。诊疗中的图文对话、音视频资料等过程记录保存时间不得少于 3 年。

第二十条 互联网医院变更名称时，所保管的病历等数据信息应当由变更后的互联网医院继续保管。

互联网医院注销后，所保管的病历等数据信息由依托的实体医疗机构继续保管。所依托的实体医疗机构注销后，可以由省级卫生健康主管部门或者省级卫生健康主管部门指定的机构按照规定妥善保管。

第二十一条 医疗机构开展互联网诊疗活动应当严格遵守《处方管理办法》等规定，加强药品管理。处方应由接诊医师本人开具，严禁使用人工智能等自动生成处方。处方药应当凭医师处方销售、调剂和使用。严禁在处方开具前，

向患者提供药品。严禁以商业目的进行统方。

第二十二条 医疗机构自行或委托第三方开展药品配送的，相关协议、处方流转信息应当可追溯，并向省级监管平台开放数据接口。

第二十三条 互联网诊疗的医疗服务收费项目和收费标准应当在互联网诊疗平台进行公示，方便患者查询。

第二十四条 医疗机构要自觉加强行风建设，严格执行《医疗机构工作人员廉洁从业九项准则》等有关规定，医务人员的个人收入不得与药品收入相挂钩，严禁以谋取个人利益为目的转介患者、指定地点购买药品、耗材等。

第二十五条 医疗机构应当保证互联网诊疗活动全程留痕、可追溯，并向省级监管平台开放数据接口。省级卫生健康主管部门应当按照“最少可用原则”采集医疗机构的相关数据，重点包括医疗机构资质、医务人员资质、诊疗科目、诊疗病种、电子病历、电子处方、用药情况、满意度评价、患者投诉、医疗质量(安全)不良事件等信息，对互联网诊疗整体情况进行分析，定期向各医疗机构及其登记机关反馈问题，并明确整改期限，医疗机构在收到省级卫生健康主管部门问题反馈后应当及时整改，并将整改情况上传至省级监管平台，同时报其登记机关。

鼓励有条件的省份在省级监管平台中设定互联网诊疗合理性判定规则，运用人工智能、大数据等新兴技术实施分析和监管。

第五章 质量安全监管

第二十六条 医疗机构开展互联网诊疗活动应当遵守医疗质量、医疗安全、网络安全等有关法律法规和规定。

第二十七条 医疗机构应建立网络安全、数据安全、个人信息保护、隐私保护等制度，并与相关合作方签订协议，明确各方权责关系。

第二十八条 医疗机构发生患者个人信息、医疗数据泄露等网络安全事件时，应当及时向相关主管部门报告，并采取有效应对措施。

第二十九条 医疗机构应当对互联网诊疗活动的质量安全进行控制，并设置患者投诉处理的信息反馈渠道。

第三十条 医疗机构应当建立医疗质量(安全)不良事件报告制度，指定专门部门负责医疗质量(安全)不良事件报告的收集、分析和总结工作，鼓励医务人

员积极报告不良事件。

第三十一条 医疗机构应当加强互联网诊疗信息发布的内容管理，确保信息合法合规、真实有效。

第三十二条 地方各级卫生健康主管部门应当指导医疗机构加强医疗质量安全管理工作，实现持续改进。

第三十三条 省级监管平台和医疗机构用于互联网诊疗平台应当实施第三级及以上信息安全等级保护，并将等保测评结果上传至省级监管平台。

第六章 监管责任

第三十四条 取得《医疗机构执业许可证》并独立设置的互联网医院，依法承担法律责任；实体医疗机构以互联网医院作为第二名称时，实体医疗机构依法承担法律责任。互联网医院合作各方按照合作协议书依法依规承担相应法律责任。

第三十五条 医疗机构和医务人员在互联网诊疗过程中，有违反《医师法》《传染病防治法》《中医药法》《医疗机构管理条例》《医疗事故处理条例》《护士条例》等法律法规行为的，按照有关法律法规和规定处理。

第三十六条 医疗机构在开展互联网诊疗活动过程中发生医疗事故或者引发医疗纠纷的，应当按照《医疗事故处理条例》《医疗纠纷预防和处理条例》等有关法律法规和规定处理。医疗机构所在地县级以上卫生健康主管部门应当按照相关法律法规履行相应处理责任。

第三十七条 省级卫生健康主管部门应当将互联网诊疗纳入当地医疗质量控制体系，开展线上线下一体化监管，确保医疗质量和医疗安全。

第七章 附 则

第三十八条 国家通过信息系统对全国互联网诊疗相关数据进行监测分析。

第三十九条 省级卫生健康主管部门应当根据本细则并结合当地实际情况，制定实施办法。

第四十条 本细则由国家卫生健康委负责解释。

第四十一条 本细则自印发之日起施行。

国家卫生健康委 国家中医药局 国家疾控局关于印发医疗卫生机构网络安全管理办法的通知

国卫规划发〔2022〕29 号

各省、自治区、直辖市及新疆生产建设兵团卫生健康委、中医药局，国家卫生健康委机关各司局、委直属和联系单位、中国老龄协会，国家中医药局、国家疾控局机关各司局、各直属单位：

为指导医疗卫生机构加强网络安全管理，国家卫生健康委、国家中医药局、国家疾控局制定了《医疗卫生机构网络安全管理办法》。现印发给你们，请认真贯彻执行。

国家卫生健康委 国家中医药局 国家疾控局

2022 年 8 月 8 日

医疗卫生机构网络安全管理办法

第一章 总 则

第一条 为加强医疗卫生机构网络安全管理，进一步促进“互联网+医疗健康”发展，充分发挥健康医疗大数据作为国家重要基础性战略资源的作用，加强医疗卫生机构网络安全管理，防范网络安全事件发生，根据《基本医疗卫生与健康促进法》《网络安全法》《密码法》《数据安全法》《个人信息保护法》《关键信息基础设施安全保护条例》《网络安全审查办法》以及网络安全等级保护制度等有关法律法规标准，制定本办法。

第二条 坚持网络安全为人民、网络安全靠人民、坚持网络安全教育、技术、产业融合发展、坚持促进发展和依法管理相统一、坚持安全可控和开放创新并重。

坚持分等级保护、突出重点。重点保障关键信息基础设施、网络安全等级保护第三级(以下简称第三级)及以上网络以及重要数据和个人信息安全。

坚持积极防御、综合防护。充分利用人工智能、大数据分析等技术，强化安全监测、态势感知、通报预警和应急处置等重点工作，落实网络安全保护“实战化、体系化、常态化”和“动态防御、主动防御、纵深防御、精准防护、整体防控、联防联控”的“三化六防”措施。

坚持“管业务就要管安全”“谁主管谁负责、谁运营谁负责、谁使用谁负责”的原则，落实网络安全责任制，明确各方责任。

第三条 本办法所称的网络是指由计算机或者其他信息终端及相关设备组成

的按照一定的规则和程序对信息进行收集、存储、传输、交换、处理的系统。

本办法所称的数据为网络数据，是指医疗卫生机构通过网络收集、存储、传输、处理和产生的各种电子数据，包括但不限于各类临床、科研、管理等业务数据、医疗设备产生的数据、个人信息以及数据衍生物。

本办法适用于医疗卫生机构运营网络的安全管理。未纳入区域基层卫生信息系统的基层医疗卫生机构参照执行。

第四条 国家卫生健康委、国家中医药局、国家疾控局负责统筹规划、指导、评估、监督医疗卫生机构网络安全工作。县级以上地方卫生健康行政部门(含中医药和疾控部门，下同)负责本行政区域内医疗卫生机构网络安全指导监督工作。

医疗卫生机构对本单位网络安全管理负主体责任，各医疗卫生机构应当与信息化建设参与单位及相关医疗设备生产经营企业书面约定各方的网络安全义务和违约责任。

第二章 网络安全管理

第五条 各医疗卫生机构应成立网络安全和信息化工作领导小组，由单位主要负责人任领导小组组长，每年至少召开一次网络安全办公会，部署安全重点工作，落实《关键信息基础设施安全保护条例》和网络安全等级保护制度要求。有二级及以上网络的医疗卫生机构应明确负责网络安全管理工作的职能部门，明确承担安全主管、安全管理员等职责的岗位；建立网络安全管理制度体系，加强网络安全防护，强化应急处置，在此基础上对关键信息基础设施实行重点保护，防止网络安全事件发生。

第六条 各医疗卫生机构按照“谁主管谁负责、谁运营谁负责、谁使用谁负责”的原则，在网络建设过程中明确本单位各网络的主管部门、运营部门、信息化部门、使用部门等管理职责，对本单位运营范围内的网络进行等级保护定级、备案、测评、安全建设整改等工作。

(一)对新建网络，应在规划和申报阶段确定网络安全保护等级。各医疗卫生机构应全面梳理本单位各类网络，特别是云计算、物联网、区块链、5G、大数据等新技术应用的基本情况，并根据网络的功能、服务范围、服务对象和处理数据等情况，依据相关标准科学确定网络的安全保护等级，并报上级主管部

门审核同意。

(二)新建网络投入使用应依法依规开展等级保护备案工作。第二级以上网络应在网络安全保护等级确定后 10 个工作日内，由其运营者向公安机关备案，并将备案情况报上级卫生健康行政部门，因网络撤销或变更安全保护等级的，应在 10 个工作日内向原备案公安机关撤销或变更，同步上报上级卫生健康行政部门。

(三)全面梳理分析网络安全保护需求，按照“一个中心(安全管理中心)，三重防护(安全通信网络、安全区域边界、安全计算环境)”的要求，制定符合网络安全保护等级要求的整体规划和建设方案，加强信息系统自行开发或外包开发过程中的安全管理，认真开展网络安全建设，全面落实安全保护措施。

(四)各医疗卫生机构对已定级备案网络的安全性进行检测评估，第三级或第四级的网络应委托等级保护测评机构，每年至少一次开展网络安全等级测评。第二级的网络应委托等级保护测评机构定期开展网络安全等级测评，其中涉及 10 万人以上个人信息的网络应至少三年开展一次网络安全等级测评，其他的网络至少五年开展一次网络安全等级测评。新建的网络上线运行前应进行安全性测试。

(五)针对等级测评中发现的问题隐患，各医疗卫生机构要结合外在的威胁风险，按照法律法规、政策和标准要求，制定网络安全整改方案，有针对性地开展整改，及时消除风险隐患，补强管理和技术短板，提升安全防护能力。

第七条 各医疗卫生机构应依托国家网络安全信息通报机制，加强本单位网络安全通报预警力量建设。鼓励三级医院探索态势感知平台建设，及时收集、汇总、分析各方网络安全信息，加强威胁情报工作，组织开展网络安全威胁分析和态势研判，及时通报预警和处置，防止网络被破坏、数据外泄等事件。

第八条 各医疗卫生机构应建立应急处置机制，通过建立完善应急预案、组织应急演练等方式，有效处理网络中断、网络攻击、数据泄露等安全事件，提高应对网络安全事件能力。积极参加网络安全攻防演练，提升保护和对抗能力。

第九条 各医疗卫生机构在网络运营过程中，应每年开展文档核验、漏洞扫描、渗透测试等多种形式的安全自查，及时发现可能存在的问题和隐患。针对

安全自查、监测预警、安全通报等过程中发现的安全隐患应认真开展整改加固，防止网络带病运行，并按要求将安全自查整改情况报上级卫生健康行政部门。自查整改可与等级测评问题整改一并实施。

每年安全自查整改工作包括：

(一)依据上级主管监管机构要求，各医疗卫生机构完成信息资产梳理，摸清本单位网络定级、备案等情况，形成资产清单，组织安全自查。

(二)依据上级主管监管机构要求，各医疗卫生机构依据安全自查结果，对发现的问题和隐患进行整改，形成整改报告向有关主管监管机构报备。

第十条 关键信息基础设施运营者应对安全管理机构负责人和关键岗位人员进行安全背景审查。各医疗卫生机构要加强网络运营相关人员管理，包括本单位内部人员及第三方人员，明确内部人员入职、培训、考核、离岗全流程安全管理，针对第三方应明确人员接触网络时的申请及批准流程，做好实名登记、人员背景审查、保密协议签署等工作，防止因人员资质及违规操作引发的安全风险。

第十一条 加强网络运维管理，制定运维操作规范和工作流程。加强物理安全防护，完善机房、办公环境及运维现场等安全控制措施，防止非授权访问物理环境造成信息泄露。加强远程运维管理，因业务确需通过互联网远程运维的，应进行评估论证，并采取相应的安全管控措施，防止远程端口暴露引发安全事件。

第十二条 各医疗卫生机构应加强业务连续性管理并持续监测网络运行状态。对于第三级及以上的网络应加强保障关键链路、关键设备冗余备份，有条件的医疗卫生机构应建立应用级容灾备份，防止关键业务中断。

第十三条 应用大数据、人工智能、区块链等新技术开展服务时，上线前应评估新技术的安全风险并进行安全管控，达到应用与安全的平衡。

第十四条 各医疗卫生机构应规范和加强医疗设备数据、个人信息保护和网络安全管理，建立健全医疗设备招标采购、安装调试、运行使用、维护维修、报废处置等相关网络安全管理制度，定期检查或评估医疗设备网络安全，并采取相应的安全管控措施，确保医疗设备网络安全。

第十五条 各医疗卫生机构应按照《密码法》等有关法律法规和密码应用相

关标准规范，在网络建设过程中同步规划、同步建设、同步运行密码保护措施，使用符合相关要求的密码产品和服务。

第十六条 各医疗卫生机构应关注整个网络全链条参与者的安全管理，涉及非本单位的第三方时，应对设计、建设、运行、维护等服务实施安全管理，采购安全的网络产品和服务，防止发生第三方安全事件。

第十七条 各医疗卫生机构应加强废止网络的安全管理，对废止网络的相关设备进行风险评估，及时对其采取封存或销毁措施，确保废止网络中的数据处置安全，防止网络数据泄露。

第三章 数据安全管理

第十八条 各医疗卫生机构应按照有关法律法规的规定，参照国家网络安全标准，履行数据安全保护义务，坚持保障数据安全与发展并重，通过管理和技术手段保障数据安全和数据应用的有效平衡。关键信息基础设施运营者应拟定关键信息基础设施安全保护计划，建立健全数据安全和个人信息保护制度。

第十九条 应建立数据安全管理组织架构，明确业务部门与管理部门在数据安全活动中的主体责任，通过安全责任书等方式，规范本单位数据管理部门、业务部门、信息化部门在数据安全管理全生命周期当中的权责，建立数据安全工作责任制，落实追责追究制度。

第二十条 各医疗卫生机构应每年对数据资产进行全面梳理，在落实网络安全等级保护制度的基础上，依据数据的重要程度以及遭到破坏后的危害程度建立本单位数据分类分级标准。数据分类分级应遵循合法合规原则、可执行原则、时效性原则、自主性原则、差异性原则及客观性原则。

第二十一条 各医疗卫生机构应建立健全数据安全管理制度、操作规程及技术规范，涉及的管理制度每年至少修订一次，建议相关人员每年度签署保密协议。每年对本单位的数据进行数据安全风险评估，及时掌握数据安全状态。加强数据安全教育培训，组织安全意识教育和数据安全管理制度宣传培训。结合本单位实际，建立完善数据使用申请及批准流程，遵循“谁主管、谁审查”、遵循事前申请及批准、事中监管、事后审核原则，严格执行业务管理部门同意、医疗卫生机构领导核准的工作程序，指导数据活动流程合规。

第二十二条 各医疗卫生机构应加强数据收集、存储、传输、处理、使用、

交换、销毁全生命周期安全管理工作，数据全生命周期活动应在境内开展，因业务确需向境外提供的，应当按照相关法律法规及有关要求进行安全评估或审核，针对影响或者可能影响国家安全的数据处理活动需提交国家安全审查，防止数据安全事件发生。

(一)各医疗卫生机构应加强数据收集合法性管理，明确业务部门和管理部门在数据收集合法性中的主体责任。采取数据脱敏、数据加密、链路加密等防控措施，防止数据收集过程中数据被泄露。

(二)在数据分类分级的基础上，进一步明确不同安全级别数据的加密传输要求。加强传输过程中的接口安全控制，确保在通过接口传输时的安全性，防止数据被窃取。

(三)各医疗卫生机构应按照有关法规标准，选择合适的数据存储架构和介质在境内存储，并采取备份、加密等措施加强数据的存储安全。涉及到云上存储数据时，应当评估可能带来的安全风险。数据存储周期不应超出数据使用规则确定的保存期限。加强存储过程中访问控制安全、数据副本安全、数据归档安全管控。

(四)各医疗卫生机构应严格规定不同人员的权限，加强数据使用过程中的申请及批准流程管理，确保数据在可控范围内使用，加强日志留存及管理工作，杜绝篡改、删除日志的现象发生，防止数据越权使用。各数据使用部门和数据使用人须严格按照申请所述用途与范围使用数据，对数据的安全负责。未经批准，任何部门和个人不得将未对外公开的信息数据传递至部门外，不得以任何方式将其泄露。

(五)各医疗卫生机构发布、共享数据时应当评估可能带来的安全风险，并采取必要的安全防控措施；涉及数据上报时，应由数据上报提出方负责解读上报要求，确定上报范围和上报规则，确保数据上报安全可控。

(六)各医疗卫生机构开展人脸识别或人脸辨识时，应同时提供非人脸识别的身份识别方式，不得因数据主体不同意收集人脸识别数据而拒绝数据主体使用其基本业务功能，人脸识别数据不得用于除身份识别之外的其他目的，包括但不限于评估或预测数据主体工作表现、经济状况、健康状况、偏好、兴趣等。各医疗卫生机构应采取安全措施存储和传输人脸识别数据，包括但不限于

加密存储和传输人脸识别数据，采用物理或逻辑隔离方式分别存储人脸识别和个人身份信息等。

(七)数据销毁时应采用确保数据无法还原的销毁方式，重点关注数据残留风险及数据备份风险。

第四章 监督管理

第二十三条 各医疗卫生机构应积极配合有关主管监管机构监督管理，接受网络安全管理日常检查，做好网络安全防护等工作。

第二十四条 各医疗卫生机构应及时整改有关主管监管机构检查过程中发现的漏洞和隐患等问题，杜绝重大网络安全事件发生。

第二十五条 发生个人信息和数据泄露、毁损、丢失等安全事件和网络系统遭攻击、入侵、控制等网络安全事件，或者发现网络存在漏洞隐患、网络安全风险明显增大时，各医疗卫生机构应当立即启动应急预案，采取必要的补救和处置措施，及时以电话、短信、邮件或信函等多种方式告知相关主体，并按照要求向有关主管监管部门报告。

第二十六条 各级卫生健康行政部门应建立网络安全事件通报工作机制，及时通报网络安全事件。

第二十七条 发生网络安全事件时，各医疗卫生机构应及时向卫生健康行政部门、公安机关报告，做好现场保护、留存相关记录，为公安机关等监管部门依法维护国家安全和开展侦查调查等活动提供技术支持和协助。

第五章 管理保障

第二十八条 各医疗卫生机构应高度重视网络安全管理工作，将其列入重要议事日程，加强统筹领导和规划设计，依法依规落实人员、经费投入、安全保护措施建设等重大问题，保证信息系统建设时安全保护措施同步规划、同步建设和同步使用。

第二十九条 各医疗卫生机构应加强网络安全业务交流，严格执行网络安全继续教育制度，鼓励管理岗位和技术岗位持证上岗。通过组织开展学术交流及比武竞赛的方式，发现选拔网络安全人才，建立人才库，建立健全人才发现、培养、选拔和使用机制，为做好网络安全工作提供人才保障。

第三十条 各医疗卫生机构应保障开展网络安全等级测评、风险评估、攻防

演练竞赛、安全建设整改、安全保护平台建设、密码保障系统建设、运维、教育培训等经费投入。新建信息化项目的网络安全预算不低于项目总预算的 5%。

第三十一条 各医疗卫生机构应进一步完善网络安全考核评价制度，明确考核指标，组织开展考核。鼓励有条件的医疗卫生机构将考核与绩效挂钩。

第六章 附 则

第三十二条 违反本办法规定，发生个人信息和数据泄露，或者出现重大网络安全事件的，按《网络安全法》《密码法》《基本医疗卫生与健康促进法》《数据安全法》《个人信息保护法》《关键信息基础设施安全保护条例》以及网络安全等级保护制度等法律法规处理。

第三十三条 涉及国家秘密的网络，按照国家有关规定执行。

第三十四条 本办法自印发之日起实施。

第十四章 国家能源局

国家能源局关于印发《电力行业网络安全管理办法》的通知

国能发安全规〔2022〕100 号

各省(自治区、直辖市)能源局，有关省(自治区、直辖市)及新疆生产建设兵团发展改革委、工业和信息化主管部门，北京市城市管理委，各派出机构，全国电力安全生产委员会各企业成员单位，有关电力企业：

为深入贯彻习近平总书记关于网络强国的重要思想，加强电力行业网络安全监督管理，规范电力行业网络安全工作，国家能源局对《电力行业网络与信息安全管理办法》(国能安全〔2014〕317 号)进行了修订。现将修订后的《电力行业网络安全管理办法》 印发你们，请遵照执行。

国家能源局

2022 年 11 月 16 日

电力行业网络安全管理办法

第一章 总 则

第一条 为加强电力行业网络安全监督管理，规范电力行业网络安全工作，根据《中华人民共和国网络安全法》《中华人民共和国密码法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》《中华人民共和国计算机信

息系统安全保护条例》《关键信息基础设施安全保护条例》及国家有关规定，制定本办法。

第二条 电力行业网络安全工作的目标是建立健全网络安全保障体系和工作责任体系，提高网络安全防护能力，保障电力系统安全稳定运行和电力可靠供应。

第三条 电力企业在中华人民共和国境内建设、运营、维护和使用网络(除核安全外)，以及网络安全的监督管理，适用本办法。

本办法所称网络是指由计算机或者其他信息终端及相关设备组成的按照一定的规则和程序对信息进行收集、存储、传输、交换、处理的系统，包括电力监控系统、管理信息系统及通信网络设施。

本办法不适用于涉及国家秘密的网络。涉及国家秘密的网络应当按照国家保密工作部门有关涉密信息系统管理规定和技术标准，结合网络实际情况进行管理。

第四条 电力行业网络安全工作坚持“积极防御、综合防范”的方针，遵循“依法管理、分工负责，统筹规划、突出重点”的原则。

第二章 监督管理职责

第五条 国家能源局及其派出机构、负有电力行业网络安全监督管理职责的地方能源主管部门(以下简称行业部门)在各自职责范围内依法依规履行电力行业网络安全监督管理职责。

第六条 电力行业网络安全监督管理工作主要包括以下内容：

(一)组织落实国家关于网络安全的方针、政策和重大部署，并与电力生产安全监督管理工作相衔接；

(二)组织制定电力行业网络安全等级保护、关键信息基础设施安全保护、电力监控系统安全防护、网络安全监测预警和信息通报、网络安全事件应急处置等方面的政策规定及技术规范，并监督实施；

(三)组织认定电力行业关键信息基础设施，制定关键信息基础设施安全规划，建立关键信息基础设施网络安全监测预警制度，组织开展关键信息基础设施网络安全检查检测，指导关键信息基础设施运营者做好网络安全事件应对处置；

(四)组织或参与网络安全事件的调查与处理;

(五)督促电力企业落实网络安全责任、保障网络安全经费、开展网络安全防护能力建设等工作;

(六)组织开展电力行业网络安全信息通报等工作;

(七)指导督促电力企业做好网络安全宣传教育工作;

(八)推动网络安全仿真验证环境(靶场)建设,组织建立网络安全监督管理技术支撑体系;

(九)电力行业网络安全监督管理的其它事项。

第七条 电力调度机构负责直接调度范围内的下一级电力调度机构、集控中心、变电站(换流站)、发电厂(站)等各类机构涉网部分的电力监控系统安全防护的技术监督。主要包括以下内容:

(一)自行组织或委托电力监控系统安全防护评估机构开展调度范围内电力监控系统的自评估工作,配合开展电力监控系统的检查评估工作,负责统一指挥调度范围内的电力监控系统安全应急处理,参与电力监控系统的网络安全事件调查和分析工作;

(二)组织并督促各相关单位开展电力监控系统安全防护技术培训和交流工作,贯彻执行国家和行业有关电力监控系统安全防护的标准、规程和规范;

(三)负责对电力监控系统专用安全产品开展监督管理,制定电力监控系统专用安全产品管理办法并监督实施;

(四)将并网电厂涉网部分电力监控系统网络安全运行状态纳入监测;

(五)每年 11 月 1 日前将技术监督工作开展情况报送行业部门。

第三章 电力企业责任义务

第八条 电力企业是本单位网络安全的责任主体,负责本单位的网络安全工作。

第九条 电力企业主要负责人是本单位网络安全的第一责任人。电力企业应当建立健全网络安全管理、评价考核制度体系,成立工作领导机构,明确责任部门,设立专职岗位,定义岗位职责,明确人员分工和技能要求,建立健全网络安全责任制。

电力行业关键信息基础设施运营者的主要负责人对关键信息基础设施安全

保护负总责，要明确一名领导班子成员（非公有制经济组织运营者明确一名核心经营管理团队成员）作为首席网络安全官，专职管理或分管关键信息基础设施安全保护工作；为每个关键信息基础设施明确一名安全管理责任人；设立专门安全管理机构，确定关键岗位及人员，并对机构负责人和关键岗位人员进行安全背景审查。

第十条 电力企业应当依法依规开展关键信息基础设施信息报送工作，关键信息基础设施发生较大变化，可能影响其认定结果的，关键信息基础设施运营者发生合并、分立、解散等情况的，应当及时将相关情况报告行业部门。

第十一条 电力企业应当按照国家网络安全等级保护制度、关键信息基础设施安全保护制度、数据安全制度、网络安全审查工作机制和电力监控系统安全防护规定的要求，对本单位的网络进行安全保护，并将网络安全纳入安全生产管理体系。

第十二条 电力企业应当选用符合国家有关规定、满足网络安全要求的网络产品和服务，开展网络安全建设或改建工作。接入生产控制大区的涉网安全产品需经电力调度机构同意。

第十三条 电力行业关键信息基础设施运营者应当优先采购安全可信的网络产品和服务，并按照有关要求开展风险预判工作，评估投入使用后可能对关键信息基础设施安全、电力生产安全和国家安全的影响，形成评估报告。影响或者可能影响国家安全的，应当按照国家网络安全规定通过安全审查。

第十四条 电力企业规划设计网络时，应当明确安全保护需求，保证安全措施同步规划、同步建设、同步使用，设计合理的总体安全方案并经专业技术人员评审通过，制定安全实施计划，负责网络安全建设工程的实施。网络上线前，电力企业应当委托网络安全服务机构开展第三方安全测试。

第十五条 电力企业应当按照国家有关规定开展电力监控系统安全防护评估、网络安全等级保护测评、关键信息基础设施网络安全检测和风险评估、商用密码应用安全性评估和网络安全审查等工作，未达到要求的应当及时进行整改。

第十六条 电力企业不得委托在近 3 年内被行业部门通报有不良行为或被相关部门通报整改的网络安全服务机构。

第十七条 电力企业应当按照国家有关规定开展网络安全风险评估工作，建立健全网络安全风险评估的自评估和检查评估制度，完善网络安全风险管理机制。发现风险隐患可能对电力行业网络安全产生较大影响的，应当向行业部门报告。

第十八条 电力企业应当依据国家和行业相关标准、规程和规范开展网络安全技术监督工作，可委托网络安全服务机构协助开展。

第十九条 电力企业应当建立健全网络产品安全漏洞信息接收渠道并保持畅通，发现或者获知存在安全漏洞后，应当立即评估安全漏洞的影响范围及程度，及时对安全漏洞进行验证并完成修补。

第二十条 电力企业应当建立健全本单位网络安全监测预警和信息通报机制，及时掌握本单位网络安全运行状况、安全态势，及时处置网络安全威胁与隐患，定期向行业部门报告有关情况。

电力行业关键信息基础设施运营者应当建立 7×24 小时值班值守制度，建设网络安全态势感知平台，并与行业部门、公安机关等有关平台对接。

第二十一条 电力企业应当按照电力行业网络安全事件应急预案，制修订本单位网络安全事件应急预案，每年至少开展一次应急演练。制修订电力监控系统专项网络安全事件应急预案并定期组织演练。定期组织开展网络攻防演习，检验安全防护和应急处置能力。

第二十二条 电力企业应当在国家重要活动、会议期间结合实际制定网络安全保障专项工作方案和应急预案，成立保障组织机构，明确目标任务，细化措施要求，组织预案演练，确保重要信息系统、电力监控系统安全稳定运行。

第二十三条 电力企业发生网络安全事件后，应当立即启动网络安全事件应急预案，对网络安全事件进行调查和评估，采取技术措施和其他必要措施，消除安全隐患，防止危害扩大，注意保护现场，并按照规定向有关主管部门报告。

第二十四条 电力企业应当按照国家有关规定，建立健全容灾备份制度，对重要系统和重要数据进行有效备份。

第二十五条 电力企业应当建立健全全流程数据安全管理和个人信息保护制度，按照国家和行业重要数据目录及数据分类分级保护相关要求，确定本单位

的重要数据具体目录，对列入目录的数据进行重点保护。

第二十六条 电力企业应当建立网络安全资金保障制度，安排网络安全专项预算，确保网络安全投入不低于信息化总投入的 5%。

第二十七条 电力企业应当加强网络安全从业人员考核和管理，建立与网络安全工作特点相适应的人才培养机制，做好全员网络安全宣传教育，提高网络安全意识。从业人员应当定期接受相应的政策规范和专业技能培训，并经培训合格后上岗。

第二十八条 电力企业应当督促电力监控系统专用安全产品研发单位和供应商按照国家有关要求做好保密工作，防止关键技术泄露。严禁在互联网上销售、购买电力监控系统专用安全产品。

第二十九条 电力企业应当于每年 11 月 1 日前，将当年网络安全工作的专项总结报行业部门。总结内容应当包括但不限于网络安全工作开展情况、网络安全等级保护情况、电力监控系统安全防护评估情况、数据安全情况、安全监测预警情况、风险隐患治理情况、网络安全事件应对处置情况、应急预案及演练情况、网络产品和服务采购情况、下一年度工作计划等。

电力行业关键信息基础设施运营者应当于每年 11 月 1 日前，将当年关键信息基础设施安全保护工作的专项总结报行业部门。总结内容应当包括但不限于关键信息基础设施的运行情况、认定报送情况、安全监测预警情况、网络安全检测和风险评估情况、网络安全事件应对处置情况、应急预案及演练情况、网络产品和服务采购情况、密码使用情况、下一年度安全保护计划等。

第四章 监督检查

第三十条 行业部门在各自职责范围内依法依规对电力企业网络安全工作进行监督检查，定期组织开展电力行业关键信息基础设施网络安全检查检测。

第三十一条 行业部门进行监督检查和事件调查时，可以采取下列措施：

(一)进入电力企业进行检查；

(二)询问相关单位的工作人员，要求其对有关检查事项作出说明；

(三)查阅、复制与检查事项有关的文件、资料，对可能被转移、隐匿、损毁的文件、资料予以封存；

(四)对检查中发现的问题，责令其当场改正或者限期改正。

第三十二条 行业部门在履行网络安全监督管理职责中，发现网络存在较大安全风险或者发生安全事件的，可以按照规定的权限和程序对该电力企业法定代表人或者主要负责人进行约谈，情节严重的依据国家有关法律、法规予以处理。

行业部门可就网络安全缺陷、漏洞等风险，网络攻击、恶意软件等威胁，网络安全事件开展行业通报，电力企业应当及时排查并采取风险防范措施。

第三十三条 行业部门工作人员必须对在履行监督管理职责中知悉的国家秘密、工作秘密、商业秘密、重要数据、个人信息和隐私严格保密，不得泄露、出售或者非法向他人提供。

第五章 附 则

第三十四条 本办法由国家能源局负责解释。

第三十五条 本办法自发布之日起施行，有效期 5 年。《电力行业网络与信息安全管理办法》（国能安全〔2014〕317 号）同时废止。

国家能源局关于印发《电力行业网络安全等级保护管理办法》的通知

国能发安全规〔2022〕101 号

各省(自治区、直辖市)能源局，有关省(自治区、直辖市)及新疆生产建设兵团发展改革委、工业和信息化主管部门，北京市城市管理委，各派出机构，全国电力安全生产委员会各企业成员单位，有关电力企业：

为深入贯彻习近平总书记关于网络强国的重要思想，规范电力行业网络安全等级保护管理，提高电力行业网络安全保障能力和水平，国家能源局对《电力行业信息安全等级保护管理办法》（国能安全〔2014〕318 号）进行了修订。现将修订后的《电力行业网络安全等级保护管理办法》印发你们，请遵照执行。

国家能源局

2022 年 11 月 16 日

电力行业网络安全等级保护管理办法

第一章 总 则

第一条 为规范电力行业网络安全等级保护管理，提高电力行业网络安全保障能力和水平，维护国家安全、社会稳定和公共利益，根据《中华人民共和国

网络安全法》《中华人民共和国密码法》《中华人民共和国计算机信息系统安全保护条例》《关键信息基础设施安全保护条例》《信息安全等级保护管理办法》等法律法规和规范性文件，制定本办法。

第二条 电力企业在中华人民共和国境内建设、运营、维护、使用网络(除核安全外)，开展网络安全等级保护工作，适用本办法。

本办法所称网络是指由计算机或者其他信息终端及相关设备组成的按照一定的规则和程序对信息进行收集、存储、传输、交换、处理的系统，包括电力监控系统、管理信息系统及通信网络设施。

本办法不适用于涉及国家秘密的网络。涉及国家秘密的网络应当按照国家保密工作部门有关涉密信息系统分级保护的管理规定和技术标准，结合网络实际情况进行管理。

第三条 国家能源局根据国家网络安全等级保护政策法规和技术标准要求，结合行业实际，组织制定适用于电力行业的网络安全等级保护管理规范和技术标准，对电力行业网络安全等级保护工作的实施进行指导和监督管理。国家能源局各派出机构根据国家能源局授权，对本辖区电力企业网络安全等级保护工作的实施进行监督管理。

电力企业依照国家和电力行业相关法律法规和规范性文件，履行网络安全等级保护的义务和责任。

第二章 等级划分与保护

第四条 根据电力行业网络在国家安全、经济建设、社会生活中的重要程度，以及一旦遭到破坏、丧失功能或者数据被篡改、泄露、丢失、损毁后，对国家安全、社会秩序、公共利益以及公民、法人和其他组织的合法权益的危害程度等因素，电力行业网络划分为五个安全保护等级：

第一级，受到破坏后，会对相关公民、法人和其他组织的合法权益造成一般损害，但不危害国家安全、社会秩序和公共利益。

第二级，受到破坏后，会对相关公民、法人和其他组织的合法权益造成严重损害或特别严重损害，或者对社会秩序和公共利益造成危害，但不危害国家安全。

第三级，受到破坏后，会对社会秩序和公共利益造成严重危害，或者对国

家安全造成危害。

第四级，受到破坏后，会对社会秩序和公共利益造成特别严重危害，或者对国家安全造成严重危害。

第五级，受到破坏后，会对国家安全造成特别严重危害。

第五条 电力行业网络安全等级保护坚持分等级保护、突出重点、积极防御、综合防范的原则。

第三章 等级保护的实施与管理

第六条 国家能源局根据《信息安全技术 网络安全等级保护定级指南》(GB/T 22240)等国家标准规范，结合电力行业网络特点，制定电力行业网络安全等级保护定级指南，指导电力行业网络安全等级保护定级工作。

第七条 电力企业应当在网络规划设计阶段，依据《信息安全技术 网络安全等级保护定级指南》(GB/T 22240)等国家标准规范和电力行业网络安全等级保护定级指南，确定定级对象(网络)及其安全保护等级，并在网络功能、服务范围、服务对象和处理的数据等发生重大变化时，及时申请变更其安全保护等级。

对拟定为第二级及以上的网络，电力企业应当组织网络安全专家进行定级评审。其中，拟定为第四级及以上的网络，还应当由国家能源局统一组织国家网络安全等级保护专家进行定级评审。

第八条 全国电力安全生产委员会企业成员单位汇总集团总部拟定为第二级及以上网络的定级结果和专家评审意见，报国家能源局审核。各区域(省)内的电力企业汇总本单位拟定为第二级及以上网络的定级结果，报国家能源局派出机构审核。

第九条 电力企业办理网络安全等级保护定级审核手续时，应当提交《电力行业网络安全等级保护定级审核表》(详见附件)，含各定级对象的定级报告及专家评审意见。

国家能源局或其派出机构应当在收到审核材料之日起 30 日内反馈审核意见。

第十条 电力企业应当在收到国家能源局或其派出机构审核意见后，按照有关规定向公安机关备案并按照第八条规定的定级审核权限向国家能源局或其派

出机构报告定级备案结果。

第十一条 电力企业应当采购、使用符合国家法律法规和有关标准规范要求且满足网络安全等级保护需求的网络产品和服务。

对于电力监控系统，应当按照电力监控系统安全防护有关要求，采购和使用电力专用横向单向安全隔离装置、电力专用纵向加密认证装置或者加密认证网关等设备设施；在设备选型及配置时，禁止选用经国家能源局通报存在漏洞和风险的系统及设备，对已经投入运行的系统及设备应及时整改并加强运行管理和安全防护。

采购网络产品和服务，影响或可能影响国家安全的，应当按照国家网络安全规定通过安全审查。

第十二条 电力企业在网络规划、建设、运营过程中，应当遵循同步规划、同步建设、同步使用的原则，并按照该网络的安全保护等级要求，建设网络安全设备设施，制定并落实安全管理制度，健全网络安全防护体系。

第十三条 网络建设完成后，电力企业应当依据国家和行业有关标准或规范要求，定期对网络安全等级保护状况开展网络安全等级保护测评。第二级网络应当每两年进行一次等级保护测评，第三级及以上网络应当每年进行一次等级保护测评。新建的第三级及以上网络应当在通过等级保护测评后投入运行。

电力监控系统网络安全等级保护测评工作应当与电力监控系统安全防护评估、关键信息基础设施网络安全检测评估、商用密码应用安全性评估工作相衔接，避免重复测评。

电力企业应当定期对网络安全状况、安全保护制度及措施的落实情况进行自查。第二级电力监控系统应当每两年至少进行一次自查，第三级及以上网络应当每年至少进行一次自查。

电力企业应当对自查和等级保护测评中发现的安全风险隐患，制定整改方案，并开展安全建设整改。

电力企业应当要求网络安全等级保护测评机构(以下简称测评机构)组织专家对第三级及以上网络的等级保护测评报告进行评审，并随测评报告提交专家评审意见。

第十四条 电力企业应当按照第八条规定的定级审核权限，每年向国家能源

局或其派出机构报告网络安全等级保护工作情况，包括网络安全等级保护定级备案、等级保护测评、安全建设整改、安全自查等情况。

第十五条 国家能源局及其派出机构结合关键信息基础设施网络安全检查，定期组织对运营有第三级及以上网络的电力企业开展抽查。开展网络安全检查时应当加强协同配合和信息沟通，避免不必要的检查和交叉重复检查。

检查事项主要包括：

(一)网络安全等级保护定级工作开展情况，包括定级评审、审核、备案及根据网络安全需求变化调整定级等情况；

(二)电力企业网络安全管理制度、措施的落实情况；

(三)电力企业对网络安全状况的自查情况；

(四)网络安全等级保护测评工作开展情况；

(五)网络安全产品使用情况；

(六)网络安全建设整改情况；

(七)备案材料与电力企业及其网络的符合情况；

(八)其他应当进行监督检查的事项。

第十六条 电力企业应当接受国家能源局及其派出机构的安全监督、检查、指导，根据需要如实提供下列有关网络安全等级保护的信息资料及数据文件：

(一)网络安全等级保护定级备案事项变更情况；

(二)网络安全组织、人员、岗位职责的变动情况；

(三)网络安全管理制度、措施变更情况；

(四)网络运行状况记录；

(五)电力企业对网络安全状况的自查记录；

(六)测评机构出具的网络安全等级保护测评报告；

(七)网络安全产品使用的变更情况；

(八)网络安全事件应急预案，网络安全事件应急处置结果报告；

(九)网络数据容灾备份情况；

(十)网络安全建设、整改结果报告；

(十一)其他需要提供的材料。

第十七条 针对网络安全检查发现的问题，电力企业应当按照网络安全等级

保护管理规范和技术标准组织整改。必要时，国家能源局及其派出机构可对整改情况进行抽查。

第十八条 电力企业选择测评机构进行网络安全等级保护测评时，应当遵循以下要求：

(一)测评机构应当获得由国家认证认可委员会批准的认证机构发放的《网络安全等级测评与检测评估机构服务认证证书》(以下简称测评机构服务认证证书)；

(二)从事电力监控系统网络安全等级保护测评的机构应当熟悉电力监控系统网络安全管理和技术防护要求，具备相应的服务能力和经验。从事电力监控系统第二级网络等级保护测评的机构应当具备近 2 年内 30 套以上工业控制系统等级保护测评或风险评估服务经验；从事电力监控系统第三级网络等级保护测评的机构应当具备近 3 年内 50 套以上电力监控系统等级保护测评或安全防护评估服务经验；从事电力监控系统第四级及以上网络等级保护测评的机构应当具备近 5 年内 90 套以上电力监控系统等级保护测评或安全防护评估服务经验；

(三)对属于电力行业关键信息基础设施的网络，选择测评机构时应当保证其安全可信，必要时可要求测评机构及其主要负责人、技术骨干提供无犯罪记录证明等材料；

(四)不得委托近 3 年内被国家能源局通报有本办法规定不良行为，或被认证机构通报取消或暂停使用测评机构服务认证证书，或被国家网络安全等级保护工作主管部门、行业协会通报暂停开展等级保护测评业务并处于整改期内的测评机构；

(五)电力企业应当采取签署保密协议、开展安全保密培训和现场监督等措施，加强对测评机构、测评人员和测评过程的安全保密管理，避免发生失泄密事件。

第十九条 国家能源局及其派出机构在开展电力企业网络安全检查工作时，可同步对测评机构开展的测评工作情况进行监督检查。

第二十条 国家能源局鼓励电力企业按照国家有关要求开展测评机构建设、申请测评机构服务认证，支持电力企业参与制定电力行业网络安全等级保护技术标准。

第四章 网络安全等级保护的密码管理

第二十一条 电力企业采用密码进行等级保护的，应当遵照《中华人民共和国密码法》等有关法律法规和国家密码管理部门制定的网络安全等级保护密码技术标准执行。

第二十二条 电力企业网络安全等级保护中密码的配备、使用和管理等，应当严格执行国家密码管理的有关规定。运用密码技术进行网络安全等级保护建设与整改时，应当采用商用密码检测、认证机构检测认证合格的商用密码产品和服务。涉及商用密码进口的，还应当符合国家商用密码进口许可有关要求。

第二十三条 电力企业应当按照有关法律法规要求，开展商用密码应用安全性评估工作。

第二十四条 各级密码管理部门对网络安全等级保护工作中密码配备、使用和管理的情况进行检查和安全性评估时，相关电力企业应当积极配合。对于检查和安全性评估发现的问题，应当按照要求及时整改。

第五章 法律责任

第二十五条 电力企业违反国家相关规定及本办法规定，由国家能源局及其派出机构按照职责分工责令其限期改正；逾期不改正的，给予警告，并向其上级部门通报情况，建议对其直接负责的主管人员和其他直接责任人员予以处理，造成严重损害的，由公安机关、密码管理部门依照有关法律、法规予以处理。

第二十六条 有关部门及其工作人员在履行监督管理职责中，玩忽职守、滥用职权、徇私舞弊的，依法给予行政处分；构成犯罪的，依法追究刑事责任。

第二十七条 测评机构违反有关法律法规和规范性文件要求，发生以下不良行为时，国家能源局可向国家有关部门、认证机构、行业协会等提出限期整改、取消/暂停使用测评机构服务认证证书等建议，并向电力企业通报相关风险信息：

(一)提供不客观、不公正的等级保护测评服务，出具虚假或不符合实际情况的测评报告，影响等级保护测评的质量和效果；

(二)泄露、出售或者非法向他人提供在服务中知悉的国家秘密、工作秘密、商业秘密、重要数据、个人信息和隐私，非法使用或擅自发布、披露在服

务中收集掌握的数据信息和系统漏洞、恶意代码、网络入侵攻击等网络安全信息；

(三)由于测评机构从业人员的因素，导致发生网络安全事件；

(四)未向公安机关报备，测评机构从业人员擅自参加境外组织的网络安全竞赛等活动；

(五)其他危害或可能危害电力生产安全或网络安全的行为。

第六章 附 则

第二十八条 本办法自发布之日起施行，有效期5年。《电力行业信息安全等级保护管理办法》(国能安全〔2014〕318号)同时废止。

附件：电力行业网络安全等级保护定级审核表

附件

电力行业网络安全等级保护定级审核表

填表日期： 年 月 日

<table>
<tr><td colspan="6">一、单位信息</td></tr>
<tr><td>单位名称</td><td colspan="5"></td></tr>
<tr><td>单位地址</td><td colspan="5"></td></tr>
<tr><td>联系人</td><td></td><td>职务</td><td></td><td>联系电话</td><td></td></tr>
<tr><td colspan="6">二、网络安全等级保护定级情况</td></tr>
<tr><td>定级对象名称</td><td colspan="3">定级对象概况</td><td colspan="2">拟定级结果(SAG)</td></tr>
<tr><td></td><td colspan="3"></td><td colspan="2"></td></tr>
<tr><td></td><td colspan="3"></td><td colspan="2"></td></tr>
<tr><td></td><td colspan="3"></td><td colspan="2"></td></tr>
<tr><td></td><td colspan="3"></td><td colspan="2"></td></tr>
<tr><td></td><td colspan="3"></td><td colspan="2"></td></tr>
<tr><td colspan="6">三、本单位网络安全管理部门审核意见</td></tr>
<tr><td colspan="6">

部门： (公章)
日期： 年 月 日</td></tr>
<tr><td colspan="6">四、行业主管/监管部门审核意见</td></tr>
<tr><td colspan="6">

审核部门： (公章)
日期： 年 月 日</td></tr>
</table>

注：1.拟定级结果需填写拟定业务信息安全保护等级和系统服务安全保护等级；

2.每个定级对象需单独提交定级报告(包含网络概况、定级分析、定级结果)及专家评审意见。

国家能源局关于印发《电力二次系统安全管理若干规定》的通知

国能发安全规〔2022〕92 号

各省(自治区、直辖市)能源局，有关省(自治区、直辖市)及新疆生产建设兵团发展改革委、工业和信息化主管部门，北京市城市管理委员会，各派出机构，全国电力安全生产委员会企业成员单位，各有关电力企业：

为贯彻落实习近平总书记关于安全生产重要论述，进一步加强电力系统安全监管，提升电力二次系统安全管理的针对性、有效性，更好地服务电力行业安全高质量发展，国家能源局对《电力二次系统安全管理若干规定》(电监安全〔2011〕19 号)进行了修订。现将修订后的《电力二次系统安全管理若干规定》印发你们，请遵照执行。

国家能源局

2022 年 10 月 17 日

电力二次系统安全管理若干规定

第一章 总 则

第一条 为加强电力二次系统安全管理，确保电力系统安全稳定运行，依据《中华人民共和国电力法》《中华人民共和国网络安全法》《电力监管条例》《电网调度管理条例》《关键信息基础设施安全保护条例》《电力监控系统安全防护规定》等相关法律法规、规章，制定本规定。

第二条 电网调度机构(以下简称调度机构)、电力企业及相关电力用户等各相关单位依据本规定开展电力二次系统安全管理工作。

第三条 本规定所称电力二次系统包括继电保护和安全自动装置，发电机励磁和调速系统，新能源发电控制系统，电力调度通信和调度自动化系统，直流控制保护系统，负荷控制系统，储能电站监控系统等(以下简称二次系统)；涉网二次系统是指电源及相关电力用户中与电网安全稳定运行相关的二次系统。

第四条 国家能源局及其派出机构依法对二次系统管理工作实施监督管理。

第五条 电力企业及相关电力用户是二次系统安全管理的责任主体，应当遵照国家及行业有关电力安全生产的法律法规、规章制度和技术标准，负责本单

位的二次系统安全管理工作。

第六条 调度机构应加强调度管辖区域内电力企业及相关电力用户二次系统技术监督工作的指导，定期统计和汇总分析电力企业及相关电力用户技术监督工作开展情况，并将有关问题和情况及时报送国家能源局及其派出机构。调度机构按照国家相关规定负责调度管辖范围内涉网二次系统的技术监督工作。

第七条 调度机构、电力企业及相关电力用户应当配备足够的二次系统专业技术人员，具备设备运维、故障排查处置等工作能力。

第八条 调度机构应按照有关法律法规和国家能源局监管要求组织并督促二次系统专业技术培训和技术交流工作；应组织各相关单位贯彻执行国家和行业有关二次系统的标准、规程和规范；应组织制定(修订)调度管辖范围内二次系统的规程、规范和相关管理制度，并将与电力监管相关的事项报告国家能源局及其派出机构；应定期组织召开二次系统专业会议；组织开展二次系统运行统计分析工作，及时发布分析报告。

第九条 电力企业及相关电力用户应保障二次系统网络安全投入，并遵循“同步规划、同步建设、同步使用”的原则。

第十条 国家能源局及其派出机构加强对调度机构技术监督工作的监督管理，建立二次系统安全管理情况书面报告制度。省级、区域调度机构按月向国家能源局相关派出机构报告二次系统安全管理情况，国家电力调控中心和南方电网电力调控中心按季度向国家能源局报告二次系统安全管理情况，南方电网电力调控中心同时报南方能源监管局。相关二次系统安全管理情况按有关规定，在并网电厂涉网安全管理联席会议上通报。

第十一条 国家能源局及其派出机构可以依据相关规定对二次系统管理工作中的有关争议进行调解，经调解仍不能达成一致的，由国家能源局及其派出机构依照《电力监管条例》裁决。

第二章 规划建设管理

第十二条 二次系统规划设计应满足国家和行业相关技术标准和有关规定。

第十三条 二次系统规划设计应满足电网安全稳定运行和网络安全的要求。

第十四条 二次系统设备选型及配置应满足国家和行业相关技术标准，以及设备技术规程、规范的要求。涉网二次系统规划设计、设备选型及配置还应征

求调度机构意见，并满足调度机构相关技术规定及电网反事故措施的有关要求。

第十五条 电力企业及相关电力用户应按国家相关部门、调度机构要求配置网络安全专用防护产品，并报调度机构备案。

第十六条 二次系统设备应选择具备相应资质的质检机构检验合格的产品。

第十七条 二次系统安装、试验、验收应满足国家和行业相关标准、规范，及调度机构有关规程和管理制度的要求。涉网二次系统应按照有关规定进行并网安全评价，确保满足并网条件。

第十八条 二次系统项目建设完成应由项目监理单位出具相关质量评估报告，其中涉网二次系统应经调度机构确认。

第十九条 二次系统网络安全防护应满足《电力监控系统安全防护规定》要求。

第二十条 电力企业及相关电力用户的数字证书、密码产品等应满足国家相关部门、调度机构对二次系统密码应用管理的相关要求。

第三章 运行维护管理

第二十一条 电力企业及相关电力用户应按照国家、行业标准及调度机构相关规程和管理制度组织二次系统的定期检查和日常维护工作。

第二十二条 电力企业及相关电力用户各自负责所属电力通信、调度自动化及网络安全系统的运行维护工作。

第二十三条 相关电力用户应按政府有关要求和调度机构相关规程落实负荷控制、稳定控制、低频减负荷、低压减负荷等控制措施。

第二十四条 二次系统设备、装置及功能应按照相关规定投退，不得随意投入、停用或改变参数设置。属调度机构调度管辖范围的二次系统设备、装置及功能因故需要投入、退出、停用或改变参数设置的应报相应调度机构批准同意后方可进行。

第二十五条 电力企业及相关电力用户应对不满足电力系统安全稳定运行要求的二次系统及时进行更新、改造，并进行相关试验。需要进行联合调试的，调度机构负责安排相关运行方式，为联合调试创造条件。

第二十六条 已运行的二次系统(包括硬件和软件)需要改造升级的，应满足

本规定关于规划设计、设备选型、网络安全防护等要求。

第二十七条 电力企业及相关电力用户所进行的影响电力系统安全及二次系统运行的重要设备投运和重大试验工作，应严密组织，防止引发电网事故和设备事故，调度机构应提前将有关投运和试验安排通知相关单位。

第二十八条 电力企业及相关电力用户应加强二次系统网络安全监视，当发生危害网络安全的事件时应立即采取措施，影响涉网二次系统安全的应同时向调度机构报告。

第二十九条 电力企业及相关电力用户应建立二次系统安全双重预防体系，加强二次系统安全风险管控和隐患排查治理。

第三十条 电力系统发生异常与故障后，各相关单位应依据调度规程和现场运行有关规定，正确、迅速进行处理，保全现场文档，并及时向调度机构报告设备状态和处理情况。

第三十一条 各相关单位应加强沟通，互相提供有关资料，积极查找异常与事故原因，配合相关部门进行电力安全事故调查工作，并根据调查情况分别制定措施，落实整改。

第三十二条 调度机构负责组织或参与涉网二次系统的安全检查工作，参与涉网二次系统的电力安全事故调查、事故分析工作，并制定反事故措施。

第三十三条 电力二次系统网络安全专用防护产品的使用单位应督促研发单位和供应商按国家有关要求做好保密工作，防止关键技术泄露。严禁在互联网上销售、购买电力二次系统网络安全专用防护产品。

第四章 定值和参数管理

第三十四条 与电网安全稳定运行紧密相关的继电保护及安全自动装置定值由调度机构负责管理。调度机构下达限额或定值，发电企业及相关电力用户按调度机构要求整定，并报调度机构审核和备案。

其他与电网安全稳定运行相关的继电保护及安全自动装置定值由发电企业及相关电力用户自行管理，并负责整定，定值应报调度机构备案。

第三十五条 继电保护及安全自动装置整定工作原则上应由本企业专业人员具体负责；如需委托外单位，应委托具备相应专业能力的单位承担。

第三十六条 调度机构应及时将影响涉网二次系统运行和整定的系统阻抗等

有关变化情况，书面通知发电企业及相关电力用户；发电企业及相关电力用户应及时校核定值和参数，在调度机构指导下及时调整二次系统的运行方式和有关定值。

第三十七条 发电企业应按调度机构要求提供系统分析用的发电机励磁系统(包括电力系统稳定器 PSS)和调速系统、新能源发电控制系统等二次设备的技术资料和实测参数，以及继电保护整定计算所需的发电机、变压器等主要设备技术规范、技术参数和实测参数等资料。

第三十八条 发电企业的发电机励磁系统和调速系统定值和参数应报送调度机构备案。

第三十九条 发电企业的涉网试验方案、试验结果和试验报告应经调度机构确认。

第四十条 发电企业应根据电力系统网络结构变化、发电机励磁系统和调速系统等主要设备变化、相关控制系统发生重大改变，重新进行相关试验，并根据试验结论和调度机构的技术要求调整发电机励磁系统和调速系统定值参数，满足电力系统安全稳定运行要求。

第四十一条 调度机构应指导发电企业做好发电机励磁系统与调速系统等参数优化和管理工作，并配合发电企业进行相关试验工作。

第四十二条 涉网调度通信设备的数据配置、运行方式由调度机构或受其委托的通信运维单位下达，发电企业及相关电力用户应按要求执行，执行结果向相关单位报备。

第四十三条 发电企业及相关电力用户调度数据网设备的配置参数由调度机构负责管理，按调度机构下达的参数要求配置，并报调度机构备案。

第五章 附 则

第四十四条 本规定所称相关电力用户是指农林水利、工矿企业、交通运输、公共服务等具有二次系统的大负荷用户，以及能够响应调度指令的负荷聚合商等。

第四十五条 本规定所称发电企业是电力企业的一种类别，是指并入电网运行的火力（燃煤、燃油、燃气及生物质）、水力、核能、风力、太阳能、抽水蓄能、新型储能、地热能、海洋能等发电厂(场、站)。

第四十六条 本规定所称“与电网安全稳定运行紧密相关的继电保护及安全自动装置”，是指电源及相关电力用户中主要为电网安全稳定运行服务的继电保护与安全自动装置。

第四十七条 本规定所称“其他与电网安全稳定运行相关的继电保护及安全自动装置”，是指电源及相关电力用户中主要为保护电源及相关电力用户而配置的，与电网存在配合关系的继电保护与安全自动装置。

第四十八条 国家能源局各派出机构可根据情况制定相应的实施细则。

第四十九条 电力企业及相关电力用户应按照本规定和相关实施细则及时修订相关规程和管理制度。

第五十条 本规定自发布之日起施行，有效期 5 年。原国家电力监管委员会《电力二次系统安全管理若干规定》(电监安全〔2011〕19 号)同时废止。

国家能源局关于印发《电力网络安全事件应急预案》的通知

国能发安全〔2024〕34 号

各派出机构，全国电力安全生产委员会企业成员单位，有关电力企业：

为深入贯彻习近平总书记关于网络强国的重要思想，加强电力网络安全事件应急能力建设，规范各单位电力网络安全事件应急处置工作，有效预防、及时控制和最大限度消除电力网络安全事件带来的危害和影响，国家能源局制定了《电力网络安全事件应急预案》。现印发给你们，请遵照执行。

国家能源局

2024 年 5 月 16 日

电力网络安全事件应急预案

一、总则

(一)编制目的

完善电力网络安全事件应对工作机制，有效预防、及时控制和最大限度消除电力网络安全事件带来的危害和影响，保障电力系统安全稳定运行和电力可靠供应。

(二)编制依据

《中华人民共和国突发事件应对法》(中华人民共和国主席令第六十九号)、《中华人民共和国网络安全法》(中华人民共和国主席令第五十三号)、《关

键信息基础设施安全保护条例》（中华人民共和国国务院令第 745 号）、《电力安全事故应急处置和调查处理条例》（中华人民共和国国务院令第 599 号）、《电力监管条例》（中华人民共和国国务院令第 432 号）、《突发事件应急预案管理办法》（国办发〔2024〕5 号）、《国家大面积停电事件应急预案》（国办函〔2015〕134 号）、《国家网络安全事件应急预案》（中网办发文〔2017〕4 号）、《电力安全生产监督管理办法》（中华人民共和国国家发展和改革委员会 2015 年第 21 号令）、《电力监控系统安全防护规定》（中华人民共和国国家发展和改革委员会 2014 年第 14 号令）、《电力行业网络安全管理办法》（国能发安全规〔2022〕100 号）、《重大活动电力安全保障工作规定》（国能发安全〔2020〕18 号）、《电力安全事件监督管理规定》（国能安全〔2014〕205 号）等。

（三）适用范围

本预案所指电力网络安全事件是指由计算机病毒或网络攻击、网络侵入等危害网络安全行为导致的，对电力网络和信息系统造成危害，可能影响电力系统安全稳定运行或者影响电力正常供应的事件。

本预案适用于电力网络安全事件的应对工作。涉及电力企业但不属于本预案定义范围内的网络安全事件，参照《国家网络安全事件应急预案》及电力企业所属省、自治区、直辖市制定的本地区网络安全事件应急预案等应对。

（四）工作原则

国家能源局及其派出机构统一指导、电力调度机构分级指挥、各电力企业具体负责，各方面力量密切协同、预防为主、快速反应、科学处置，共同做好电力网络安全事件的预防和处置工作。

（五）事件分级

根据电力网络安全事件造成停电等后果的影响程度，电力网络安全事件分为特别重大、重大、较大和一般四级。

造成《电力安全事故应急处置和调查处理条例》中定义的重大及以上电力安全事故的，为特别重大电力网络安全事件。

造成《电力安全事故应急处置和调查处理条例》中定义的一般或较大电力安全事故的，为重大电力网络安全事件。

造成《电力安全事件监督管理规定》中定义的需重点监督管理的电力安全

事件的，为较大电力网络安全事件。

造成电力一次设备被恶意操控，但未构成需重点监督管理的电力安全事件的，为一般电力网络安全事件。

二、职责分工

国家能源局统筹指导电力网络安全事件应对工作，并根据需要组织提供技术支持，具体工作由国家能源局电力安全监管司承担。国家能源局派出机构(以下简称派出机构)在国家能源局统一领导下，统筹指导本辖区电力网络安全事件预防和应对工作，并根据需要组织提供技术支持。

电力调度机构在国家能源局及其派出机构的指导下，负责统一指挥调度范围内的电力网络安全事件应急处置。

各电力企业负责电力网络安全事件的应对工作，负责建立健全本企业的电力网络安全事件应对工作机制，具体负责本企业电力网络安全事件的预防、监测、报告和应急处置工作，在国家能源局及其派出机构的组织下，为其他电力企业的电力网络安全事件应对提供技术支持。

三、监测预警

(一)预警分级

电力网络安全事件预警等级分为四级：由高到低依次用红色、橙色、黄色和蓝色表示，分别对应发生或可能发生特别重大、重大、较大和一般电力网络安全事件。

(二)预警监测

各电力企业应组织对本单位建设运行的网络和信息系统开展网络安全监测工作。电力调度机构将并网电厂涉网部分电力监控系统网络安全运行状态纳入监测，掌握调度范围内网络安全状况。派出机构结合实际统筹组织开展本辖区电力网络安全事件监测工作。派出机构、国家电力调度控制中心(以下简称国调中心)、中国南方电网电力调度控制中心(以下简称南网总调)、全国电力安全生产委员会企业成员单位将重要监测信息报国家能源局，国家能源局组织开展跨区域网络安全信息共享。

(三)预警研判和发布

各电力企业组织对监测信息进行研判，认为需要立即采取防范措施的，应

当组织开展处置，对可能发生电力网络安全事件的信息，应立即向其上级电力调度机构以及当地派出机构报告，并提出预警信息的发布建议；全国电力安全生产委员会企业成员单位对可能发生较大及以上电力网络安全事件的信息，应同步报告国家能源局。

派出机构联合电力调度机构组织对监测信息进行研判，认为需要立即采取防范措施的，应当及时通知有关单位，对可能发生较大及以上电力网络安全事件的信息及时向国家能源局报告。派出机构可根据监测研判情况，发布本区域黄色及以下预警，并报告国家能源局。

国家能源局组织研判，确定和发布橙色预警和涉及多区域的预警，对可能发生重大及以上电力网络安全事件的信息及时向国家网络安全应急办公室报告。

预警信息包括事件的类别、预警级别、起始时间、可能影响范围、警示事项、应采取的措施和时限要求、发布单位等。

(四)预警响应

红色预警信息发布后，在国家网络安全应急办公室统一领导、指挥、协调下，在国家能源局指导下，由国调中心或南网总调负责指挥相关电力企业开展预警响应工作。橙色预警和涉及多区域的预警信息发布后，在国家能源局指导下，由国调中心或南网总调负责指挥相关电力企业开展预警响应工作。黄色、蓝色预警信息发布后，根据事件影响范围，在派出机构指导下，由跨省、自治区、直辖市电力调度机构，或省、自治区、直辖市级电力调度机构负责指挥相关电力企业开展预警响应工作。

预警范围内的各单位应做好应急队伍、应急物资等准备工作；采取有效的风险防控措施降低或控制风险，控制威胁蔓延；持续监测威胁蔓延、预警风险及影响发展情况；组织专业技术队伍开展现场分析、处置等工作；做好预警信息要求的其他工作。

(五)预警解除

经研判不会发生电力网络安全事件的，按照“谁发布、谁解除”的原则，由发布单位宣布解除预警，适时终止相关措施。

四、应急响应

(一)事件报告

电力网络安全事件发生后，事件发生单位应立即启动应急预案，实施处置并立即向其上级电力调度机构、当地派出机构、属地公安部门及当地网信部门报告。全国电力安全生产委员会企业成员单位同时报告国家能源局。发生较大及以上电力网络安全事件的，应 1 小时内报告，一般电力网络安全事件应 12 小时内报告。

电力调度机构接到电力网络安全事件报告或者监测到相关信息后，应当立即进行核实，对电力网络安全事件级别作出初步认定，及时向上级电力调度机构和当地派出机构报告。派出机构接到电力网络安全事件报告或者监测到相关信息后，应当立即核实有关情况并向国家能源局报告。对初判为重大及以上的电力网络安全事件，国家能源局要立即按程序向国家网络安全应急办公室报告。

(二)响应分级

按照电力网络安全事件的严重程度和发展态势，将应急响应设定为Ⅰ级、Ⅱ级、Ⅲ级和Ⅳ级四个等级。初判发生特别重大电力网络安全事件，启动Ⅰ级应急响应，在国家网络安全事件应急指挥部统一领导、指挥、协调下，在国家能源局指导下，由国调中心或南网总调负责指挥相关电力企业开展应对工作。初判发生重大电力网络安全事件，由国家能源局启动Ⅱ级应急响应，在国家能源局指导下，由国调中心或南网总调负责指挥相关电力企业开展应对工作。初判发生较大、一般电力网络安全事件，由相关派出机构分别启动Ⅲ级、Ⅳ级应急响应，根据事件影响范围，在派出机构指导下，由跨省、自治区、直辖市电力调度机构，或省、自治区、直辖市级电力调度机构负责指挥相关电力企业开展应对工作。

(三)响应措施

电力网络安全事件发生后，事件发生单位必须立即启动应急预案，实施先期处置，全力控制事件发展态势，减少损失，并保护现场和证据。

事件发生单位应通过技术等手段，及时阻断威胁蔓延并监测跟踪影响发展情况，密切监控事件发展及对电力生产业务的影响。

事件发生单位应尽快进行分析，根据信息系统运行、使用、承载业务的情

况，初步判断发生电力网络安全事件的原因、影响、破坏程度、波及的范围等，提出初步应对措施建议。

事件发生单位应保留相关证据，可采取记录、截屏、备份、录像等手段，对事件的发生、发展、处置过程、步骤、结果进行详细记录。

相应电力调度机构进入应急状态，负责指挥应急处置或支援保障工作。

(四)响应结束

I 级响应结束由国家能源局报国家网络安全应急办公室，国家网络安全应急办公室提出建议，报国家网络安全事件应急指挥部批准；II 级响应结束由国家能源局决定并报国家网络安全应急办公室；III 级、IV 级响应结束由派出机构决定并报国家能源局。

(五)信息发布

按照及时准确、公开透明、客观统一的原则，加强信息发布，主动向社会发布电力网络安全事件相关信息和应对工作情况，提示相关注意事项和应对措施，及时回应社会关切，澄清不实信息。

五、后期处置

(一)恢复生产

事件发生单位应制定详细可行的工作计划，快速、有效地消除事件造成的不利影响，尽快恢复生产秩序及系统设备正常运行，并做好善后处理等事项。

(二)事件调查及评估

特别重大电力网络安全事件在国家网络安全应急办公室组织下进行调查处理和总结评估。重大电力网络安全事件由国家能源局组织调查处理和总结评估，相关总结调查报告报国家网络安全应急办公室。较大及以下电力网络安全事件由派出机构组织调查处理和总结评估，相关总结调查报告报国家能源局，未造成人员伤亡或未造成供电用户停电的，派出机构也可以委托事件发生单位组织调查处理。国家能源局认为有必要的，可以组织事故调查组对电力网络安全事件进行提级调查。负责该事件指挥应对工作的电力调度机构应按照有关规定的权限和程序参与事件调查处理和总结评估。

事件发生单位应查明事件起因、性质、影响、责任等情况，提出防范、整改措施和处理建议，于应急响应结束后 5 天内完成自查，向组织事件调查的机

关提交自查报告。

事件的调查处理和总结评估工作原则上在应急响应结束后 30 天内完成。总结调查报告应对事件的起因、性质、影响、责任等进行分析评估，提出处理意见和改进措施。

六、预防工作

(一)日常管理

各电力企业应按职责做好电力网络安全事件日常预防工作，做好网络安全检查、隐患排查、风险评估和容灾备份，健全本单位网络安全监测预警和信息通报机制，及时采取有效措施，减少和避免电力网络安全事件的发生及危害，提高应对电力网络安全事件的能力。

(二)演练

国家能源局定期组织演练，检验和完善预案，提高实战能力。

各电力企业每年至少开展一次应急演练，并将演练情况报送相关派出机构及上级电力调度机构，全国电力安全生产委员会企业成员单位应同步报送国家能源局。

(三)培训

各电力企业应将电力网络安全事件的应急知识列入有关人员的培训内容，加强网络安全特别是网络安全应急预案的培训，提高防范意识及技能。

(四)重大活动期间的预防措施

在国家重要活动、会议期间，有关电力调度机构、电力企业应加强网络安全监测和分析研判，及时预警可能造成重大影响的风险和隐患。重点部门、重点岗位保持 24 小时值班，及时发现和处置电力网络安全事件隐患。具体参照《重大活动电力安全保障工作规定》执行。

七、保障措施

(一)制度保障

各电力企业要落实网络安全应急工作责任制，把责任落实到具体部门、具体岗位和个人，并建立健全应急工作机制。

(二)经费保障

各电力企业应为电力网络安全事件应急处置提供必要的资金保障，以支撑

电力网络安全事件应急物资保障、技术支撑力量保障、基础平台保障、技术保障、指挥保障、预案演练等工作开展。

(三)应急物资保障

各电力企业应根据潜在电力网络安全事件的影响，结合本单位网络安全工作需要，明确应急装备与备品备件的配置标准，购置和储备应急所需物资。各电力企业应掌握所属各单位应急物资储备情况，增强应急资源的统一调配能力，提高应急资源利用效率。各电力企业应加强应急物资动态管理，及时调整、升级软件硬件工具，不断增强应急技术支撑能力。

(四)技术支撑力量保障

加强网络安全应急技术支撑队伍建设，做好电力网络安全事件的监测预警、预防防护、应急处置、应急技术支持工作。国家能源局推动国家级电力网络安全靶场建设，按需组织国家级电力网络安全靶场等行业技术力量，为电力网络安全事件应对处置提供技术支持。各电力企业应建立本单位的网络安全事件应急处置技术支持队伍，加强专家队伍建设，充分发挥在本单位及行业的电力网络安全事件应急处置工作中的作用。

(五)基础平台保障

国家能源局指导电力行业共建共用行业级监测预警、信息通报和漏洞资源基础设施。电力调度机构、主要电力企业积极参与行业级基础设施建设，充分利用行业级基础设施，共享信息、协同研判，共同做好电力网络安全事件的预防和处置工作。

电力调度机构、主要电力企业应加强基础平台建设，做到电力网络安全事件早发现、早预警、早响应，提高应急处置能力。

(六)技术保障

各电力企业应按照“同步规划、同步建设、同步使用”要求，在新建或改建项目的规划、立项、设计、建设、运行等环节落实电力网络安全事件应急处置技术保障。

各电力企业应加强网络安全监测预警、预防防护、处置救援、应急服务等技术研究，不断改进技术装备。

(七)指挥保障

电力调度机构应加强应急指挥队伍的建设和管理，保障资金投入，配备必要的指挥装备，并定期开展应急指挥的培训和演练。

八、附则

(一)预案管理

根据实际情况的变化，国家能源局组织修订本预案。电力企业应参照本预案，制定或修订本单位电力网络安全事件应急预案，并根据企业实际情况的变化，及时修订本单位电力网络安全事件应急预案。

(二)罚则

国家能源局对不按照规定制定预案和组织开展演练，迟报、谎报、瞒报和漏报电力网络安全事件重要情况或者应急管理工作中有其他失职、渎职行为的，依照相关规定对有关责任人给予处理。

(三)与其他文件的衔接关系

因电力网络安全事件进一步引发电力安全事故(事件)的，同时按《电力安全事故应急处置和调查处理条例》《国家大面积停电事件应急预案》《电力安全事件监督管理规定》等有关规定开展事件报告、先期处置及事故调查。涉及电力关键信息基础设施的电力网络安全事件，同时按《关键信息基础设施安全保护条例》等相关规定开展处置。

(四)实施时间

本预案自印发之日起施行。

第十五章 交通运输部

网络预约出租汽车经营服务管理暂行办法

(2016 年 7 月 27 日交通运输部、工业和信息化部、公安部、商务部、工商总局、质检总局、国家网信办发布，根据 2019 年 12 月 28 日《交通运输部 工业和信息化部 公安部 商务部 市场监管总局 国家网信办关于修改〈网络预约出租汽车经营服务管理暂行办法〉的决定》第一次修正，根据 2022 年 11 月 30 日《交通运输部 工业和信息化部 公安部 商务部 市场监管总局 国家网信办关于修改〈网络预约出租汽车经营服务管理暂行办法〉的决定》第二次修正)

第一章 总 则

第一条 为更好地满足社会公众多样化出行需求，促进出租汽车行业和互联网融合发展，规范网络预约出租汽车经营服务行为，保障运营安全和乘客合法权益，根据国家有关法律、行政法规，制定本办法。

第二条 从事网络预约出租汽车(以下简称网约车)经营服务，应当遵守本办法。

本办法所称网约车经营服务，是指以互联网技术为依托构建服务平台，整合供需信息，使用符合条件的车辆和驾驶员，提供非巡游的预约出租汽车服务的经营活动。

本办法所称网络预约出租汽车经营者(以下称网约车平台公司)，是指构建网络服务平台，从事网约车经营服务的企业法人。

第三条 坚持优先发展城市公共交通、适度发展出租汽车，按照高品质服务、差异化经营的原则，有序发展网约车。

网约车运价实行市场调节价，城市人民政府认为有必要实行政府指导价的除外。

第四条 国务院交通运输主管部门负责指导全国网约车管理工作。

各省、自治区人民政府交通运输主管部门在本级人民政府领导下， 负责指导本行政区域内网约车管理工作。

直辖市、设区的市级或者县级交通运输主管部门或人民政府指定的其他出租汽车行政主管部门 (以下称出租汽车行政主管部门)在本级人民政府领导下，负责具体实施网约车管理。

其他有关部门依据法定职责，对网约车实施相关监督管理。

第二章 网约车平台公司

第五条 申请从事网约车经营的，应当具备线上线下服务能力，符合下列条件：

(一)具有企业法人资格；

(二)具备开展网约车经营的互联网平台和与拟开展业务相适应的信息数据交互及处理能力，具备供交通、通信、公安、税务、网信等相关监管部门依法调取查询相关网络数据信息的条件，网络服务平台数据库接入出租汽车行政主管部门监管平台，服务器设置在中国内地，有符合规定的网络安全管理制度和安全

保护技术措施；

(三)使用电子支付的，应当与银行、非银行支付机构签订提供支付结算服务的协议；

(四)有健全的经营管理制度、安全生产管理制度和服务质量保障制度；

(五)在服务所在地有相应服务机构及服务能力；

(六)法律法规规定的其他条件。

外商投资网约车经营的，除符合上述条件外，还应当符合外商投资相关法律法规的规定。

第六条 申请从事网约车经营的，应当根据经营区域向相应的出租汽车行政主管部门提出申请，并提交以下材料：

(一)网络预约出租汽车经营申请表(见附件)；

(二)投资人、负责人身份、资信证明及其复印件， 经办人的身份证明及其复印件和委托书；

(三)企业法人营业执照，属于分支机构的还应当提交营业执照；

(四)服务所在地办公场所、负责人员和管理人员等信息；

(五)具备互联网平台和信息数据交互及处理能力的证明材料，具备供交通、通信、公安、税务、网信等相关监管部门依法调取查询相关网络数据信息条件的证明材料，数据库接入情况说明，服务器设置在中国内地的情况说明，依法建立并落实网络安全管理制度和安全保护技术措施的证明材料；

(六)使用电子支付的，应当提供与银行、非银行支付机构签订的支付结算服务协议；

(七)经营管理制度、安全生产管理制度和服务质量保障制度文本；

(八)法律法规要求提供的其他材料。

首次从事网约车经营的，应当向企业注册地相应出租汽车行政主管部门提出申请，前款第(五)、第(六)项有关线上服务能力材料由网约车平台公司注册地省级交通运输主管部门商同级通信、公安、税务、网信、人民银行等部门审核认定，并提供相应认定结果，认定结果全国有效。网约车平台公司在注册地以外申请从事网约车经营的，应当提交前款第(五)、第(六)项有关线上服务能力认定结果。

其他线下服务能力材料，由受理申请的出租汽车行政主管部门进行审核。

第七条 出租汽车行政主管部门应当自受理之日起 20 日内作出许可或者不予许可的决定。20 日内不能作出决定的，经实施机关负责人批准，可以延长 10 日，并应当将延长期限的理由告知申请人。

第八条 出租汽车行政主管部门对于网约车经营申请作出行政许可决定的，应当明确经营范围、经营区域、经营期限等， 并发放《网络预约出租汽车经营许可证》。

第九条 出租汽车行政主管部门对不符合规定条件的申请作出不予行政许可决定的，应当向申请人出具《不予行政许可决定书》。

第十条 网约车平台公司应当在取得相应《网络预约出租汽车经营许可证》并向企业注册地省级通信主管部门申请互联网信息服务备案后，方可开展相关业务。备案内容包括经营者真实身份信息、接入信息、出租汽车行政主管部门核发的《网络预约出租汽车经营许可证》等。涉及经营电信业务的， 还应当符合电信管理的相关规定。

网约车平台公司应当自网络正式联通之日起 30 日内，到网约车平台公司管理运营机构所在地的省级人民政府公安机关指定的受理机关办理备案手续。

第十一条 网约车平台公司暂停或者终止运营的，应当提前 30 日向服务所在地出租汽车行政主管部门书面报告，说明有关情况，通告提供服务的车辆所有人和驾驶员，并向社会公告。终止经营的， 应当将相应《网络预约出租汽车经营许可证》交回原许可机关。

第三章 网约车车辆和驾驶员

第十二条 拟从事网约车经营的车辆，应当符合以下条件：

(一)7 座及以下乘用车；

(二)安装具有行驶记录功能的车辆卫星定位装置、应急报警装置；

(三)车辆技术性能符合运营安全相关标准要求。

车辆的具体标准和营运要求，由相应的出租汽车行政主管部门，按照高品质服务、差异化经营的发展原则，结合本地实际情况确定。

第十三条 服务所在地出租汽车行政主管部门依车辆所有人或者网约车平台公司申请，按第十二条规定的条件审核后，对符合条件并登记为预约出租客运的车辆，发放《网络预约出租汽车运输证》。

城市人民政府对网约车发放《网络预约出租汽车运输证》另有规定的，从其规定。

第十四条 从事网约车服务的驾驶员，应当符合以下条件：

(一)取得相应准驾车型机动车驾驶证并具有 3 年以上驾驶经历；

(二)无交通肇事犯罪、危险驾驶犯罪记录，无吸毒记录，无饮酒后驾驶记录，最近连续 3 个记分周期内没有记满 12 分记录；

(三)无暴力犯罪记录；

(四)城市人民政府规定的其他条件。

第十五条 服务所在地设区的市级出租汽车行政主管部门依驾驶员或者网约车平台公司申请，按第十四条规定的条件核查并按规定考核后，为符合条件且考核合格的驾驶员，发放《网络预约出租汽车驾驶员证》。

第四章 网约车经营行为

第十六条 网约车平台公司承担承运人责任，应当保证运营安全，保障乘客合法权益。

第十七条 网约车平台公司应当保证提供服务车辆具备合法营运资质，技术状况良好，安全性能可靠，具有营运车辆相关保险，保证线上提供服务的车辆与线下实际提供服务的车辆一致，并将车辆相关信息向服务所在地出租汽车行政主管部门报备。

第十八条 网约车平台公司应当保证提供服务的驾驶员具有合法从业资格，按照有关法律法规规定，根据工作时长、服务频次等特点，与驾驶员签订多种形式的劳动合同或者协议，明确双方的权利和义务。网约车平台公司应当维护和保障驾驶员合法权益，开展有关法律法规、职业道德、服务规范、安全运营等方面的岗前培训和日常教育，保证线上提供服务的驾驶员与线下实际提供服务的驾驶员一致，并将驾驶员相关信息向服务所在地出租汽车行政主管部门报备。

网约车平台公司应当记录驾驶员、约车人在其服务平台发布的信息内容、用户注册信息、身份认证信息、订单日志、上网日志、网上交易日志、行驶轨迹日志等数据并备份。

第十九条 网约车平台公司应当公布确定符合国家有关规定的计程计价方式，明确服务项目和质量承诺，建立服务评价体系和乘客投诉处理制度，如实采集与

记录驾驶员服务信息。在提供网约车服务时， 提供驾驶员姓名、照片、手机号码和服务评价结果，以及车辆牌照等信息。

第二十条 网约车平台公司应当合理确定网约车运价，实行明码标价，并向乘客提供相应的出租汽车发票。

第二十一条 网约车平台公司不得妨碍市场公平竞争，不得侵害乘客合法权益和社会公共利益。

网约车平台公司不得有为排挤竞争对手或者独占市场，以低于成本的价格运营扰乱正常市场秩序，损害国家利益或者其他经营者合法权益等不正当价格行为，不得有价格违法行为。

第二十二条 网约车应当在许可的经营区域内从事经营活动，超出许可的经营区域的，起讫点一端应当在许可的经营区域内。

第二十三条网约车平台公司应当依法纳税，为乘客购买承运人责任险等相关保险，充分保障乘客权益。

第二十四条 网约车平台公司应当加强安全管理，落实运营、网络等安全防范措施，严格数据安全保护和管理，提高安全防范和抗风险能力，支持配合有关部门开展相关工作。

第二十五条 网约车平台公司和驾驶员提供经营服务应当符合国家有关运营服务标准，不得途中甩客或者故意绕道行驶，不得违规收费，不得对举报、投诉其服务质量或者对其服务作出不满意评价的乘客实施报复行为。

第二十六条 网约车平台公司应当通过其服务平台以显著方式将驾驶员、约车人和乘客等个人信息的采集和使用的目的、方式和范围进行告知。未经信息主体明示同意，网约车平台公司不得使用前述个人信息用于开展其他业务。

网约车平台公司采集驾驶员、约车人和乘客的个人信息，不得超越提供网约车业务所必需的范围。

除配合国家机关依法行使监督检查权或者刑事侦查权外，网约车平台公司不得向任何第三方提供驾驶员、约车人和乘客的姓名、联系方式、家庭住址、银行账户或者支付账户、地理位置、出行线路等个人信息，不得泄露地理坐标、地理标志物等涉及国家安全的敏感信息。发生信息泄露后，网约车平台公司应当及时向相关主管部门报告，并采取及时有效的补救措施。

第二十七条 网约车平台公司应当遵守国家网络和信息安全有关规定，所采集的个人信息和生成的业务数据，应当在中国内地存储和使用，保存期限不少于2年，除法律法规另有规定外，上述信息和数据不得外流。

网约车平台公司不得利用其服务平台发布法律法规禁止传播的信息，不得为企业、个人及其他团体、组织发布有害信息提供便利， 并采取有效措施过滤阻断有害信息传播。发现他人利用其网络服务平台传播有害信息的， 应当立即停止传输，保存有关记录，并向国家有关机关报告。

网约车平台公司应当依照法律规定，为公安机关依法开展国家安全工作，防范、调查违法犯罪活动提供必要的技术支持与协助。

第二十八条 任何企业和个人不得向未取得合法资质的车辆、驾驶员提供信息对接开展网约车经营服务。不得以私人小客车合乘名义提供网约车经营服务。

网约车车辆和驾驶员不得通过未取得经营许可的网络服务平台提供运营服务。

第五章 监督检查

第二十九条 出租汽车行政主管部门应当建设和完善政府监管平台，实现与网约车平台信息共享。共享信息应当包括车辆和驾驶员基本信息、服务质量以及乘客评价信息等。

出租汽车行政主管部门应当加强对网约车市场监管，加强对网约车平台公司、车辆和驾驶员的资质审查与证件核发管理。

出租汽车行政主管部门应当定期组织开展网约车服务质量测评，并及时向社会公布本地区网约车平台公司基本信息、服务质量测评结果、乘客投诉处理情况等信息。

出租汽车行政主管、公安等部门有权根据管理需要依法调取查阅管辖范围内网约车平台公司的登记、运营和交易等相关数据信息。

第三十条 通信主管部门和公安、网信部门应当按照各自职责，对网约车平台公司非法收集、存储、处理和利用有关个人信息、违反互联网信息服务有关规定、危害网络和信息安全、应用网约车服务平台发布有害信息或者为企业、个人及其他团体组织发布有害信息提供便利的行为，依法进行查处，并配合出租汽车行政主管部门对认定存在违法违规行为的网约车平台公司进行依法处置。

公安机关、网信部门应当按照各自职责监督检查网络安全管理制度和安全保护技术措施的落实情况，防范、查处有关违法犯罪活动。

第三十一条 发展改革、价格、通信、公安、人力资源社会保障、商务、人民银行、税务、市场监管、网信等部门按照各自职责， 对网约车经营行为实施相关监督检查，并对违法行为依法处理。

第三十二条 各有关部门应当按照职责建立网约车平台公司和驾驶员信用记录，并纳入全国信用信息共享平台。同时将网约车平台公司行政许可和行政处罚等信用信息在国家企业信用信息公示系统上予以公示。

第三十三条 出租汽车行业协会组织应当建立网约车平台公司和驾驶员不良记录名单制度，加强行业自律。

第六章 法律责任

第三十四条 违反本规定，擅自从事或者变相从事网约车经营活动，有下列行为之一的，由县级以上出租汽车行政主管部门责令改正，予以警告，并按照以下规定分别予以罚款；构成犯罪的，依法追究刑事责任：

(一)未取得《网络预约出租汽车经营许可证》的，对网约车平台公司处以10000 元以上 30000 元以下罚款；

(二)未取得《网络预约出租汽车运输证》的，对当事人处以3000 元以上 10000 元以下罚款；

(三)未取得《网络预约出租汽车驾驶员证》的，对当事人处以 200 元以上 2000 元以下罚款。

伪造、变造或者使用伪造、变造、失效的《网络预约出租汽车运输证》《网络预约出租汽车驾驶员证》从事网约车经营活动的， 分别按照前款第(二)项、第(三)项的规定予以罚款。

第三十五条 网约车平台公司违反本规定，有下列行为之一的，由县级以上出租汽车行政主管部门和价格主管部门按照职责责令改正，对每次违法行为处以5000 元以上 10000 元以下罚款；情节严重的，处以 10000 元以上 30000 元以下罚款：

(一)提供服务车辆未取得《网络预约出租汽车运输证》，或者线上提供服务车辆与线下实际提供服务车辆不一致的；

(二)提供服务驾驶员未取得《网络预约出租汽车驾驶员证》，或者线上提供服务驾驶员与线下实际提供服务驾驶员不一致的；

(三)未按照规定保证车辆技术状况良好的；

(四)起讫点均不在许可的经营区域从事网约车经营活动的；

(五)未按照规定将提供服务的车辆、驾驶员相关信息向服务所在地出租汽车行政主管部门报备的；

(六)未按照规定制定服务质量标准、建立并落实投诉举报制度的；

(七)未按照规定提供共享信息，或者不配合出租汽车行政主管部门调取查阅相关数据信息的；

(八)未履行管理责任，出现甩客、故意绕道、违规收费等严重违反国家相关运营服务标准行为的。

网约车平台公司不再具备线上线下服务能力或者有严重违法行为的，由县级以上出租汽车行政主管部门依据相关法律法规的有关规定责令停业整顿、吊销相关许可证件。

第三十六条 网约车驾驶员违反本规定，有下列情形之一的，由县级以上出租汽车行政主管部门和价格主管部门按照职责责令改正，对每次违法行为处以50 元以上 200 元以下罚款：

(一)途中甩客或者故意绕道行驶的；

(二)违规收费的；

(三)对举报、投诉其服务质量或者对其服务作出不满意评价的乘客实施报复行为的。

网约车驾驶员不再具备从业条件或者有严重违法行为的，由县级以上出租汽车行政主管部门依据相关法律法规的有关规定撤销或者吊销从业资格证件。

对网约车驾驶员的行政处罚信息计入驾驶员和网约车平台公司信用记录。

第三十七条 网约车平台公司违反本规定第十、十八、二十六、二十七条有关规定的，由网信部门、公安机关和通信主管部门按各自职责依照相关法律法规规定给予处罚；给信息主体造成损失的，依法承担民事责任；涉嫌犯罪的，依法追究刑事责任。

网约车平台公司及网约车驾驶员违法使用或者泄露约车人、乘客个人信息

的，由公安、网信等部门依照各自职责处以 2000 元以上 10000 元以下罚款；给信息主体造成损失的，依法承担民事责任；涉嫌犯罪的，依法追究刑事责任。

网约车平台公司拒不履行或者拒不按要求为公安机关依法开展国家安全工作，防范、调查违法犯罪活动提供技术支持与协助的，由公安机关依法予以处罚；构成犯罪的，依法追究刑事责任。

第七章 附 则

第三十八条 私人小客车合乘，也称为拼车、顺风车， 按城市人民政府有关规定执行。

第三十九条 网约车行驶里程达到 60 万千米时强制报废。行驶里程未达到 60 万千米但使用年限达到 8 年时，退出网约车经营。

小、微型非营运载客汽车登记为预约出租客运的，按照网约车报废标准报废。其他小、微型营运载客汽车登记为预约出租客运的， 按照该类型营运载客汽车报废标准和网约车报废标准中先行达到的标准报废。

省、自治区、直辖市人民政府有关部门要结合本地实际情况， 制定网约车报废标准的具体规定，并报国务院商务、公安、交通运输等部门备案。

第四十条 本办法自 2016 年 11 月 1 日起实施。各地可根据本办法结合本地实际制定具体实施细则。

铁路关键信息基础设施安全保护管理办法

中华人民共和国交通运输部令 2023 年第 20 号

《铁路关键信息基础设施安全保护管理办法》已于 2023 年 12 月 1 日经第 27 次部务会议通过，现予公布，自 2024 年 2 月 1 日起施行。

部 长 李小鹏

2023 年 12 月 17 日

铁路关键信息基础设施安全保护管理办法

第一章 总 则

第一条 为了保障铁路关键信息基础设施安全，维护网络安全，根据《中华人民共和国网络安全法》、《关键信息基础设施安全保护条例》等法律、行政法规，制定本办法。

第二条 铁路关键信息基础设施的安全保护和监督管理工作，适用本办法。

本办法所称铁路关键信息基础设施，是指在铁路领域，一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生和公共利益的重要网络设施、信息系统等。

第三条 国家铁路局是负责铁路领域关键信息基础设施安全保护工作的部门，在职责范围内负责全国铁路关键信息基础设施安全保护和监督管理工作。

地区铁路监督管理局按照国家铁路局要求，开展本辖区铁路关键信息基础设施的安全保护和监督管理工作。

第四条 铁路关键信息基础设施安全保护坚持强化和落实铁路关键信息基础设施运营者(以下简称运营者)主体责任，加强和规范保护工作部门监督管理，发挥社会各方面的作用，共同保护铁路关键信息基础设施安全。

第五条 任何个人和组织不得实施非法侵入、干扰、破坏铁路关键信息基础设施的活动，不得危害铁路关键信息基础设施安全。

第二章 铁路关键信息基础设施认定

第六条 国家铁路局负责制定铁路关键信息基础设施认定规则，并报国务院公安部门备案，抄送国家网信部门。

制定认定规则应当主要考虑下列因素：

(一)网络设施、信息系统等对于铁路关键核心业务的重要程度；

(二)网络设施、信息系统等一旦遭到破坏、丧失功能或者数据泄露可能带来的危害程度；

(三)对其他行业和领域的关联性影响。

第七条 国家铁路局根据认定规则，负责组织认定铁路关键信息基础设施，及时将认定结果通知运营者，并通报国务院公安部门，抄送国家网信部门。

第八条 铁路关键信息基础设施发生改建、扩建、运营者变更等较大变化，可能影响认定结果的，运营者应当及时将相关情况报告国家铁路局。国家铁路局自收到报告之日起 3 个月内完成重新认定，将认定结果通知运营者，并通报国务院公安部门，抄送国家网信部门。

第三章 运营者责任和义务

第九条 铁路关键信息基础设施的网络安全保护等级应当不低于第三级。

运营者应当依照有关法律、行政法规的规定以及国家标准的强制性要求， 在

国家网络安全等级保护制度的基础上，突出保护重点，落实防护措施，加强全生命周期管理，保障铁路关键信息基础设施安全稳定运行，维护数据的完整性、保密性和可用性。

第十条 新建、改建、扩建铁路关键信息基础设施的，运营者应当做到安全防护措施与关键信息基础设施同步规划、同步建设、同步使用，并采取检测评估、安全演练等方式验证安全保护措施的有效性。

第十一条 运营者应当建立健全网络安全保护制度和责任制，保障人力、财力、物力投入。

运营者的主要负责人对所运营的铁路关键信息基础设施安全保护负总责，领导关键信息基础设施安全保护和重大网络安全事件处置工作，组织研究解决重大网络安全问题。

运营者应当为每个铁路关键信息基础设施明确安全管理责任人。

第十二条 运营者应当设置专门安全管理机构，保障专门安全管理机构的运行经费、配备相应的人员， 开展与网络安全和信息化有关的决策应当有专门安全管理机构人员参与。

运营者应当对专门安全管理机构负责人和关键岗位人员进行安全背景审查。专门安全管理机构的负责人和关键岗位人员的身份、安全背景等发生变化或者必要时，运营者应当根据情况重新进行安全背景审查。

第十三条 专门安全管理机构具体负责本单位的铁路关键信息基础设施安全保护工作，履行下列职责：

(一)建立健全网络安全管理、评价考核制度， 拟订铁路关键信息基础设施安全保护计划；

(二)组织推动网络安全防护能力建设，开展网络安全监测、检测和风险评估；

(三)按照国家及铁路行业要求，制定本单位网络安全事件应急预案，定期开展应急演练，处置网络安全事件；

(四)认定网络安全关键岗位，组织开展网络安全工作考核，提出奖励和惩处建议；

(五)组织网络安全教育、培训；

(六)履行个人信息和数据安全保护责任，建立健全个人信息和数据安全保护

制度；

(七)对铁路关键信息基础设施设计、建设、运行、维护等服务实施安全管理；

(八)按照规定报告网络安全事件和重要事项。

第十四条 运营者应当加强铁路关键信息基础设施供应链安全保护，优先采购安全可信的网络产品和服务。运营者采购网络产品和服务， 应当预判该产品和服务投入使用后对国家安全的影响。可能影响国家安全的， 应当按照国家有关规定申报网络安全审查。

第十五条 运营者应当加强数据安全保护，明确重要数据和个人信息的保护措施，将在我国境内运营中收集和产生的个人信息和重要数据存储在境内。因业务需要，确需向境外提供数据的，应当按照国家相关规定和标准进行安全评估。法律、行政法规另有规定的，依照其规定执行。

第十六条 运营者应当自行或者委托网络安全服务机构对铁路关键信息基础设施每年至少进行一次网络安全检测和风险评估，对发现的安全问题及时整改，并按照国家铁路局要求报送情况。

第十七条 法律、行政法规和国家有关规定要求使用商用密码进行保护的铁路关键信息基础设施，运营者应当使用商用密码进行保护，自行或者委托商用密码检测机构每年至少开展一次商用密码应用安全性评估。

商用密码应用安全性评估应当与铁路关键信息基础设施安全检测和风险评估、网络安全等级测评制度相衔接，避免重复评估、测评。

第十八条 运营者应当加强全过程保密管理，采购网络产品和服务，应当按照规定与提供者签订安全保密协议，明确提供者的技术支持和安全保密义务与责任，并对义务与责任履行情况进行监督。

第十九条 运营者应当制定本单位的监测预警和信息通报制度，加强对铁路关键信息基础设施监测，研判整体安全态势。

第二十条 铁路关键信息基础设施发生重大网络安全事件或者发现重大网络安全威胁时，运营者应当按照有关规定向国家铁路局、公安机关报告， 并立即启动本单位网络安全事件应急预案。

铁路关键信息基础设施发生特别重大网络安全事件或者发现特别重大网络安全威胁时，国家铁路局应当在收到报告后，及时向国家网信部门、国务院公安

部门报告。

第二十一条 运营者发生合并、分立、解散等情况，应当及时报告国家铁路局，并按照国家铁路局的要求对铁路关键信息基础设施进行处置，确保安全。

第四章 保障和监督

第二十二条 国家铁路局应当制定铁路关键信息基础设施安全规划，明确保护目标、基本要求、工作任务、具体措施。

第二十三条 国家铁路局应当依托国家网络安全信息共享机制，组织建立铁路关键信息基础设施网络安全监测预警制度，及时掌握铁路关键信息基础设施运行状况、安全态势，预警通报网络安全威胁和隐患，指导做好安全防范工作。

第二十四条 国家铁路局应当组织建立健全铁路关键信息基础设施网络安全事件应急预案体系，定期组织应急演练；指导运营者做好网络安全事件应对处置，并根据需要组织提供技术支持与协助。

第二十五条 国家铁路局定期组织开展铁路关键信息基础设施网络安全检查检测，指导监督运营者及时整改安全隐患、完善安全措施。

检查工作不得收取费用，不得要求被检查单位购买指定品牌或者指定生产、销售单位的产品和服务。

第二十六条 运营者对国家铁路局依法开展的网络安全检查检测工作，以及公安、国家安全、保密行政管理、密码管理等有关部门依法开展的铁路关键信息基础设施网络安全检查工作应当予以配合。

第二十七条 国家铁路局、网络安全服务机构及其工作人员对于在铁路关键信息基础设施安全保护过程中获取的信息，只能用于维护网络安全，并严格按照有关法律、行政法规的要求确保信息安全， 不得泄露、出售、非法向他人提供或者进行其他违法活动。

第五章 法律责任

第二十八条 运营者违反本办法规定的，由国家铁路局依照《中华人民共和国网络安全法》、《关键信息基础设施安全保护条例》等法律、行政法规的规定予以处罚。

第二十九条 国家铁路局及其工作人员存在下列情形之一的，按照有关法律、行政法规的规定予以处分：

(一)未履行铁路关键信息基础设施安全保护和监督管理职责或者玩忽职守、滥用职权、徇私舞弊的;

(二)在开展铁路关键信息基础设施网络安全检查工作中收取费用,或者要求被检查单位购买指定品牌或者指定生产、销售单位的产品和服务的;

(三)将在铁路关键信息基础设施安全保护工作中获取的信息泄露、出售、非法向他人提供或者进行其他违法活动的。

第六章 附 则

第三十条 本办法自 2024 年 2 月 1 日起施行。

快递市场管理办法

中华人民共和国交通运输部令 2023 年第 22 号

《快递市场管理办法》已于 2023 年 12 月 8 日经第 28 次部务会议通过,现予公布,自 2024 年 3 月 1 日起施行。

部长 李小鹏

2023 年 12 月 17 日

快递市场管理办法

第一章 总 则

第一条 为了加强快递市场监督管理,保障快递服务质量和安全,维护用户、快递从业人员和经营快递业务的企业的合法权益,促进快递业健康发展,根据《中华人民共和国邮政法》《快递暂行条例》等法律、行政法规,制定本办法。

第二条 在中华人民共和国境内从事快递业务经营、使用快递服务以及对快递市场实施监督管理,适用本办法。

第三条 经营快递业务的企业应当遵守法律法规和公序良俗,依法节约资源、保护生态环境,为用户提供迅速、准确、安全、方便的快递服务。

第四条 两个以上经营快递业务的企业使用统一的商标、字号、快递运单及其配套的信息系统的,应当签订书面协议,明确各自的权利义务,遵守共同的服务约定,在服务质量、安全保障、业务流程、生态环保、从业人员权益保障等方面实行统一管理。

商标、字号、快递运单及其配套的信息系统的归属企业,简称为总部快递

企业。

第五条 用户使用快递服务应当遵守法律、行政法规以及国务院和国务院有关部门关于禁止寄递或者限制寄递物品的规定，真实、准确地向经营快递业务的企业提供使用快递服务所必需的信息。

第六条 国务院邮政管理部门负责对全国快递市场实施监督管理。

省、自治区、直辖市邮政管理机构负责对本行政区域的快递市场实施监督管理。

按照国务院规定设立的省级以下邮政管理机构负责对本辖区的快递市场实施监督管理。

国务院邮政管理部门和省、自治区、直辖市邮政管理机构及省级以下邮政管理机构，统称为邮政管理部门。

第七条 邮政管理部门对快递市场实施监督管理应当公开、公正，鼓励公平竞争，支持高质量发展，加强线上线下一体化监督管理。

第八条 依法成立的快递行业组织应当维护经营快递业务的企业、快递末端网点和快递从业人员的合法权益，依照法律、法规以及组织章程规定，制定快递行业规范公约，加强行业自律，倡导企业守法、诚信、安全、绿色经营。

第九条 经营快递业务的企业应当坚持绿色低碳发展，落实生态环境保护责任。

经营快递业务的企业应当按照国家规定，推进快递包装标准化、循环化、减量化、无害化，避免过度包装。

第二章 发展保障

第十条 国务院邮政管理部门制定快递业发展规划，促进快递业高质量发展。

省、自治区、直辖市邮政管理机构可以结合地方实际制定本行政区域的快递业发展规划。

第十一条 邮政管理部门会同有关部门支持、引导经营快递业务的企业在城乡设置快件收投服务场所和智能收投设施。

邮政管理部门支持在公共服务设施布局中统筹建设具有公共服务属性的收投服务场所和智能收投设施。

邮政管理部门对快递服务类型和快递服务设施实施分类代码管理。

第十二条 国务院邮政管理部门会同国家有关部门支持建设进出境快件处理中心，在交通枢纽配套建设快件运输通道和接驳场所，优化快递服务网络布局。

第十三条 邮政管理部门支持创新快递商业模式和服务方式，引导快递市场新业态数字化、智能化、规范化发展，加强服务质量监督管理。

第三章 绿色低碳发展

第十四条 邮政管理部门应当引导用户使用绿色包装和减量包装，鼓励经营快递业务的企业开展绿色设计、选择绿色材料、实施绿色运输、使用绿色能源。

第十五条 经营快递业务的企业应当加强包装操作规范，运用信息技术，优化包装结构，优先使用产品原包装，在设计、生产、销售、使用等环节全链条推进快递包装绿色化。

第十六条 经营快递业务的企业应当优先采购有利于保护环境的产品，使用符合国家强制性标准的包装产品，不得使用国家禁止使用的塑料制品。

第十七条 经营快递业务的企业应当积极回收利用包装物，不断提高快递包装复用比例，推广应用可循环、易回收、可降解的快递包装。

第四章 市场秩序

第十八条 经营快递业务的企业应当在快递业务经营许可范围内依法经营快递业务，不得超越许可的业务范围和地域范围。

经营快递业务的企业设立分支机构，应当向邮政管理部门备案，报告分支机构的营业执照信息。

第十九条 经营快递业务的企业不得以任何方式委托未取得快递业务经营许可的企业经营快递业务。

经营快递业务的企业不得以任何方式超越许可范围委托、受托经营快递业务。

第二十条 总部快递企业依照法律、行政法规规定，对使用其商标、字号、快递运单及其配套的信息系统经营快递业务的企业实施统一管理，履行统一管理责任。

总部快递企业应当建立规范化标准化管理制度和机制，对使用其商标、字号、快递运单及其配套的信息系统经营快递业务的企业实施合理的管理措施，保障向用户正常提供快递服务。

第二十一条 经营快递业务的企业不得实施下列行为：

(一)明知他人从事危害国家安全、社会公共利益或者他人合法权益活动仍配合提供快递服务；

(二)违法虚构快递服务信息；

(三)出售、泄露或者非法提供快递服务过程中知悉的用户信息；

(四)法律、法规以及国家规定禁止的其他行为。

第五章 快递服务

第二十二条 经营快递业务的企业应当按照法律、行政法规的规定，在门户网站、营业场所公示或者以其他明显方式向社会公布其服务种类、服务地域、服务时限、营业时间、资费标准、快件查询、损失赔偿、投诉处理等服务事项。

经营快递业务的企业公示或者公布的服务地域，应当以建制村、社区为基本单元，明确服务地域范围。鼓励经营快递业务的企业以县级行政区域为基本单元公布资费标准，明确重量误差范围。

除不可抗力外，前两款规定的事项发生变更的，经营快递业务的企业应当提前 10 日向社会发布服务提示公告。

第二十三条 经营快递业务的企业为电子商务经营者交付商品提供快递服务的，应当书面告知电子商务经营者在其销售商品的网页上明示快递服务品牌，保障用户对快递服务的知情权。

第二十四条 经营快递业务的企业提供快递服务，应当与寄件人订立服务合同，明确权利和义务。经营快递业务的企业对不能提供服务的建制村、社区等区域，应当以醒目的方式提前告知寄件人。

第二十五条 经营快递业务的企业应当采取有效技术手段，保证用户、邮政管理部门能够通过快递运单码号或者信息系统查知下列内容：

(一)订立、履行快递服务合同所必需的用户个人信息范围以及处理个人信息前应当依法告知的事项；

(二)快递服务承诺事项以及投递方式和完成标准;

(三)快递物品的名称、数量、重量;

(四)该快件的快递服务费金额;

(五)服务纠纷的解决方式。

用户查询前款规定的信息的,经营快递业务的企业应当按照《中华人民共和国个人信息保护法》的要求采取措施防止未经授权的查询以及个人信息泄露。

第二十六条 经营快递业务的企业应当建立服务质量管理制度和业务操作规范,保障服务质量,并符合下列要求:

(一)提供快递服务时,恪守社会公德,诚信经营,保障用户的合法权益,不得设定不公平、不合理的交易条件,不得强制交易;

(二)提醒寄件人在提供快递运单信息前,认真阅读快递服务合同条款、遵守禁止寄递和限制寄递物品的有关规定,告知相关保价规则和保险服务项目;

(三)依法对寄件人身份进行查验,登记身份信息,寄件人拒绝提供身份信息或者提供身份信息不实的,不得收寄;

(四)对寄件人交寄的信件以外的物品进行查验,登记内件品名等信息,寄件人拒绝提供内件信息或者提供的内件信息与查验情况不符的,不得收寄;

(五)在快递运单上如实标注快件重量;

(六)寄件人提供的收寄地址与快件实际收寄地址不一致的,在快递运单上一并如实记录;

(七)按照快件的种类和时限分别处理、分区作业、规范操作,并按规定录入、上传处理信息;

(八)保障快件安全,防止快件丢失、损毁、内件短少,不得抛扔、踩踏快件;

(九)除因不可抗力因素外,按照约定在承诺的时限内将快件投递到收件地址、收件人;

(十)向用户提供快件寄递跟踪查询服务,不得将快件进行不合理绕行,不得隐瞒、虚构寄递流程信息,保证用户知悉其使用快递服务的真实情况;

(十一)法律、行政法规规定的其他要求。

第二十七条 经营快递业务的企业投递快件，应当告知收件人有权当面验收快件，查看内件物品与快递运单记载是否一致。快递包装出现明显破损或者内件物品为易碎品的，应当告知收件人可以查看内件物品或者拒收快件。

经营快递业务的企业与寄件人事先书面约定收件人查看内件物品具体方式的，经营快递业务的企业应当在快递运单上以醒目方式注明。

除法律、行政法规另有规定外，收件人收到来源不明的快件，要求经营快递业务的企业提供寄件人姓名（名称）、地址、联系电话等必要信息的，经营快递业务的企业应当提供其掌握的信息。

第二十八条 收件人可以签字或者其他易于辨认、保存的明示方式确认收到快件，也可指定代收人验收快件和确认收到快件。

收件人或者收件人指定的代收人不能当面验收快件的，经营快递业务的企业应当与用户另行约定快件投递服务方式和确认收到快件方式。

经营快递业务的企业未经用户同意，不得代为确认收到快件，不得擅自将快件投递到智能快件箱、快递服务站等快递末端服务设施。

第二十九条 经营快递业务的企业应当按照法律、行政法规处理无法投递又无法退回的快件(以下称无着快件)，并建立无着快件的核实、保管和处理制度，将处理情况纳入快递业务经营许可年度报告。

经营快递业务的企业处理无着快件，不得有下列行为：

(一)在保管期限内停止查询服务；

(二)保管期限未届满擅自处置；

(三)牟取不正当利益；

(四)非法扣留应当予以没收或者销毁的物品；

(五)法律、行政法规禁止的其他行为。

第三十条 经营快递业务的企业应当建立健全用户投诉申诉处理制度，依法处理用户提出的快递服务质量异议。

用户对投诉处理结果不满意或者投诉没有得到及时处理的，可以提出快递服务质量申诉。

邮政管理部门对用户提出的快递服务质量申诉实施调解。经营快递业务的企业应当依法处理邮政管理部门转告的申诉事项并反馈结果。

第六章 安全发展

第三十一条 经营快递业务的企业应当建立健全安全生产责任制，加强从业人员安全生产教育和培训，履行法律、法规、规章规定的有关安全生产义务。

经营快递业务的企业的主要负责人是安全生产的第一责任人，对本单位的安全生产工作全面负责。其他负责人对职责范围内的安全生产工作负责。

总部快递企业应当督促其他使用与其统一的商标、字号、快递运单及其配套的信息系统经营快递业务的企业及其从业人员遵守安全自查、安全教育、安全培训等安全制度。

第三十二条 经营快递业务的企业应当遵守收寄验视、实名收寄、安全检查和禁止寄递物品管理制度。任何单位或者个人不得利用快递服务从事危害国家安全、社会公共利益、他人合法权益的活动。

第三十三条 新建快件处理场所投入使用的，经营快递业务的企业应当按照邮政管理部门的规定报告。

第三十四条 经营快递业务的企业使用快件处理场所，应当遵守下列规定：

(一)在有较大危险因素的快件处理场所和有关设施、设备上设置明显的安全警示标志，以及通信、报警、紧急制动等安全设备，并保证其处于适用状态；

(二)配备栅栏或者隔离桩等安全设备，并设置明显的人车分流安全警示标志；

(三)对场所设备、设施进行经常性维护、保养和定期检测，并将检查及处理情况形成书面记录；

(四)及时发现和整改安全隐患。

第三十五条 经营快递业务的企业在生产经营过程中，获取用户个人信息的范围，应当限于履行快递服务合同所必需，不得过度收集用户个人信息。

经营快递业务的企业应当依法建立用户个人信息安全管理制度和操作规程，不得实施下列行为：

(一)除法律、行政法规另有规定或者因向用户履行快递服务合同需要外，未经用户同意，收集、存储、使用、加工、传输、提供、公开用户信息；

(二)以概括授权、默认授权、拒绝服务等方式，强迫或者变相强迫用户同

意，收集、使用与经营活动无关的用户信息；

(三)以非正当目的，向他人提供与用户关联的分析信息；

(四)法律、行政法规禁止的其他行为。

第三十六条 经营快递业务的企业应当建立快递运单(含电子运单)制作、使用、保管、销毁等管理制度和操作规程，采取加密、去标识化等安全技术措施保护快递运单信息安全。

经营快递业务的企业应当建立快递运单码号使用、销毁等管理制度，实行码号使用信息、用户信息、快递物品信息关联管理，保证快件可以跟踪查询。

任何单位和个人不得非法使用、倒卖快递运单。

第三十七条 经营快递业务的企业委托其他企业处理用户个人信息的，应当事前进行用户个人信息保护影响评估，并对受托企业处理个人信息的活动进行监督，不免除自身对用户个人信息安全承担的责任。

第三十八条 经营快递业务的企业应当及时向邮政管理部门报送生产经营过程中产生的与安全运营有关的数据信息。

经营快递业务的企业按照前款规定报送数据信息的，应当保证数据真实、准确、完整，报送方式符合国务院邮政管理部门的要求，不得漏报、错报、瞒报、谎报。

第三十九条 总部快递企业应当建立维护服务网络稳定工作制度，维护同网快递企业的服务网络稳定，并符合下列要求：

(一)实施服务网络运行监测预警和风险研判制度；

(二)建立健全应急预案；

(三)制定经营异常网点清单；

(四)及时有效排查化解企业内部矛盾纠纷，有效应对处置影响企业服务网络稳定的突发事件。

经营快递业务的企业发生服务网络阻断的，应当在 24 小时内向邮政管理部门报告，并向社会公告。

第四十条 总部快递企业按照《快递暂行条例》的规定，在安全保障方面实施统一管理，督促使用与其统一的商标、字号、快递运单及其配套信息系统经营快递业务的企业及其从业人员遵守反恐、禁毒、安全生产、寄递安全、网络

与信息安全以及应急管理等方面的规定，符合国务院邮政管理部门关于安全保障方面统一管理的要求。

第七章 监督管理

第四十一条 邮政管理部门依法履行快递市场监督管理职责，可以采取下列监督检查措施：

(一)进入被检查单位或者涉嫌发生违法活动的其他场所实施现场检查；

(二)向有关单位和个人了解情况；

(三)查阅、复制有关文件、资料、凭证、电子数据；

(四)经邮政管理部门负责人批准，依法查封与违法活动有关的场所，扣押用于违法活动的运输工具以及相关物品，对信件以外的涉嫌夹带禁止寄递或者限制寄递物品的快件开拆检查。

第四十二条 邮政管理部门以随机抽查的方式实施日常监督检查，可以依据经营快递业务的企业的信用情况，在抽查比例和频次等方面采取差异化措施。

用户申诉反映的快递服务问题涉嫌违反邮政管理的法律、行政法规、规章的，邮政管理部门应当依法调查和处理。

第四十三条 邮政管理部门工作人员对监督检查过程中知悉的商业秘密或者个人隐私，应当依法予以保密。

第四十四条 国务院邮政管理部门建立快递服务质量评价体系，组织开展快递服务质量评价工作。

邮政管理部门可以依法要求经营快递业务的企业报告从业人员、业务量、服务质量保障等经营情况。

第四十五条 邮政管理部门可以依法采取风险提示、约谈告诫、公示公告等方式指导和督促快递企业合法合规经营。

第四十六条 国务院邮政管理部门或者省、自治区、直辖市邮政管理机构对存在重大经营风险或者安全隐患的经营快递业务的企业实施重点检查，提出整改要求。

第四十七条 经营快递业务的企业快递服务行为发生异常、可能在特定地域范围内不具备提供正常服务的能力和条件的，应当向邮政管理部门报告，并向社会公告。

第八章 法律责任

第四十八条 经营快递业务的企业将快递业务委托给未取得快递业务经营许可的企业经营的，由邮政管理部门责令改正，处 5000 元以上 1 万元以下的罚款；情节严重的，处 1 万元以上 3 万元以下的罚款。

第四十九条 总部快递企业采取不合理的管理措施，导致使用其商标、字号、快递运单及其配套信息系统经营快递业务的企业不能向用户正常提供快递服务的，由邮政管理部门责令改正，予以警告或者通报批评，可以并处 3000 元以上 1 万元以下的罚款；情节严重的，处 1 万元以上 3 万元以下的罚款；涉嫌不正当竞争或者价格违法的，将线索移送有关部门。

第五十条 经营快递业务的企业未按规定公示、公布服务地域、服务时限，或者变更服务地域、服务时限未按规定提前向社会发布公告的，由邮政管理部门责令改正，予以警告或者通报批评，可以并处 3000 元以上 1 万元以下的罚款；情节严重的，处 1 万元以上 3 万元以下的罚款；涉嫌价格违法的，将线索移送有关部门。

第五十一条 经营快递业务的企业不按照公示、公布的服务地域投递快件的，由邮政管理部门责令改正，予以警告或者通报批评，可以并处快递服务费金额 1 倍至 10 倍的罚款。

第五十二条 经营快递业务的企业未采取有效技术手段保证用户、邮政管理部门通过快递运单码号或者信息系统查知本办法第二十五条规定的内容的，由邮政管理部门责令改正，予以警告或者通报批评，可以并处 3000 元以上 1 万元以下的罚款。

第五十三条 经营快递业务的企业有下列情形之一的，由邮政管理部门责令改正，处 1 万元以下的罚款；情节严重的，处 1 万元以上 3 万元以下的罚款；涉嫌进行非法活动的，将线索移送有关部门：

(一)隐瞒、虚构寄递流程信息的；

(二)虚构快递物品的名称、数量、重量信息的；

(三)虚构快递服务费金额信息的；

(四)寄件人提供的收寄地址与快件实际收寄地址不一致，未在快递运单上一并如实记录的；

(五)未按本办法第二十七条规定向收件人提供寄件人信息的。

第五十四条 经营快递业务的企业有下列情形之一的，由邮政管理部门责令改正，予以警告或者通报批评，可以并处 1 万元以下的罚款；情节严重的，处 1 万元以上 3 万元以下的罚款：

(一)未经用户同意代为确认收到快件的；

(二)未经用户同意擅自使用智能快件箱、快递服务站等方式投递快件的；

(三)抛扔快件、踩踏快件的。

第五十五条 经营快递业务的企业未按规定配合邮政管理部门处理用户申诉的，由邮政管理部门责令改正，予以警告或者通报批评；情节严重的，并处 3000 元以下的罚款。

第五十六条 经营快递业务的企业有下列情形之一的，由邮政管理部门责令改正；逾期未改正的，处 3000 元以下的罚款。法律、行政法规有规定的，从其规定：

(一)未按规定向邮政管理部门报送数据信息或者漏报、错报、瞒报、谎报的；

(二)可能在特定地域范围内不具备提供正常服务的能力和条件，未按规定报告、公告的。

第九章 附 则

第五十七条 本办法自 2024 年 3 月 1 日起施行。交通运输部于 2013 年 1 月 11 日以交通运输部令 2013 年第 1 号公布的《快递市场管理办法》同时废止。

第十六章 其他部门

网络出版服务管理规定

国家新闻出版广电总局 工业和信息化部令第 5 号

《网络出版服务管理规定》已经 2015 年 8 月 20 日国家新闻出版广电总局局务会议通过，并经工业和信息化部同意，现予公布，自 2016 年 3 月 10 日起施行。

国家新闻出版广电总局局长 蔡赴朝

工业和信息化部部长 苗圩

2016 年 2 月 4 日

网络出版服务管理规定

第一章 总 则

第一条 为了规范网络出版服务秩序，促进网络出版服务业健康有序发展，根据《出版管理条例》、《互联网信息服务管理办法》及相关法律法规， 制定本规定。

第二条 在中华人民共和国境内从事网络出版服务，适用本规定。

本规定所称网络出版服务，是指通过信息网络向公众提供网络出版物。

本规定所称网络出版物，是指通过信息网络向公众提供的，具有编辑、制作、加工等出版特征的数字化作品，范围主要包括：

(一)文学、艺术、科学等领域内具有知识性、思想性的文字、图片、地图、游戏、动漫、音视频读物等原创数字化作品；

(二)与已出版的图书、报纸、期刊、音像制品、电子出版物等内容相一致的数字化作品；

(三)将上述作品通过选择、编排、汇集等方式形成的网络文献数据库等数字化作品；

(四)国家新闻出版广电总局认定的其他类型的数字化作品。

网络出版服务的具体业务分类另行制定。

第三条 从事网络出版服务，应当遵守宪法和有关法律、法规，坚持为人民服务、为社会主义服务的方向， 坚持社会主义先进文化的前进方向，弘扬社会主义核心价值观，传播和积累一切有益于提高民族素质、推动经济发展、促进社会进步的思想道德、科学技术和文化知识，满足人民群众日益增长的精神文化需要。

第四条 国家新闻出版广电总局作为网络出版服务的行业主管部门，负责全国网络出版服务的前置审批和监督管理工作。工业和信息化部作为互联网行业主管部门，依据职责对全国网络出版服务实施相应的监督管理。

地方人民政府各级出版行政主管部门和各省级电信主管部门依据各自职责对本行政区域内网络出版服务及接入服务实施相应的监督管理工作并做好配合工作。

第五条 出版行政主管部门根据已经取得的违法嫌疑证据或者举报，对涉嫌违法从事网络出版服务的行为进行查处时，可以检查与涉嫌违法行为有关的物品和经营场所；对有证据证明是与违法行为有关的物品，可以查封或者扣押。

第六条 国家鼓励图书、音像、电子、报纸、期刊出版单位从事网络出版服务，加快与新媒体的融合发展。

国家鼓励组建网络出版服务行业协会，按照章程，在出版行政主管部门的指导下制定行业自律规范，倡导网络文明，传播健康有益内容，抵制不良有害内容。

第二章 网络出版服务许可

第七条 从事网络出版服务，必须依法经过出版行政主管部门批准，取得《网络出版服务许可证》。

第八条 图书、音像、电子、报纸、期刊出版单位从事网络出版服务，应当具备以下条件：

(一)有确定的从事网络出版业务的网站域名、智能终端应用程序等出版平台；

(二)有确定的网络出版服务范围；

(三)有从事网络出版服务所需的必要的技术设备，相关服务器和存储设备必须存放在中华人民共和国境内。

第九条 其他单位从事网络出版服务，除第八条所列条件外，还应当具备以下条件：

(一)有确定的、不与其他出版单位相重复的， 从事网络出版服务主体的名称及章程；

(二)有符合国家规定的法定代表人和主要负责人，法定代表人必须是在境内长久居住的具有完全行为能力的中国公民，法定代表人和主要负责人至少 1 人应当具有中级以上出版专业技术人员职业资格；

(三)除法定代表人和主要负责人外，有适应网络出版服务范围需要的 8 名以上具有国家新闻出版广电总局认可的出版及相关专业技术职业资格的专职编辑出版人员，其中具有中级以上职业资格的人员不得少于 3 名；

(四)有从事网络出版服务所需的内容审校制度；

(五)有固定的工作场所；

(六)法律、行政法规和国家新闻出版广电总局规定的其他条件。

第十条　中外合资经营、中外合作经营和外资经营的单位不得从事网络出版服务。

网络出版服务单位与境内中外合资经营、中外合作经营、外资经营企业或境外组织及个人进行网络出版服务业务的项目合作，应当事前报国家新闻出版广电总局审批。

第十一条　申请从事网络出版服务，应当向所在地省、自治区、直辖市出版行政主管部门提出申请，经审核同意后，报国家新闻出版广电总局审批。国家新闻出版广电总局应当自受理申请之日起 60 日内，作出批准或者不予批准的决定。不批准的，应当说明理由。

第十二条 从事网络出版服务的申报材料，应该包括下列内容：

(一)《网络出版服务许可证申请表》；

(二)单位章程及资本来源性质证明；

(三)网络出版服务可行性分析报告，包括资金使用、产品规划、技术条件、设备配备、机构设置、人员配备、市场分析、风险评估、版权保护措施等；

(四)法定代表人和主要负责人的简历、住址、身份证明文件；

(五)编辑出版等相关专业技术人员的国家认可的职业资格证明和主要从业经历及培训证明；

(六)工作场所使用证明；

(七)网站域名注册证明、相关服务器存放在中华人民共和国境内的承诺。

本规定第八条所列单位从事网络出版服务的，仅提交前款(一)、(六)、(七)项规定的材料。

第十三条 设立网络出版服务单位的申请者应自收到批准决定之日起 30 日内办理注册登记手续：

(一)持批准文件到所在地省、自治区、直辖市出版行政主管部门领取并填写《网络出版服务许可登记表》；

(二)省、自治区、直辖市出版行政主管部门对《网络出版服务许可登记表》审核无误后，在 10 日内向申请者发放《网络出版服务许可证》；

(三)《网络出版服务许可登记表》一式三份，由申请者和省、自治区、直辖市出版行政主管部门各存一份，另一份由省、自治区、直辖市出版行政主管部门

在 15 日内报送国家新闻出版广电总局备案。

第十四条 《网络出版服务许可证》有效期为 5 年。有效期届满，需继续从事网络出版服务活动的，应于有效期届满 60 日前按本规定第十一条的程序提出申请。出版行政主管部门应当在该许可有效期届满前作出是否准予延续的决定。批准的，换发《网络出版服务许可证》。

第十五条 网络出版服务经批准后，申请者应持批准文件、《网络出版服务许可证》到所在地省、自治区、直辖市电信主管部门办理相关手续。

第十六条 网络出版服务单位变更《网络出版服务许可证》许可登记事项、资本结构，合并或者分立，设立分支机构的，应依据本规定第十一条办理审批手续，并应持批准文件到所在地省、自治区、直辖市电信主管部门办理相关手续。

第十七条 网络出版服务单位中止网络出版服务的，应当向所在地省、自治区、直辖市出版行政主管部门备案， 并说明理由和期限；网络出版服务单位中止网络出版服务不得超过 180 日。

网络出版服务单位终止网络出版服务的，应当自终止网络出版服务之日起 30 日内，向所在地省、自治区、直辖市出版行政主管部门办理注销手续后到省、自治区、直辖市电信主管部门办理相关手续。省、自治区、直辖市出版行政主管部门将相关信息报国家新闻出版广电总局备案。

第十八条 网络出版服务单位自登记之日起满 180 日未开展网络出版服务的，由原登记的出版行政主管部门注销登记，并报国家新闻出版广电总局备案。同时，通报相关省、自治区、直辖市电信主管部门。

因不可抗力或者其他正当理由发生上述所列情形的，网络出版服务单位可以向原登记的出版行政主管部门申请延期。

第十九条 网络出版服务单位应当在其网站首页上标明出版行政主管部门核发的《网络出版服务许可证》编号。

互联网相关服务提供者在为网络出版服务单位提供人工干预搜索排名、广告、推广等服务时，应当查验服务对象的《网络出版服务许可证》及业务范围。

第二十条 网络出版服务单位应当按照批准的业务范围从事网络出版服务，不得超出批准的业务范围从事网络出版服务。

第二十一条 网络出版服务单位不得转借、出租、出卖《网络出版服务许可

证》或以任何形式转让网络出版服务许可。

网络出版服务单位允许其他网络信息服务提供者以其名义提供网络出版服务，属于前款所称禁止行为。

第二十二条 网络出版服务单位实行特殊管理股制度，具体办法由国家新闻出版广电总局另行制定。

第三章 网络出版服务管理

第二十三条 网络出版服务单位实行编辑责任制度，保障网络出版物内容合法。

网络出版服务单位实行出版物内容审核责任制度、责任编辑制度、责任校对制度等管理制度，保障网络出版物出版质量。

在网络上出版其他出版单位已在境内合法出版的作品且不改变原出版物内容的，须在网络出版物的相应页面显著标明原出版单位名称以及书号、刊号、网络出版物号或者网址信息。

第二十四条 网络出版物不得含有以下内容：

(一)反对宪法确定的基本原则的；

(二)危害国家统一、主权和领土完整的；

(三)泄露国家秘密、危害国家安全或者损害国家荣誉和利益的；

(四)煽动民族仇恨、民族歧视，破坏民族团结，或者侵害民族风俗、习惯的；

(五)宣扬邪教、迷信的；

(六)散布谣言，扰乱社会秩序，破坏社会稳定的；

(七)宣扬淫秽、色情、赌博、暴力或者教唆犯罪的；

(八)侮辱或者诽谤他人，侵害他人合法权益的；

(九)危害社会公德或者民族优秀文化传统的；

(十)有法律、行政法规和国家规定禁止的其他内容的。

第二十五条 为保护未成年人合法权益，网络出版物不得含有诱发未成年人模仿违反社会公德和违法犯罪行为的内容，不得含有恐怖、残酷等妨害未成年人身心健康的内容，不得含有披露未成年人个人隐私的内容。

第二十六条 网络出版服务单位出版涉及国家安全、社会安定等方面重大选题的内容，应当按照国家新闻出版广电总局有关重大选题备案管理的规定办理备

案手续。未经备案的重大选题内容，不得出版。

第二十七条　网络游戏上网出版前，必须向所在地省、自治区、直辖市出版行政主管部门提出申请，经审核同意后，报国家新闻出版广电总局审批。

第二十八条　网络出版物的内容不真实或不公正，致使公民、法人或者其他组织合法权益受到侵害的，相关网络出版服务单位应当停止侵权，公开更正，消除影响，并依法承担其他民事责任。

第二十九条　国家对网络出版物实行标识管理，具体办法由国家新闻出版广电总局另行制定。

第三十条　网络出版物必须符合国家的有关规定和标准要求，保证出版物质量。

网络出版物使用语言文字，必须符合国家法律规定和有关标准规范。

第三十一条　网络出版服务单位应当按照国家有关规定或技术标准，配备应用必要的设备和系统，建立健全各项管理制度，保障信息安全、内容合法，　并为出版行政主管部门依法履行监督管理职责提供技术支持。

第三十二条　网络出版服务单位在网络上提供境外出版物，应当取得著作权合法授权。其中，　出版境外著作权人授权的网络游戏，须按本规定第二十七条办理审批手续。

第三十三条　网络出版服务单位发现其出版的网络出版物含有本规定第二十四条、第二十五条所列内容的，　应当立即删除，保存有关记录，并向所在地县级以上出版行政主管部门报告。

第三十四条　网络出版服务单位应记录所出版作品的内容及其时间、网址或者域名，记录应当保存 60 日，并在国家有关部门依法查询时，予以提供。

第三十五条　网络出版服务单位须遵守国家统计规定，依法向出版行政主管部门报送统计资料。

第四章　监督管理

第三十六条　网络出版服务的监督管理实行属地管理原则。

各地出版行政主管部门应当加强对本行政区域内的网络出版服务单位及其出版活动的日常监督管理，履行下列职责：

(一)对网络出版服务单位进行行业监管，对网络出版服务单位违反本规定的

情况进行查处并报告上级出版行政主管部门；

(二)对网络出版服务进行监管，对违反本规定的行为进行查处并报告上级出版行政主管部门；

(三)对网络出版物内容和质量进行监管，定期组织内容审读和质量检查，并将结果向上级出版行政主管部门报告；

(四)对网络出版从业人员进行管理，定期组织岗位、业务培训和考核；

(五)配合上级出版行政主管部门、协调相关部门、指导下级出版行政主管部门开展工作。

第三十七条 出版行政主管部门应当加强监管队伍和机构建设，采取必要的技术手段对网络出版服务进行管理。出版行政主管部门依法履行监督检查等执法职责时，网络出版服务单位应当予以配合，不得拒绝、阻挠。

各省、自治区、直辖市出版行政主管部门应当定期将本行政区域内的网络出版服务监督管理情况向国家新闻出版广电总局提交书面报告。

第三十八条 网络出版服务单位实行年度核验制度，年度核验每年进行一次。省、自治区、直辖市出版行政主管部门负责对本行政区域内的网络出版服务单位实施年度核验并将有关情况报国家新闻出版广电总局备案。年度核验内容包括网络出版服务单位的设立条件、登记项目、出版经营情况、出版质量、遵守法律规范、内部管理情况等。

第三十九条 年度核验按照以下程序进行：

(一)网络出版服务单位提交年度自检报告，内容包括：本年度政策法律执行情况，奖惩情况，网站出版、管理、运营绩效情况，网络出版物目录，对年度核验期内的违法违规行为的整改情况，编辑出版人员培训管理情况等；并填写由国家新闻出版广电总局统一印制的《网络出版服务年度核验登记表》，与年度自检报告一并报所在地省、自治区、直辖市出版行政主管部门；

(二)省、自治区、直辖市出版行政主管部门对本行政区域内的网络出版服务单位的设立条件、登记项目、开展业务及执行法规等情况进行全面审核， 并在收到网络出版服务单位的年度自检报告和《网络出版服务年度核验登记表》等年度核验材料的 45 日内完成全面审核查验工作。对符合年度核验要求的网络出版服务单位予以登记，并在其《网络出版服务许可证》上加盖年度核验章；

(三)省、自治区、直辖市出版行政主管部门应于完成全面审核查验工作的 15 日内将年度核验情况及有关书面材料报国家新闻出版广电总局备案。

第四十条 有下列情形之一的，暂缓年度核验：

(一)正在停业整顿的；

(二)违反出版法规规章，应予处罚的；

(三)未按要求执行出版行政主管部门相关管理规定的；

(四)内部管理混乱，无正当理由未开展实质性网络出版服务活动的；

(五)存在侵犯著作权等其他违法嫌疑需要进一步核查的。

暂缓年度核验的期限由省、自治区、直辖市出版行政主管部门确定， 报国家新闻出版广电总局备案，最长不得超过 180 日。暂缓年度核验期间， 须停止网络出版服务。

暂缓核验期满，按本规定重新办理年度核验手续。

第四十一条 已经不具备本规定第八条、第九条规定条件的，责令限期改正；逾期仍未改正的，不予通过年度核验，由国家新闻出版广电总局撤销《网络出版服务许可证》，所在地省、自治区、直辖市出版行政主管部门注销登记，并通知当地电信主管部门依法处理。

第四十二条 省、自治区、直辖市出版行政主管部门可根据实际情况，对本行政区域内的年度核验事项进行调整，相关情况报国家新闻出版广电总局备案。

第四十三条 省、自治区、直辖市出版行政主管部门可以向社会公布年度核验结果。

第四十四条 从事网络出版服务的编辑出版等相关专业技术人员及其负责人应当符合国家关于编辑出版等相关专业技术人员职业资格管理的有关规定。

网络出版服务单位的法定代表人或主要负责人应按照有关规定参加出版行政主管部门组织的岗位培训，并取得国家新闻出版广电总局统一印制的《岗位培训合格证书》。未按规定参加岗位培训或培训后未取得《岗位培训合格证书》的，不得继续担任法定代表人或主要负责人。

第五章 保障与奖励

第四十五条 国家制定有关政策，保障、促进网络出版服务业的发展与繁荣。鼓励宣传科学真理、传播先进文化、倡导科学精神、塑造美好心灵、弘扬社会正

气等有助于形成先进网络文化的网络出版服务，推动健康文化、优秀文化产品的数字化、网络化传播。

网络出版服务单位依法从事网络出版服务，任何组织和个人不得干扰、阻止和破坏。

第四十六条 国家支持、鼓励下列优秀的、重点的网络出版物的出版：

(一)对阐述、传播宪法确定的基本原则有重大作用的；

(二)对弘扬社会主义核心价值观，进行爱国主义、集体主义、社会主义和民族团结教育以及弘扬社会公德、职业道德、家庭美德、个人品德有重要意义的；

(三)对弘扬民族优秀文化，促进国际文化交流有重大作用的；

(四)具有自主知识产权和优秀文化内涵的；

(五)对推进文化创新，及时反映国内外新的科学文化成果有重大贡献的；

(六)对促进公共文化服务有重大作用的；

(七)专门以未成年人为对象、内容健康的或者其他有利于未成年人健康成长的；

(八)其他具有重要思想价值、科学价值或者文化艺术价值的。

第四十七条 对为发展、繁荣网络出版服务业作出重要贡献的单位和个人，按照国家有关规定给予奖励。

第四十八条 国家保护网络出版物著作权人的合法权益。网络出版服务单位应当遵守《中华人民共和国著作权法》、《信息网络传播权保护条例》、《计算机软件保护条例》等著作权法律法规。

第四十九条 对非法干扰、阻止和破坏网络出版物出版的行为，出版行政主管部门及其他有关部门，应当及时采取措施，予以制止。

第六章 法律责任

第五十条 网络出版服务单位违反本规定的，出版行政主管部门可以采取下列行政措施：

(一)下达警示通知书；

(二)通报批评、责令改正；

(三)责令公开检讨；

(四)责令删除违法内容。

警示通知书由国家新闻出版广电总局制定统一格式，由出版行政主管部门下达给相关网络出版服务单位。

本条所列的行政措施可以并用。

第五十一条 未经批准，擅自从事网络出版服务，或者擅自上网出版网络游戏(含境外著作权人授权的网络游戏)，根据《出版管理条例》第六十一条、《互联网信息服务管理办法》第十九条的规定， 由出版行政主管部门、工商行政管理部门依照法定职权予以取缔，并由所在地省级电信主管部门依据有关部门的通知，按照《互联网信息服务管理办法》第十九条的规定给予责令关闭网站等处罚； 已经触犯刑法的，依法追究刑事责任；尚不够刑事处罚的，删除全部相关网络出版物，没收违法所得和从事违法出版活动的主要设备、专用工具， 违法经营额 1 万元以上的，并处违法经营额 5 倍以上 10 倍以下的罚款；违法经营额不足 1 万元的，可以处 5 万元以下的罚款；侵犯他人合法权益的，依法承担民事责任。

第五十二条 出版、传播含有本规定第二十四条、第二十五条禁止内容的网络出版物的，根据《出版管理条例》第六十二条、《互联网信息服务管理办法》第二十条的规定，由出版行政主管部门责令删除相关内容并限期改正，没收违法所得，违法经营额 1 万元以上的，并处违法经营额 5 倍以上 10 倍以下罚款；违法经营额不足 1 万元的，可以处 5 万元以下罚款；情节严重的，责令限期停业整顿或者由国家新闻出版广电总局吊销《网络出版服务许可证》，由电信主管部门依据出版行政主管部门的通知吊销其电信业务经营许可或者责令关闭网站；构成犯罪的，依法追究刑事责任。

为从事本条第一款行为的网络出版服务单位提供人工干预搜索排名、广告、推广等相关服务的，由出版行政主管部门责令其停止提供相关服务。

第五十三条 违反本规定第二十一条的，根据《出版管理条例》第六十六条的规定，由出版行政主管部门责令停止违法行为，给予警告，没收违法所得，违法经营额 1 万元以上的，并处违法经营额 5 倍以上 10 倍以下的罚款；违法经营额不足 1 万元的，可以处 5 万元以下的罚款；情节严重的，责令限期停业整顿或者由国家新闻出版广电总局吊销《网络出版服务许可证》。

第五十四条 有下列行为之一的，根据《出版管理条例》第六十七条的规定，由出版行政主管部门责令改正，给予警告；情节严重的，责令限期停业整顿或者

由国家新闻出版广电总局吊销《网络出版服务许可证》：

(一)网络出版服务单位变更《网络出版服务许可证》登记事项、资本结构，超出批准的服务范围从事网络出版服务，合并或者分立，设立分支机构，未依据本规定办理审批手续的；

(二)网络出版服务单位未按规定出版涉及重大选题出版物的；

(三)网络出版服务单位擅自中止网络出版服务超过 180 日的；

(四)网络出版物质量不符合有关规定和标准的。

第五十五条 违反本规定第三十四条的，根据《互联网信息服务管理办法》第二十一条的规定，由省级电信主管部门责令改正；情节严重的，责令停业整顿或者暂时关闭网站。

第五十六条 网络出版服务单位未依法向出版行政主管部门报送统计资料的，依据《新闻出版统计管理办法》处罚。

第五十七条 网络出版服务单位违反本规定第二章规定，以欺骗或者贿赂等不正当手段取得许可的，由国家新闻出版广电总局撤销其相应许可。

第五十八条 有下列行为之一的，由出版行政主管部门责令改正，予以警告，并处 3 万元以下罚款：

(一)违反本规定第十条，擅自与境内外中外合资经营、中外合作经营和外资经营的企业进行涉及网络出版服务业务的合作的；

(二)违反本规定第十九条，未标明有关许可信息或者未核验有关网站的《网络出版服务许可证》的；

(三)违反本规定第二十三条，未按规定实行编辑责任制度等管理制度的；

(四)违反本规定第三十一条，未按规定或标准配备应用有关系统、设备或未健全有关管理制度的；

(五)未按本规定要求参加年度核验的；

(六)违反本规定第四十四条，网络出版服务单位的法定代表人或主要负责人未取得《岗位培训合格证书》的；

(七)违反出版行政主管部门关于网络出版其他管理规定的。

第五十九条 网络出版服务单位违反本规定被处以吊销许可证行政处罚的，其法定代表人或者主要负责人自许可证被吊销之日起 10 年内不得担任网络出版

服务单位的法定代表人或者主要负责人。

从事网络出版服务的编辑出版等相关专业技术人员及其负责人违反本规定，情节严重的，由原发证机关吊销其资格证书。

第七章 附 则

第六十条 本规定所称出版物内容审核责任制度、责任编辑制度、责任校对制度等管理制度，参照《图书质量保障体系》的有关规定执行。

第六十一条 本规定自 2016 年 3 月 10 日起施行。原国家新闻出版总署、信息产业部 2002 年 6 月 27 日颁布的《互联网出版管理暂行规定》同时废止。

在线旅游经营服务管理暂行规定

中华人民共和国文化和旅游部令第 4 号

《在线旅游经营服务管理暂行规定》已经 2020 年 7 月 20 日文化和旅游部部务会议审议通过，现予发布，自 2020 年 10 月 1 日起施行。

部长 胡和平

2020 年 8 月 20 日

在线旅游经营服务管理暂行规定

第一章 总 则

第一条 为保障旅游者合法权益，规范在线旅游市场秩序，促进在线旅游行业可持续发展，依据《中华人民共和国旅游法》《中华人民共和国消费者权益保护法》《中华人民共和国网络安全法》《中华人民共和国电子商务法》《旅行社条例》等相关法律、行政法规，制定本规定。

第二条 在中华人民共和国境内提供在线旅游经营服务，适用本规定。

本规定所称在线旅游经营服务，是指通过互联网等信息网络为旅游者提供包价旅游服务或者交通、住宿、餐饮、游览、娱乐等单项旅游服务的经营活动。

第三条 本规定所称在线旅游经营者，是指从事在线旅游经营服务的自然人、法人和非法人组织，包括在线旅游平台经营者、平台内经营者以及通过自建网站、其他网络服务提供旅游服务的经营者。

本规定所称平台经营者，是指为在线旅游经营服务交易双方或者多方提供网络经营场所、交易撮合、信息发布等服务的法人或者非法人组织。

本规定所称平台内经营者，是指通过平台经营者提供旅游服务的在线旅游经

营者。

第四条 在线旅游经营者提供在线旅游经营服务，应当遵守社会主义核心价值观的要求，坚守人身财产安全、信息内容安全、网络安全等底线，诚信经营、公平竞争，承担产品和服务质量责任，接受政府和社会的监督。

第五条 文化和旅游部按照职责依法负责全国在线旅游经营服务的指导、协调、监管工作。县级以上地方文化和旅游主管部门按照职责分工负责本辖区内在线旅游经营服务的监督管理工作。

第六条 各级文化和旅游主管部门应当积极协调相关部门在财政、税收、金融、保险等方面支持在线旅游行业发展，保障在线旅游经营者公平参与市场竞争，充分发挥在线旅游经营者在旅游目的地推广、旅游公共服务体系建设、旅游大数据应用、景区门票预约和流量控制等方面的积极作用，推动旅游业高质量发展。

第二章 运 营

第七条 在线旅游经营者应当依法建立旅游者安全保护制度，制定应急预案，结合有关政府部门发布的安全风险提示等信息进行风险监测和安全评估，及时排查安全隐患，做好旅游安全宣传与引导、风险提示与防范、应急救助与处置等工作。

第八条 在线旅游经营者发现法律、行政法规禁止发布或者传输的信息，应当立即停止传输该信息，采取消除等处置措施防止信息扩散，保存有关记录并向主管部门报告。

平台经营者应当对上传至平台的文字、图片、音视频等信息内容加强审核，确保平台信息内容安全。

第九条 在线旅游经营者应当按照《中华人民共和国网络安全法》等相关法律规定，贯彻网络安全等级保护制度，落实网络安全管理和技术措施，制定网络安全应急预案，并定期组织开展演练，确保在线旅游经营服务正常开展。

第十条 在线旅游经营者经营旅行社业务的，应当依法取得旅行社业务经营许可。

第十一条 平台经营者应当对平台内经营者的身份、地址、联系方式、行政许可、质量标准等级、信用等级等信息进行真实性核验、登记，建立登记档案，并定期核验更新。

平台经营者应当督促平台内经营者对其旅游辅助服务者的相关信息进行真实性核验、登记。

第十二条 在线旅游经营者应当提供真实、准确的旅游服务信息，不得进行虚假宣传；未取得质量标准、信用等级的， 不得使用相关称谓和标识。平台经营者应当以显著方式区分标记自营业务和平台内经营者开展的业务。

在线旅游经营者为旅游者提供交通、住宿、游览等预订服务的， 应当建立公开、透明、可查询的预订渠道，促成相关预订服务依约履行。

第十三条 在线旅游经营者应当保障旅游者的正当评价权，不得擅自屏蔽、删除旅游者对其产品和服务的评价，不得误导、引诱、替代或者强制旅游者做出评价，对旅游者做出的评价应当保存并向社会公开。在线旅游经营者删除法律、法规禁止发布或者传输的评价信息的，应当在后台记录和保存。

第十四条 在线旅游经营者应当保护旅游者个人信息等数据安全，在收集旅游者信息时事先明示收集旅游者个人信息的目的、方式和范围，并经旅游者同意。

在线旅游经营者在签订包价旅游合同或者出境旅游产品代订合同时， 应当提示旅游者提供紧急联络人信息。

第十五条 在线旅游经营者不得滥用大数据分析等技术手段，基于旅游者消费记录、旅游偏好等设置不公平的交易条件，侵犯旅游者合法权益。

第十六条 在线旅游经营者为旅游者提供包价旅游服务的，应当依法与旅游者签订合同，并在全国旅游监管服务平台填报合同有关信息。

第十七条 经营旅行社业务的在线旅游经营者应当投保旅行社责任险。

在线旅游经营者应当提示旅游者投保人身意外伤害保险。销售出境旅游产品时，应当为有购买境外旅游目的地保险需求的旅游者提供必要协助。

第十八条 在线旅游经营者应当协助文化和旅游主管部门对不合理低价游进行管理，不得为其提供交易机会。

第十九条 平台经营者应当对平台内经营者服务情况、旅游合同履行情况以及投诉处理情况等产品和服务信息、交易信息依法进行记录、保存， 进行动态管理。

第二十条 社交网络平台、移动应用商店等信息网络提供者知道或者应当知道他人利用其服务从事违法违规在线旅游经营服务，或者侵害旅游者合法权益的，

应当采取删除、屏蔽、断开链接等必要措施。

第二十一条 平台经营者应当在首页显著位置公示全国旅游投诉渠道。

平台内经营者与旅游者发生旅游纠纷的，平台经营者应当积极协助旅游者维护合法权益。鼓励平台经营者先行赔付。

第二十二条 平台经营者发现以下情况，应当立即采取必要的救助和处置措施，并依法及时向县级以上文化和旅游主管部门报告：

(一)提供的旅游产品或者服务存在缺陷，危及旅游者人身、财产安全的；

(二)经营服务过程中发生突发事件或者旅游安全事故的；

(三)平台内经营者未经许可经营旅行社业务的；

(四)出现法律、法规禁止交易的产品或者服务的；

(五)其他应当报告的事项。

第三章 监督检查

第二十三条 各级文化和旅游主管部门应当建立日常检查、定期检查以及与相关部门联合检查的监督管理制度，依法对在线旅游经营服务实施监督检查，查处违法违规行为。

在监督检查过程中，县级以上文化和旅游主管部门要求在线旅游经营者提供相关数据信息的，在线旅游经营者应当予以配合。县级以上文化和旅游主管部门应当采取必要措施保护数据信息的安全。

第二十四条 县级以上文化和旅游主管部门对有不诚信经营、侵害旅游者评价权、滥用技术手段设置不公平交易条件等违法违规经营行为的在线旅游经营者，可以通过约谈等行政指导方式予以提醒、警示、制止，并责令其限期整改。

第二十五条 在线旅游经营服务违法行为由实施违法行为的经营者住所地县级以上文化和旅游主管部门管辖。不能确定经营者住所地的， 由经营者注册登记地或者备案地、旅游合同履行地县级以上文化和旅游主管部门管辖。

受理在线旅游经营服务相关投诉，参照前款处理。

第二十六条 县级以上文化和旅游主管部门依法建立在线旅游行业信用档案，将在线旅游经营者市场主体登记、行政许可、抽查检查、列入经营异常名录或者严重违法失信企业名单、行政处罚等信息依法列入信用记录， 适时通过全国旅游监管服务平台或者本部门官方网站公示，并与相关部门建立信用档案信息共享机

制，依法对严重违法失信者实施联合惩戒措施。

第二十七条 支持在线旅游经营者成立行业组织，并按照本组织章程依法制定行业经营规范和服务标准，加强行业自律，推动行业诚信建设和服务质量评价，监督、引导本行业经营者公平参与市场竞争。

第四章 法律责任

第二十八条 平台经营者知道或者应当知道平台内经营者不符合保障旅游者人身、财产安全要求或者有其他侵害旅游者合法权益行为， 未及时采取必要措施的，依法与该平台内经营者承担连带责任。

平台经营者未对平台内经营者资质进行审核，或者未对旅游者尽到安全提示或保障义务，造成旅游者合法权益损害的，依法承担相应责任。

第二十九条 旅游者有下列情形之一的，依法承担相关责任：

(一)在旅游活动中从事违法违规活动的；

(二)未按要求提供与旅游活动相关的个人健康信息的；

(三)不听从在线旅游经营者的告知、警示，参加不适合自身条件的旅游活动，导致出现人身财产损害的；

(四)对国家应对重大突发事件暂时限制旅游活动的措施、安全防范和应急处置措施不予配合的。

第三十条 因不可抗力或者第三人造成旅游者损害的，在线旅游经营者应当及时进行救助。在线旅游经营者未及时进行救助造成旅游者损害的， 依法承担相应责任。旅游者接受救助后，依法支付应当由个人承担的费用。

第三十一条 在线旅游经营者违反本规定第八条第一款规定， 由县级以上文化和旅游主管部门依照《中华人民共和国网络安全法》第六十八条有关规定处理。

第三十二条 在线旅游经营者违反本规定第十条规定，未依法取得旅行社业务经营许可开展相关业务的，由县级以上文化和旅游主管部门依照《中华人民共和国旅游法》第九十五条的规定处理。

在线旅游经营者违反本规定第十七条第一款规定，未依法投保旅行社责任保险的，由县级以上文化和旅游主管部门依照《中华人民共和国旅游法》第九十七条有关规定处理。

第三十三条 平台经营者有下列情形之一的， 由县级以上文化和旅游主管部

门依照《中华人民共和国电子商务法》第八十条的规定处理：

(一)违反本规定第十一条第一款规定，不依法履行核验、登记义务的；

(二)违反本规定第二十二条规定，不依法对违法情形采取必要处置措施或者未报告的；

(三)违反本规定第十九条规定，不依法履行商品和服务信息、交易信息保存义务的。

第三十四条 在线旅游经营者违反本规定第十二条第一款有关规定，未取得质量标准、信用等级使用相关称谓和标识的， 由县级以上文化和旅游主管部门责令改正，给予警告，可并处三万元以下罚款。

第三十五条 违反本规定第十六条规定，未在全国旅游监管服务平台填报包价旅游合同有关信息的，由县级以上文化和旅游主管部门责令改正，给予警告；拒不改正的，处一万元以下罚款。

第三十六条 在线旅游经营者违反本规定第十八条规定，为以不合理低价组织的旅游活动提供交易机会的，由县级以上文化和旅游主管部门责令改正，给予警告，可并处三万元以下罚款。

第三十七条 法律、行政法规对违反本规定行为另有规定的，依照其规定。县级以上地方文化和旅游主管部门在监督检查过程中发现在线旅游经营者有违反《中华人民共和国电子商务法》《中华人民共和国消费者权益保护法》《中华人民共和国网络安全法》等法律、行政法规、部门规章的行为， 不属于本部门管辖的，应当及时将相关线索依法移送有关部门。

第五章 附 则

第三十八条 本规定自 2020 年 10 月 1 日起施行。

人类遗传资源管理条例实施细则

中华人民共和国科学技术部令第 21 号

《人类遗传资源管理条例实施细则》已经 2023 年 5 月 11 日科技部第 3 次部务会审议通过，现予公布，自 2023 年 7 月 1 日起施行。

部长 王志刚

2023 年 5 月 26 日

人类遗传资源管理条例实施细则

第一章 总 则

第一条 为有效保护和合理利用我国人类遗传资源，维护公众健康、国家安全和社会公共利益，根据《中华人民共和国生物安全法》《中华人民共和国人类遗传资源管理条例》（以下称《条例》）等有关法律、行政法规，制定本实施细则。

第二条 采集、保藏、利用、对外提供我国人类遗传资源，应当遵守本实施细则。

《条例》第二条所称人类遗传资源信息包括利用人类遗传资源材料产生的人类基因、基因组数据等信息资料。

前款所称人类遗传资源信息不包括临床数据、影像数据、蛋白质数据和代谢数据。

第三条 科学技术部（以下称科技部）负责全国人类遗传资源调查、行政许可、监督检查、行政处罚等管理工作。

科技部根据需要依法委托相关组织，开展人类遗传资源行政许可申请材料的形式审查、技术评审，以及人类遗传资源备案、事先报告、监督检查、行政处罚等工作。

第四条 省、自治区、直辖市科学技术厅（委、局）、新疆生产建设兵团科学技术局（以下称省级科技行政部门）负责本区域下列人类遗传资源管理工作：

（一）人类遗传资源监督检查与日常管理；

（二）职权范围内的人类遗传资源违法案件调查处理；

（三）根据科技部委托，开展本区域人类遗传资源调查、人类遗传资源行政许可、人类遗传资源违法案件调查处理等工作。

第五条 科技部和省级科技行政部门应当加强人类遗传资源监管力量，配备行政执法人员，依职权对人类遗传资源活动开展监督检查等工作，依法履行人类遗传资源监督管理职责。

第六条 科技部聘请生命科学与技术、医药、卫生、伦理、法律、信息安全等方面的专家组成人类遗传资源管理专家咨询委员会，为全国人类遗传资源管理工作提供决策咨询和技术支撑。

第七条 科技部支持合理利用人类遗传资源开展科学研究、发展生物医药产

业、提高诊疗技术，加强人类遗传资源管理与监督，优化审批服务，提高审批效率，推进审批规范化和信息公开，提升管理和服务水平。

第二章 总体要求

第八条 采集、保藏、利用、对外提供我国人类遗传资源，应当符合伦理原则，通过已在有关管理部门备案的伦理(审查)委员会的伦理审查。开展伦理审查应当遵守法律、行政法规和国家有关规定。

第九条 采集、保藏、利用、对外提供我国人类遗传资源，应当尊重和保障人类遗传资源提供者的隐私权和个人信息等权益，按规定获取书面知情同意，确保人类遗传资源提供者的合法权益不受侵害。

第十条 采集、保藏、利用、对外提供我国人类遗传资源，应当遵守科技活动的相关要求及技术规范，包括但不限于标准、规范、规程等。

第十一条 在我国境内采集、保藏我国人类遗传资源或者向境外提供我国人类遗传资源，必须由我国科研机构、高等学校、医疗机构或者企业(以下称中方单位)开展。设在港澳的内资实控机构视为中方单位。

境外组织及境外组织、个人设立或者实际控制的机构(以下称外方单位)以及境外个人不得在我国境内采集、保藏我国人类遗传资源，不得向境外提供我国人类遗传资源。

第十二条 本实施细则第十一条所称境外组织、个人设立或者实际控制的机构，包括下列情形：

(一)境外组织、个人持有或者间接持有机构百分之五十以上的股份、股权、表决权、财产份额或者其他类似权益；

(二)境外组织、个人持有或者间接持有机构的股份、股权、表决权、财产份额或者其他类似权益不足百分之五十，但其所享有的表决权或者其他权益足以对机构的决策、管理等行为进行支配或者施加重大影响；

(三)境外组织、个人通过投资关系、协议或者其他安排，足以对机构的决策、管理等行为进行支配或者施加重大影响；

(四)法律、行政法规、规章规定的其他情形。

第十三条 采集、保藏、利用、对外提供我国人类遗传资源的单位应当加强管理制度建设，对涉及人类遗传资源开展科学研究的目的和研究方案等事项进

行审查，确保人类遗传资源合法使用。

第十四条 利用我国人类遗传资源开展国际科学研究合作，应当保证中方单位及其研究人员全过程、实质性地参与研究，依法分享相关权益。国际科学研究合作过程中，利用我国人类遗传资源产生的所有记录以及数据信息等应当完全向中方单位开放，并向中方单位提供备份。

第十五条 科技部加强人类遗传资源管理信息化建设，建立公开统一的人类遗传资源行政许可、备案与安全审查工作信息系统平台，为申请人通过互联网办理行政许可、备案等事项提供便利，推进实时动态管理，实现人类遗传资源管理信息可追溯、可查询。

第十六条 科技部会同国务院有关部门及省级科技行政部门推动我国科研机构、高等学校、医疗机构和企业依法依规开展人类遗传资源保藏工作，推进标准化、规范化的人类遗传资源保藏基础平台和大数据建设，并依照国家有关规定向有关科研机构、高等学校、医疗机构和企业开放。

第十七条 针对公共卫生事件等突发事件，科技部建立快速审批机制，对突发事件应急处置中涉及的人类遗传资源行政许可申请，应当加快办理。

对实施快速审批的人类遗传资源行政许可申请，科技部按照统一指挥、高效快速、科学审批的原则，加快组织开展行政许可申请的受理、评审、审查等工作。快速审批的情形、程序、时限、要求等事项由科技部另行规定。

第十八条 科技部制定并及时发布采集、保藏、利用、对外提供我国人类遗传资源行政许可、备案等服务指南和示范文本，为申请人办理人类遗传资源行政许可、备案等事项提供便捷和专业的指导和服务。

第十九条 科技部定期对从事人类遗传资源采集、保藏、利用、对外提供等活动的科研人员和相关部门管理人员进行培训，增强法律意识和责任意识，提升管理服务能力。

第二十条 科技部和省级科技行政部门应当建立并不断完善廉政风险防控措施，健全监督制约机制，加强对本机关人类遗传资源管理重要环节和关键岗位的监督。

第三章 调查与登记

第二十一条 科技部负责组织开展全国人类遗传资源调查工作。省级科技行

政部门受科技部委托，负责开展本区域人类遗传资源调查工作。

第二十二条 全国人类遗传资源调查每五年开展一次，必要时可以根据实际需要开展。

第二十三条 科技部组织相关领域专家制定全国人类遗传资源调查工作方案。省级科技行政部门完成本区域人类遗传资源调查工作后，应当将取得的调查数据、信息及时汇总并报送科技部。

第二十四条 科技部在全国人类遗传资源调查等工作基础上，组织开展重要遗传家系和特定地区人类遗传资源研究，逐步建立我国重要遗传家系和特定地区人类遗传资源清单目录，并适时修订完善。

第二十五条 科技部负责重要遗传家系和特定地区人类遗传资源登记工作，制定申报登记管理办法，建立申报登记管理信息服务平台。

第二十六条 我国科研机构、高等学校、医疗机构、企业发现重要遗传家系和特定地区人类遗传资源，应当及时通过申报登记管理信息服务平台进行申报。

第四章 行政许可与备案

第一节 采集、保藏行政许可

第二十七条 人类遗传资源采集行政许可适用于拟在我国境内开展的下列活动：

(一)重要遗传家系人类遗传资源采集活动。重要遗传家系是指患有遗传性疾病、具有遗传性特殊体质或者生理特征的有血缘关系的群体，且该群体中患有遗传性疾病、具有遗传性特殊体质或者生理特征的成员涉及三代或者三代以上，高血压、糖尿病、红绿色盲、血友病等常见疾病不在此列。首次发现的重要遗传家系应当按照本实施细则第二十六条规定及时进行申报。

(二)特定地区人类遗传资源采集活动。特定地区人类遗传资源是指在隔离或者特殊环境下长期生活，并具有特殊体质特征或者在生理特征方面有适应性性状发生的人类遗传资源。特定地区不以是否为少数民族聚居区为划分依据。

(三)用于大规模人群研究且人数大于 3000 例的人类遗传资源采集活动。大规模人群研究包括但不限于队列研究、横断面研究、临床研究、体质学研究等。为取得相关药品和医疗器械在我国上市许可的临床试验涉及的人类遗传资

源采集活动不在此列，无需申请人类遗传资源采集行政许可。

第二十八条 人类遗传资源保藏行政许可适用于在我国境内开展人类遗传资源保藏、为科学研究提供基础平台的活动。

人类遗传资源保藏活动是指将有合法来源的人类遗传资源保存在适宜环境条件下，保证其质量和安全，用于未来科学研究的行为，不包括以教学为目的、在实验室检测后按照法律法规要求或者临床研究方案约定的临时存储行为。

第二十九条 应当申请行政许可的人类遗传资源保藏活动同时涉及人类遗传资源采集的，申请人仅需要申请人类遗传资源保藏行政许可，无需另行申请人类遗传资源采集行政许可。

第三十条 人类遗传资源保藏单位应当依据《条例》第十五条规定，于每年1月31日前向科技部提交上一年度本单位保藏人类遗传资源情况年度报告。年度报告应当载明下列内容：

(一)保藏的人类遗传资源情况；

(二)人类遗传资源来源信息和使用信息；

(三)人类遗传资源保藏相关管理制度的执行情况；

(四)本单位用于保藏人类遗传资源的场所、设施、设备的维护和变动情况；

(五)本单位负责保藏工作的主要管理人员变动情况。

人类遗传资源保藏单位应当加强管理，确保保藏的人类遗传资源来源合法。科技部组织各省级科技行政部门每年对本区域人类遗传资源保藏单位的保藏活动进行抽查。

第二节 国际合作行政许可与备案

第三十一条 申请人类遗传资源国际科学研究合作行政许可，应当通过合作双方各自所在国(地区)的伦理审查。外方单位确无法提供所在国(地区)伦理审查证明材料的，可以提交外方单位认可中方单位伦理审查意见的证明材料。

第三十二条 为取得相关药品和医疗器械在我国上市许可，在临床医疗卫生机构利用我国人类遗传资源开展国际合作临床试验、不涉及人类遗传资源材料出境的，不需要批准，但应当符合下列情况之一，并在开展临床试验前将拟使

用的人类遗传资源种类、数量及其用途向科技部备案：

(一)涉及的人类遗传资源采集、检测、分析和剩余人类遗传资源材料处理等在临床医疗卫生机构内进行；

(二)涉及的人类遗传资源在临床医疗卫生机构内采集，并由相关药品和医疗器械上市许可临床试验方案指定的境内单位进行检测、分析和剩余样本处理。

前款所称临床医疗卫生机构是指在我国相关部门备案，依法开展临床试验的医疗机构、疾病预防控制机构等。

为取得相关药品和医疗器械在我国上市许可的临床试验涉及的探索性研究部分，应当申请人类遗传资源国际科学研究合作行政许可。

第三十三条 国际科学研究合作行政许可、国际合作临床试验备案应当由中方单位和外方单位共同申请。合作各方应当对申请材料信息的真实性、准确性、完整性作出承诺。

拟开展的人类遗传资源国际科学研究合作、国际合作临床试验涉及多中心临床研究的，不得拆分后申请行政许可或者备案。

第三十四条 开展多中心临床研究的，组长单位通过伦理审查后即可由申办方或者组长单位申请行政许可或者备案。

申办方或者组长单位取得行政许可或者完成备案后，参与临床研究的医疗卫生机构将本单位伦理审查批件或者认可组长单位所提供伦理审查批件的证明材料以及本单位出具的承诺书提交科技部，即可开展国际合作临床研究。

第三十五条 取得国际科学研究合作行政许可或者完成国际合作临床试验备案的合作双方，应当在行政许可或者备案有效期限届满后六个月内，共同向科技部提交合作研究情况报告。合作研究情况报告应当载明下列内容：

(一)研究目的、内容等事项变化情况；

(二)研究方案执行情况；

(三)研究内容完成情况；

(四)我国人类遗传资源使用、处置情况；

(五)研究过程中的所有记录以及数据信息的记录、储存、使用等情况；

(六)中方单位及其研究人员全过程、实质性参与研究情况以及外方单位参

与研究情况；

(七)研究成果产出、归属与权益分配情况；

(八)研究涉及的伦理审查情况。

第三节 对外提供、开放使用事先报告

第三十六条 将人类遗传资源信息向境外组织、个人及其设立或者实际控制的机构提供或者开放使用的，中方信息所有者应当向科技部事先报告并提交信息备份。向科技部事先报告应当报送下列事项信息：

(一)向境外组织、个人及其设立或者实际控制的机构提供或者开放使用我国人类遗传资源信息的目的、用途；

(二)向境外组织、个人及其设立或者实际控制的机构提供或者开放使用我国人类遗传资源信息及信息备份情况；

(三)接收人类遗传资源信息的境外组织、个人及其设立或者实际控制的机构的基本情况；

(四)向境外组织、个人及其设立或者实际控制的机构提供或者开放使用对我国人类遗传资源保护的潜在风险评估情况。

已取得行政许可的国际科学研究合作或者已完成备案的国际合作临床试验实施过程中，中方单位向外方单位提供合作产生的人类遗传资源信息的，如国际合作协议中已约定由合作双方使用，不需要单独事先报告和提交信息备份。

第三十七条 将人类遗传资源信息向境外组织、个人及其设立或者实际控制的机构提供或者开放使用，可能影响我国公众健康、国家安全和社会公共利益的，应当通过科技部组织的安全审查。

应当进行安全审查的情形包括：

(一)重要遗传家系的人类遗传资源信息；

(二)特定地区的人类遗传资源信息；

(三)人数大于 500 例的外显子组测序、基因组测序信息资源；

(四)可能影响我国公众健康、国家安全和社会公共利益的其他情形。

第三十八条 科技部会同相关部门制定安全审查规则，组织相关领域专家进行安全评估，并根据安全评估意见作出审查决定。

人类遗传资源出口过程中如相关物项涉及出口管制范围，须遵守国家出口

管制法律法规。

第四节 行政许可、备案与事先报告流程

第三十九条 申请人的申请材料齐全、形式符合规定的，科技部应当受理并出具加盖专用印章和注明日期的纸质或者电子凭证。

申请材料不齐全或者不符合法定形式的，科技部应当在收到正式申请材料之日起五个工作日内一次性告知申请人需要补正的全部内容。

第四十条 科技部根据技术评审和安全审查工作需要，组建专家库并建立专家管理制度。

科技部按照随机抽取方式从专家库中选取评审专家，对人类遗传资源行政许可申请事项进行技术评审，对应当进行安全审查的人类遗传资源信息对外提供或者开放使用事项进行安全评估。技术评审意见、安全评估意见作为作出行政许可决定或者安全审查决定的参考依据。

专家参与技术评审和安全审查一般采用网络方式，必要时可以采用会议、现场勘查等方式。

第四十一条 科技部应当自受理之日起二十个工作日内，对人类遗传资源行政许可申请作出行政许可决定。二十个工作日内不能作出行政许可决定的，经科技部负责人批准，可以延长十个工作日，并将延长期限的理由告知申请人。

第四十二条 科技部作出行政许可决定，依法需要听证、检验、检测、检疫、鉴定、技术评审的，所需时间不计算在本实施细则第四十一条规定的期限内，但应当将所需时间书面告知申请人。

第四十三条 科技部作出行政许可决定后，应当将行政许可决定书面告知申请人，并抄送申请人所在地的省级科技行政部门。

依法作出准予行政许可决定的，应当在科技部网站予以公开。依法作出不予行政许可决定的，应当说明理由，并告知申请人享有依法申请行政复议或者提起行政诉讼的权利。

第四十四条 取得人类遗传资源采集行政许可后，采集活动参与单位、采集目的、采集方案或者采集内容等重大事项发生变更的，被许可人应当向科技部提出变更申请。

第四十五条 取得人类遗传资源保藏行政许可后，保藏目的、保藏方案或者

保藏内容等重大事项发生变更的，被许可人应当向科技部提出变更申请。

第四十六条 取得人类遗传资源国际科学研究合作行政许可后，开展国际科学研究合作过程中，研究目的、研究内容发生变更，研究方案涉及的人类遗传资源种类、数量、用途发生变更，或者申办方、组长单位、合同研究组织、第三方实验室等其他重大事项发生变更的，被许可人应当向科技部提出变更申请。

第四十七条 取得人类遗传资源国际科学研究合作行政许可后，出现下列情形的，被许可人不需要提出变更申请，但应当向科技部提交事项变更的书面说明及相应材料：

研究内容或者研究方案不变，仅涉及总量累计不超过获批数量 10%变更的；

本实施细则第四十六条所列合作单位以外的参与单位发生变更的；

合作方法人单位名称发生变更的；

研究内容或者研究方案发生变更，但不涉及人类遗传资源种类、数量、用途的变化或者变更后内容不超出已批准范围的。

第四十八条 被许可人对本实施细则第四十四条至第四十六条所列事项提出变更申请的，科技部应当审查并作出是否准予变更的决定。符合法定条件、标准的，科技部应当予以变更。

变更申请的受理、审查、办理期限、决定、告知等程序参照本实施细则第三十九条至第四十三条有关行政许可申请的规定执行。

第四十九条 行政许可决定作出前，申请人书面撤回申请的，科技部终止对行政许可申请的审查。

第五十条 有下列情形之一的，科技部根据利害关系人请求或者依据职权，可以撤销人类遗传资源行政许可：

(一)滥用职权、玩忽职守作出准予行政许可决定的；

(二)超越法定职权作出准予行政许可决定的；

(三)违反法定程序作出准予行政许可决定的；

(四)对不具备申请资格或者不符合法定条件的申请人准予行政许可的；

(五)依法可以撤销行政许可的其他情形。

被许可人以欺骗、贿赂等不正当手段取得行政许可的，科技部应当予以撤销。

依照前两款的规定撤销行政许可，可能对公共利益造成重大损害的，不予撤销。

第五十一条 申请国际合作临床试验备案的，应当事先取得药品监督管理部门临床试验批件、通知书或者备案登记材料。

第五十二条 申请国际合作临床试验备案，应当提交下列材料：

(一)合作各方基本情况；

(二)研究涉及使用的人类遗传资源种类、数量和用途；

(三)研究方案；

(四)组长单位伦理审查批件；

(五)其他证明材料。

第五十三条 国际合作临床试验完成备案后，涉及的人类遗传资源种类、数量、用途发生变更，或者合作方、研究方案、研究内容、研究目的等重大事项发生变更的，备案人应当及时办理备案变更。

研究方案或者研究内容变更不涉及人类遗传资源种类、数量、用途变化的，不需要办理备案变更，但应当在变更活动开始前向科技部提交事项变更的书面说明及相应材料。

第五十四条 向境外组织、个人及其设立或者实际控制的机构提供或者开放使用人类遗传资源信息向科技部事先报告后，用途、接收方等事项发生变更的，应当在变更事项实施前向科技部提交事项变更报告。

第五十五条 被许可人需要延续行政许可有效期的，应当在该行政许可有效期限届满三十个工作日前向科技部提出申请。科技部应当根据被许可人的申请，在该行政许可有效期限届满前作出是否准予延续的决定；逾期未作出决定的，视为准予延续。

备案人需要延续备案有效期的，应当在该备案有效期限届满三十个工作日前向科技部提出申请。科技部应当在该备案有效期限届满前完成延续备案；逾期未完成的，视为已完成延续备案。

第五章 监督检查

第五十六条 科技部负责全国人类遗传资源监督检查，各省级科技行政部门负责本区域人类遗传资源监督检查。监督检查事项主要包括：

(一)人类遗传资源采集、保藏、利用、对外提供有关单位落实主体责任，建立、完善和执行有关规章制度的情况；

(二)获批人类遗传资源项目的有关单位采集、保藏、利用人类遗传资源的情况，材料或者信息出境、对外提供、开放使用以及出境后使用情况；

(三)利用人类遗传资源的剩余材料处置、知识产权及利益分享等情况；

(四)人类遗传资源备案事项的真实性等情况；

(五)科技部或者省级科技行政部门认为需要监督检查的其他事项。

第五十七条 科技部和省级科技行政部门应当编制年度监督检查计划，实施人类遗传资源风险管理。

年度监督检查计划应当包括检查事项、检查方式、检查频次以及抽查项目种类、抽查比例等内容。

第五十八条 对近三年内因人类遗传资源违法行为被实施过行政处罚、存在人类遗传资源管理风险未及时改正，以及被记入相关失信惩戒名单的单位，科技部和省级科技行政部门应当加大监督检查频次，纳入年度日常监督检查计划并开展监督检查。对管理体系和管理规范明显改进、未再发生违法行为的单位，可以适时减少监督检查频次。

第五十九条 对本实施细则第五十八条规定以外的其他单位，科技部和省级科技行政部门可以在该单位人类遗传资源活动范围内随机确定监督检查事项，随机选派监督检查人员，实施监督检查。

第六十条 遇有严重违法行为或者临时性、突发性任务以及通过投诉举报、转办交办、数据监测等发现的问题，科技部和省级科技行政部门可以部署开展专项监督检查。

第六十一条 科技部和省级科技行政部门应当及时记录、汇总人类遗传资源活动日常监督检查信息，完善日常监督检查措施。

第六十二条 发现被监督检查对象可能存在违反《条例》有关规定的风险时，科技部或者省级科技行政部门可以对其法定代表人、主要负责人等进行行政约谈。

第六十三条 发现被监督检查对象可能存在违反《条例》规定的行为，科技部或者省级科技行政部门应当进行调查，必要时可以采取下列措施：

(一)依法采取记录、复制、拍照、录像等措施；

(二)依法采取查封、扣押等行政强制措施；

(三)依法对相关物品进行检测、检验、检疫或者鉴定。

第六十四条 科技部或者省级科技行政部门实施行政强制措施应当依照《中华人民共和国行政强制法》规定的程序进行。

第六十五条 科技部和省级科技行政部门采取或者解除行政强制措施，应当经本机关负责人批准。

依法实施查封、扣押强制措施的，应当制作并当场向当事人交付查封、扣押决定书和清单。情况紧急，不及时查封、扣押可能影响案件查处，或者存在可能导致人类遗传资源损毁灭失等隐患，可以先行实施查封、扣押，并在二十四小时内补办查封、扣押决定书，送达当事人。

第六章 行政处罚

第六十六条 科技部和省级科技行政部门应当规范行使人类遗传资源行政处罚裁量权，综合考虑违法行为的事实、性质、情节以及社会危害程度，在《条例》规定范围内合理确定行政处罚的种类和幅度，确保过罚相当，防止畸轻畸重。

人类遗传资源行政处罚裁量基准由科技部另行制定并向社会公布。

第六十七条 拟给予行政处罚的案件，科技部和省级科技行政部门在作出行政处罚决定之前，应当书面告知当事人拟作出的行政处罚内容及事实、理由、依据，并告知当事人依法享有陈述、申辩的权利。拟作出的行政处罚属于听证范围的，还应当告知当事人有要求听证的权利。

当事人行使陈述、申辩权或者要求听证的，应当自告知书送达之日起五个工作日内书面提出，逾期未提出的，视为放弃上述权利。

科技部和省级科技行政部门不得因当事人陈述、申辩或者听证而给予更重的处罚。

第六十八条 科技部或者省级科技行政部门拟作出下列行政处罚决定，当事人要求听证的，应当组织听证：

(一)对法人、其他组织处以一百万元以上罚款或者对公民处以十万元以上罚款的;

(二)没收法人、其他组织违法所得三百万元以上或者没收公民违法所得三十万元以上的;

(三)禁止一年以上从事采集、保藏、利用、对外提供我国人类遗传资源活动的;

(四)二年以上不受理人类遗传资源行政许可申请的;

(五)撤销已取得的人类遗传资源行政许可的;

(六)法律、行政法规规定应当组织听证的其他情形。

第六十九条 科技部或者省级科技行政部门作出人类遗传资源行政处罚决定前,本部门案件办理机构应当将拟作出的行政处罚决定及案件材料送本部门负责法制审核的工作机构进行法制审核。未经法制审核或者审核未通过的,不得作出决定。

拟作出的行政处罚决定仅涉及警告的,不需要进行法制审核。

第七十条 行政处罚决定书作出后,科技部或者省级科技行政部门应当在七个工作日内依照有关法律规定,将行政处罚决定书送达当事人或者其他的法定受送达人。

第七十一条 行政处罚决定应当自立案之日起九十日内作出。案情复杂,不能在九十日内作出行政处罚决定的,经本机关负责人批准,可以延长九十日。案情特别复杂,经延期仍不能作出行政处罚决定的,经本机关负责人集体讨论决定是否继续延期。决定延期的,应当同时确定延长的合理期限,但最长不得超过六十日。

案件办理过程中,听证、公告、检测、检验、检疫、鉴定、审计、中止等时间,不计入本条第一款所指的案件办理期限。

第七十二条 《条例》第三十六条、第三十九条、第四十一条、第四十二条、第四十三条规定的违法所得,以实施违法行为所获得的全部收入扣除适当的合理支出计算;难以计算的,以违法行为涉及的人类遗传资源价值计算或者为人类遗传资源投入的资金数额作为违法所得。

第七十三条 在人类遗传资源监督检查或者违法案件调查处理中,发现相关

公民、法人或者其他组织不具备人类遗传资源存储条件的，科技部或者省级科技行政部门应当组织将其存储的人类遗传资源转移至具备存储条件的单位临时存储。

第七十四条 省级科技行政部门依法作出人类遗传资源行政处罚的，应当自行政处罚决定作出之日起十五个工作日内将案件处理情况及行政处罚决定书副本报送科技部。

第七十五条 科技部有权对省级科技行政部门实施的人类遗传资源行政处罚进行监督，依法对有关违法或者不当行为责令改正。

第七章 附 则

第七十六条 本实施细则中涉及期限的规定，注明为工作日的，不包含法定节假日；未注明为工作日的，为自然日。

第七十七条 本实施细则所称“以上”“不超过”均包含本数，“大于”“不足”不包含本数。

第七十八条 本实施细则自 2023 年 7 月 1 日施行。

人力资源服务机构管理规定

(2023 年 6 月 29 日人力资源社会保障部令第 50 号公布 自 2023 年 8 月 1 日起施行)

第一章 总 则

第一条 为了加强对人力资源服务机构的管理，规范人力资源服务活动，健全统一开放、竞争有序的人力资源市场体系，促进高质量充分就业和优化人力资源流动配置，根据《中华人民共和国就业促进法》《人力资源市场暂行条例》等法律、行政法规，制定本规定。

第二条 在中华人民共和国境内的人力资源服务机构从事人力资源服务活动，适用本规定。

第三条 县级以上人力资源社会保障行政部门依法开展本行政区域内的人力资源服务机构管理工作。

第四条 人力资源社会保障行政部门应当加强人力资源服务标准化、信息化建设，指导人力资源服务行业协会加强行业自律。

第二章 行政许可和备案

第五条 经营性人力资源服务机构从事职业中介活动的，应当在市场主体登记办理完毕后，依法向住所地人力资源社会保障行政部门申请行政许可，取得人力资源服务许可证。从事网络招聘服务的，还应当依法取得电信业务经营许可证。

本规定所称职业中介活动是指为用人单位招用人员和劳动者求职提供中介服务，包括为用人单位推荐劳动者、为劳动者介绍用人单位、组织开展招聘会、开展网络招聘服务、开展高级人才寻访(猎头)服务等经营性活动。

第六条 申请从事职业中介活动的，应当具备下列条件：

(一)有明确的章程和管理制度；

(二)有开展业务必备的固定场所、办公设施和一定数额的开办资金；

(三)有 3 名以上专职工作人员；

(四)法律、法规规定的其他条件。

第七条 申请从事职业中介活动的，可以自愿选择按照一般程序或者告知承诺制方式申请行政许可。按照一般程序申请的，应当向住所地人力资源社会保障行政部门提交以下申请材料：

(一)从事职业中介活动的申请书；

(二)机构章程和管理制度；

(三)场所的所有权证明或者租赁合同；

(四)专职工作人员的基本情况表；

(五)法律、法规规定的其他材料。

前款规定的申请材料通过政务信息共享可以获得的，人力资源社会保障行政部门应当通过政务信息共享获取。提交申请材料不齐全的，人力资源社会保障行政部门应当当场一次性告知需要补正的全部材料。

按照告知承诺制方式申请的，只须提交从事职业中介活动的申请书和承诺书。申请人有较严重不良信用记录或者存在曾作出虚假承诺等情形的，在信用修复前不适用告知承诺制。

第八条 按照一般程序申请行政许可的，人力资源社会保障行政部门应当自收到申请之日起 20 日内依法作出行政许可决定。按照告知承诺制方式申请行政许可的，人力资源社会保障行政部门应当经形式审查后当场作出行政许可决

定。

符合条件，人力资源社会保障行政部门作出准予行政许可决定的，应当自作出决定之日起 10 日内向申请人颁发、送达人力资源服务许可证；不符合条件，人力资源社会保障行政部门作出不予行政许可书面决定的，应当说明理由，并告知申请人享有依法申请行政复议或者提起行政诉讼的权利。

第九条 经营性人力资源服务机构开展人力资源供求信息的收集和发布、就业和创业指导、人力资源管理咨询、人力资源测评、人力资源培训、人力资源服务外包等人力资源服务业务的，应当自开展业务之日起 15 日内向住所地人力资源社会保障行政部门备案，备案事项包括机构名称、法定代表人、住所地、服务范围等。

备案事项齐全的，人力资源社会保障行政部门应当予以备案，并出具备案凭证，载明备案事项、备案机关以及日期等；备案事项不齐全的，人力资源社会保障行政部门应当当场一次性告知需要补正的全部事项。

经营性人力资源服务机构开展劳务派遣、对外劳务合作业务的，执行国家有关劳务派遣、对外劳务合作的规定。

第十条 依法取得的人力资源服务许可证在全国范围内长期有效。

第十一条 人力资源服务许可证分为纸质证书(正、副本)和电子证书，具有同等法律效力。

人力资源服务许可证纸质证书样式、编号规则以及电子证书标准由人力资源社会保障部制定。

第十二条 经营性人力资源服务机构设立分支机构的，应当自市场主体登记办理完毕之日起 15 日内，书面报告分支机构住所地人力资源社会保障行政部门，书面报告事项包括机构名称、统一社会信用代码、许可证编号以及分支机构名称、负责人姓名、住所地、服务范围等。

人力资源社会保障行政部门收到书面报告后，应当出具收据，载明书面报告的名称、分支机构名称、页数以及收到时间等，并由经办人员签名或者盖章。

第十三条 经营性人力资源服务机构变更名称、住所、法定代表人或者终止经营活动的，应当自市场主体变更登记或者注销登记办理完毕之日起 15 日内，

书面报告住所地人力资源社会保障行政部门。人力资源社会保障行政部门应当及时换发或者收回人力资源服务许可证、备案凭证。

经营性人力资源服务机构跨管辖区域变更住所的，应当书面报告迁入地人力资源社会保障行政部门。迁出地人力资源社会保障行政部门应当及时移交经营性人力资源服务机构申请行政许可、办理备案的原始材料。

第十四条 人力资源社会保障行政部门应当公开申请行政许可和办理备案的材料目录、办事指南和咨询监督电话等信息，优化办理流程，推行当场办结、一次办结、限时办结等制度，实现集中办理、就近办理、网上办理，提升经营性人力资源服务机构申请行政许可、办理备案便利化程度。

人力资源社会保障行政部门应当及时向社会公布依法取得行政许可或者经过备案的经营性人力资源服务机构名单及其变更、注销等情况，并提供查询服务。

第三章 服务规范

第十五条 人力资源服务机构接受用人单位委托招聘人员的，发布招聘信息应当真实、合法，不得含有民族、种族、性别、宗教信仰等方面的歧视性内容。

人力资源服务机构不得违反国家规定，在户籍、地域、身份等方面设置限制人力资源流动的条件。

第十六条 人力资源服务机构接受用人单位委托招聘人员的，应当建立招聘信息管理制度，依法对用人单位所提供材料的真实性、合法性进行审查，并将相关审查材料存档备核。审查内容应当包括以下方面：

(一)用人单位招聘简章；

(二)用人单位营业执照或者有关部门批准设立的文件；

(三)经办人员的身份证件、用人单位的委托证明。

经办人员与用人单位的委托关系，人力资源服务机构可以依法通过企业银行结算账户等途径确认。

接受用人单位委托招聘外国人的，应当符合《外国人在中国就业管理规定》等法律、法规、规章的规定。

第十七条 人力资源服务机构不得有下列行为：

(一)伪造、涂改、转让人力资源服务许可证;

(二)为无合法证照的用人单位提供职业中介服务;

(三)介绍未满 16 周岁的未成年人就业;

(四)为无合法身份证件的劳动者提供职业中介服务;

(五)介绍劳动者从事法律、法规禁止从事的职业;

(六)介绍用人单位、劳动者从事违法活动;

(七)以欺诈、暴力、胁迫等方式开展相关服务活动;

(八)以开展相关服务为名牟取不正当利益;

(九)以欺诈、伪造证明材料等手段骗取社会保险基金支出、社会保险待遇;

(十)其他违反法律、法规规定的行为。

第十八条 人力资源服务机构对其发布的求职招聘信息,应当标注有效期限或者及时更新。

第十九条 人力资源服务机构接受委托或者自行组织开展人力资源培训的,不得危害国家安全、损害参训人员身心健康或者诱骗财物。

第二十条 人力资源服务机构举办现场招聘会,应当制定组织实施办法、应急预案和安全保卫工作方案,核实参加招聘会的招聘单位及其招聘简章的真实性、合法性,提前将招聘会信息向社会公布,并对招聘中的各项活动进行管理。

举办网络招聘会,除遵守前款规定外,还应当加强网络安全管理,履行网络安全保护义务,采取技术措施或者其他必要措施,确保网络招聘系统和用户信息安全。

举办大型现场招聘会,应当符合《大型群众性活动安全管理条例》等法律、法规的规定。

第二十一条 人力资源服务机构开展人力资源供求信息收集和发布的,应当建立健全信息发布审查和投诉处理机制,确保发布的人力资源供求信息真实、合法、有效,不得以人力资源供求信息收集和发布的名义开展职业中介活动。

人力资源服务机构在业务活动中收集用人单位信息的,不得泄露或者违法使用所知悉的商业秘密。

第二十二条 人力资源服务机构通过收集、存储、使用、加工、传输、提供、公开、删除等方式处理个人信息的，应当遵循合法、正当、必要和诚信原则，遵守法律、法规有关个人信息保护的规定。

人力资源服务机构收集个人信息应当限于劳动者本人基本信息以及与应聘岗位相关的知识、技能、工作经历等情况。

人力资源服务机构应当建立个人信息保护、个人信息安全监测预警等机制，不得泄露、篡改、损毁或者非法出售、非法向他人提供所收集的个人信息，并采取必要措施防范盗取个人信息等违法行为；应当对个人信息保护情况每年至少进行一次自查，记录自查情况，及时消除自查中发现的安全隐患。

第二十三条 人力资源服务机构因业务需要，确需向境外提供在中华人民共和国境内运营中收集和产生的个人信息和重要数据的，应当遵守有关法律、法规的规定。

第二十四条 人力资源服务机构应当建立和完善举报投诉处理机制，公布举报投诉方式，及时受理并处理有关举报投诉。

人力资源服务机构发现用人单位、与其合作的人力资源服务机构存在虚假招聘等违法活动的，应当保存有关记录，暂停或者终止提供有关服务，并向人力资源社会保障行政部门以及有关管理部门报告。

第二十五条 人力资源服务机构应当加强内部制度建设，健全财务管理制度，建立服务台账，如实记录服务对象、服务过程、服务结果等信息。服务台账应当保存 2 年以上。

以网络招聘服务平台方式从事网络招聘服务的人力资源服务机构应当记录、保存平台上发布的招聘信息、服务信息，并确保信息的完整性、保密性、可用性。招聘信息、服务信息应当自服务完成之日起保存 3 年以上。

第二十六条 经营性人力资源服务机构应当在服务场所明示营业执照、服务项目、收费标准、监督机关和监督电话等事项，并接受人力资源社会保障行政部门和市场监督管理、价格等主管部门的监督检查。

从事职业中介活动的，还应当在服务场所明示人力资源服务许可证。从事网络招聘服务的，应当依照《网络招聘服务管理规定》第十三条的规定公示相关信息。

第二十七条 经营性人力资源服务机构不得向个人收取明示服务项目以外的服务费用，不得以各种名目诱导、强迫个人参与贷款、入股、集资等活动。

经营性人力资源服务机构不得向个人收取押金，或者以担保等名义变相收取押金。

第二十八条 经营性人力资源服务机构接受用人单位委托，提供人力资源管理、开发、配置等人力资源服务外包的，不得有下列行为：

(一)以欺诈、胁迫、诱导劳动者注册为个体工商户等方式，改变用人单位与劳动者的劳动关系，帮助用人单位规避用工主体责任；

(二)以人力资源服务外包名义，实际上按劳务派遣，将劳动者派往其他单位工作；

(三)与用人单位串通侵害劳动者的合法权益。

第二十九条 经营性人力资源服务机构应当公平竞争，不得扰乱人力资源市场价格秩序，不得采取垄断、不正当竞争等手段开展服务活动。

第三十条 经营性人力资源服务机构提供公益性人力资源服务的，可以通过政府购买服务等方式给予支持。

第四章 监督管理

第三十一条 人力资源社会保障行政部门采取随机抽取检查对象、随机选派执法人员的方式和法律、法规规定的措施，对经营性人力资源服务机构实施监督检查。被检查单位应当配合监督检查，如实提供相关资料和信息，不得隐瞒、拒绝、阻碍。

人力资源社会保障行政部门应当将监督检查情况及时向社会公布。其中，行政处罚、监督检查结果可以通过国家企业信用信息公示系统或者其他途径向社会公示。

对按照告知承诺制方式取得人力资源服务许可证的，人力资源社会保障行政部门在实施监督检查时，应当重点对告知承诺事项真实性进行检查。

第三十二条 人力资源社会保障行政部门对经营性人力资源服务机构实施监督检查，按照“谁许可、谁监管，谁备案、谁监管”的原则，由作出行政许可决定或者办理备案的人力资源社会保障行政部门依法履行监督管理职责。

在作出行政许可决定、办理备案的人力资源社会保障行政部门管辖区域

外，或者未经行政许可、未备案，违法从事人力资源服务活动的，由违法行为发生地人力资源社会保障行政部门管辖。多个地方人力资源社会保障行政部门对违法行为均具有管辖权的，由最先立案的人力资源社会保障行政部门管辖；发生管辖争议的，由共同的上一级人力资源社会保障行政部门指定管辖。

上级人力资源社会保障行政部门根据工作需要，可以调查处理下级人力资源社会保障行政部门管辖的案件；对重大复杂案件，可以直接指定管辖。

第三十三条 人力资源社会保障行政部门应当加强对经营性人力资源服务机构的事中事后监管，建立监管风险分析研判、市场主体警示退出等新型监管机制。

人力资源社会保障行政部门负责人力资源服务领域行政许可、备案的机构和劳动保障监察机构，应当健全监督管理协作机制。

人力资源社会保障行政部门应当加强与市场监督管理、公安等部门的信息共享和协同配合，健全跨部门综合监管机制。

第三十四条 人力资源社会保障行政部门应当依法督促经营性人力资源服务机构在规定期限内提交上一年度的经营情况年度报告，并在政府网站进行不少于 30 日的信息公示或者引导经营性人力资源服务机构在其服务场所公示年度报告的有关内容。

人力资源社会保障行政部门通过与市场监督管理等部门信息共享可以获取的信息，不得要求经营性人力资源服务机构重复提供。

第三十五条 人力资源社会保障行政部门应当加强人力资源市场诚信体系建设，制定经营性人力资源服务机构信用评价制度，建立健全诚信典型树立和失信行为曝光机制，依法依规实施守信激励和失信惩戒。

第三十六条 人力资源社会保障行政部门应当畅通对经营性人力资源服务机构的举报投诉渠道，依法及时处理有关举报投诉。

第三十七条 有下列情形之一的，人力资源社会保障行政部门可以依法撤销行政许可：

(一)工作人员滥用职权、玩忽职守作出准予许可决定的；

(二)超越法定职权作出准予许可决定的；

(三)违反法定程序作出准予许可决定的；

(四)对不具备申请资格或者不符合申请条件的申请人作出准予许可决定的;

(五)依法可以撤销行政许可的其他情形。

被许可人通过欺骗、贿赂等不正当手段取得行政许可的，应当予以撤销。

人力资源社会保障行政部门发现存在第一款、第二款规定情形的，应当及时开展调查核实，情况属实的，依法撤销行政许可。相关经营性人力资源服务机构及其人员无法联系或者拒不配合的，人力资源社会保障行政部门可以将人力资源服务许可证编号、行政许可时间等通过政府网站向社会公示，公示期为45 日。公示期内没有提出异议的，人力资源社会保障行政部门可以作出撤销行政许可的决定。

第三十八条 有下列情形之一的，人力资源社会保障行政部门应当依法办理行政许可注销手续:

(一)经营性人力资源服务机构依法终止经营的;

(二)人力资源服务许可证被依法吊销或者行政许可依法被撤销的;

(三)因不可抗力导致行政许可事项无法实施的;

(四)法律、法规规定的应当注销行政许可的其他情形。

第五章 法律责任

第三十九条 违反本规定第五条第一款规定，未经许可擅自从事职业中介活动的，由人力资源社会保障行政部门依照《人力资源市场暂行条例》第四十二条第一款的规定处罚。

违反本规定第九条第一款规定，开展人力资源服务业务未备案，违反本规定第十二条、第十三条规定，设立分支机构、办理变更登记或者注销登记未书面报告的，由人力资源社会保障行政部门依照《人力资源市场暂行条例》第四十二条第二款的规定处罚。

第四十条 违反本规定第十五条第一款规定，发布的招聘信息不真实、不合法，违反本规定第二十一条的规定，未依法开展人力资源供求信息收集和发布的，由人力资源社会保障行政部门依照《人力资源市场暂行条例》第四十三条的规定处罚。

第四十一条 违反本规定第十七条第(一)(二)项规定，伪造、涂改、转让人

力资源服务许可证，为无合法证照的用人单位提供职业中介服务的，由人力资源社会保障行政部门依照《中华人民共和国就业促进法》第六十五条的规定处罚。

违反本规定第十七条第(三)项规定，介绍未满 16 周岁的未成年人就业的，依照国家禁止使用童工的规定处罚。

违反本规定第十七条第(四)(五)项规定，为无合法身份证件的劳动者提供职业中介服务，介绍劳动者从事法律、法规禁止从事的职业的，由人力资源社会保障行政部门责令改正，没有违法所得的，可处以 1 万元以下的罚款；有违法所得的，可处以不超过违法所得 3 倍的罚款，最高不得超过 3 万元；情节严重的，提请市场监督管理部门吊销营业执照；对当事人造成损害的，应当承担赔偿责任。

违反本规定第十七条第(六)(七)(八)项规定，未依法开展人力资源服务业务，牟取不正当利益的，由人力资源社会保障行政部门依照《人力资源市场暂行条例》第四十三条的规定处罚。

违反本规定第十七条第(九)项规定，骗取社会保险基金支出、社会保险待遇的，由人力资源社会保障行政部门依照《中华人民共和国社会保险法》第八十七条、第八十八条的规定处罚。

第四十二条 违反本规定第二十条第一款规定，未依法举办现场招聘会活动，违反本规定第二十八条规定，未依法开展人力资源服务外包的，由人力资源社会保障行政部门依照《人力资源市场暂行条例》第四十三条的规定处罚。

第四十三条 违反本规定第二十二条、第二十三条规定，未依法处理个人信息的，由有关主管部门依照《中华人民共和国个人信息保护法》《中华人民共和国网络安全法》等法律、法规的规定处罚。

第四十四条 未依照本规定第二十五条第一款规定建立健全内部制度或者保存服务台账，未依照本规定第二十六条规定明示有关事项，未依照本规定第三十四条第一款规定提交经营情况年度报告的，由人力资源社会保障行政部门依照《人力资源市场暂行条例》第四十四条的规定处罚。

第四十五条 违反本规定第二十七条第一款规定，向个人收取明示服务项目以外的服务费用，或者以各种名目诱导、强迫个人参与贷款、入股、集资等活

动的，由人力资源社会保障行政部门依照《人力资源市场暂行条例》第四十三条的规定处罚。违反本规定第二十七条第二款规定，向个人收取押金的，由人力资源社会保障行政部门依照《中华人民共和国就业促进法》第六十六条的规定处罚。

第四十六条 违反本规定第二十九条规定，扰乱人力资源市场价格秩序，采取垄断、不正当竞争等手段开展服务活动的，由有关主管部门依照《中华人民共和国反垄断法》《中华人民共和国反不正当竞争法》等法律、法规的规定处罚。

第四十七条 人力资源社会保障行政部门和有关主管部门及其工作人员有下列情形之一的，对直接负责的领导人员和其他直接责任人员依法给予处分：

(一)不依法作出行政许可决定的；

(二)在办理行政许可或者备案、实施监督检查中，索取或者收受他人财物，或者谋取其他利益的；

(三)不依法履行监督职责或者监督不力，造成严重后果的；

(四)其他滥用职权、玩忽职守、徇私舞弊的情形。

第四十八条 违反本规定，侵害劳动者合法权益，造成财产损失或者其他损害的，依法承担民事责任。

违反本规定，构成违反治安管理行为的，依法给予治安管理处罚；构成犯罪的，依法追究刑事责任。

第六章 附 则

第四十九条 在实行相对集中行政许可权改革或者综合行政执法改革的地区，对经营性人力资源服务机构从事人力资源服务活动的行政许可、监督管理等职责，法律、行政法规和国务院决定等另有规定的，依照有关规定执行。

第五十条 公共就业和人才服务机构的设立和管理，依照《中华人民共和国就业促进法》《就业服务与就业管理规定》等规定执行。

第五十一条 本规定自 2023 年 8 月 1 日起施行。此前人力资源社会保障部发布的人力资源服务机构管理有关规定，凡与本规定不一致的，依照本规定执行。

国家邮政局关于修订印发《寄递服务用户个人信息安全管理规定》的通知

国邮发〔2023〕7 号

各省、自治区、直辖市邮政管理局，中国邮政集团有限公司，各主要快递企业总部：

修订后的《寄递服务用户个人信息安全管理规定》于 2023 年 2 月 6 日经国家邮政局 2023 年第 2 次局长办公会议审议通过，现印发给你们，请遵照执行。

国家邮政局

2023 年 2 月 13 日

寄递服务用户个人信息安全管理规定

第一条 为加强寄递服务用户个人信息安全管理，保护用户合法权益，维护邮政通信与信息安全，促进邮政行业健康发展，根据《中华人民共和国邮政法》《中华人民共和国网络安全法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》以及《快递暂行条例》《邮政业寄递安全监督管理办法》等法律、行政法规和有关规定，制定本规定。

第二条 在中华人民共和国境内经营和使用寄递服务涉及用户个人信息安全的活动以及邮政管理部门监督管理工作，适用本规定。

第三条 本规定所称寄递服务用户个人信息，是指用户在使用寄递服务过程中记录的个人信息，包括《中华人民共和国民法典》第一千零三十四条所列的姓名、身份证件号码、生物识别信息、住址、电话号码等信息以及运单号、时间、物品明细等信息。

第四条 邮政管理部门应当与有关部门相互配合，健全寄递服务用户个人信息安全保障机制，维护寄递服务用户个人信息安全。

第五条 寄递企业应当建立健全寄递服务用户个人信息安全保障制度和措施，明确企业部门、岗位的安全保护责任，合理确定寄递服务用户个人信息处理的操作权限，定期对从业人员进行安全教育和培训。

第六条 使用统一的商标、字号或者快递运单经营快递业务的，商标、字号或者快递运单所属企业应当对使用其商标、字号或者快递运单的企业的信息安全保障实行统一管理，发生寄递服务用户个人信息安全事件时，应当依法承担相应责任。

第七条 寄递企业收集寄递服务用户个人信息应仅限于完成寄递服务全流程

操作目的的最小范围，不得过度收集用户个人信息。

寄递企业应当与其从业人员签订寄递服务用户个人信息保密协议，明确保密义务。

第八条 寄递企业为完成寄递服务全流程操作委托第三方或者其他寄递企业等开展代收代投、清关等业务，需要对寄递服务用户个人信息数据进行委托处理时，应当事前进行寄递服务用户个人信息保护影响评估，并依法约定委托处理的目的、期限、处理方式、个人信息种类、保护措施及双方权利义务，并对受托人的个人信息处理活动进行监督。

受托方发生寄递服务用户个人信息安全事件导致信息泄露、篡改、丢失的，寄递企业应当依法承担相应责任。

第九条 寄递企业应当建立寄递服务用户个人信息安全投诉处理及请求响应机制，公布有效联系方式，接受并及时处理有关投诉及请求。

第十条 寄递企业应当建立寄递服务用户个人信息安全应急处置机制。发现信息安全隐患、漏洞等风险的，或者发生信息安全突发事件的，应当立即采取处置措施，按照规定报告邮政管理部门，并配合邮政管理部门和相关部门的调查处理工作，不得迟报、漏报、谎报、瞒报。

第十一条 处理寄递服务用户个人信息达到国家网信部门规定数量的寄递企业应当指定寄递服务用户个人信息保护负责人，负责对信息处理活动以及采取的保护措施等进行监督，并公开寄递服务用户个人信息保护负责人的联系方式，将负责人的姓名、联系方式等向所在地市级邮政管理部门报送。负责人发生变更的，应在 7 个工作日内重新报送并公告。

前款规定的寄递企业同时符合《中华人民共和国个人信息保护法》第五十八条规定条件的，还应当依法履行该条规定的建立健全寄递服务用户个人信息保护合规制度体系、成立主要由外部成员组成的独立机构对个人信息保护情况进行监督、定期发布寄递服务用户个人信息保护社会责任报告并接受社会监督等义务。

第十二条 寄递企业因业务等需要，确需向中华人民共和国境外提供寄递服务用户个人信息的，应当按照相关法律法规的规定执行。

寄递企业应当将在中华人民共和国境内收集和产生的个人信息存储在境

内。

第十三条 寄递企业应当对快递电子运单单号资源实施全过程管理，并采用射频识别、虚拟安全号码、电子纸等有效技术手段对快递电子运单信息进行去标识化处理，防止运单信息在寄递过程中泄露。

寄递企业与电商平台或者快递电子运单集成系统运营企业等第三方对接寄递信息或者授权使用分配本企业单号资源时，应要求其对快递电子运单信息进行去标识化处理，并确保不影响正常寄递服务。存在寄递服务用户个人信息安全风险或可能影响正常寄递服务的，寄递企业不得对接寄递信息或授权使用分配本企业单号资源。

法律、行政法规另有规定，或者用户有要求的，可以不对快递电子运单信息进行去标识化处理。

第十四条 寄递企业应当保证建设与寄递服务用户个人信息相关的信息系统时，在网络传输、访问控制、终端防护、恶意代码防护、监控审计等方面采取有效措施，确保同步规划、同步建设和同步使用。

寄递企业应当建立存储介质使用管理制度，使用独立物理区域采用加密方式存储用户个人信息，加强存储安全管理。

第十五条 寄递企业应当加强寄递服务用户个人信息的应用安全管理，对所有批量导出、复制、销毁等操作进行事先审核，采取防泄密措施，并记录保存操作人员、时间、地点和事项等信息，作为信息安全审计依据。

寄递企业应当加强对离岗人员的信息安全审计，删除或者禁用离岗人员系统账户。

第十六条 寄递企业应当强化对寄递服务用户个人信息安全的实时监测能力，严格落实安全管理和技术防范措施，防范和遏制重大安全风险、事件发生。

第十七条 寄递企业应当制定本企业与市场相关主体的信息系统互联的安全技术规则，对存储寄递服务用户个人信息的信息系统实行接入审查，定期进行安全风险评估。

第十八条 寄递企业应当加强营业场所、处理场所管理，严禁无关人员进出相关场所，严禁无关人员接触、翻阅、留存、拍照、摄录、复制、传抄运单信

息。

第十九条 邮政管理部门应当依法监督寄递企业落实寄递服务用户个人信息安全责任制，加强个人信息安全管理，防范重大个人信息安全事件，及时处理有关举报。

第二十条 邮政管理部门可以在行业内通报寄递企业违反本规定的行为、个人信息安全事件，以及对有关责任人员进行处理的情况。必要时，可以向社会公布上述信息，但涉及国家秘密、商业秘密和个人隐私的除外。

第二十一条 邮政管理部门及其工作人员应当对在履行职责过程中知悉的寄递服务用户个人信息保密。在监督管理工作中滥用职权、玩忽职守、徇私舞弊，构成犯罪的，依法追究刑事责任；尚不构成犯罪的，依法给予处分。

第二十二条 邮政管理部门发现寄递企业存在违反本规定行为，妨害或者可能妨害个人信息安全保护的，应当依法调查处理。违法行为涉及其他部门管理职权的，应当依法向相关部门移送线索。

第二十三条 本规定自 2023 年 2 月 13 日起施行，2014 年 3 月 19 日发布的《寄递服务用户个人信息安全管理规定》同时废止。

国家邮政局 商务部关于规范快递与电子商务数据互联共享的指导意见

国邮发〔2019〕54 号

各省、自治区、直辖市邮政管理局、商务主管部门，各计划单列市及新疆生产建设兵团商务主管部门：

电子商务与快递数据互联互通和有序共享，是促进电子商务与快递协同发展的重要条件。为贯彻落实《国务院办公厅关于推进电子商务与快递物流协同发展的意见》，建立完善电子商务与快递数据互联共享规则，促进电子商务经营者、经营快递业务的企业数据管理和自身治理能力的全面升级，按照《中华人民共和国电子商务法》《中华人民共和国网络安全法》《快递暂行条例》等法律法规的规定，现提出以下指导意见。

一、保障电子商务与快递数据正常传输

(一)电子商务经营者提供寄递数据

电子商务当事人约定采用快递方式交付商品的，支持电子商务经营者通过约定的信息传输方式及时将必要的寄递数据(包括但不限于寄件人和收件人姓

名、地址、联系电话、内件等数据)提供给经营快递业务的企业。电子商务平台经营者不得通过限制数据互联共享，阻碍电子商务当事人自由选择快递服务。鼓励为电子商务经营者提供快递信息服务的平台企业履行与电子商务平台经营者同等的数据互联共享义务。

(二)经营快递业务的企业提供快件数据

支持经营快递业务的企业提供电子商务寄递服务时，通过约定的信息传输方式及时将必要的快件数据(包括但不限于快件收寄、分拣、运输、投递等节点和轨迹数据)提供给电子商务经营者。经营快递业务的企业不得通过限制数据互联共享，阻碍电子商务经营者获取为消费者提供服务所必需的快件数据。

二、加强电子商务与快递数据管控

(三)依法采集共享用户数据

通过电子商务平台使用快递服务的用户应当严格遵守邮件快件实名收寄相关规定，按照规范要求如实填写必要的用户信息。电子商务经营者和经营快递业务的企业采集、共享用户信息时，应当遵守法律、行政法规有关信息保护的规定，不得用于与其提供寄递服务无关的用途。

(四)妥善存储使用用户数据

电子商务经营者和经营快递业务的企业应当妥善存储用户数据。开展数据挖掘时，应当采用加密、脱敏等方式保护用户数据安全。利用用户大数据进行增值应用的，应当经过用户同意，并不得将具有个人隐私特征的数据提供给其他单位和个人。涉及数据跨境流动的，依照相关法律法规规定。

三、加强电子商务与快递数据互联共享管理

(五)建立完善的数据互联共享机制

在确保用户信息安全的前提下，鼓励电子商务经营者与经营快递业务的企业之间依据相关标准开展数据互联共享，共同提升配送效率。支持电子商务经营者与经营快递业务的企业加强系统互联和业务联动，推动作业流程、数据交换有效衔接。

四、建立电子商务与快递数据中断通知报告制度

(六)建立数据中断风险评估制度

鼓励电子商务经营者和经营快递业务的企业建立数据中断风险评估制度，

实现数据互联自动检查、全程监控。电子商务经营者、经营快递业务的企业不得恶意中断数据传输。

(七)完善提前通知和事先报告制度

电子商务经营者和经营快递业务的企业因约定期满等正当理由中断数据传输的，应当提前通知对方。通知后，双方应当就数据传输进行充分协商，对后续事项做出妥善安排。双方不能协商一致且可能对用户和消费者造成重大影响的，应事先将有关情况及时报告商务主管部门和邮政管理部门。电子商务经营者和经营快递业务的企业应当及时将相关情况向用户、平台内经营者等主体公示。

五、提高电子商务与快递数据安全防护水平

(八)加强数据安全保障

电子商务经营者和经营快递业务的企业应当完善自身数据管理体系和安全保障体系，采取技术手段和其他必要措施保证数据安全，建立健全信息安全风险评估和应急工作机制，完善安全防护体系。双方要高度重视数据传输中的安全隐患和不规范问题，增强电子商务与快递数据传输的安全技术保障能力，严格系统安全管理，确保用户信息安全。

(九)加强数据安全应急管理

电子商务经营者和经营快递业务的企业要制定网络安全事件应急预案，有效应对网络安全事件，防范网络违法犯罪活动。发生危害网络安全事件时，电子商务经营者和经营快递业务的企业应当立即依法启动应急预案，采取相应的补救措施，并向有关主管部门报告。

六、加强电子商务与快递数据政府监管

(十)完善相关标准

商务主管部门和邮政管理部门推动制定电子商务和快递数据采集、传输、使用、共享、安全风险防范等相关标准，提高电子商务和快递数据互联共享效率，保障数据安全。

(十一)依法加强监管

商务主管部门和邮政管理部门利用大数据等技术，优化电子商务与快递业监管，客观评估数据互联共享状况，加强行业监测分析，提高政府科学决策和

风险预判能力，加强对市场主体的事中事后监管。

(十二)协调化解纠纷

电子商务经营者和经营快递业务的企业就数据互联共享发生纠纷，并可能引发市场风险的，商务主管部门和邮政管理部门可采取约谈等方式，协调处理相关纠纷，并视情况将相关处理情况向社会公示。

国家邮政局 商务部

2019 年 6 月 12 日

教育部等八部门关于引导规范教育移动互联网应用有序健康发展的意见

教技函〔2019〕55 号

各省、自治区、直辖市教育厅(教委)、网信办、通信管理局、公安厅(局)、民政厅(局)、市场监管局、新闻出版局、“扫黄打非”办公室，新疆生产建设兵团教育局、网信办、公安局、民政局、市场监管局，部属各高等学校，各直属单位，中国教育和科研计算机网网络中心：

教育移动互联网应用程序(教育 APP，以下简称教育移动应用)是指以教职工、学生、家长为主要用户，以教育、学习为主要应用场景，服务于学校教学与管理、学生学习与生活以及家校互动等方面的互联网移动应用。近年来，教育移动应用快速发展、广泛应用，在提高教学效率和管理水平、满足学生个性化学习需求和兴趣发展、优化师生体验等方面发挥了积极作用。但一些学校出现了应用泛滥、平台垄断、强制使用等现象，一些教育移动应用存在有害信息传播、广告丛生等问题，给广大师生、家长带来了困扰，产生了不良的社会影响。为引导和规范教育移动应用有序健康发展，更好地发挥教育信息化的驱动引领作用，现提出以下意见。

一、总体要求

(一)指导思想

以习近平新时代中国特色社会主义思想为指导，深入贯彻党的十九大精神，全面落实全国教育大会精神、全国网络安全和信息化工作会议精神，根据《中华人民共和国教育法》《中华人民共和国网络安全法》等国家有关法律法规，围绕落实立德树人根本任务，积极发展“互联网+教育”、办好网络教育，全面深化“放管服”改革，实施包容审慎监管，引导教育移动应用健康有序发

展，为广大师生营造健康、有序、安全的网络空间和学习环境。

(二)基本原则

科学施策、分类引导。正确处理政府与市场、管理与服务、安全与发展的关系。分类引导不同教育阶段和类型、不同用户群体、不同功能用途的教育移动应用，构建良好教育生态。

问题导向、标本兼治。围绕群众反映强烈的问题，从供给侧和需求侧两端进行规范。开展专项行动治理乱象，建章立制规范管理，提质增效支撑发展，综合施策打好组合拳。

多方参与、协同联动。以构建常态化的治理体系为关键，建立政府管理、企业履责、专家献策、学校把关、家长监护、社会监督、行业自律等多主体参与、职责明晰的综合协同治理体系。

(三)工作目标

全面治理教育移动应用乱象，补齐监督短板，规范全生命周期管理，提高开发供给质量，营造优良发展生态，促进教育移动应用有序健康发展。2019 年底，完成教育移动应用备案工作。开展教育移动应用专项治理行动，群众反映强烈的问题得到有效缓解。2020 年底，建立健全教育移动应用管理制度、规范和标准，形成常态化的监管机制，初步建成科学高效的治理体系。

二、提高供给质量

(四)建立备案制度。教育移动应用提供者应当在取得 ICP 备案(涉及经营电信业务的，还应当申请电信业务经营许可)、网络安全等级保护定级备案的证明、等级测评报告后，向机构住所地的省级教育行政部门进行教育业务备案，登记单位基本信息和所开发的教育移动应用信息。已备案的教育移动应用提供者上线新应用前，应当在备案单位更新相关信息。教育部制定备案办法，明确备案流程和内容，依托国家教育资源公共服务平台为备案登记工作提供信息化支撑，汇总各省级教育行政部门备案信息，并向社会提供查询渠道。

(五)加强内容建设。教育移动应用提供者呈现的内容应当严格遵守国家法律法规，符合党的教育方针，体现素质教育导向，呈现的广告应当与提供的服务相契合。以未成年人为主要用户的教育移动应用应当限制使用时长、明确适龄范围，对内容进行严格把关。鼓励以高校师生为主要用户的教育移动应用增

强优质网络教育资源供给能力，成为加强网络思想政治工作的有效载体。具备论坛、社区、留言等功能的教育移动应用应当建立信息审核制度。面向各教育阶段实施培训的教育移动应用应当对提供服务的主体进行审核、登记，其中：在校外线上培训机构实施学科类培训的人员应当取得教师资格证；聘用外籍人员实施培训的应当审查教学资质、学历和能力，并严格落实国家相关要求。

(六)规范数据管理。教育移动应用提供者应当建立覆盖个人信息收集、储存、传输、使用等环节的数据保障机制。按照“后台实名、前台自愿”的原则，对注册用户进行身份信息认证。收集使用个人信息应当明示收集使用信息的目的、方式和范围，并经用户同意。收集使用未成年人信息应当取得监护人同意、授权。不得以默认、捆绑、停止安装使用等手段变相强迫用户授权，不得收集与其提供服务无关的个人信息，不得违反法律法规与用户约定，不得泄露、非法出售或非法向他人提供个人信息。

(七)保障网络安全。教育移动应用提供者应当落实网络安全主体责任，采取有效措施，防范应对网络攻击，保障系统的平稳、安全运行。教育移动应用和后台系统应当统一落实网络安全等级保护要求。应用商店等移动应用分发平台提供者应当加强教育移动应用上架审核管理，建立开发者真实身份信息登记制度，对教育移动应用开展安全审核，及时处理违法违规教育移动应用。鼓励教育移动应用提供者参加网络安全认证、检测，全面提高网络安全保障水平。

三、规范应用管理

(八)落实主体责任。教育行政部门和学校是本单位自主开发的教育移动应用的主管单位和选用第三方教育移动应用的责任单位，应当加强统筹管理，明确职能部门归口，将教育移动应用、公众号和小程序等移动互联网平台纳入本地区、本单位的重要议事日程予以部署。按照“谁主管谁负责、谁开发谁负责、谁选用谁负责”的原则，建立健全教育移动应用管理责任体系，切实维护广大师生和家长的切身利益。

(九)建立推荐机制。省级教育行政部门应当根据地方实际，会同网信等职能部门探索本地区教育移动应用的推荐机制，按照公平、公正、公开原则，组织开展教育移动应用的评议，形成推荐名单并向社会公开，同时报教育部。推荐名单应保证质量，并保持动态更新。鼓励通过第三方评估，组织对教育移动

应用的合法合规、功能性能、安全保障等方面进行检测，对教育移动应用呈现的内容进行检查，为推荐工作提供技术支撑。

(十)健全选用机制。教育行政部门和学校应当制定教育移动应用的选用制度。选用应当充分尊重教职工、学生和家长的意见，并严格选用标准、控制数量，避免造成不必要的负担。确定选用的教育移动应用应当报上级教育行政部门进行备案。未经教育行政部门、学校集体决策选用的教育移动应用，不得要求学生使用。中小学学习类教育移动应用应当落实教育行政部门和学校的“双审核”制度；各省级教育行政部门可根据地方实际结合推荐制度简化审核流程。

(十一)规范进校合作。教育行政部门和学校应当规范教育移动应用的进校管理。作为教学、管理工具要求统一使用的教育移动应用，不得向学生及家长收取任何费用，不得植入商业广告和游戏。推荐使用的教育移动应用应当遵循自愿原则，不得与教学管理行为绑定，不得与学分、成绩和评优挂钩。对于承担招生录取、考试报名、成绩查询等重要业务的教育移动应用，原则上应当由教育行政部门和学校自行运行管理。确需选用第三方应用的，不得签订排他协议，或实际由单一应用垄断业务。鼓励高校联合省级教育行政部门、招生考试机构、教育部“阳光高考”平台优化公共服务。

(十二)促进整合共享。教育行政部门和学校应当创新教育资源供给模式，探索通过国家数字教育资源公共服务体系，汇聚优质教育资源，集成各类应用，使网络学习空间成为教育移动应用的主要入口。面向师生提供管理和服务的教育移动应用应当整合为“互联互通、业务协同、信息共享”的综合性教育移动应用。鼓励教育移动应用将收集的机构、师生信息与国家基础数据库进行统一校验，并统一汇聚至国家教育基础数据库。

四、健全监管体系

(十三)加强行业规范。教育移动应用提供者应当自觉接受社会监督，设置便捷的投诉举报渠道，及时处理投诉。应用商店等移动应用分发平台提供者应当落实监督责任，健全资质核验、内容审核，配合进行适龄提示管理，并将教育业务备案作为上架应用商店的重要条件。鼓励移动终端提供者为家长监护提供技术支撑，提供未成年人监管功能。积极发挥行业协会的作用，制定行业公

约，建立行业信用评价体系和服务评议制度，促进行业规范发展。

(十四)建立协同机制。建立多部门协同联动的监管机制。教育行政部门牵头负责教育移动应用治理工作，负责统筹协调，指导和监督学校落实主体责任，会同相关部门开展联合治理。网信部门、电信主管部门、公安部门依据职责重点做好教育移动应用提供者、应用商店等移动应用分发平台提供者、移动终端制造商的监管工作。新闻出版部门重点做好教材、教辅等网络出版物的监管工作。民政部门重点做好教育类民办非企业单位的登记管理工作。市场监管部门重点做好线上盈利性教育机构的登记管理，依法查处违规收费，虚假、违法广告等行为。公安部门重点做好打击整治相关违法犯罪活动。

(十五)拓展监督渠道。教育行政部门应当加强与有关职能部门、专业机构、行业协会和企业的合作，通过技术检测和人工查看相结合的方式，建立常态化的监测预警通报机制。通过家长委员会，满足家长对学校教学管理工作的知情权、评议权、参与权和监督权。引导家长履行监护责任，通过加强家庭交流互动、设置移动终端限制等方式，引导学生正确使用教育移动应用。教育行政部门应当全面掌握教育动态，及时受理投诉建议，主动回应社会关切，切实解决群众痛点难点问题。

(十六)加强考核问责。省级教育行政部门应当建立教育移动应用的选用退出机制、负面清单和黑名单制度，推动将黑名单信息纳入全国信用信息共享平台，按有关规定实施联合惩戒。教育督导部门应当将教育移动应用治理情况纳入对下级政府履行教育职责督导评估和对学校的综合督导评估。教育行政部门应当将教育移动应用治理纳入网络安全责任制等相关考核。对责任不落实、措施不到位的教育行政部门和学校予以约谈、通报。对因失职、渎职造成严重后果的，依法依规对相关负责人严肃问责。

五、加强支撑保障

(十七)加强组织领导。教育行政部门和学校应当将引导规范教育移动应用工作纳入重要议事日程，建立由教育行政部门牵头，宣传、“扫黄打非”、网信、电信、公安、民政、市场监管等部门共同参与的部门协同机制，制订工作方案，明确职责分工、时间节点、实施路径和保障措施。建立本地区的教育移动应用重点任务台账，统筹协调校外线上培训机构治理等重点工作，监督指导

各项任务落实到位。

(十八)健全制度规范。教育行政部门应当完善教育移动应用的备案、推荐、选用、监督检查等制度，构建覆盖全生命周期的管理机制。健全教育移动应用评估、监测、检查、防护等技术规范，推进教育移动应用治理制度化、规范化、标准化。组织行业专家和相关企业共同完善教育移动应用的标准，规范程序开发、运行管理等环节，提高教育移动应用的服务质量和保障水平。

(十九)提升信息素养。教育行政部门和学校应当组织管理和技术人员培训，将规范教育移动应用管理作为重要内容，切实提高管理水平和保障能力。同时，应当加强宣传引导和教育，以开学教育、网络安全宣传周等活动为契机，培养在校师生科学的使用习惯；通过家长会、家长学校、专题报告等形式，促进家长树立正确的用网观念，全方位地提高广大师生、家长的信息素养。

(二十)落实工作保障。教育行政部门应当加强对教育移动应用管理的经费支持，保障备案推荐、监测评估、监督检查等重点任务开展。教育行政部门和学校应当利用国家教育资源公共服务体系和国家教育管理公共服务平台为教育移动应用治理工作提供信息化支撑，探索“政府统筹引导、企业参与建设、学校购买服务”的教育移动应用供给机制，提供优质的教育资源和应用服务。

教育部 中央网信办 工业和信息化部

公安部 民政部 市场监管总局

国家新闻出版署 全国“扫黄打非”工作小组办公室

2019 年 8 月 10 日

教育部办公厅关于印发《教育移动互联网应用程序备案管理办法》的通知

教技厅〔2019〕3 号

各省、自治区、直辖市教育厅(教委)，新疆生产建设兵团教育局，部属各高等学校，各直属单位：

《教育移动互联网应用程序备案管理办法》(以下简称《办法》)已经教育部网络安全和信息化领导小组审定同意。现印发给你们，请遵照执行，并就做好教育移动互联网应用程序(以下简称教育移动应用)备案工作通知如下。

一、高度重视教育移动应用备案工作。落实备案制度是规范教育移动应用

管理的基础。请各单位高度重视备案工作，明确职能部门统筹教育移动应用管理工作，组织开展备案工作。各省级教育行政部门应组织本地区的企业、社会机构等单位做好提供者备案，指导本地区的教育行政部门和学校做好提供者备案和使用者备案。

二、分阶段完成教育移动应用备案工作。备案工作将依托国家数字教育资源公共服务体系（网址：http://app.eduyun.cn，以下简称公共服务体系）常态化开展。请各单位于 2019 年 12 月 1 日至 2020 年 1 月 31 日前完成对现有教育移动应用的备案工作，并结合实际建立本地区、本单位的备案信息动态更新机制，确保数据准确性。

三、设置 ICP 备案和等级保护备案缓冲期。2019 年 12 月 1 日至 2020 年 1 月 31 日为备案缓冲期，期间 ICP 备案和等级保护备案不作为备案的前置条件。请教育移动应用提供者在 2020 年 1 月 31 日前完成 ICP 备案和等级保护备案，并及时在公共服务体系上传、更新信息。2020 年 2 月 1 日起，未完成上述两个备案的教育移动应用备案将被撤销，并予以通报。

四、加强政策宣传解读。各单位应向教育移动应用提供者和使用者认真解读教育移动应用相关政策文件，介绍《办法》明确的备案流程和要求，指导工作人员开展备案工作。加强对广大师生使用教育移动应用的宣传教育，介绍相关政策，鼓励在校师生共同维护切身利益。

五、提高事中事后监管能力。各单位应以备案为基础建立监测预警通报机制，及时发现、处置问题隐患和安全事件。省级教育行政部门应建立本地区的监测预警通报机制，并与教育部进行数据共享。2020 年 2 月 1 日起，公共服务体系将向社会公众提供备案信息查询，接受社会监督。

联系人及电话：教育部科技司 潘润恺 010-66096457

中央电化教育馆 刘学 010-66490222

教育部办公厅

2019 年 11 月 11 日

教育移动互联网应用程序备案管理办法

第一章 总 则

第一条 为做好教育移动互联网应用程序(以下简称教育移动应用)备案管理

工作，加强教育移动应用事中事后监管，根据国家“放管服”改革精神和《教育部等八部门关于引导规范教育移动互联网应用有序健康发展的意见》（以下简称《意见》）的要求，制定本办法。

第二条 本办法所指的教育移动应用是以教职工、学生、家长为主要用户，以教育、学习为主要应用场景，服务于学校教学与管理、学生学习与生活以及家校互动等方面的互联网移动应用程序。

第三条 教育移动应用的备案分为提供者备案和使用者备案。提供者备案按照“全国统一标准、各省分头实施、单位属地备案”的原则开展，使用者备案根据隶属关系向主管教育行政部门备案。

第四条 教育移动应用备案依托国家数字教育资源公共服务体系（以下简称公共服务体系）为教育移动应用提供信息化支撑，实现备案全程网上办理，一省备案全国有效，切实减轻企业和学校的负担。备案结果网上公示，接受社会公众查询。

第二章 工作职责

第五条 教育部负责统筹教育移动应用备案管理工作，制定教育移动应用备案管理办法，明确备案条件。组织直属单位和部属高校开展教育移动应用使用者备案。指导省级教育行政部门做好本地区备案工作。

第六条 省级教育行政部门负责统筹本地区教育移动应用备案管理工作。组织本地区的教育移动应用提供者开展提供者备案，组织所属单位并指导本地区的教育行政部门和学校做好使用者备案。

第七条 教育移动应用提供者（以下简称提供者）应按照本办法的要求通过公共服务体系进行提供者备案，并配合注册地省级教育行政部门做好备案审核工作。

第八条 教育行政部门及其所属单位、各级各类学校是教育移动应用的机构使用者（以下简称使用者），应建立教育移动应用的选用制度，选用已完成提供者备案的教育移动应用，并通过公共服务体系进行使用者备案。

第三章 提供者备案

第九条 提供者应在完成互联网信息服务（ICP）备案和网络安全等级保护定级备案后，进行提供者备案。

第十条 教育行政部门、学校、企业和社会组织均向其住所地或注册地省级教育行政部门进行提供者备案。省级教育行政部门开发的教育移动应用向教育部进行备案。小程序、企业号等平台第三方应用统一到平台方提交备案信息，并由平台方向教育部共享备案信息。

第十一条 提供者备案实行“一省备案，全国有效”。提供者在注册地备案后，在其他地区开展业务无需重复备案。各子公司(分公司)或分支机构开发的教育移动应用，由总公司统筹汇总并向总公司注册地的省级教育行政部门进行备案。

第十二条 提供者应登录公共服务体系，准确填写《教育移动应用提供者备案信息表》(附件 1)，包括企业信息、业务系统信息和教育移动应用信息。

第十三条 省级教育行政部门对其填报的备案信息进行核验，信息有误的应在 10 个工作日内通过公共服务体系反馈提供者。提供者应在收到反馈后的 10 个工作日内补充提交材料，逾期未反馈视同放弃备案。公共服务体系与国家数据共享交换平台建立信息共享，为备案信息审核提供数据支撑和决策参考。

第十四条 省级教育行政部门对备案材料齐全、信息准确且符合要求的提供者，应在备案信息提交 10 个工作日内完成备案并编号，备案信息将通过公共服务体系向社会公布。提供者应在教育移动应用中公示备案信息以便用户查询。

第十五条 提供者已有备案信息发生变化的，应在 10 个工作日内登录公共服务体系更新备案信息，并重新进行备案核验。

第十六条 教育部将建立完善与网信、电信、公安等职能部门的协助机制，共同指导应用商店等移动应用分发平台落实监督责任，规范教育移动应用的管理，并推动将提供者备案作为教育移动应用上架应用商店的重要条件。

第四章 机构使用者备案

第十七条 自主开发、自主选用和上级部门要求使用的教育移动应用均应进行使用者备案。

第十八条 使用者应登录公共服务体系，在已完成提供者备案的教育移动应用中进行勾选，并填写《教育移动应用使用者备案信息表》(附件 2)，完成使用者备案。

第十九条 根据“逐级管理、分级负责”的原则，学校和所属单位的使用者

备案信息由其主管教育行政部门进行确认，教育行政部门的使用者备案信息由上级教育行政部门进行确认。

第二十条 使用者已有备案信息发生变化的，应在 10 个工作日内及时登录公共服务体系更新备案信息，并提请重新确认。

第二十一条 使用者自主开发，服务于本单位内部管理且不对外单位提供服务的教育移动应用，应在使用者备案时勾选“自研自用”的选项，并提交提供者备案信息。自研自用的教育移动应用按行政隶属关系进行备案。

第五章 监督管理

第二十二条 通过公共服务体系公布提供者和使用者备案信息供社会公众查询。同时，在公共服务体系建立投诉举报通道，接受社会公众的投诉举报。

第二十三条 教育部对各地教育移动应用备案情况进行检查，定期通报教育移动应用备案工作进展。同时，将教育移动应用备案情况纳入网络安全责任制等相关考核评价。对备案工作落实不到位的教育行政部门和学校予以约谈、通报。

第二十四条 教育移动应用存在违法违规或违反《意见》要求且整改不及时的，将列入教育移动应用提供者黑名单，向教育系统通报，并撤销涉事教育移动应用备案。涉事单位六个月内不得再提交备案申请。

第六章 附 则

第二十五条 本办法解释权归教育部。

第二十六条 各省级教育行政部门可根据本办法制定本地区教育移动应用备案的实施细则。

第二十七条 本办法自发布之日起实施。

附件：1.教育移动应用提供者备案信息表

2.教育移动应用使用者备案信息表

关于印发《关于加强网络直播规范管理工作的指导意见》的通知

国信办发文〔2021〕3 号

各省、自治区、直辖市和新疆生产建设兵团网信办、“扫黄打非”办公室、通信管理局、公安厅(局)、文化和旅游厅(局)、市场监管局(厅、委)、广电局：

为进一步加强网络直播行业的规范管理，促进行业健康有序发展，国家互

联网信息办公室、全国“扫黄打非”工作小组办公室、工业和信息化部、公安部、文化和旅游部、国家市场监督管理总局、国家广播电视总局等七部委联合发布《关于加强网络直播规范管理工作的指导意见》。现印发你们，请结合实际，认真贯彻执行。

国家互联网信息办公室

全国“扫黄打非”工作小组办公室

工业和信息化部

公安部

文化和旅游部

国家市场监督管理总局

国家广播电视总局

2021 年 2 月 9 日

关于加强网络直播规范管理工作的指导意见

近年来，网络直播以其内容和形式的直观性、即时性和互动性，在促进经济社会发展、丰富人民群众精神文化生活等方面发挥了重要作用。随着移动互联网新技术新应用的迭代升级，网络直播行业进入了快速发展期，其媒体属性、社交属性、商业属性、娱乐属性日益凸显，深刻影响网络生态。与此同时，网络直播行业存在的主体责任缺失、内容生态不良、主播良莠不齐、充值打赏失范、商业营销混乱、青少年权益遭受侵害等问题，严重制约网络直播行业健康发展，给意识形态安全、社会公共利益和公民合法权益带来挑战，必须高度重视、认真解决。为切实加强网络直播行业正面引导和规范管理，保护广大网民合法权益，倡导行业加强网络文明建设，培育向上向善的网络文化，践行社会主义核心价值观，促进网络直播行业健康有序发展，经中央领导同志同意，现提出如下指导意见。

一、明确总体要求

全面贯彻党的十九大和十九届二中、三中、四中、五中全会精神，以习近平新时代中国特色社会主义思想为指导，坚持正确政治方向、舆论导向、价值取向，坚持依法办网、依法治网，准确把握网络直播行业特点规律和发展趋势，有效解决突出问题、难点问题、痛点问题，科学规范行业运行规则，构建

良好产业生态，为广大网民特别是青少年营造积极健康、内容丰富、正能量充沛的网络直播空间。

二、督促落实主体责任

1.压实平台主体责任。网络直播平台提供互联网直播信息服务，应当严格遵守法律法规和国家有关规定；严格履行网络直播平台法定职责义务，落实网络直播平台主体责任清单，对照网络直播行业主要问题清单建立健全和严格落实总编辑负责、内容审核、用户注册、跟帖评论、应急响应、技术安全、主播管理、培训考核、举报受理等内部管理制度。

2.明确主播法律责任。自然人和组织机构利用网络直播平台开展直播活动，应当严格按照《互联网用户账号名称管理规定》等有关要求，落实网络实名制注册账号并规范使用账号名称。网络主播依法依规开展网络直播活动，不得从事危害国家安全、破坏社会稳定、扰乱社会秩序、侵犯他人合法权益、传播淫秽色情信息等法律法规禁止的活动；不得超许可范围发布互联网新闻信息；不得接受未经其监护人同意的未成年人充值打赏；不得从事平台内或跨平台违法违规交易；不得组织、煽动用户实施网络暴力；不得组织赌博或变相赌博等线上线下违法活动。

3.强化用户行为规范。网络直播用户参与直播互动时，应当严格遵守法律法规，文明互动、理性表达、合理消费；不得在直播间发布、传播违法违规信息；不得组织、煽动对网络主播或用户的攻击和谩骂；不得利用机器软件或组织“水军”发表负面评论和恶意“灌水”；不得营造斗富炫富、博取眼球等不良互动氛围。

三、确保导向正确和内容安全

4.提升主流价值引领。网络直播平台应当坚持把社会效益放在首位、社会效益和经济效益相统一，强化导向意识，大力弘扬社会主义核心价值观，大力扶持优质主播，扩大优质内容生产供给；培养网络主播正确的世界观、价值观、人生观，有效提升直播平台“以文化人”的精神气质和文化力量。

5.切实维护网民权益。网络直播平台应当严格遵守个人信息保护相关规定，规范收集和合法使用用户身份、地理位置、联系方式等个人信息行为；充分保障用户知情权、选择权和隐私权等合法权益；依法依规引导和规范用户合

理消费、理性打赏；依法依规留存直播图像、互动留言、充值打赏等记录；加大对各类侵害网民权益行为的打击力度，切实维护网络直播行业秩序。

6.加强未成年人保护。网络直播平台应当严禁为未满 16 周岁的未成年人提供网络主播账号注册服务，为已满 16 周岁未满 18 周岁未成年人提供网络主播账号注册服务应当征得监护人同意；应当向未成年人用户提供“青少年模式”，防范未成年人沉迷网络直播，屏蔽不利于未成年人健康成长的网络直播内容，不得向未成年人提供充值打赏服务；建立未成年人专属客服团队，优先受理、及时处置涉未成年人的相关投诉和纠纷，对未成年人冒用成年人账号打赏的，核查属实后须按规定办理退款。

7.筑牢信息安全屏障。网络直播平台应当建立健全信息安全管理制度，严格落实信息内容安全管理责任制，具备与创新发展相适应的安全可控的技术保障和防范措施；对新技术新应用新功能上线具有舆论属性或社会动员能力的直播信息服务，应严格进行安全评估；利用基于深度学习、虚拟现实等技术制作、发布的非真实直播信息内容，应当以显著方式予以标识。

8.严惩违法违规行为。坚决打击利用网络直播颠覆国家政权、散播历史虚无主义、煽动宗教极端主义、宣扬民族分裂思想、教唆暴力恐怖等违法犯罪活动；严厉查处淫秽色情、造谣诽谤、赌博诈骗、侵权盗版、侵犯公民个人信息等违法犯罪行为；全面清理低俗庸俗、封建迷信、打“擦边球”等违法和不良信息。

四、建立健全制度规范

9.强化准入备案管理。开展经营性网络表演活动的直播平台须持有《网络文化经营许可证》并进行 ICP 备案；开展网络视听节目服务的直播平台须持有《信息网络传播视听节目许可证》(或在全国网络视听平台信息登记管理系统中完成登记)并进行 ICP 备案；开展互联网新闻信息服务的直播平台须持有《互联网新闻信息服务许可证》。网络直播平台应当及时向属地网信等主管部门履行企业备案手续，停止提供直播服务的平台应当及时注销备案。

10.构建行业制度体系。网络直播平台应当建立健全和严格落实相关管理制度。建立直播账号分类分级规范管理制度，对主播账号实行基于主体属性、运营内容、粉丝数量、直播热度等因素的分类分级管理；针对不同类别级别的网

络主播账号应当在单场受赏总额、直播热度、直播时长和单日直播场次、场次时间间隔等方面合理设限，对违法违规主播实施必要的警示措施。建立直播打赏服务管理规则，明确平台向用户提供的打赏服务为信息和娱乐的消费服务，应当对单个虚拟消费品、单次打赏额度合理设置上限，对单日打赏额度累计触发相应阈值的用户进行消费提醒，必要时设置打赏冷静期和延时到账期。建立直播带货管理制度，依据主播账号分级规范设定具有营销资格的账号级别，依法依规确定推广商品和服务类别。

五、增强综合治理能力

11.建立完善工作机制。各部门应当切实履行职能职责，依法依规加强对网络直播行业相关业务的监督管理。网信部门要进一步强化网络直播行业管理的统筹协调和日常监管，建立健全部门协调联动长效机制，制定出台支持和促进网络直播行业健康发展、生态治理和规范管理的政策措施；“扫黄打非”部门要履行网上“扫黄打非”联席会议牵头单位职责，会同有关部门挂牌督办重特大案件；工业和信息化部门要严格落实网络接入实名制管理要求，强化 ICP 备案管理；公安部门要全面提升对网络直播犯罪行为实施全方位遏制打击力度；文化和旅游部门要加强网络表演行业管理和执法工作，指导相关行业组织加强网络表演行业自律；市场监管部门要加强网络直播营销领域的监督管理；广电部门要研究制定网络视听节目等管理规范及准入标准。

12.积极倡导社会监督。鼓励社会各界广泛参与网络直播行业治理，切实加强网络直播平台和政府、媒体、公众间的信息交流和有效沟通，构建网络直播规范管理的良好舆论环境。网络直播平台应当自觉接受社会监督，有效拓宽举报渠道，简化举报环节，及时受理、处置并反馈公众投诉举报。

13.发挥行业组织作用。网络社会组织要积极发挥桥梁纽带作用，大力倡导行业自律，积极开展公益活动，参与净化网络直播环境、维护良好网络生态。建立健全网络主播信用评价体系，为网络直播行业健康有序发展营造良好氛围。

关于印发《网络直播营销管理办法(试行)》的通知

国信办发文〔2021〕5 号

各省、自治区、直辖市和新疆生产建设兵团网信办、公安厅(局)、商务厅

(局)、文化和旅游厅(局)、市场监管局(厅、委)、广电局，国家税务总局各省、自治区、直辖市和计划单列市税务局：

现将《网络直播营销管理办法(试行)》印发给你们，请认真遵照执行。

网信办

公安部

商务部

文化和旅游部

税务总局

市场监管总局

广电总局

2021 年 4 月 16 日

网络直播营销管理办法(试行)

第一章 总 则

第一条 为加强网络直播营销管理，维护国家安全和公共利益，保护公民、法人和其他组织的合法权益，促进网络直播营销健康有序发展，根据《中华人民共和国网络安全法》《中华人民共和国电子商务法》《中华人民共和国广告法》《中华人民共和国反不正当竞争法》《网络信息内容生态治理规定》等法律、行政法规和国家有关规定，制定本办法。

第二条 在中华人民共和国境内，通过互联网站、应用程序、小程序等，以视频直播、音频直播、图文直播或多种直播相结合等形式开展营销的商业活动，适用本办法。

本办法所称直播营销平台，是指在网络直播营销中提供直播服务的各类平台，包括互联网直播服务平台、互联网音视频服务平台、电子商务平台等。

本办法所称直播间运营者，是指在直播营销平台上注册账号或者通过自建网站等其他网络服务，开设直播间从事网络直播营销活动的个人、法人和其他组织。

本办法所称直播营销人员，是指在网络直播营销中直接向社会公众开展营销的个人。

本办法所称直播营销人员服务机构，是指为直播营销人员从事网络直播营

销活动提供策划、运营、经纪、培训等的专门机构。

从事网络直播营销活动，属于《中华人民共和国电子商务法》规定的“电子商务平台经营者”或“平台内经营者”定义的市场主体，应当依法履行相应的责任和义务。

第三条 从事网络直播营销活动，应当遵守法律法规，遵循公序良俗，遵守商业道德，坚持正确导向，弘扬社会主义核心价值观，营造良好网络生态。

第四条 国家网信部门和国务院公安、商务、文化和旅游、税务、市场监督管理、广播电视等有关主管部门建立健全线索移交、信息共享、会商研判、教育培训等工作机制，依据各自职责做好网络直播营销相关监督管理工作。

县级以上地方人民政府有关主管部门依据各自职责做好本行政区域内网络直播营销相关监督管理工作。

第二章 直播营销平台

第五条 直播营销平台应当依法依规履行备案手续，并按照有关规定开展安全评估。

从事网络直播营销活动，依法需要取得相关行政许可的，应当依法取得行政许可。

第六条 直播营销平台应当建立健全账号及直播营销功能注册注销、信息安全管理、营销行为规范、未成年人保护、消费者权益保护、个人信息保护、网络和数据安全管理等机制、措施。

直播营销平台应当配备与服务规模相适应的直播内容管理专业人员，具备维护互联网直播内容安全的技术能力，技术方案应符合国家相关标准。

第七条 直播营销平台应当依据相关法律法规和国家有关规定，制定并公开网络直播营销管理规则、平台公约。

直播营销平台应当与直播营销人员服务机构、直播间运营者签订协议，要求其规范直播营销人员招募、培训、管理流程，履行对直播营销内容、商品和服务的真实性、合法性审核义务。

直播营销平台应当制定直播营销商品和服务负面目录，列明法律法规规定的禁止生产销售、禁止网络交易、禁止商业推销宣传以及不适宜以直播形式营销的商品和服务类别。

第八条 直播营销平台应当对直播间运营者、直播营销人员进行基于身份证件信息、统一社会信用代码等真实身份信息认证，并依法依规向税务机关报送身份信息和其他涉税信息。直播营销平台应当采取必要措施保障处理的个人信息安全。

直播营销平台应当建立直播营销人员真实身份动态核验机制，在直播前核验所有直播营销人员身份信息，对与真实身份信息不符或按照国家有关规定不得从事网络直播发布的，不得为其提供直播发布服务。

第九条 直播营销平台应当加强网络直播营销信息内容管理，开展信息发布审核和实时巡查，发现违法和不良信息，应当立即采取处置措施，保存有关记录，并向有关主管部门报告。

直播营销平台应当加强直播间内链接、二维码等跳转服务的信息安全管理，防范信息安全风险。

第十条 直播营销平台应当建立健全风险识别模型，对涉嫌违法违规的高风险营销行为采取弹窗提示、违规警示、限制流量、暂停直播等措施。直播营销平台应当以显著方式警示用户平台外私下交易等行为的风险。

第十一条 直播营销平台提供付费导流等服务，对网络直播营销进行宣传、推广，构成商业广告的，应当履行广告发布者或者广告经营者的责任和义务。

直播营销平台不得为直播间运营者、直播营销人员虚假或者引人误解的商业宣传提供帮助、便利条件。

第十二条 直播营销平台应当建立健全未成年人保护机制，注重保护未成年人身心健康。网络直播营销中包含可能影响未成年人身心健康内容的，直播营销平台应当在信息展示前以显著方式作出提示。

第十三条 直播营销平台应当加强新技术新应用新功能上线和使用管理，对利用人工智能、数字视觉、虚拟现实、语音合成等技术展示的虚拟形象从事网络直播营销的，应当按照有关规定进行安全评估，并以显著方式予以标识。

第十四条 直播营销平台应当根据直播间运营者账号合规情况、关注和访问量、交易量和金额及其他指标维度，建立分级管理制度，根据级别确定服务范围及功能，对重点直播间运营者采取安排专人实时巡查、延长直播内容保存时间等措施。

直播营销平台应当对违反法律法规和服务协议的直播间运营者账号，视情采取警示提醒、限制功能、暂停发布、注销账号、禁止重新注册等处置措施，保存记录并向有关主管部门报告。

直播营销平台应当建立黑名单制度，将严重违法违规的直播营销人员及因违法失德造成恶劣社会影响的人员列入黑名单，并向有关主管部门报告。

第十五条 直播营销平台应当建立健全投诉、举报机制，明确处理流程和反馈期限，及时处理公众对于违法违规信息内容、营销行为投诉举报。

消费者通过直播间内链接、二维码等方式跳转到其他平台购买商品或者接受服务，发生争议时，相关直播营销平台应当积极协助消费者维护合法权益，提供必要的证据等支持。

第十六条 直播营销平台应当提示直播间运营者依法办理市场主体登记或税务登记，如实申报收入，依法履行纳税义务，并依法享受税收优惠。直播营销平台及直播营销人员服务机构应当依法履行代扣代缴义务。

第三章 直播间运营者和直播营销人员

第十七条 直播营销人员或者直播间运营者为自然人的，应当年满十六周岁；十六周岁以上的未成年人申请成为直播营销人员或者直播间运营者的，应当经监护人同意。

第十八条 直播间运营者、直播营销人员从事网络直播营销活动，应当遵守法律法规和国家有关规定，遵循社会公序良俗，真实、准确、全面地发布商品或服务信息，不得有下列行为：

(一)违反《网络信息内容生态治理规定》第六条、第七条规定的；

(二)发布虚假或者引人误解的信息，欺骗、误导用户；

(三)营销假冒伪劣、侵犯知识产权或不符合保障人身、财产安全要求的商品；

(四)虚构或者篡改交易、关注度、浏览量、点赞量等数据流量造假；

(五)知道或应当知道他人存在违法违规或高风险行为，仍为其推广、引流；

(六)骚扰、诋毁、谩骂及恐吓他人，侵害他人合法权益；

(七)传销、诈骗、赌博、贩卖违禁品及管制物品等；

(八)其他违反国家法律法规和有关规定的行为。

第十九条 直播间运营者、直播营销人员发布的直播内容构成商业广告的，应当履行广告发布者、广告经营者或者广告代言人的责任和义务。

第二十条 直播营销人员不得在涉及国家安全、公共安全、影响他人及社会正常生产生活秩序的场所从事网络直播营销活动。

直播间运营者、直播营销人员应当加强直播间管理，在下列重点环节的设置应当符合法律法规和国家有关规定，不得含有违法和不良信息，不得以暗示等方式误导用户：

(一)直播间运营者账号名称、头像、简介；

(二)直播间标题、封面；

(三)直播间布景、道具、商品展示；

(四)直播营销人员着装、形象；

(五)其他易引起用户关注的重点环节。

第二十一条 直播间运营者、直播营销人员应当依据平台服务协议做好语音和视频连线、评论、弹幕等互动内容的实时管理，不得以删除、屏蔽相关不利评价等方式欺骗、误导用户。

第二十二条 直播间运营者应当对商品和服务供应商的身份、地址、联系方式、行政许可、信用情况等信息进行核验，并留存相关记录备查。

第二十三条 直播间运营者、直播营销人员应当依法依规履行消费者权益保护责任和义务，不得故意拖延或者无正当理由拒绝消费者提出的合法合理要求。

第二十四条 直播间运营者、直播营销人员与直播营销人员服务机构合作开展商业合作的，应当与直播营销人员服务机构签订书面协议，明确信息安全管理、商品质量审核、消费者权益保护等义务并督促履行。

第二十五条 直播间运营者、直播营销人员使用其他人肖像作为虚拟形象从事网络直播营销活动的，应当征得肖像权人同意，不得利用信息技术手段伪造等方式侵害他人的肖像权。对自然人声音的保护，参照适用前述规定。

第四章 监督管理和法律责任

第二十六条 有关部门根据需要对直播营销平台履行主体责任情况开展监督

检查，对存在问题的平台开展专项检查。

直播营销平台对有关部门依法实施的监督检查，应当予以配合，不得拒绝、阻挠。直播营销平台应当为有关部门依法调查、侦查活动提供技术支持和协助。

第二十七条 有关部门加强对行业协会商会的指导，鼓励建立完善行业标准，开展法律法规宣传，推动行业自律。

第二十八条 违反本办法，给他人造成损害的，依法承担民事责任；构成犯罪的，依法追究刑事责任；尚不构成犯罪的，由网信等有关主管部门依据各自职责依照有关法律法规予以处理。

第二十九条 有关部门对严重违反法律法规的直播营销市场主体名单实施信息共享，依法开展联合惩戒。

第五章 附 则

第三十条 本办法自 2021 年 5 月 25 日起施行。

自然资源部关于促进智能网联汽车发展维护测绘地理信息安全的通知

自然资规〔2022〕1 号

各省、自治区、直辖市自然资源主管部门，新疆生产建设兵团自然资源局，陕西、黑龙江、四川、海南测绘地理信息局，有关汽车生产企业、网约车经营企业以及导航电子地图制作测绘资质单位：

当前，智能网联汽车(包括智能汽车、网约车、智能公交以及移动智能配送装置等)新业态迅猛发展，为方便出行、减少污染、改善交通提供了有效的解决方案，具有广阔的市场前景，同时其运行和服务高度依赖实时的高精度坐标、高清影像等数据支持。为统筹发展与安全，在守牢安全底线的前提下，积极扶持智能网联汽车新技术、新业态的发展，扩大内需、促进消费，现就测绘地理信息数据采集和管理等相关法律法规政策的适用与执行问题明确如下。

一、智能网联汽车安装或集成了卫星导航定位接收模块、惯性测量单元、摄像头、激光雷达等传感器后，在运行、服务和道路测试过程中对车辆及周边道路设施空间坐标、影像、点云及其属性信息等测绘地理信息数据进行采集、存储、传输和处理的行为，属于《中华人民共和国测绘法》规定的测绘活动，应当依照测绘法律法规政策进行规范和管理。

各类车载传感器以及智能网联汽车的制造、集成、销售等，不属于法定的测绘活动。

二、对智能网联汽车运行、服务和道路测试过程中产生的空间坐标、影像、点云及其属性信息等测绘地理信息数据进行收集、存储、传输和处理者，是测绘活动的行为主体，应遵守相关规定并依法承担相应责任。

从当前市场运行的情况看，数据的收集、存储、传输和处理者大多为车企、服务商及部分智能驾驶软件提供商，而仅获得辅助驾驶等服务的智能网联汽车驾乘人员，不属于有关测绘活动的行为人。

三、需要从事相关数据收集、存储、传输和处理的车企、服务商及智能驾驶软件提供商等，属于内资企业的，应依法取得相应测绘资质，或委托具有相应测绘资质的单位开展相应测绘活动；属于外商投资企业的，应委托具有相应测绘资质的单位开展相应测绘活动，由被委托的测绘资质单位承担收集、存储、传输和处理相关空间坐标、影像、点云及其属性信息等业务及提供地理信息服务与支持。

四、根据《外商投资准入特别管理措施(负面清单)(2021 年版)》的规定，地面移动测量、导航电子地图编制等属外资禁入领域。取得这些专业类别测绘资质的内资企业，应严格执行国家有关规定。

五、目前已在提供智能网联汽车售后和运营服务的企业，存在向境外传输相关空间坐标、影像、点云及其属性信息等测绘地理信息数据行为或计划的，应严格执行国家有关法律法规，依法履行对外提供审批或地图审核程序等，在此之前应停止数据境外传输行为。同时按照本通知第三条要求，尽快申办导航电子地图制作等测绘资质，或委托具有相应测绘资质的单位开展。

六、各级自然资源主管部门要积极创造条件，提升行政效率，为相关企业申办测绘资质、使用基础测绘成果、导航电子地图送审以及政策咨询等提供便利。按照《中华人民共和国测绘法》《中华人民共和国数据安全法》等法律法规规定，切实加强智能网联汽车新业态发展中涉及测绘活动及测绘地理信息数据的监督管理，强化与有关部门的协同与信息通报，依法查处有关违法违规行为，在维护国家安全的前提下，促进智能网联汽车产业发展。

自然资源部

2022 年 8 月 25 日

自然资源部关于印发《自然资源领域数据安全管理办法》的通知

自然资发〔2024〕57 号

各省、自治区、直辖市自然资源主管部门，新疆生产建设兵团自然资源局，上海市海洋局、福建省海洋与渔业局、山东省海洋局、广西壮族自治区海洋局，国家林业和草原局，中国地质调查局及部其他直属单位，各派出机构，部机关各司局：

经国家数据安全工作协调机制批准，部领导同意，现将《自然资源领域数据安全管理办法》印发给你们，请结合实际认真贯彻执行。

自然资源部

2024 年 3 月 22 日

自然资源领域数据安全管理办法

第一章 总 则

第一条 为规范自然资源领域数据处理活动，加强数据安全管理，保障数据安全，促进数据开发利用，保护个人、组织的合法权益，维护国家安全和发展利益，根据《中华人民共和国数据安全法》《中华人民共和国网络安全法》《中华人民共和国个人信息保护法》《中华人民共和国密码法》等法律法规，制定本办法。

第二条 在中华人民共和国境内开展的，或在境外履行自然资源部门职责过程中开展的自然资源领域非涉密数据处理活动及其安全监管，应当遵守相关法律法规和本办法的要求。

第三条 本办法所称自然资源领域数据，是指在开展自然资源活动中收集和产生的数据，主要包括基础地理信息、遥感影像等地理信息数据，土地、矿产、森林、草原、水、湿地、海域海岛等自然资源调查监测数据，总体规划、详细规划、专项规划等国土空间规划数据，用途管制、资产管理、耕地保护、生态修复、开发利用、不动产登记等自然资源管理数据。

本办法所称自然资源领域数据处理者(以下简称数据处理者)，是指开展自然资源领域数据处理活动的自然资源行业各类单位。

本办法所称数据安全，是指通过采取必要措施，确保数据处于有效保护和

合法利用的状态，以及具备保障持续安全状态的能力。

第四条 在国家数据安全工作协调机制统筹协调下，自然资源部承担自然资源行业、领域数据安全监管职责，负责督促指导各省、自治区、直辖市自然资源主管部门、海洋主管部门（以下统称地方行业监管部门）开展数据安全监管。国家林业和草原局具体承担森林草原、湿地荒漠等数据安全监管职责，参照本办法制定具体制度。

地方行业监管部门分别负责对本地区自然资源领域数据处理活动和安全保护进行监督管理。

自然资源部、国家林业和草原局及地方行业监管部门统称为行业监管部门。

行业监管部门将数据安全纳入党委（党组）国家安全责任制，按照“谁管业务，谁管数据，谁管数据安全”原则，落实本行业本地区本领域数据安全指导监管责任。

第五条 自然资源部、国家林业和草原局推进自然资源领域数据开发利用和数据安全标准体系建设，组织开展相关标准制修订及推广应用。

第六条 鼓励自然资源领域数据依法共享开放和开发利用，支持数据创新应用。积极构建数据开发利用和安全产业协调共进的发展模式，不断提升数据安全保障能力，维护国家安全、社会稳定、组织和个人权益。

第七条 支持开展经常性的自然资源领域数据安全宣传教育。采取多种方式培养数据开发利用技术和数据安全专业人才，促进人才交流。

第二章 数据分类分级管理

第八条 自然资源部组织制定自然资源领域数据分类分级、重要数据和核心数据识别认定、数据安全保护等标准规范，指导开展数据分类分级管理工作，编制行业重要数据和核心数据目录并实施动态管理。国家林业和草原局按照自然资源领域数据分类分级标准规范，结合工作需要编制林草领域数据安全标准规范，指导开展林草数据分类分级工作，编制林草重要数据和核心数据目录并实施动态管理。

地方行业监管部门按照自然资源领域数据分类分级标准规范，分别组织开展本地区自然资源领域数据分类分级管理及重要数据和核心数据识别审核工

作，编制本地区自然资源领域重要数据和核心数据目录，并上报自然资源部，目录发生变化的，应及时上报更新。

数据处理者应当定期按照自然资源领域数据分类分级标准规范梳理填报重要数据和核心数据目录。

第九条 根据行业特点和业务应用，自然资源领域数据分类类别包括但不限于地理信息、自然资源调查监测、国土空间规划、自然资源管理等，具体参照自然资源领域数据分类分级标准规范。

通过对自然资源领域数据重要性、精度、规模、安全风险，以及数据价值、可用性、可共享性、可开放性等进行综合分析，判断数据遭到篡改、破坏、泄露或者非法获取、非法利用后的影响对象、影响程度、影响范围进行分级，分为一般数据、重要数据、核心数据。

数据处理者可在此基础上细分数据的类别和一般数据级别。

第十条 核心数据是指对领域、群体、区域具有较高覆盖度或达到较高精度、较大规模、一定深度的重要数据，一旦被非法使用或共享，可能直接影响政治安全。核心数据主要包括关系国家安全重点领域的数据，关系国民经济命脉、重要民生和重大公共利益的数据，经国家有关部门评估确定的其他数据。

重要数据是指特定领域、特定群体、特定区域或达到一定精度和规模，一旦被泄露或篡改、损毁，可能直接危害国家安全、经济运行、社会稳定、公共健康和安全的数据。

一般数据是指除重要数据、核心数据以外的其他数据。

结合自然资源领域数据特点，满足以下两项(含)以上参考指标的为重要数据。

(一)支撑党中央和国务院赋予的“两统一”职责产生的具有不可替代性和行业唯一性的，一旦发生数据篡改、泄露或服务中断等安全事故，将影响自然资源部门履行职责，对全国范围内服务对象产生重要影响的数据。

(二)涉及国民经济和重要民生的，为其他行业、领域提供自然资源基础数据支撑的，一旦发生数据安全事故会对其他行业、领域造成重要影响的数据。

(三)覆盖多个省份甚至全国，规模大、精度高，且极具敏感性、重要性的数据。

(四)直接影响国家关键信息基础设施正常运行服务的数据。

(五)危害国家安全、国家经济竞争力、危害公众接受公共服务、危害公民生存条件和安定工作生活环境、危害公民的生命财产安全和其他合法利益、导致社会恐慌等的数据。

(六)我国法律法规及规范性文件规定的其他自然资源重要数据。

符合重要数据指标，且关系国家经济命脉、重要民生和重大公共利益、影响政治安全的数据为核心数据。

第十一条 自然资源部所属的数据处理者应当将本单位重要数据和核心数据目录向自然资源部报备，国家林业和草原局所属的数据处理者应当将本单位重要数据和核心数据目录向国家林业和草原局报备，其他数据处理者应当将本单位重要数据和核心数据目录向本地区行业监管部门报备。报备内容包括但不限于数据类别、级别、规模、精度、来源、载体、使用范围、对外共享、跨境传输、 安全情况及责任单位情况等，不包括数据内容本身。

地方行业监管部门应当在数据处理者提交报备申请后的二十个工作日内完成审核工作，报备内容符合要求的，报自然资源部审核认定，自然资源部接到申请后二十个工作日完成重要数据认定，核心数据须报国家数据安全工作协调机制认定；不符合要求的应当及时反馈申请单位并说明理由。申请单位应当在收到反馈后的十五个工作日内再次提交申请。

报备内容发生重大变化的，数据处理者应当在发生变化的三个月内履行变更手续。重大变化是指数据内容发生变化导致原有级别不再适用的，或某类重要数据和核心数据规模变化 30%以上的，等等。

第三章 数据全生命周期安全管理

第十二条 数据处理者应当对数据处理活动安全负主体责任，对各类数据实行分级防护，不同级别数据同时被处理且难以分别采取保护措施的，应当按照其中级别最高的要求实施保护，确保数据持续处于有效保护和合法利用的状态。

(一)建立数据安全管理制度，针对不同级别数据，制定数据全生命周期各环节的具体分级防护要求和操作规程。

(二)根据需要配备数据安全管理人员，统筹负责数据处理活动的安全监督

管理，协助行业监管部门开展工作。

(三)利用互联网等信息网络开展数据处理活动时，要落实网络安全等级保护、关键信息基础设施安全保护、密码保护和保密等制度要求。

(四)应当采取相应技术措施和其他必要措施保障数据安全，防范数据被篡改、破坏、泄露或者非法获取、非法利用等风险。

(五)合理确定数据处理活动的操作权限，严格实施人员权限管理。

(六)根据应对数据安全事件的需要，制定应急预案， 并开展应急演练。

(七)定期对从业人员开展数据安全知识和技能相关教育培训。

(八)法律法规等规定的其他措施。

重要数据和核心数据处理者，还应当：

(一)建立覆盖本单位相关部门的数据安全工作体系， 明确数据安全负责人和管理机构，建立常态化沟通与协作机制。本单位法定代表人或主要负责人是数据安全第一责任人，领导班子中分管数据安全的班子成员是直接责任人，其他成员对职责范围内的数据安全工作负领导责任，履行数据安全保护义务，接受监督。

(二)明确数据处理关键岗位和岗位职责，并要求关键岗位人员签署数据安全责任书，责任书内容包括但不限于数据安全岗位职责、义务、处罚措施、注意事项等内容。应当按照业务工作需要和最小授权原则，依据岗位职责设定数据处理权限，控制重要数据接触范围，人员变动时应及时调整权限。涉及核心数据的相关关键岗位人员、信息系统建设和运维单位等，提交公安机关、国家安全机关进行国家安全背景审查。

(三)建立内部登记、审批机制，对重要数据和核心数据的处理活动进行严格管理并留存记录不少于六个月。

(四)在数据全生命周期的各环节，应当综合运用加密、鉴权、认证、脱敏、校验、审计等技术手段进行安全保护，并按照法律法规和国家有关规定要求使用商用密码进行保护。

(五)涉重要数据信息系统建设、运维项目未经委托方批准不得转包、分包。建设运维人员未经委托方明确授权，不得处理委托方的重要数据。在提供涉重要数据信息系统建设、运维过程中收集、产生的数据，不得用于其他用

途，服务完成后按照与委托方约定处理或及时删除。

(六)应当加强人员和经费保障。

第十三条 数据处理者收集数据应当遵循合法、正当的原则，不得窃取或者以其他非法方式收集数据。法律法规对收集数据的目的、范围有规定的，应当在法律法规规定的目的和范围内收集。

数据收集过程中，应当根据数据安全级别采取相应的安全措施，加强重要数据和核心数据收集生产人员、设备的管理， 并对收集来源、时间、类型、数量、精度、区域、频度、流向等进行记录。

通过间接途径获取重要数据和核心数据的，数据处理者应当与数据提供方通过签署相关协议、承诺书等方式，明确双方法律责任。

第十四条 数据处理者应当依据法律法规规定的方式和期限存储数据，可以从物理和环境安全、网络和通信安全、设备和计算安全、应用和数据安全等方面，加强数据存储安全管控，保障存储数据的完整性、保密性、真实性和可用性。

存储重要数据的，要落实第三级及以上网络安全等级保护要求。存储核心数据的，要落实关键信息基础设施安全保护要求或第四级网络安全等级保护要求。

第十五条 数据处理者开展数据加工使用处理活动，应当采取访问控制、数据防泄露、操作审计等管控措施，确保过程安全、合规、可控、可溯源，防范数据关联挖掘、分析过程中有价值信息和个人隐私泄露的安全风险，明确数据使用加工过程中的相关责任，保证数据的正当加工使用。加工使用过程中，应当按照数据级别采取相应的措施保护数据的安全性，所使用的数据必须是真实可靠的，数据来源、收集过程须经过审查和核实。涉及利用数据进行自动化决策的，应当保证决策的透明度和结果公平合理。加工使用重要数据和核心数据，还应当实施严格的访问控制，建立数据可信可控、日志留存审计、风险监测评估、实时监控、应急处置、数据溯源等相关技术和管理机制。

第十六条 数据处理者应当根据传输的数据类型、级别和应用场景，制定安全策略并采取保护措施。传输重要数据和核心数据的，应当采取校验技术、密码技术、安全传输通道或者安全传输协议等措施。

第十七条 数据处理者应当按照有关规定安全有序提供数据，明确提供的范围、类别、条件、程序等，提供的数据应当限于实现数据接收方处理目的的最小范围，并告知数据接收方按照对应级别进行分类分级保护，采取必要的安全保护措施，涉及重要数据的，与数据接收方签订数据安全协议。重要数据在共享、调用过程中应当加强安全管控，采取技术措施定期监测数据共享、调用的情况，并配备风险隔离、认证鉴权、威胁告警等安全保护措施。涉及提供、共享核心数据的，应当采取必要的安全保护措施，并上报自然资源部，自本年度1月1日起可能累计达到总量30%及以上的，应当经自然资源部报国家数据安全工作协调机制组织风险评估。涉及国家机关依法履职或单位内部流动的除外。

第十八条 数据处理者应当在数据公开前分析研判可能对国家安全、公共利益产生的影响，存在显著负面影响或风险的，不得公开。政府机关部门应当遵守公正、公平、便民的原则，按照规定及时、准确地公开政务数据，依法不予公开的除外。

第十九条 数据处理者应当建立数据销毁制度，明确销毁对象、规则、流程和技术等要求，对销毁活动进行记录和留存。依据法律法规规定、合同约定等请求销毁的，数据处理者应当销毁相应数据。

销毁重要数据和核心数据的，要采取必要的安全保护措施，并事前向行业监管部门报告数据销毁方案。引起重要数据和核心数据目录变化的，应当及时向行业监管部门报备，不得以任何理由、任何方式对销毁数据进行恢复。

第二十条 数据处理者在中华人民共和国境内收集和产生的重要数据，应当在境内存储，确需向境外提供的，数据处理者应当落实国家网信部门数据出境安全评估有关规定。

第二十一条 数据处理者因重组等原因需要转移数据的，应当明确数据转移方案。涉及重要数据的，应当采取必要的安全保护措施，事前向行业监管部门报告数据转移方案。引起重要数据目录发生变化的，应当及时向行业监管部门报备。

第二十二条 数据处理者委托他人处理、与他人共同处理数据的，数据安全责任不因委托而改变，应当通过签订合同协议等方式，明确委托方与受托方的数据安全责任和义务。涉及重要数据的，委托方要把安全作为重要考虑因素，

应当对受托方的数据安全保护能力、资质进行评估或核实，经过严格的审批程序，明确受托方的数据处理权限和保护责任，并监督受托方履行数据安全保护义务。

除法律法规等另有规定外，未经委托方同意，受托方不得将数据提供给第三方。

第二十三条 数据处理者应当在数据全生命周期处理过程中，记录数据处理、权限管理、人员操作等日志，并采用商用密码技术保护日志的完整性。其中，一般数据的日志留存时间不少于六个月，涉及重要数据安全事件处置、溯源的，相关日志留存时间不少于一年；涉及向他人提供、委托处理、共同处理重要数据的，相关日志留存时间不少于三年。涉及核心数据安全事件处置、溯源的相关日志留存时间不少于三年。

第四章 数据安全监测预警与应急管理

第二十四条 自然资源部按照国家相关标准和流程，组织建立自然资源领域数据安全风险监测机制，建立自然资源领域数据安全风险监测预警体系，划分数据安全风险和事件等级，组织建设数据安全监测预警技术手段，形成监测、溯源、预警、处置等能力，与相关部门加强信息共享。国家林业和草原局组织建立林草数据安全风险监测预警机制，划分林草数据安全风险和事件等级，组织建设林草数据监测预警技术手段。

地方行业监管部门分别建设本地区数据安全监测预警机制，组织开展本地区自然资源领域数据安全风险监测，按照有关规定及时发布预警信息，通知本地区数据处理者及时采取应对措施。

数据处理者应当开展数据安全风险监测，及时排查安全隐患，采取必要的措施防范数据安全风险。

第二十五条 自然资源部组织指导开展自然资源领域数据安全风险评估等工作。国家林业和草原局组织指导开展林草数据安全风险评估等工作。

地方行业监管部门分别负责组织开展本地区自然资源领域数据安全风险评估工作。

重要数据处理者应当自行或委托第三方评估机构，每年对其数据处理活动至少开展一次风险评估，及时整改风险问题，并向行业监管部门报送风险评估

报告。风险评估报告应当包括处理的重要数据的类别、数量，开展数据处理活动的情况，面临的数据安全风险、应对措施及其有效程度等。数据处理者应当保留风险评估报告至少三年。核心数据处理者优先使用第三方评估机构开展风险评估。

数据处理者在组织重要数据安全风险评估时，应当对其数据查询、下载、修改、删除等重点操作的日志开展审计分析，发现违规或异常行为，应及时采取相应处置措施。

第二十六条　自然资源部组织建立自然资源领域数据安全风险信息通报机制，统一汇集、分析、研判、通报数据安全风险信息。国家林业和草原局组织建立林草数据安全风险信息通报机制。

地方行业监管部门分别汇总分析本地区自然资源领域数据安全风险，根据数据安全风险的发展态势、规模大小、关联程度、现实危害等综合研判，及时将可能造成重大及以上安全事件的风险向自然资源部报告。

数据处理者及时将可能造成较大及以上安全事件的风险向行业监管部门报告。

第二十七条　自然资源部组织制定自然资源领域数据安全事件应急预案，组织协调重要数据和核心数据安全事件应急处置工作。国家林业和草原局组织建立林草数据安全事件应急预案，组织协调重要数据和核心数据安全事件应急处置工作。

地方行业监管部门分别组织开展本地区自然资源领域数据安全事件应急处置工作。涉及重要数据和核心数据的安全事件，应当立即报自然资源部，并及时报告事件发展和处置情况。

数据处理者在数据安全事件发生后，应当按照应急预案，及时开展应急处置，涉及重要数据和核心数据的安全事件，第一时间向行业监管部门、属地公安部门报告，事件处置完成后在一周以内形成总结报告。每年向行业监管部门报告数据安全事件处置情况。

数据处理者对发生的可能损害用户合法权益的数据安全事件，应当及时告知用户，并提供减轻危害措施。

第五章　监督检查

第二十八条 行业监管部门对数据处理者落实数据分类分级保护及本办法要求的情况进行监督检查。数据处理者应当对行业监管部门监督检查予以配合。

第二十九条 在国家数据安全工作协调机制统一组织下，自然资源部依法配合有关部门，对影响或者可能影响国家安全的自然资源领域数据处理活动开展数据安全审查工作。

第三十条 数据处理者及其委托的数据安全风险评估机构工作人员对在履行职责中知悉的个人信息、商业秘密等，应当严格保密，不得泄露或者非法向他人提供。

第六章 法律责任

第三十一条 行业监管部门在履行数据安全监督管理职责中，发现数据处理活动存在较大安全风险的，可以按照规定权限和程序对数据处理者进行约谈，并要求采取措施进行整改，消除隐患。

第三十二条 对于违反有关规定的，依照《中华人民共和国数据安全法》及有关法律法规予以处理，根据情节严重程度给与相应行政处罚，构成犯罪的，依法追究刑事责任。

第七章 附 则

第三十三条 开展涉及个人信息的数据处理活动，还应当遵守有关法律法规的规定。

第三十四条 涉及国家秘密信息或自然资源领域数据汇聚关联后属于国家秘密事项的数据处理活动，应当符合国家及部相关保密规定。

第三十五条 法律法规规定开展数据处理活动应当取得行政许可的，数据处理者应当依法取得许可。

第三十六条 本办法由自然资源部负责解释。

第三十七条 本办法自印发之日起施行。

中国科学技术法学会关于公布团体标准《个人信息处理法律合规性评估指引》(T/CLAST 001-2021)第一次修订版本的公告

各有关单位：

《中华人民共和国个人信息保护法》于 2021 年 8 月 20 日通过， 自 2021 年 11 月 1 日起正式施行，成为保护个人信息权益、规范个人信息处理活动、促进

个人信息合理利用的专门性法律。为更好推动个人信息处理依法合规开展，在国家有关部门指导下，中国科学技术法学会于 2021 年 4 月 28 日公开发布团体标准《个人信息处理法律合规性评估指引》(T/CLAST 001-2021)，自 2021 年 6 月 6 日正式施行以来，受到社会各界广泛关注。

为符合《中华人民共和国个人信息保护法》有关规定，中国科学技术法学会大数据治理专业委员会组织有关人员对《个人信息处理法律合规性评估指引》进行修订，并于 2021 年 11 月 1 日向社会广泛征求意见。自征求意见公告发布以来，收到多家单位的修改建议，中国科学技术法学会大数据治理专业委员会组织有关人员对标《中华人民共和国个人信息保护法》有关规定，对收到的修改意见进行认真审阅。

经讨论修改后，最终形成《个人信息处理法律合规性评估指引》(T/CLAST 001-2021)第一次修订版文本，特此公告，第一次修订版将于 2022 年 1 月 1 日正式施行。

附件：个人信息处理法律合规性评估指引

中国科学技术法学会

2021 年 12 月 6 日

关于发布中国网络安全产业联盟技术规范《数据安全和个人信息保护社会责任指南》的通知

CCIA〔2022〕009 号

各会员单位：

现批准《数据安全和个人信息保护社会责任指南》为联盟技术规范，编号为 T/CCIA 002-2022，自 2023 年 2 月 1 日起实施。

附件：《数据安全和个人信息保护社会责任指南》(T/CCIA 002-2022)

中国网络安全产业联盟

2022 年 12 月 30 日

关于发布中国网络安全产业联盟技术规范《儿童智能手表个人信息和权益保护指南》的通知

CCIA〔2023〕007 号

各会员单位：

现批准《儿童智能手表个人信息和权益保护指南》为联盟技术规范，编号为 T/CCIA 003-2023，自 2024 年 3 月 31 日起实施

附件：《儿童智能手表个人信息和权益保护指南》(T/CCIA 003-2023)

中国网络安全产业联盟

2023 年 12 月 31 日

深圳市信息服务业区块链协会关于发布《数据安全合规评估方法》团体标准的公告

深链协〔2023〕第 001 号

各会员单位及相关企业：

依据《深圳市信息服务业区块链协会团体标准管理办法》的规定，《数据安全合规评估方法》团体标准已通过审批，自 2023 年 1 月 25 日起实施，现予以公告。

附件：数据安全合规评估方法

深圳市信息服务业区块链协会

2023 年 1 月 19 日

中国信通院 北京国际大数据交易联合发布《数据清洗、去标识化、匿名化业务规程(试行)》

为规范数据处理行为，激活数据要素市场，北京市经济和信息化局指导中国信息通信研究院产业与规划研究所、北京国际大数据交易所联合编制、发布国内首个系统梳理数据清洗、去标识化、匿名化处理相关流程方法的技术分析报告——《数据清洗、去标识化、匿名化业务规程(试行)》，以期为行业主体开展相关数据处理活动和相应测试评估提供参考，支撑数据共享、交易、开放等流通活动合规、有序进行。

附件：数据清洗、去标识化、匿名化业务规程(试行)

中国网络社会组织联合会发布《互联网弹窗信息推送服务要求》等 5 项团体标准的公告

各有关单位：

按照《中国网络社会组织联合会团体标准管理规定(暂行)》，《互联网弹窗信息推送服务要求》等 5 项团体标准已通过审查，现准予发布，编号如下：

1.《互联网弹窗信息推送服务要求》编号为 T/CFIS 0006—2023；

2.《互联网用户账号命名要求》编号为 T/CFIS 0007—2023；

3.《互联网企业 ESG 评估指南》编号为 T/CFIS 0008—2023；

4.《基于区块链的数据资产确权与交易规范》编号为 T/CFIS 0009—2023；

5.《元宇宙内容风险评估通则》编号为 T/CFIS 0010—2023。

中国网络社会组织联合会

2023 年 12 月 27 日

中国电子信息行业联合会关于发布《数据合规审计 指南》团体标准及编制说明的公告

电子联函〔2024〕9 号

为助力加快构建数据合规与治理生态，提升数据合规意识和风险防范能力，改进传统审计方法论应对数字经济和新兴技术的不足，以合规审计促进数据要素健康有序流通，为应用数据合规审计的各类组织提供通用的工作导则，促进数字经济健康发展和引导合规审计业务创新。我会组织相关单位联合编制了《数据合规审计 指南》团体标准及《编制说明》，并经过专家论证、公开意见征集等环节，现予以发布。各有关单位在团体标准执行过程中，如有意见或建议请及时与我会联系。

联系电话：010-68208088

邮箱：wangyanshan@citif.org.cn

附件：

1、《数据合规审计 指南》

2、《数据合规审计 指南》编制说明

中国电子信息行业联合会

2024 年 2 月 18 日

中国电子商会关于发布《生成式人工智能数据应用合规指南》团体标准的公告

各有关单位：

根据《中国电子商会团体标准工作管理办法》要求，现批准《生成式人工智能数据应用合规指南》为中国电子商会团体标准，编号为 T/CECC 027-2024，2024 年 5 月 1 日起实施。

特此公告。

附件：中国电子商会团体标准发布公告-生成式人工智能数据应用合规指南.pdf

中国电子商会

标准化工作委员会

2024 年 4 月 16 日

第十七章 人民法院

最高人民法院、最高人民检察院关于办理危害计算机信息系统安全刑事案件应用法律若干问题的解释

法释〔2011〕19 号

《最高人民法院、最高人民检察院关于办理危害计算机信息系统安全刑事案件应用法律若干问题的解释》已于 2011 年 6 月 20 日由最高人民法院审判委员会第 1524 次会议、2011 年 7 月 11 日由最高人民检察院第十一届检察委员会第 63 次会议通过，现予公布，自 2011 年 9 月 1 日起施行。

二〇一一年八月一日

最高人民法院、最高人民检察院

关于办理危害计算机信息系统安全刑事案件应用法律若干问题的解释

(2011 年 6 月 20 日最高人民法院审判委员会第 1524 次会议、2011 年 7 月 11 日最高人民检察院第十一届检察委员会第 63 次会议通过)

为依法惩治危害计算机信息系统安全的犯罪活动，根据《中华人民共和国刑法》、《全国人民代表大会常务委员会关于维护互联网安全的决定》的规定，现就办理这类刑事案件应用法律的若干问题解释如下：

第一条 非法获取计算机信息系统数据或者非法控制计算机信息系统，具有下列情形之一的，应当认定为刑法第二百八十五条第二款规定的“情节严重”：

(一)获取支付结算、证券交易、期货交易等网络金融服务的身份认证信息十组以上的;

(二)获取第(一)项以外的身份认证信息五百组以上的;

(三)非法控制计算机信息系统二十台以上的;

(四)违法所得五千元以上或者造成经济损失一万元以上的;

(五)其他情节严重的情形。

实施前款规定行为,具有下列情形之一的,应当认定为刑法第二百八十五条第二款规定的“情节特别严重”:

(一)数量或者数额达到前款第(一)项至第(四)项规定标准五倍以上的;

(二)其他情节特别严重的情形。

明知是他人非法控制的计算机信息系统,而对该计算机信息系统的控制权加以利用的,依照前两款的规定定罪处罚。

第二条 具有下列情形之一的程序、工具,应当认定为刑法第二百八十五条第三款规定的“专门用于侵入、非法控制计算机信息系统的程序、工具”:

(一)具有避开或者突破计算机信息系统安全保护措施,未经授权或者超越授权获取计算机信息系统数据的功能的;

(二)具有避开或者突破计算机信息系统安全保护措施,未经授权或者超越授权对计算机信息系统实施控制的功能的;

(三)其他专门设计用于侵入、非法控制计算机信息系统、非法获取计算机信息系统数据的程序、工具。

第三条 提供侵入、非法控制计算机信息系统的程序、工具, 具有下列情形之一的,应当认定为刑法第二百八十五条第三款规定的“情节严重”:

(一)提供能够用于非法获取支付结算、证券交易、期货交易等网络金融服务身份认证信息的专门性程序、工具五人次以上的;

(二)提供第(一)项以外的专门用于侵入、非法控制计算机信息系统的程序、工具二十人次以上的;

(三)明知他人实施非法获取支付结算、证券交易、期货交易等网络金融服务身份认证信息的违法犯罪行为而为其提供程序、工具五人次以上的;

(四)明知他人实施第(三)项以外的侵入、非法控制计算机信息系统的违法犯

罪行为而为其提供程序、工具二十人次以上的；

(五)违法所得五千元以上或者造成经济损失一万元以上的；

(六)其他情节严重的情形。

实施前款规定行为，具有下列情形之一的，应当认定为提供侵入、非法控制计算机信息系统的程序、工具“情节特别严重”：

(一)数量或者数额达到前款第(一)项至第(五)项规定标准五倍以上的；

(二)其他情节特别严重的情形。

第四条 破坏计算机信息系统功能、数据或者应用程序，具有下列情形之一的，应当认定为刑法第二百八十六条第一款和第二款规定的“后果严重”：

(一)造成十台以上计算机信息系统的主要软件或者硬件不能正常运行的；

(二)对二十台以上计算机信息系统中存储、处理或者传输的数据进行删除、修改、增加操作的；

(三)违法所得五千元以上或者造成经济损失一万元以上的；

(四)造成为一百台以上计算机信息系统提供域名解析、身份认证、计费等基础服务或者为一万以上用户提供服务的计算机信息系统不能正常运行累计一小时以上的；

(五)造成其他严重后果的。

实施前款规定行为，具有下列情形之一的，应当认定为破坏计算机信息系统“后果特别严重”：

(一)数量或者数额达到前款第(一)项至第(三)项规定标准五倍以上的；

(二)造成为五百台以上计算机信息系统提供域名解析、身份认证、计费等基础服务或者为五万以上用户提供服务的计算机信息系统不能正常运行累计一小时以上的；

(三)破坏国家机关或者金融、电信、交通、教育、医疗、能源等领域提供公共服务的计算机信息系统的功能、数据或者应用程序， 致使生产、生活受到严重影响或者造成恶劣社会影响的；

(四)造成其他特别严重后果的。

第五条 具有下列情形之一的程序，应当认定为刑法第二百八十六条第三款规定的“计算机病毒等破坏性程序”：

(一)能够通过网络、存储介质、文件等媒介， 将自身的部分、全部或者变种进行复制、传播，并破坏计算机系统功能、数据或者应用程序的；

(二)能够在预先设定条件下自动触发，并破坏计算机系统功能、数据或者应用程序的；

(三)其他专门设计用于破坏计算机系统功能、数据或者应用程序的程序。

第六条 故意制作、传播计算机病毒等破坏性程序，影响计算机系统正常运行，具有下列情形之一的，应当认定为刑法第二百八十六条第三款规定的“后果严重”：

(一)制作、提供、传输第五条第(一)项规定的程序，导致该程序通过网络、存储介质、文件等媒介传播的；

(二)造成二十台以上计算机系统被植入第五条第(二)、(三)项规定的程序的；

(三)提供计算机病毒等破坏性程序十人次以上的；

(四)违法所得五千元以上或者造成经济损失一万元以上的；

(五)造成其他严重后果的。

实施前款规定行为，具有下列情形之一的，应当认定为破坏计算机信息系统“后果特别严重”：

(一)制作、提供、传输第五条第(一)项规定的程序，导致该程序通过网络、存储介质、文件等媒介传播， 致使生产、生活受到严重影响或者造成恶劣社会影响的；

(二)数量或者数额达到前款第(二)项至第(四)项规定标准五倍以上的；

(三)造成其他特别严重后果的。

第七条 明知是非法获取计算机信息系统数据犯罪所获取的数据、非法控制计算机信息系统犯罪所获取的计算机信息系统控制权，而予以转移、收购、代为销售或者以其他方法掩饰、隐瞒， 违法所得五千元以上的，应当依照刑法第三百一十二条第一款的规定，以掩饰、隐瞒犯罪所得罪定罪处罚。

实施前款规定行为，违法所得五万元以上的，应当认定为刑法第三百一十二条第一款规定的“情节严重”。

单位实施第一款规定行为的，定罪量刑标准依照第一款、第二款的规定执行。

第八条 以单位名义或者单位形式实施危害计算机信息系统安全犯罪，达到

本解释规定的定罪量刑标准的，应当依照刑法第二百八十五条、第二百八十六条的规定追究直接负责的主管人员和其他直接责任人员的刑事责任。

第九条 明知他人实施刑法第二百八十五条、第二百八十六条规定的行为，具有下列情形之一的，应当认定为共同犯罪，依照刑法第二百八十五条、第二百八十六条的规定处罚：

(一)为其提供用于破坏计算机信息系统功能、数据或者应用程序的程序、工具，违法所得五千元以上或者提供十人次以上的；

(二)为其提供互联网接入、服务器托管、网络存储空间、通讯传输通道、费用结算、交易服务、广告服务、技术培训、技术支持等帮助， 违法所得五千元以上的；

(三)通过委托推广软件、投放广告等方式向其提供资金五千元以上的。

实施前款规定行为，数量或者数额达到前款规定标准五倍以上的，应当认定为刑法第二百八十五条、第二百八十六条规定的“情节特别严重”或者“后果特别严重”。

第十条 对于是否属于刑法第二百八十五条、第二百八十六条规定的“ 国家事务、国防建设、尖端科学技术领域的计算机信息系统”、“专门用于侵入、非法控制计算机信息系统的程序、工具”、“计算机病毒等破坏性程序”难以确定的，应当委托省级以上负责计算机信息系统安全保护管理工作的部门检验。司法机关根据检验结论，并结合案件具体情况认定。

第十一条 本解释所称“计算机信息系统”和“计算机系统”，是指具备自动处理数据功能的系统，包括计算机、网络设备、通信设备、自动化控制设备等。

本解释所称“身份认证信息”，是指用于确认用户在计算机信息系统上操作权限的数据，包括账号、口令、密码、数字证书等。

本解释所称“经济损失”，包括危害计算机信息系统犯罪行为给用户直接造成的经济损失，以及用户为恢复数据、功能而支出的必要费用。

最高人民法院关于审理侵害信息网络传播权民事纠纷案件适用法律若干问题的规定

(2012 年 11 月 26 日由最高人民法院审判委员会第 1561 次会议通过，根据 2020 年 12 月 23 日最高人民法院审判委员会第 1823 次会议通过的《最高人民法院关

于修改〈最高人民法院关于审理侵犯专利权纠纷案件应用法律若干问题的解释(二)〉等十八件知识产权类司法解释的决定》修正)

为正确审理侵害信息网络传播权民事纠纷案件，依法保护信息网络传播权，促进信息网络产业健康发展，维护公共利益，根据《中华人民共和国民法典》《中华人民共和国著作权法》《中华人民共和国民事诉讼法》等有关法律规定，结合审判实际，制定本规定。

第一条 人民法院审理侵害信息网络传播权民事纠纷案件，在依法行使裁量权时，应当兼顾权利人、网络服务提供者和社会公众的利益。

第二条 本规定所称信息网络，包括以计算机、电视机、固定电话机、移动电话机等电子设备为终端的计算机互联网、广播电视网、固定通信网、移动通信网等信息网络，以及向公众开放的局域网络。

第三条 网络用户、网络服务提供者未经许可，通过信息网络提供权利人享有信息网络传播权的作品、表演、录音录像制品，除法律、行政法规另有规定外，人民法院应当认定其构成侵害信息网络传播权行为。

通过上传到网络服务器、设置共享文件或者利用文件分享软件等方式， 将作品、表演、录音录像制品置于信息网络中， 使公众能够在个人选定的时间和地点以下载、浏览或者其他方式获得的， 人民法院应当认定其实施了前款规定的提供行为。

第四条 有证据证明网络服务提供者与他人以分工合作等方式共同提供作品、表演、录音录像制品，构成共同侵权行为的，人民法院应当判令其承担连带责任。网络服务提供者能够证明其仅提供自动接入、自动传输、信息存储空间、搜索、链接、文件分享技术等网络服务， 主张其不构成共同侵权行为的，人民法院应予支持。

第五条 网络服务提供者以提供网页快照、缩略图等方式实质替代其他网络服务提供者向公众提供相关作品的，人民法院应当认定其构成提供行为。

前款规定的提供行为不影响相关作品的正常使用，且未不合理损害权利人对该作品的合法权益，网络服务提供者主张其未侵害信息网络传播权的，人民法院应予支持。

第六条 原告有初步证据证明网络服务提供者提供了相关作品、表演、录音

录像制品，但网络服务提供者能够证明其仅提供网络服务，且无过错的，人民法院不应认定为构成侵权。

第七条 网络服务提供者在提供网络服务时教唆或者帮助网络用户实施侵害信息网络传播权行为的，人民法院应当判令其承担侵权责任。

网络服务提供者以言语、推介技术支持、奖励积分等方式诱导、鼓励网络用户实施侵害信息网络传播权行为的，人民法院应当认定其构成教唆侵权行为。

网络服务提供者明知或者应知网络用户利用网络服务侵害信息网络传播权，未采取删除、屏蔽、断开链接等必要措施， 或者提供技术支持等帮助行为的，人民法院应当认定其构成帮助侵权行为。

第八条 人民法院应当根据网络服务提供者的过错，确定其是否承担教唆、帮助侵权责任。网络服务提供者的过错包括对于网络用户侵害信息网络传播权行为的明知或者应知。

网络服务提供者未对网络用户侵害信息网络传播权的行为主动进行审查的，人民法院不应据此认定其具有过错。

网络服务提供者能够证明已采取合理、有效的技术措施， 仍难以发现网络用户侵害信息网络传播权行为的，人民法院应当认定其不具有过错。

第九条 人民法院应当根据网络用户侵害信息网络传播权的具体事实是否明显，综合考虑以下因素，认定网络服务提供者是否构成应知：

(一)基于网络服务提供者提供服务的性质、方式及其引发侵权的可能性大小，应当具备的管理信息的能力；

(二)传播的作品、表演、录音录像制品的类型、知名度及侵权信息的明显程度；

(三)网络服务提供者是否主动对作品、表演、录音录像制品进行了选择、编辑、修改、推荐等；

(四)网络服务提供者是否积极采取了预防侵权的合理措施；

(五)网络服务提供者是否设置便捷程序接收侵权通知并及时对侵权通知作出合理的反应；

(六)网络服务提供者是否针对同一网络用户的重复侵权行为采取了相应的合理措施；

(七)其他相关因素。

第十条 网络服务提供者在提供网络服务时，对热播影视作品等以设置榜单、目录、索引、描述性段落、内容简介等方式进行推荐， 且公众可以在其网页上直接以下载、浏览或者其他方式获得的， 人民法院可以认定其应知网络用户侵害信息网络传播权。

第十一条 网络服务提供者从网络用户提供的作品、表演、录音录像制品中直接获得经济利益的，人民法院应当认定其对该网络用户侵害信息网络传播权的行为负有较高的注意义务。

网络服务提供者针对特定作品、表演、录音录像制品投放广告获取收益， 或者获取与其传播的作品、表演、录音录像制品存在其他特定联系的经济利益， 应当认定为前款规定的直接获得经济利益。网络服务提供者因提供网络服务而收取一般性广告费、服务费等，不属于本款规定的情形。

第十二条 有下列情形之一的，人民法院可以根据案件具体情况，认定提供信息存储空间服务的网络服务提供者应知网络用户侵害信息网络传播权：

(一)将热播影视作品等置于首页或者其他主要页面等能够为网络服务提供者明显感知的位置的；

(二)对热播影视作品等的主题、内容主动进行选择、编辑、整理、推荐，或者为其设立专门的排行榜的；

(三)其他可以明显感知相关作品、表演、录音录像制品为未经许可提供， 仍未采取合理措施的情形。

第十三条 网络服务提供者接到权利人以书信、传真、电子邮件等方式提交的通知及构成侵权的初步证据，未及时根据初步证据和服务类型采取必要措施的，人民法院应当认定其明知相关侵害信息网络传播权行为。

第十四条 人民法院认定网络服务提供者转送通知、采取必要措施是否及时，应当根据权利人提交通知的形式，通知的准确程度，采取措施的难易程度，网络服务的性质，所涉作品、表演、录音录像制品的类型、知名度、数量等因素综合判断。

第十五条 侵害信息网络传播权民事纠纷案件由侵权行为地或者被告住所地人民法院管辖。侵权行为地包括实施被诉侵权行为的网络服务器、计算机终端等

设备所在地。侵权行为地和被告住所地均难以确定或者在境外的，原告发现侵权内容的计算机终端等设备所在地可以视为侵权行为地。

第十六条 本规定施行之日起，《最高人民法院关于审理涉及计算机网络著作权纠纷案件适用法律若干问题的解释》（法释〔2006〕11 号）同时废止。

本规定施行之后尚未终审的侵害信息网络传播权民事纠纷案件，适用本规定。本规定施行前已经终审，当事人申请再审或者按照审判监督程序决定再审的，不适用本规定。

最高人民法院、最高人民检察院关于办理利用信息网络实施诽谤等刑事案件适用法律若干问题的解释

法释〔2013〕21 号

《最高人民法院、最高人民检察院关于办理利用信息网络实施诽谤等刑事案件适用法律若干问题的解释》已于 2013 年 9 月 5 日由最高人民法院审判委员会第 1589 次会议、2013 年 9 月 2 日由最高人民检察院第十二届检察委员会第 9 次会议通过，现予公布，自 2013 年 9 月 10 日起施行。

最高人民法院 最高人民检察院

2013 年 9 月 6 日

最高人民法院、最高人民检察院

关于办理利用信息网络实施诽谤等刑事案件适用法律若干问题的解释

为保护公民、法人和其他组织的合法权益，维护社会秩序，根据《中华人民共和国刑法》《全国人民代表大会常务委员会关于维护互联网安全的决定》等规定，对办理利用信息网络实施诽谤、寻衅滋事、敲诈勒索、非法经营等刑事案件适用法律的若干问题解释如下：

第一条 具有下列情形之一的，应当认定为刑法第二百四十六条第一款规定的“捏造事实诽谤他人”：

（一）捏造损害他人名誉的事实，在信息网络上散布，或者组织、指使人员在信息网络上散布的；

（二）将信息网络上涉及他人的原始信息内容篡改为损害他人名誉的事实，在信息网络上散布，或者组织、指使人员在信息网络上散布的；

明知是捏造的损害他人名誉的事实，在信息网络上散布，情节恶劣的，以“捏

造事实诽谤他人”论。

第二条 利用信息网络诽谤他人，具有下列情形之一的，应当认定为刑法第二百四十六条第一款规定的“情节严重”：

(一)同一诽谤信息实际被点击、浏览次数达到五千次以上， 或者被转发次数达到五百次以上的；

(二)造成被害人或者其近亲属精神失常、自残、自杀等严重后果的；

(三)二年内曾因诽谤受过行政处罚，又诽谤他人的；

(四)其他情节严重的情形。

第三条 利用信息网络诽谤他人，具有下列情形之一的，应当认定为刑法第二百四十六条第二款规定的“严重危害社会秩序和国家利益”：

(一)引发群体性事件的；

(二)引发公共秩序混乱的；

(三)引发民族、宗教冲突的；

(四)诽谤多人，造成恶劣社会影响的；

(五)损害国家形象，严重危害国家利益的；

(六)造成恶劣国际影响的；

(七)其他严重危害社会秩序和国家利益的情形。

第四条 一年内多次实施利用信息网络诽谤他人行为未经处理，诽谤信息实际被点击、浏览、转发次数累计计算构成犯罪的，应当依法定罪处罚。

第五条 利用信息网络辱骂、恐吓他人，情节恶劣，破坏社会秩序的，依照刑法第二百九十三条第一款第(二)项的规定，以寻衅滋事罪定罪处罚。

编造虚假信息，或者明知是编造的虚假信息，在信息网络上散布，或者组织、指使人员在信息网络上散布，起哄闹事，造成公共秩序严重混乱的，依照刑法第二百九十三条第一款第(四)项的规定，以寻衅滋事罪定罪处罚。

第六条 以在信息网络上发布、删除等方式处理网络信息为由，威胁、要挟他人，索取公私财物，数额较大，或者多次实施上述行为的，依照刑法第二百七十四条的规定，以敲诈勒索罪定罪处罚。

第七条 违反国家规定，以营利为目的，通过信息网络有偿提供删除信息服务，或者明知是虚假信息，通过信息网络有偿提供发布信息等服务，扰乱市场秩

序，具有下列情形之一的，属于非法经营行为“情节严重”，依照刑法第二百二十五条第(四)项的规定，以非法经营罪定罪处罚：

(一)个人非法经营数额在五万元以上，或者违法所得数额在二万元以上的；

(二)单位非法经营数额在十五万元以上，或者违法所得数额在五万元以上的。

实施前款规定的行为，数额达到前款规定的数额五倍以上的，应当认定为刑法第二百二十五条规定的“情节特别严重”。

第八条 明知他人利用信息网络实施诽谤、寻衅滋事、敲诈勒索、非法经营等犯罪，为其提供资金、场所、技术支持等帮助的，以共同犯罪论处。

第九条 利用信息网络实施诽谤、寻衅滋事、敲诈勒索、非法经营犯罪，同时又构成刑法第二百二十一条规定的损害商业信誉、商品声誉罪， 第二百七十八条规定的煽动暴力抗拒法律实施罪，第二百九十一条之一规定的编造、故意传播虚假恐怖信息罪等犯罪的，依照处罚较重的规定定罪处罚。

第十条 本解释所称信息网络，包括以计算机、电视机、固定电话机、移动电话机等电子设备为终端的计算机互联网、广播电视网、固定通信网、移动通信网等信息网络，以及向公众开放的局域网络。

最高人民法院、最高人民检察院、公安部关于办理网络犯罪案件适用刑事诉讼程序若干问题的意见

公通字〔2014〕10 号

各省、自治区、直辖市高级人民法院，人民检察院，公安厅、局， 新疆维吾尔自治区高级人民法院生产建设兵团分院，新疆生产建设兵团人民检察院、公安局：

为解决近年来公安机关、人民检察院、人民法院在办理网络犯罪案件中遇到的新情况、新问题， 依法惩治网络犯罪活动，根据《中华人民共和国刑法》、《中华人民共和国刑事诉讼法》及有关司法解释的规定，结合侦查、起诉、审判实践，现就办理网络犯罪案件适用刑事诉讼程序问题提出以下意见：

一、关于网络犯罪案件的范围

1、本意见所称网络犯罪案件包括：

(1)危害计算机信息系统安全犯罪案件；

(2)通过危害计算机信息系统安全实施的盗窃、诈骗、敲诈勒索等犯罪案件；

(3)在网络上发布信息或者设立主要用于实施犯罪活动的网站、通讯群组，

针对或者组织、教唆、帮助不特定多数人实施的犯罪案件；

(4)主要犯罪行为在网络上实施的其他案件。

二、关于网络犯罪案件的管辖

2、网络犯罪案件由犯罪地公安机关立案侦查。必要时，可以由犯罪嫌疑人居住地公安机关立案侦查。

网络犯罪案件的犯罪地包括用于实施犯罪行为的网站服务器所在地，网络接入地，网站建立者、管理者所在地，被侵害的计算机信息系统或其管理者所在地，犯罪嫌疑人、被害人使用的计算机信息系统所在地， 被害人被侵害时所在地，以及被害人财产遭受损失地等。

涉及多个环节的网络犯罪案件，犯罪嫌疑人为网络犯罪提供帮助的，其犯罪地或者居住地公安机关可以立案侦查。

3、有多个犯罪地的网络犯罪案件，由最初受理的公安机关或者主要犯罪地公安机关立案侦查。有争议的，按照有利于查清犯罪事实、有利于诉讼的原则，由共同上级公安机关指定有关公安机关立案侦查。需要提请批准逮捕、移送审查起诉、提起公诉的，由该公安机关所在地的人民检察院、人民法院受理。

4、具有下列情形之一的，有关公安机关可以在其职责范围内并案侦查，需要提请批准逮捕、移送审查起诉、提起公诉的， 由该公安机关所在地的人民检察院、人民法院受理：

(1)一人犯数罪的；

(2)共同犯罪的；

(3)共同犯罪的犯罪嫌疑人、被告人还实施其他犯罪的；

(4)多个犯罪嫌疑人、被告人实施的犯罪存在关联，并案处理有利于查明案件事实的。

5、对因网络交易、技术支持、资金支付结算等关系形成多层级链条、跨区域的网络犯罪案件，共同上级公安机关可以按照有利于查清犯罪事实、有利于诉讼的原则，指定有关公安机关一并立案侦查，需要提请批准逮捕、移送审查起诉、提起公诉的，由该公安机关所在地的人民检察院、人民法院受理。

6、具有特殊情况，由异地公安机关立案侦查更有利于查清犯罪事实、保证案件公正处理的跨省(自治区、直辖市)重大网络犯罪案件，可以由公安部商最高

人民检察院和最高人民法院指定管辖。

7、人民检察院对于公安机关移送审查起诉的网络犯罪案件，发现犯罪嫌疑人还有犯罪被其他公安机关立案侦查的，应当通知移送审查起诉的公安机关。

人民法院受理案件后，发现被告人还有犯罪被其他公安机关立案侦查的，可以建议人民检察院补充侦查。人民检察院经审查， 认为需要补充侦查的，应当通知移送审查起诉的公安机关。

经人民检察院通知，有关公安机关根据案件具体情况，可以对犯罪嫌疑人所犯其他犯罪并案侦查。

8、为保证及时结案，避免超期羁押，人民检察院对于公安机关提请批准逮捕、移送审查起诉的网络犯罪案件， 第一审人民法院对于已经受理的网络犯罪案件，经审查发现没有管辖权的，可以依法报请共同上级人民检察院、人民法院指定管辖。

9、部分犯罪嫌疑人在逃，但不影响对已到案共同犯罪嫌疑人、被告人的犯罪事实认定的网络犯罪案件，可以依法先行追究已到案共同犯罪嫌疑人、被告人的刑事责任。在逃的共同犯罪嫌疑人、被告人归案后， 可以由原公安机关、人民检察院、人民法院管辖其所涉及的案件。

三、关于网络犯罪案件的初查

10、对接受的案件或者发现的犯罪线索， 在审查中发现案件事实或者线索不明，需要经过调查才能够确认是否达到犯罪追诉标准的，经办案部门负责人批准，可以进行初查。初查过程中， 可以采取询问、查询、勘验、检查、鉴定、调取证据材料等不限制初查对象人身、财产权利的措施， 但不得对初查对象采取强制措施和查封、扣押、冻结财产。

四、关于网络犯罪案件的跨地域取证

11、公安机关跨地域调查取证的， 可以将办案协作函和相关法律文书及凭证电传或者通过公安机关信息化系统传输至协作地公安机关。协作地公安机关经审查确认，在传来的法律文书上加盖本地公安机关印章后，可以代为调查取证。

12、询(讯)问异地证人、被害人以及与案件有关联的犯罪嫌疑人的， 可以由办案地公安机关通过远程网络视频等方式进行询(讯)问并制作笔录。

远程询(讯)问的，应当由协作地公安机关事先核实被询(讯)问人的身份。办

案地公安机关应当将询(讯)问笔录传输至协作地公安机关。询(讯)问笔录经被询(讯)问人确认并逐页签名、捺指印后，由协作地公安机关协作人员签名或者盖章，并将原件提供给办案地公安机关。询(讯)问人员收到笔录后，应当在首页右上方写明“于某年某月某日收到”，并签名或者盖章。

远程询(讯)问的，应当对询(讯)问过程进行录音录像，并随案移送。

异地证人、被害人以及与案件有关联的犯罪嫌疑人亲笔书写证词、供词的，参照本条第二款规定执行。

五、关于电子数据的取证与审查

13、收集、提取电子数据， 应当由二名以上具备相关专业知识的侦查人员进行。取证设备和过程应当符合相关技术标准， 并保证所收集、提取的电子数据的完整性、客观性。

14、收集、提取电子数据， 能够获取原始存储介质的，应当封存原始存储介质，并制作笔录，记录原始存储介质的封存状态，由侦查人员、原始存储介质持有人签名或者盖章；持有人无法签名或者拒绝签名的，应当在笔录中注明，由见证人签名或者盖章。有条件的，侦查人员应当对相关活动进行录像。

15、具有下列情形之一，无法获取原始存储介质的，可以提取电子数据，但应当在笔录中注明不能获取原始存储介质的原因、原始存储介质的存放地点等情况，并由侦查人员、电子数据持有人、提供人签名或者盖章； 持有人、提供人无法签名或者拒绝签名的，应当在笔录中注明，由见证人签名或者盖章；有条件的，侦查人员应当对相关活动进行录像：

(1)原始存储介质不便封存的；

(2)提取计算机内存存储的数据、网络传输的数据等不是存储在存储介质上的电子数据的；

(3)原始存储介质位于境外的；

(4)其他无法获取原始存储介质的情形。

16、收集、提取电子数据应当制作笔录，记录案由、对象、内容， 收集、提取电子数据的时间、地点、方法、过程， 电子数据的清单、规格、类别、文件格式、完整性校验值等， 并由收集、提取电子数据的侦查人员签名或者盖章。远程提取电子数据的，应当说明原因，有条件的，应当对相关活动进行录像。通过数

据恢复、破解等方式获取被删除、隐藏或者加密的电子数据的， 应当对恢复、破解过程和方法作出说明。

17、收集、提取的原始存储介质或者电子数据，应当以封存状态随案移送，并制作电子数据的复制件一并移送。对文档、图片、网页等可以直接展示的电子数据，可以不随案移送电子数据打印件，但应当附有展示方法说明和展示工具；人民法院、人民检察院因设备等条件限制无法直接展示电子数据的， 公安机关应当随案移送打印件。

对侵入、非法控制计算机信息系统的程序、工具以及计算机病毒等无法直接展示的电子数据，应当附有电子数据属性、功能等情况的说明。

对数据统计数量、数据同一性等问题，公安机关应当出具说明。

18、对电子数据涉及的专门性问题难以确定的， 由司法鉴定机构出具鉴定意见，或者由公安部指定的机构出具检验报告。

六、关于网络犯罪案件的其他问题

19、采取技术侦查措施收集的材料作为证据使用的， 应当随案移送批准采取技术侦查措施的法律文书和所收集的证据材料。使用有关证据材料可能危及有关人员的人身安全，或者可能产生其他严重后果的，应当采取不暴露有关人员身份、技术方法等保护措施，必要时，可以由审判人员在庭外进行核实。

20、对针对或者组织、教唆、帮助不特定多数人实施的网络犯罪案件， 确因客观条件限制无法逐一收集相关言词证据的，可以根据记录被害人数、被侵害的计算机信息系统数量、涉案资金数额等犯罪事实的电子数据、书证等证据材料，在慎重审查被告人及其辩护人所提辩解、辩护意见的基础上，综合全案证据材料，对相关犯罪事实作出认定。

最高人民法院

最高人民检察院

公安部

二〇一四年五月四日

最高人民法院关于审理利用信息网络侵害人身权益民事纠纷案件适用法律若干问题的规定

（2014 年 6 月 23 日由最高人民法院审判委员会第 1621 次会议通过，根据 2020

年 12 月 23 日最高人民法院审判委员会第 1823 次会议通过的《最高人民法院关于修改〈最高人民法院关于在民事审判工作中适用《中华人民共和国工会法》若干问题的解释〉等二十七件民事类司法解释的决定》修正)

为正确审理利用信息网络侵害人身权益民事纠纷案件，根据《中华人民共和国民法典》《全国人民代表大会常务委员会关于加强网络信息保护的决定》《中华人民共和国民事诉讼法》等法律的规定，结合审判实践，制定本规定。

第一条 本规定所称的利用信息网络侵害人身权益民事纠纷案件，是指利用信息网络侵害他人姓名权、名称权、名誉权、荣誉权、肖像权、隐私权等人身权益引起的纠纷案件。

第二条 原告依据民法典第一千一百九十五条、第一千一百九十七条的规定起诉网络用户或者网络服务提供者的，人民法院应予受理。

原告仅起诉网络用户，网络用户请求追加涉嫌侵权的网络服务提供者为共同被告或者第三人的，人民法院应予准许。

原告仅起诉网络服务提供者，网络服务提供者请求追加可以确定的网络用户为共同被告或者第三人的，人民法院应予准许。

第三条 原告起诉网络服务提供者，网络服务提供者以涉嫌侵权的信息系网络用户发布为由抗辩的，人民法院可以根据原告的请求及案件的具体情况，责令网络服务提供者向人民法院提供能够确定涉嫌侵权的网络用户的姓名(名称)、联系方式、网络地址等信息。

网络服务提供者无正当理由拒不提供的，人民法院可以依据民事诉讼法第一百一十四条的规定对网络服务提供者采取处罚等措施。

原告根据网络服务提供者提供的信息请求追加网络用户为被告的，人民法院应予准许。

第四条 人民法院适用民法典第一千一百九十五条第二款的规定，认定网络服务提供者采取的删除、屏蔽、断开链接等必要措施是否及时，应当根据网络服务的类型和性质、有效通知的形式和准确程度、网络信息侵害权益的类型和程度等因素综合判断。

第五条 其发布的信息被采取删除、屏蔽、断开链接等措施的网络用户，主张网络服务提供者承担违约责任或者侵权责任，网络服务提供者以收到民法典

第一千一百九十五条第一款规定的有效通知为由抗辩的，人民法院应予支持。

第六条 人民法院依据民法典第一千一百九十七条认定网络服务提供者是否“知道或者应当知道”，应当综合考虑下列因素：

(一)网络服务提供者是否以人工或者自动方式对侵权网络信息以推荐、排名、选择、编辑、整理、修改等方式作出处理；

(二)网络服务提供者应当具备的管理信息的能力，以及所提供服务的性质、方式及其引发侵权的可能性大小；

(三)该网络信息侵害人身权益的类型及明显程度；

(四)该网络信息的社会影响程度或者一定时间内的浏览量；

(五)网络服务提供者采取预防侵权措施的技术可能性及其是否采取了相应的合理措施；

(六)网络服务提供者是否针对同一网络用户的重复侵权行为或者同一侵权信息采取了相应的合理措施；

(七)与本案相关的其他因素。

第七条 人民法院认定网络用户或者网络服务提供者转载网络信息行为的过错及其程度，应当综合以下因素：

(一)转载主体所承担的与其性质、影响范围相适应的注意义务；

(二)所转载信息侵害他人人身权益的明显程度；

(三)对所转载信息是否作出实质性修改，是否添加或者修改文章标题，导致其与内容严重不符以及误导公众的可能性。

第八条 网络用户或者网络服务提供者采取诽谤、诋毁等手段，损害公众对经营主体的信赖，降低其产品或者服务的社会评价，经营主体请求网络用户或者网络服务提供者承担侵权责任的，人民法院应依法予以支持。

第九条 网络用户或者网络服务提供者，根据国家机关依职权制作的文书和公开实施的职权行为等信息来源所发布的信息，有下列情形之一，侵害他人人身权益，被侵权人请求侵权人承担侵权责任的，人民法院应予支持：

(一)网络用户或者网络服务提供者发布的信息与前述信息来源内容不符；

(二)网络用户或者网络服务提供者以添加侮辱性内容、诽谤性信息、不当标题或者通过增删信息、调整结构、改变顺序等方式致人误解；

(三)前述信息来源已被公开更正，但网络用户拒绝更正或者网络服务提供者不予更正；

(四)前述信息来源已被公开更正，网络用户或者网络服务提供者仍然发布更正之前的信息。

第十条 被侵权人与构成侵权的网络用户或者网络服务提供者达成一方支付报酬，另一方提供删除、屏蔽、断开链接等服务的协议，人民法院应认定为无效。

擅自篡改、删除、屏蔽特定网络信息或者以断开链接的方式阻止他人获取网络信息，发布该信息的网络用户或者网络服务提供者请求侵权人承担侵权责任的，人民法院应予支持。接受他人委托实施该行为的，委托人与受托人承担连带责任。

第十一条 网络用户或者网络服务提供者侵害他人人身权益，造成财产损失或者严重精神损害，被侵权人依据民法典第一千一百八十二条和第一千一百八十三条的规定，请求其承担赔偿责任的，人民法院应予支持。

第十二条 被侵权人为制止侵权行为所支付的合理开支，可以认定为民法典第一千一百八十二条规定的财产损失。合理开支包括被侵权人或者委托代理人对侵权行为进行调查、取证的合理费用。人民法院根据当事人的请求和具体案情，可以将符合国家有关部门规定的律师费用计算在赔偿范围内。

被侵权人因人身权益受侵害造成的财产损失以及侵权人因此获得的利益难以确定的，人民法院可以根据具体案情在 50 万元以下的范围内确定赔偿数额。

第十三条 本规定施行后人民法院正在审理的一审、二审案件适用本规定。

本规定施行前已经终审，本规定施行后当事人申请再审或者按照审判监督程序决定再审的案件，不适用本规定。

最高人民法院、最高人民检察院关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释

法释〔2017〕10 号

《最高人民法院、最高人民检察院关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释》已于 2017 年 3 月 20 日由最高人民法院审判委员会第 1712 次会议、2017 年 4 月 26 日由最高人民检察院第十二届检察委员会第 63 次会议

通过，现予公布，自 2017 年 6 月 1 日起施行。

最高人民法院 最高人民检察院

2017 年 5 月 8 日

最高人民法院、最高人民检察院
关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释

为依法惩治侵犯公民个人信息犯罪活动，保护公民个人信息安全和合法权益，根据《中华人民共和国刑法》《中华人民共和国刑事诉讼法》的有关规定，现就办理此类刑事案件适用法律的若干问题解释如下：

第一条刑法第二百五十三条之一规定的“公民个人信息”，是指以电子或者其他方式记录的能够单独或者与其他信息结合识别特定自然人身份或者反映特定自然人活动情况的各种信息，包括姓名、身份证件号码、通信通讯联系方式、住址、账号密码、财产状况、行踪轨迹等。

第二条违反法律、行政法规、部门规章有关公民个人信息保护的规定的， 应当认定为刑法第二百五十三条之一规定的“违反国家有关规定”。

第三条向特定人提供公民个人信息，以及通过信息网络或者其他途径发布公民个人信息的，应当认定为刑法第二百五十三条之一规定的“提供公民个人信息”。

未经被收集者同意，将合法收集的公民个人信息向他人提供的，属于刑法第二百五十三条之一规定的“提供公民个人信息”，但是经过处理无法识别特定个人且不能复原的除外。

第四条违反国家有关规定，通过购买、收受、交换等方式获取公民个人信息，或者在履行职责、提供服务过程中收集公民个人信息的， 属于刑法第二百五十三条之一第三款规定的“以其他方法非法获取公民个人信息”。

第五条非法获取、出售或者提供公民个人信息， 具有下列情形之一的，应当认定为刑法第二百五十三条之一规定的“情节严重”：

(一)出售或者提供行踪轨迹信息，被他人用于犯罪的；

(二)知道或者应当知道他人利用公民个人信息实施犯罪，向其出售或者提供的；

(三)非法获取、出售或者提供行踪轨迹信息、通信内容、征信信息、财产信息五十条以上的；

(四)非法获取、出售或者提供住宿信息、通信记录、健康生理信息、交易信息等其他可能影响人身、财产安全的公民个人信息五百条以上的;

(五)非法获取、出售或者提供第三项、第四项规定以外的公民个人信息五千条以上的;

(六)数量未达到第三项至第五项规定标准,但是按相应比例合计达到有关数量标准的;

(七)违法所得五千元以上的;

(八)将在履行职责或者提供服务过程中获得的公民个人信息出售或者提供给他人,数量或者数额达到第三项至第七项规定标准一半以上的;

(九)曾因侵犯公民个人信息受过刑事处罚或者二年内受过行政处罚,又非法获取、出售或者提供公民个人信息的;

(十)其他情节严重的情形。

实施前款规定的行为,具有下列情形之一的,应当认定为刑法第二百五十三条之一第一款规定的“情节特别严重”:

(一)造成被害人死亡、重伤、精神失常或者被绑架等严重后果的;

(二)造成重大经济损失或者恶劣社会影响的;

(三)数量或者数额达到前款第三项至第八项规定标准十倍以上的;

(四)其他情节特别严重的情形。

第六条为合法经营活动而非法购买、收受本解释第五条第一款第三项、第四项规定以外的公民个人信息,具有下列情形之一的,应当认定为刑法第二百五十三条之一规定的“情节严重”:

(一)利用非法购买、收受的公民个人信息获利五万元以上的;

(二)曾因侵犯公民个人信息受过刑事处罚或者二年内受过行政处罚,又非法购买、收受公民个人信息的;

(三)其他情节严重的情形。

实施前款规定的行为,将购买、收受的公民个人信息非法出售或者提供的,定罪量刑标准适用本解释第五条的规定。

第七条单位犯刑法第二百五十三条之一规定之罪的,依照本解释规定的相应自然人犯罪的定罪量刑标准,对直接负责的主管人员和其他直接责任人员定罪处

罚，并对单位判处罚金。

第八条设立用于实施非法获取、出售或者提供公民个人信息违法犯罪活动的网站、通讯群组， 情节严重的，应当依照刑法第二百八十七条之一的规定，以非法利用信息网络罪定罪处罚；同时构成侵犯公民个人信息罪的，依照侵犯公民个人信息罪定罪处罚。

第九条网络服务提供者拒不履行法律、行政法规规定的信息网络安全管理义务，经监管部门责令采取改正措施而拒不改正，致使用户的公民个人信息泄露，造成严重后果的，应当依照刑法第二百八十六条之一的规定，以拒不履行信息网络安全管理义务罪定罪处罚。

第十条实施侵犯公民个人信息犯罪，不属于“情节特别严重”，行为人系初犯，全部退赃，并确有悔罪表现的，可以认定为情节轻微，不起诉或者免予刑事处罚；确有必要判处刑罚的，应当从宽处罚。

第十一条非法获取公民个人信息后又出售或者提供的，公民个人信息的条数不重复计算。

向不同单位或者个人分别出售、提供同一公民个人信息的，公民个人信息的条数累计计算。

对批量公民个人信息的条数，根据查获的数量直接认定，但是有证据证明信息不真实或者重复的除外。

第十二条对于侵犯公民个人信息犯罪，应当综合考虑犯罪的危害程度、犯罪的违法所得数额以及被告人的前科情况、认罪悔罪态度等， 依法判处罚金。罚金数额一般在违法所得的一倍以上五倍以下。

第十三条本解释自 2017 年 6 月 1 日起施行。

最高人民检察院关于印发《检察机关办理侵犯公民个人信息案件指引》的通知

高检发侦监字〔2018〕13 号

各省、自治区、直辖市人民检察院，新疆生产建设兵团人民检察院：

《检察机关办理侵犯公民个人信息案件指引》已经 2018 年 8 月 24 日最高人民检察院第十三届检察委员会第五次会议通过，现印发你们，供参考。

最高人民检察院

2018 年 11 月 9 日

最高人民检察院检察机关办理侵犯公民个人信息案件指引

根据《中华人民共和国刑法》第二百五十三条之一的规定，侵犯公民个人信息罪是指违反国家有关规定，向他人出售、提供公民个人信息，或者通过窃取等方法非法获取公民个人信息，情节严重的行为。结合《最高人民法院、最高人民检察院关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释》(法释〔2017〕10 号)(以下简称《解释》)，办理侵犯公民个人信息案件，应当特别注意以下问题：一是对“公民个人信息”的审查认定；二是对“违反国家有关规定”的审查认定；三是对“非法获取”的审查认定；四是对“情节严重”和“情节特别严重”的审查认定；五是对关联犯罪的审查认定。

一、审查证据的基本要求

(一)审查逮捕

1.有证据证明发生了侵犯公民个人信息犯罪事实

(1)证明侵犯公民个人信息案件发生

主要证据包括：报案登记、受案登记、立案决定书、破案经过、证人证言、被害人陈述、犯罪嫌疑人供述和辩解以及证人、被害人提供的短信、微信或 QQ 截图等电子数据。

(2)证明被侵犯对象系公民个人信息

主要证据包括：扣押物品清单、勘验检查笔录、电子数据、司法鉴定意见及公民信息查询结果说明、被害人陈述、被害人提供的原始信息资料和对比资料等。

2.有证据证明侵犯公民个人信息行为是犯罪嫌疑人实施的

(1)证明违反国家有关规定的证据：犯罪嫌疑人关于所从事的职业的供述、其所在公司的工商注册资料、公司出具的犯罪嫌疑人职责范围说明、劳动合同、保密协议及公司领导、同事关于犯罪嫌疑人职责范围的证言等。

(2)证明出售、提供行为的证据：远程勘验笔录及QQ、微信等即时通讯工具聊天记录、论坛、贴吧、电子邮件、手机短信记录等电子数据，证明犯罪嫌疑人通过上述途径向他人出售、提供、交换公民个人信息的情况。公民个人信息贩卖者、提供者、担保交易人及购买者、收受者的证言或供述，相关银行账户明细、第三方支付平台账户明细，证明出售公民个人信息违法所得情况。此

外，如果犯罪嫌疑人系通过信息网络发布方式提供公民个人信息，证明该行为的证据还包括远程勘验笔录、扣押笔录、扣押物品清单、对手机、电脑存储介质、云盘、FTP 等的司法鉴定意见等。

(3)证明犯罪嫌疑人或公民个人信息购买者、收受者控制涉案信息的证据：搜查笔录、扣押笔录、扣押物品清单，对手机、电脑存储介质等的司法鉴定意见等，证实储存有公民个人信息的电脑、手机、U 盘或者移动硬盘、云盘、FTP 等介质与犯罪嫌疑人或公民个人信息购买者、收受者的关系。犯罪嫌疑人供述、辨认笔录及证人证言等，证实犯罪嫌疑人或公民个人信息购买者、收受者所有或实际控制、使用涉案存储介质。

(4)证明涉案公民个人信息真实性的证据：被害人陈述、被害人提供的原始信息资料、公安机关或相关单位出具的涉案公民个人信息与权威数据库内信息同一性的比对说明。针对批量的涉案公民个人信息的真实性问题，根据《解释》精神，可以根据查获的数量直接认定，但有证据证明信息不真实或重复的除外。

(5)证明违反国家规定，通过窃取、购买、收受、交换等方式非法获取公民个人信息的证据：主要证据与上述以出售、提供方式侵犯公民个人信息行为的证据基本相同。针对窃取的方式如通过技术手段非法获取公民个人信息的行为，需证明犯罪嫌疑人实施上述行为，除被害人陈述、犯罪嫌疑人供述和辩解外，还包括侦查机关从被害公司数据库中发现入侵电脑 IP 地址情况、从犯罪嫌疑人电脑中提取的侵入被害公司数据的痕迹等现场勘验检查笔录，以及涉案程序(木马)的司法鉴定意见等。

3.有证据证明犯罪嫌疑人具有侵犯公民个人信息的主观故意

(1)证明犯罪嫌疑人明知没有获取、提供公民个人信息的法律依据或资格，主要证据包括：犯罪嫌疑人的身份证明、犯罪嫌疑人关于所从事职业的供述、其所在公司的工商资料和营业范围、公司关于犯罪嫌疑人的职责范围说明、公司主要负责人的证人证言等。

(2)证明犯罪嫌疑人积极实施窃取、出售、提供、购买、交换、收受公民个人信息的行为，主要证据除了证人证言、犯罪嫌疑人供述和辩解外，还包括远程勘验笔录、手机短信记录、即时通讯工具聊天记录、电子数据司法鉴定意

见、银行账户明细、第三方支付平台账户明细等。

4.有证据证明“情节严重”或“情节特别严重”

(1)公民个人信息购买者或收受者的证言或供述。

(2)公民个人信息购买、收受公司工作人员利用公民个人信息进行电话或短信推销、商务调查等经营性活动后出具的证言或供述。

(3)公民个人信息购买者或者收受者利用所获信息从事违法犯罪活动后出具的证言或供述。

(4)远程勘验笔录、电子数据司法鉴定意见书、最高人民检察院或公安部指定的机构对电子数据涉及的专门性问题出具的报告、公民个人信息资料等。证明犯罪嫌疑人通过即时通讯工具、电子邮箱、论坛、贴吧、手机等向他人出售、提供、购买、交换、收受公民个人信息的情况。

(5)银行账户明细、第三方支付平台账户明细。

(6)死亡证明、伤情鉴定意见、医院诊断记录、经济损失鉴定意见、相关案件起诉书、判决书等。

(二)审查起诉

除审查逮捕阶段证据审查基本要求之外，对侵犯公民个人信息案件的审查起诉工作还应坚持“犯罪事实清楚，证据确实、充分”的标准，保证定罪量刑的事实都有证据证明；据以定案的证据均经法定程序查证属实；综合全案证据，对所认定的事实已排除合理怀疑。

1.有确实充分的证据证明发生了侵犯公民个人信息犯罪事实。该证据与审查逮捕的证据类型相同。

2.有确实充分的证据证明侵犯公民个人信息行为是犯罪嫌疑人实施的

(1)对于证明犯罪行为是犯罪嫌疑人实施的证据审查，需要结合《解释》精神，准确把握对“违反国家有关规定”“出售、提供行为”“窃取或以其他方法”的认定。

(2)对证明违反国家有关规定的证据审查，需要明确国家有关规定的具体内容，违反法律、行政法规、部门规章有关公民个人信息保护规定的，应当认定为刑法第二百五十三条之一规定的“违反国家有关规定”。

(3)对证明出售、提供行为的证据审查，应当明确“出售、提供”包括在履

职或提供服务的过程中将合法持有的公民个人信息出售或者提供给他人的行为：向特定人提供、通过信息网络或者其他途径发布公民个人信息、未经被收集者同意，将合法收集的公民个人信息(经过处理无法识别特定个人且不能复原的除外)向他人提供的，均属于刑法第二百五十三条之一规定的“提供公民个人信息”。应当全面审查犯罪嫌疑人所出售提供公民个人信息的来源、途经与去向，对相关供述、物证、书证、证人证言、被害人陈述、电子数据等证据种类进行综合审查，针对使用信息网络进行犯罪活动的，需要结合专业知识，根据证明该行为的远程勘验笔录、扣押笔录、扣押物品清单、电子存储介质、网络存储介质等的司法鉴定意见进行审查。

(4)对证明通过窃取或以其他非法方法获取公民个人信息等方式非法获取公民个人信息的证据审查，应当明确“以其他方法获取公民个人信息”包括购买、收受、交换等方式获取公民个人信息，或者在履行职责、提供服务过程中收集公民个人信息的行为。

针对窃取行为，如通过信息网络窃取公民个人信息，则应当结合犯罪嫌疑人供述、证人证言、被害人陈述，着重审查证明犯罪嫌疑人侵入信息网络、数据库时的 IP 地址、MAC 地址、侵入工具、侵入痕迹等内容的现场勘验检查笔录以及涉案程序(木马)的司法鉴定意见等。

针对购买、收受、交换行为，应当全面审查购买、收受、交换公民个人信息的来源、途经、去向，结合犯罪嫌疑人供述和辩解、辨认笔录、证人证言等证据，对搜查笔录、扣押笔录、扣押物品清单、涉案电子存储介质等司法鉴定意见进行审查，明确上述证据同犯罪嫌疑人或公民个人信息购买、收受、交换者之间的关系。

针对履行职责、提供服务过程中收集公民个人信息的行为，应当审查证明犯罪嫌疑人所从事职业及其所负职责的证据，结合法律、行政法规、部门规章等国家有关公民个人信息保护的规定，明确犯罪嫌疑人的行为属于违反国家有关规定，以其他方法非法获取公民个人信息的行为。

(5)对证明涉案公民个人信息真实性证据的审查，应当着重审查被害人陈述、被害人提供的原始信息资料、公安机关或其他相关单位出具的涉案公民个人信息与权威数据库内信息同一性的对比说明。对批量的涉案公民个人信息的

真实性问题，根据《解释》精神，可以根据查获的数量直接认定，但有证据证明信息不真实或重复的除外。

3.有确实充分的证据证明犯罪嫌疑人具有侵犯公民个人信息的主观故意

(1)对证明犯罪嫌疑人主观故意的证据审查，应当综合审查犯罪嫌疑人的身份证明、犯罪嫌疑人关于所从事职业的供述、其所在公司的工商资料和营业范围、公司关于犯罪嫌疑人的职责范围说明、公司主要负责人的证人证言等，结合国家公民个人信息保护的相关规定，夯实犯罪嫌疑人在实施犯罪时的主观明知。

(2)对证明犯罪嫌疑人积极实施窃取或者以其他方法非法获取公民个人信息行为的证据审查，应当结合犯罪嫌疑人供述、证人证言，着重审查远程勘验笔录、手机短信记录、即时通讯工具聊天记录、电子数据司法鉴定意见、银行账户明细、第三方支付平台账户明细等，明确犯罪嫌疑人在实施犯罪时的积极作为。

4.有确实充分的证据证明“情节严重”或“情节特别严重”。该证据与审查逮捕的证据类型相同。

二、需要特别注意的问题

在侵犯公民个人信息案件审查逮捕、审查起诉中，要根据相关法律、司法解释等规定，结合在案证据，重点注意以下问题：

(一)对“公民个人信息”的审查认定

根据《解释》的规定，公民个人信息是指以电子或者其他方式记录的能够单独或者与其他信息结合识别特定自然人身份或者反映特定自然人活动情况的各种信息，包括姓名、身份证件号码、通信通讯联系方式、住址、账号密码、财产状况、行踪轨迹等。经过处理无法识别特定自然人且不能复原的信息，虽然也可能反映自然人活动情况，但与特定自然人无直接关联，不属于公民个人信息的范畴。

对于企业工商登记等信息中所包含的手机、电话号码等信息，应当明确该号码的用途。对由公司购买、使用的手机、电话号码等信息，不属于个人信息的范畴，从而严格区分“手机、电话号码等由公司购买，归公司使用”与“公司经办人在工商登记等活动中登记个人电话、手机号码”两种不同情形。

(二)对“违反国家有关规定”的审查认定

《中华人民共和国刑法修正案(九)》将原第二百五十三条之一的“违反国家规定”修改为“违反国家有关规定”，后者的范围明显更广。根据刑法第九十六条的规定，“国家规定”仅限于全国人大及其常委会制定的法律和决定，国务院制定的行政法规、规定的行政措施、发布的决定和命令。而“国家有关规定”还包括部门规章，这些规定散见于金融、电信、交通、教育、医疗、统计、邮政等领域的法律、行政法规或部门规章中。

(三)对“非法获取”的审查认定

在窃取或者以其他方法非法获取公民个人信息的行为中，需要着重把握“其他方法”的范围问题。“其他方法”，是指“窃取”以外，与窃取行为具有同等危害性的方法，其中，购买是最常见的非法获取手段。侵犯公民个人信息犯罪作为电信网络诈骗的上游犯罪，诈骗分子往往先通过网络向他人购买公民个人信息，然后自己直接用于诈骗或转发给其他同伙用于诈骗，诈骗分子购买公民个人信息的行为属于非法获取行为，其同伙接收公民个人信息的行为明显也属于非法获取行为。同时，一些房产中介、物业管理公司、保险公司、担保公司的业务员往往与同行通过QQ、微信群互相交换各自掌握的客户信息，这种交换行为也属于非法获取行为。此外，行为人在履行职责、提供服务过程中，违反国家有关规定，未经他人同意收集公民个人信息，或者收集与提供的服务无关的公民个人信息的，也属于非法获取公民个人信息的行为。

(四)对“情节严重”和“情节特别严重”的审查认定

1.关于“情节严重”的具体认定标准，根据《解释》第五条第一款的规定，主要涉及五个方面：

(1)信息类型和数量。①行踪轨迹信息、通信内容、征信信息、财产信息，此类信息与公民人身、财产安全直接相关，数量标准为五十条以上，且仅限于上述四类信息，不允许扩大范围。对于财产信息，既包括银行、第三方支付平台、证券期货等金融服务账户的身份认证信息(一组确认用户操作权限的数据，包括账号、口令、密码、数字证书等)，也包括存款、房产、车辆等财产状况信息。②住宿信息、通信记录、健康生理信息、交易信息等可能影响公民人身、财产安全的信息，数量标准为五百条以上，此类信息也与人身、财产安全直接

相关，但重要程度要弱于行踪轨迹信息、通信内容、征信信息、财产信息。对“其他可能影响人身、财产安全的公民个人信息”的把握，应当确保所适用的公民个人信息涉及人身、财产安全，且与“住宿信息、通信记录、健康生理信息、交易信息”在重要程度上具有相当性。③除上述两类信息以外的其他公民个人信息，数量标准为五千条以上。

(2)违法所得数额。对于违法所得，可直接以犯罪嫌疑人出售公民个人信息的收入予以认定，不必扣减其购买信息的犯罪成本。同时，在审查认定违法所得数额过程中，应当以查获的银行交易记录、第三方支付平台交易记录、聊天记录、犯罪嫌疑人供述、证人证言综合予以认定，对于犯罪嫌疑人无法说明合法来源的用于专门实施侵犯公民个人信息犯罪的银行账户或第三方支付平台账户内资金收入，可综合全案证据认定为违法所得。

(3)信息用途。公民个人信息被他人用于违法犯罪活动的，不要求他人的行为必须构成犯罪，只要行为人明知他人非法获取公民个人信息用于违法犯罪活动即可。

(4)主体身份。如果行为人系将在履行职责或者提供服务过程中获得的公民个人信息出售或者提供给他人的，涉案信息数量、违法所得数额只要达到一般主体的一半，即可认为“情节严重”。

(5)主观恶性。曾因侵犯公民个人信息受过刑事处罚或者二年内受过行政处罚，又非法获取、出售或者提供公民个人信息的，即可认为“情节严重”。

2.关于“情节特别严重”的认定标准，根据《解释》，主要分为两类：一是信息数量、违法所得数额标准。二是信息用途引发的严重后果，其中造成人身伤亡、经济损失、恶劣社会影响等后果，需要审查认定侵犯公民个人信息的行为与严重后果间存在因果关系。

对于涉案公民个人信息数量的认定，根据《解释》第十一条，非法获取公民个人信息后又出售或者提供的，公民个人信息的条数不重复计算；向不同单位或者个人分别出售、提供同一公民个人信息的，公民个人信息的条数累计计算；对批量出售、提供公民个人信息的条数，根据查获的数量直接认定，但是有证据证明信息不真实或者重复的除外。在实践中，如犯罪嫌疑人多次获取同一条公民个人信息，一般认定为一条，不重复累计；但获取的该公民个人信息

内容发生了变化的除外。

对于涉案公民个人信息的数量、社会危害性等因素的审查，应当结合刑法第二百五十三条和《解释》的规定进行综合审查。涉案公民个人信息数量极少，但造成被害人死亡等严重后果的，应审查犯罪嫌疑人行为与该后果之间的因果关系，符合条件的，可以认定为实施《解释》第五条第一款第十项“其他情节严重的情形”的行为，造成被害人死亡等严重后果，从而认定为“情节特别严重”。如涉案公民个人信息数量较多，但犯罪嫌疑人仅仅获取而未向他人出售或提供，则可以在认定相关犯罪事实的基础上，审查该行为是否符合《解释》第五条第一款第三、四、五、六、九项及第二款第三项的情形，符合条件的，可以分别认定为“情节严重”“情节特别严重”。

此外，针对为合法经营活动而购买、收受公民个人信息的行为，在适用《解释》第六条的定罪量刑标准时须满足三个条件：一是为了合法经营活动，对此可以综合全案证据认定，但主要应当由犯罪嫌疑人一方提供相关证据；二是限于普通公民个人信息，即不包括可能影响人身、财产安全的敏感信息；三是信息没有再流出扩散，即行为方式限于购买、收受。如果将购买、收受的公民个人信息非法出售或者提供的，定罪量刑标准应当适用《解释》第五条的规定。

(五)对关联犯罪的审查认定

对于侵犯公民个人信息犯罪与电信网络诈骗犯罪相交织的案件，应严格按照《最高人民法院、最高人民检察院、公安部关于办理电信网络诈骗等刑事案件适用法律若干问题的意见》(法发〔2016〕32 号)的规定进行审查认定，即通过认真审查非法获取、出售、提供公民个人信息的犯罪嫌疑人对电信网络诈骗犯罪的参与程度，结合能够证实其认知能力的学历文化、聊天记录、通话频率、获取固定报酬还是参与电信网络诈骗犯罪分成等证据，分析判断其是否属于诈骗共同犯罪、是否应该数罪并罚。

根据《解释》第八条的规定，设立用于实施出售、提供或者非法获取公民个人信息违法犯罪活动的网站、通讯群组，情节严重的，应当依照刑法第二百八十七条之一的规定，以非法利用信息网络罪定罪；同时构成侵犯公民个人信息罪的，应当认定为侵犯公民个人信息罪。

对于违反国家有关规定，采用技术手段非法侵入合法存储公民个人信息的单位数据库窃取公民个人信息的行为，也符合刑法第二百八十五条第二款非法获取计算机信息系统数据罪的客观特征，同时触犯侵犯公民个人信息罪和非法获取计算机信息系统数据罪的，应择一重罪论处。

此外，针对公安民警在履行职责过程中，违反国家有关规定，查询、提供公民个人信息的情形，应当认定为“违反国家有关规定，将在履行职责或者提供服务过程中以其他方法非法获取或提供公民个人信息”。但同时，应当审查犯罪嫌疑人除该行为之外有无其他行为侵害其他法益，从而对可能存在的其他犯罪予以准确认定。

三、社会危险性及羁押必要性审查

(一)审查逮捕

1.犯罪动机：一是出售牟利；二是用于经营活动；三是用于违法犯罪活动。犯罪动机表明犯罪嫌疑人主观恶性，也能证明犯罪嫌疑人是否可能实施新的犯罪。

2.犯罪情节。犯罪嫌疑人的行为直接反映其人身危险性。具有下列情节的侵犯公民个人信息犯罪，能够证实犯罪嫌疑人主观恶性和人身危险性较大，实施新的犯罪的可能性也较大，可以认为具有较大的社会危险性：一是犯罪持续时间较长、多次实施侵犯公民个人信息犯罪的；二是被侵犯的公民个人信息数量或违法所得巨大的；三是利用公民个人信息进行违法犯罪活动的；四是犯罪手段行为本身具有违法性或者破坏性，即犯罪手段恶劣的，如骗取、窃取公民个人信息，采取胁迫、植入木马程序侵入他人计算机系统等方式非法获取信息。

犯罪嫌疑人实施侵犯公民个人信息犯罪，不属于“情节特别严重”，系初犯，全部退赃，并确有悔罪表现的，可以认定社会危险性较小，没有逮捕必要。

(二)审查起诉

在审查起诉阶段，要结合侦查阶段取得的事实证据，进一步引导侦查机关加大捕后侦查力度，及时审查新证据。在羁押期限届满前对全案进行综合审查，对于未达到逮捕证明标准的，撤销原逮捕决定。

经羁押必要性审查，发现犯罪嫌疑人具有下列情形之一的，应当向办案机关提出释放或者变更强制措施的建议：

1.案件证据发生重大变化，没有证据证明有犯罪事实或者犯罪行为系犯罪嫌疑人、被告人所为的。

2.案件事实或者情节发生变化，犯罪嫌疑人、被告人可能被判处拘役、管制、独立适用附加刑、免予刑事处罚或者判决无罪的。

3.继续羁押犯罪嫌疑人、被告人，羁押期限将超过依法可能判处的刑期的。

4.案件事实基本查清，证据已经收集固定，符合取保候审或者监视居住条件的。

经羁押必要性审查，发现犯罪嫌疑人、被告人具有下列情形之一，且具有悔罪表现，不予羁押不致发生社会危险性的，可以向办案机关提出释放或者变更强制措施的建议：

1.预备犯或者中止犯；共同犯罪中的从犯或者胁从犯。

2.主观恶性较小的初犯。

3.系未成年人或者年满七十五周岁的人。

4.与被害方依法自愿达成和解协议，且已经履行或者提供担保的。

5.患有严重疾病、生活不能自理的。

6.系怀孕或者正在哺乳自己婴儿的妇女。

7.系生活不能自理的人的唯一扶养人。

8.可能被判处一年以下有期徒刑或者宣告缓刑的。

9.其他不需要继续羁押犯罪嫌疑人、被告人的情形。

最高人民法院、最高人民检察院关于办理非法利用信息网络、帮助信息网络犯罪活动等刑事案件适用法律若干问题的解释

法释〔2019〕15号

《最高人民法院、最高人民检察院关于办理非法利用信息网络、帮助信息网络犯罪活动等刑事案件适用法律若干问题的解释》已于2019年6月3日由最高人民法院审判委员会第1771次会议、2019年9月4日由最高人民检察院第十三届检察委员会第二十三次会议通过，现予公布，自2019年11月1日起施行。

最高人民法院 最高人民检察院

2019 年 10 月 21 日

最高人民法院、最高人民检察院
关于办理非法利用信息网络、帮助信息网络犯罪活动等刑事案件适用法律若干问题的解释

为依法惩治拒不履行信息网络安全管理义务、非法利用信息网络、帮助信息网络犯罪活动等犯罪，维护正常网络秩序，根据《中华人民共和国刑法》《中华人民共和国刑事诉讼法》的规定，现就办理此类刑事案件适用法律的若干问题解释如下：

第一条 提供下列服务的单位和个人，应当认定为刑法第二百八十六条之一第一款规定的“网络服务提供者”：

(一)网络接入、域名注册解析等信息网络接入、计算、存储、传输服务；

(二)信息发布、搜索引擎、即时通讯、网络支付、网络预约、网络购物、网络游戏、网络直播、网站建设、安全防护、广告推广、应用商店等信息网络应用服务；

(三)利用信息网络提供的电子政务、通信、能源、交通、水利、金融、教育、医疗等公共服务。

第二条 刑法第二百八十六条之一第一款规定的“监管部门责令采取改正措施”，是指网信、电信、公安等依照法律、行政法规的规定承担信息网络安全监管职责的部门，以责令整改通知书或者其他文书形式，责令网络服务提供者采取改正措施。

认定“经监管部门责令采取改正措施而拒不改正”，应当综合考虑监管部门责令改正是否具有法律、行政法规依据，改正措施及期限要求是否明确、合理，网络服务提供者是否具有按照要求采取改正措施的能力等因素进行判断。

第三条 拒不履行信息网络安全管理义务，具有下列情形之一的，应当认定为刑法第二百八十六条之一第一款第一项规定的“致使违法信息大量传播”：

(一)致使传播违法视频文件二百个以上的；

(二)致使传播违法视频文件以外的其他违法信息二千个以上的；

(三)致使传播违法信息，数量虽未达到第一项、第二项规定标准，但是按相

应比例折算合计达到有关数量标准的；

(四)致使向二千个以上用户账号传播违法信息的；

(五)致使利用群组成员账号数累计三千以上的通讯群组或者关注人员账号数累计三万以上的社交网络传播违法信息的；

(六)致使违法信息实际被点击数达到五万以上的；

(七)其他致使违法信息大量传播的情形。

第四条 拒不履行信息网络安全管理义务，致使用户信息泄露，具有下列情形之一的，应当认定为刑法第二百八十六条之一第一款第二项规定的“造成严重后果”：

(一)致使泄露行踪轨迹信息、通信内容、征信信息、财产信息五百条以上的；

(二)致使泄露住宿信息、通信记录、健康生理信息、交易信息等其他可能影响人身、财产安全的用户信息五千条以上的；

(三)致使泄露第一项、第二项规定以外的用户信息五万条以上的；

(四)数量虽未达到第一项至第三项规定标准，但是按相应比例折算合计达到有关数量标准的；

(五)造成他人死亡、重伤、精神失常或者被绑架等严重后果的；

(六)造成重大经济损失的；

(七)严重扰乱社会秩序的；

(八)造成其他严重后果的。

第五条 拒不履行信息网络安全管理义务，致使影响定罪量刑的刑事案件证据灭失，具有下列情形之一的，应当认定为刑法第二百八十六条之一第一款第三项规定的“情节严重”：

(一)造成危害国家安全犯罪、恐怖活动犯罪、黑社会性质组织犯罪、贪污贿赂犯罪案件的证据灭失的；

(二)造成可能判处五年有期徒刑以上刑罚犯罪案件的证据灭失的；

(三)多次造成刑事案件证据灭失的；

(四)致使刑事诉讼程序受到严重影响的；

(五)其他情节严重的情形。

第六条 拒不履行信息网络安全管理义务，具有下列情形之一的，应当认定

为刑法第二百八十六条之一第一款第四项规定的“有其他严重情节”：

(一)对绝大多数用户日志未留存或者未落实真实身份信息认证义务的；

(二)二年内经多次责令改正拒不改正的；

(三)致使信息网络服务被主要用于违法犯罪的；

(四)致使信息网络服务、网络设施被用于实施网络攻击， 严重影响生产、生活的；

(五)致使信息网络服务被用于实施危害国家安全犯罪、恐怖活动犯罪、黑社会性质组织犯罪、贪污贿赂犯罪或者其他重大犯罪的；

(六)致使国家机关或者通信、能源、交通、水利、金融、教育、医疗等领域提供公共服务的信息网络受到破坏，严重影响生产、生活的；

(七)其他严重违反信息网络安全管理义务的情形。

第七条 刑法第二百八十七条之一规定的“违法犯罪”，包括犯罪行为和属于刑法分则规定的行为类型但尚未构成犯罪的违法行为。

第八条 以实施违法犯罪活动为目的而设立或者设立后主要用于实施违法犯罪活动的网站、通讯群组， 应当认定为刑法第二百八十七条之一第一款第一项规定的“用于实施诈骗、传授犯罪方法、制作或者销售违禁物品、管制物品等违法犯罪活动的网站、通讯群组”。

第九条 利用信息网络提供信息的链接、截屏、二维码、访问账号密码及其他指引访问服务的，应当认定为刑法第二百八十七条之一第一款第二项、第三项规定的“发布信息”。

第十条 非法利用信息网络，具有下列情形之一的，应当认定为刑法第二百八十七条之一第一款规定的“情节严重”：

(一)假冒国家机关、金融机构名义，设立用于实施违法犯罪活动的网站的；

(二)设立用于实施违法犯罪活动的网站，数量达到三个以上或者注册账号数累计达到二千以上的；

(三)设立用于实施违法犯罪活动的通讯群组，数量达到五个以上或者群组成员账号数累计达到一千以上的；

(四)发布有关违法犯罪的信息或者为实施违法犯罪活动发布信息，具有下列情形之一的：

1.在网站上发布有关信息一百条以上的；

2.向二千个以上用户账号发送有关信息的；

3.向群组成员数累计达到三千以上的通讯群组发送有关信息的；

4.利用关注人员账号数累计达到三万以上的社交网络传播有关信息的；

(五)违法所得一万元以上的；

(六)二年内曾因非法利用信息网络、帮助信息网络犯罪活动、危害计算机信息系统安全受过行政处罚，又非法利用信息网络的；

(七)其他情节严重的情形。

第十一条 为他人实施犯罪提供技术支持或者帮助，具有下列情形之一的，可以认定行为人明知他人利用信息网络实施犯罪，但是有相反证据的除外：

(一)经监管部门告知后仍然实施有关行为的；

(二)接到举报后不履行法定管理职责的；

(三)交易价格或者方式明显异常的；

(四)提供专门用于违法犯罪的程序、工具或者其他技术支持、帮助的；

(五)频繁采用隐蔽上网、加密通信、销毁数据等措施或者使用虚假身份， 逃避监管或者规避调查的；

(六)为他人逃避监管或者规避调查提供技术支持、帮助的；

(七)其他足以认定行为人明知的情形。

第十二条 明知他人利用信息网络实施犯罪，为其犯罪提供帮助，具有下列情形之一的，应当认定为刑法第二百八十七条之二第一款规定的“情节严重”：

(一)为三个以上对象提供帮助的；

(二)支付结算金额二十万元以上的；

(三)以投放广告等方式提供资金五万元以上的；

(四)违法所得一万元以上的；

(五)二年内曾因非法利用信息网络、帮助信息网络犯罪活动、危害计算机信息系统安全受过行政处罚，又帮助信息网络犯罪活动的；

(六)被帮助对象实施的犯罪造成严重后果的；

(七)其他情节严重的情形。

实施前款规定的行为，确因客观条件限制无法查证被帮助对象是否达到犯罪

的程度，但相关数额总计达到前款第二项至第四项规定标准五倍以上，或者造成特别严重后果的，应当以帮助信息网络犯罪活动罪追究行为人的刑事责任。

第十三条 被帮助对象实施的犯罪行为可以确认，但尚未到案、尚未依法裁判或者因未达到刑事责任年龄等原因依法未予追究刑事责任的，不影响帮助信息网络犯罪活动罪的认定。

第十四条 单位实施本解释规定的犯罪的，依照本解释规定的相应自然人犯罪的定罪量刑标准，对直接负责的主管人员和其他直接责任人员定罪处罚，并对单位判处罚金。

第十五条 综合考虑社会危害程度、认罪悔罪态度等情节，认为犯罪情节轻微的，可以不起诉或者免予刑事处罚；情节显著轻微危害不大的，不以犯罪论处。

第十六条 多次拒不履行信息网络安全管理义务、非法利用信息网络、帮助信息网络犯罪活动构成犯罪，依法应当追诉的，或者二年内多次实施前述行为未经处理的，数量或者数额累计计算。

第十七条 对于实施本解释规定的犯罪被判处刑罚的，可以根据犯罪情况和预防再犯罪的需要，依法宣告职业禁止；被判处管制、宣告缓刑的， 可以根据犯罪情况，依法宣告禁止令。

第十八条 对于实施本解释规定的犯罪的，应当综合考虑犯罪的危害程度、违法所得数额以及被告人的前科情况、认罪悔罪态度等，依法判处罚金。

第十九条 本解释自 2019 年 11 月 1 日起施行。

最高人民检察院关于印发《人民检察院办理网络犯罪案件规定》的通知

各级人民检察院：

《人民检察院办理网络犯罪案件规定》已经 2020 年 12 月 14 日最高人民检察院第十三届检察委员会第五十七次会议通过，现印发你们，请结合实际，认真贯彻落实。

最高人民检察院

2021 年 1 月 22 日

人民检察院办理网络犯罪案件规定

第一章 一般规定

第一条 为规范人民检察院办理网络犯罪案件，维护国家安全、网络安全、

社会公共利益，保护公民、法人和其他组织的合法权益， 根据《中华人民共和国刑事诉讼法》《人民检察院刑事诉讼规则》等规定，结合司法实践，制定本规定。

第二条 本规定所称网络犯罪是指针对信息网络实施的犯罪，利用信息网络实施的犯罪，以及其他上下游关联犯罪。

第三条 人民检察院办理网络犯罪案件应当加强全链条惩治，注重审查和发现上下游关联犯罪线索。对涉嫌犯罪， 公安机关未立案侦查、应当提请批准逮捕而未提请批准逮捕或者应当移送起诉而未移送起诉的，依法进行监督。

第四条 人民检察院办理网络犯罪案件应当坚持惩治犯罪与预防犯罪并举，建立捕、诉、监、防一体的办案机制，加强以案释法，发挥检察建议的作用，促进有关部门、行业组织、企业等加强网络犯罪预防和治理，净化网络空间。

第五条 网络犯罪案件的管辖适用刑事诉讼法及其他相关规定。

有多个犯罪地的，按照有利于查清犯罪事实、有利于保护被害人合法权益、保证案件公正处理的原则确定管辖。

因跨区域犯罪、共同犯罪、关联犯罪等原因存在管辖争议的， 由争议的人民检察院协商解决，协商不成的，报请共同的上级人民检察院指定管辖。

第六条 人民检察院办理网络犯罪案件应当发挥检察一体化优势，加强跨区域协作办案，强化信息互通、证据移交、技术协作，增强惩治网络犯罪的合力。

第七条 人民检察院办理网络犯罪案件应当加强对电子数据收集、提取、保全、固定等的审查， 充分运用同一电子数据往往具有的多元关联证明作用，综合运用电子数据与其他证据，准确认定案件事实。

第八条 建立检察技术人员、其他有专门知识的人参与网络犯罪案件办理制度。根据案件办理需要， 吸收检察技术人员加入办案组辅助案件办理。积极探索运用大数据、云计算、人工智能等信息技术辅助办案， 提高网络犯罪案件办理的专业化水平。

第九条 人民检察院办理网络犯罪案件，对集团犯罪或者涉案人数众多的，根据行为人的客观行为、主观恶性、犯罪情节及地位、作用等综合判断责任轻重和刑事追究的必要性，按照区别对待原则分类处理，依法追诉。

第十条 人民检察院办理网络犯罪案件应当把追赃挽损贯穿始终，主动加强与有关机关协作，保证及时查封、扣押、冻结涉案财物，阻断涉案财物移转链条，

督促涉案人员退赃退赔。

第二章 引导取证和案件审查

第十一条 人民检察院办理网络犯罪案件应当重点围绕主体身份同一性、技术手段违法性、上下游行为关联性等方面全面审查案件事实和证据， 注重电子数据与其他证据之间的相互印证，构建完整的证据体系。

第十二条 经公安机关商请，根据追诉犯罪的需要，人民检察院可以派员适时介入重大、疑难、复杂网络犯罪案件的侦查活动， 并对以下事项提出引导取证意见：

(一)案件的侦查方向及可能适用的罪名；

(二)证据的收集、提取、保全、固定、检验、分析等；

(三)关联犯罪线索；

(四)追赃挽损工作；

(五)其他需要提出意见的事项。

人民检察院开展引导取证活动时，涉及专业性问题的，可以指派检察技术人员共同参与。

第十三条 人民检察院可以通过以下方式了解案件办理情况：

(一)查阅案件材料；

(二)参加公安机关对案件的讨论；

(三)了解讯(询)问犯罪嫌疑人、被害人、证人的情况；

(四)了解、参与电子数据的收集、提取；

(五)其他方式。

第十四条 人民检察院介入网络犯罪案件侦查活动，发现关联犯罪或其他新的犯罪线索，应当建议公安机关依法立案或移送相关部门；对于犯罪嫌疑人不构成犯罪的，依法监督公安机关撤销案件。

第十五条 人民检察院可以根据案件侦查情况，向公安机关提出以下取证意见：

(一)能够扣押、封存原始存储介质的，及时扣押、封存；

(二)扣押可联网设备时，及时采取信号屏蔽、信号阻断或者切断电源等方式，防止电子数据被远程破坏；

(三)及时提取账户密码及相应数据，如电子设备、网络账户、应用软件等的账户密码，以及存储于其中的聊天记录、电子邮件、交易记录等；

(四)及时提取动态数据，如内存数据、缓存数据、网络连接数据等；

(五)及时提取依赖于特定网络环境的数据，如点对点网络传输数据、虚拟专线网络中的数据等；

(六)及时提取书证、物证等客观证据，注意与电子数据相互印证。

第十六条 对于批准逮捕后要求公安机关继续侦查、不批准逮捕后要求公安机关补充侦查或者审查起诉退回公安机关补充侦查的网络犯罪案件，人民检察院应当重点围绕本规定第十二条第一款规定的事项，有针对性地制作继续侦查提纲或者补充侦查提纲。对于专业性问题， 应当听取检察技术人员或者其他有专门知识的人的意见。

人民检察院应当及时了解案件继续侦查或者补充侦查的情况。

第十七条 认定网络犯罪的犯罪嫌疑人，应当结合全案证据，围绕犯罪嫌疑人与原始存储介质、电子数据的关联性、犯罪嫌疑人网络身份与现实身份的同一性，注重审查以下内容：

(一)扣押、封存的原始存储介质是否为犯罪嫌疑人所有、持有或者使用；

(二)社交、支付结算、网络游戏、电子商务、物流等平台的账户信息、身份认证信息、数字签名、生物识别信息等是否与犯罪嫌疑人身份关联；

(三)通话记录、短信、聊天信息、文档、图片、语音、视频等文件内容是否能够反映犯罪嫌疑人的身份；

(四)域名、IP 地址、终端 MAC 地址、通信基站信息等是否能够反映电子设备为犯罪嫌疑人所使用；

(五)其他能够反映犯罪嫌疑人主体身份的内容。

第十八条 认定犯罪嫌疑人的客观行为，应当结合全案证据，围绕其利用的程序工具、技术手段的功能及其实现方式、犯罪行为和结果之间的关联性， 注重审查以下内容：

(一)设备信息、软件程序代码等作案工具；

(二)系统日志、域名、IP 地址、WiFi 信息、地理位置信息等是否能够反映犯罪嫌疑人的行为轨迹；

(三)操作记录、网络浏览记录、物流信息、交易结算记录、即时通信信息等是否能够反映犯罪嫌疑人的行为内容;

(四)其他能够反映犯罪嫌疑人客观行为的内容。

第十九条 认定犯罪嫌疑人的主观方面,应当结合犯罪嫌疑人的认知能力、专业水平、既往经历、人员关系、行为次数、获利情况等综合认定, 注重审查以下内容:

(一)反映犯罪嫌疑人主观故意的聊天记录、发布内容、浏览记录等;

(二)犯罪嫌疑人行为是否明显违背系统提示要求、正常操作流程;

(三)犯罪嫌疑人制作、使用或者向他人提供的软件程序是否主要用于违法犯罪活动;

(四)犯罪嫌疑人支付结算的对象、频次、数额等是否明显违反正常交易习惯;

(五)犯罪嫌疑人是否频繁采用隐蔽上网、加密通信、销毁数据等措施或者使用虚假身份;

(六)其他能够反映犯罪嫌疑人主观方面的内容。

第二十条 认定犯罪行为的情节和后果,应当结合网络空间、网络行为的特性,从违法所得、经济损失、信息系统的破坏、网络秩序的危害程度以及对被害人的侵害程度等综合判断,注重审查以下内容:

(一)聊天记录、交易记录、音视频文件、数据库信息等能够反映犯罪嫌疑人违法所得、获取和传播数据及文件的性质、数量的内容;

(二)账号数量、信息被点击次数、浏览次数、被转发次数等能够反映犯罪行为对网络空间秩序产生影响的内容;

(三)受影响的计算机信息系统数量、服务器日志信息等能够反映犯罪行为对信息网络运行造成影响程度的内容;

(四)被害人数量、财产损失数额、名誉侵害的影响范围等能够反映犯罪行为对被害人的人身、财产等造成侵害的内容;

(五)其他能够反映犯罪行为情节、后果的内容。

第二十一条 人民检察院办理网络犯罪案件,确因客观条件限制无法逐一收集相关言词证据的,可以根据记录被害人人数、被侵害的计算机信息系统数量、涉案资金数额等犯罪事实的电子数据、书证等证据材料, 在审查被告人及其辩护

人所提辩解、辩护意见的基础上，综合全案证据材料，对相关犯罪事实作出认定。

第二十二条 对于数量众多的同类证据材料，在证明是否具有同样的性质、特征或者功能时，因客观条件限制不能全部验证的，可以进行抽样验证。

第二十三条 对鉴定意见、电子数据等技术性证据材料，需要进行专门审查的，应当指派检察技术人员或者聘请其他有专门知识的人进行审查并提出意见。

第二十四条 人民检察院在审查起诉过程中，具有下列情形之一的，可以依法自行侦查：

(一)公安机关未能收集的证据，特别是存在灭失、增加、删除、修改风险的电子数据，需要及时收集和固定的；

(二)经退回补充侦查未达到补充侦查要求的；

(三)其他需要自行侦查的情形。

第二十五条 自行侦查由检察官组织实施，开展自行侦查的检察人员不得少于二人。需要技术支持和安全保障的， 由人民检察院技术部门和警务部门派员协助。必要时，可以要求公安机关予以配合。

第二十六条 人民检察院办理网络犯罪案件的部门，发现或者收到侵害国家利益、社会公共利益的公益诉讼案件线索的， 应当及时移送负责公益诉讼的部门处理。

第三章 电子数据的审查

第二十七条 电子数据是以数字化形式存储、处理、传输的，能够证明案件事实的数据，主要包括以下形式：

(一)网页、社交平台、论坛等网络平台发布的信息；

(二)手机短信、电子邮件、即时通信、通讯群组等网络通讯信息；

(三)用户注册信息、身份认证信息、数字签名、生物识别信息等用户身份信息；

(四)电子交易记录、通信记录、浏览记录、操作记录、程序安装、运行、删除记录等用户行为信息；

(五)恶意程序、工具软件、网站源代码、运行脚本等行为工具信息；

(六)系统日志、应用程序日志、安全日志、数据库日志等系统运行信息；

(七)文档、图片、音频、视频、数字证书、数据库文件等电子文件及其创建

时间、访问时间、修改时间、大小等文件附属信息。

第二十八条 电子数据取证主要包括以下方式：收集、提取电子数据；电子数据检查和侦查实验；电子数据检验和鉴定。

收集、提取电子数据可以采取以下方式：

(一)扣押、封存原始存储介质；

(二)现场提取电子数据；

(三)在线提取电子数据；

(四)冻结电子数据；

(五)调取电子数据。

第二十九条 人民检察院办理网络犯罪案件，应当围绕客观性、合法性、关联性的要求对电子数据进行全面审查。注重审查电子数据与案件事实之间的多元关联，加强综合分析，充分发挥电子数据的证明作用。

第三十条 对电子数据是否客观、真实，注重审查以下内容：

(一)是否移送原始存储介质，在原始存储介质无法封存、不便移动时， 是否说明原因，并注明相关情况；

(二)电子数据是否有数字签名、数字证书等特殊标识；

(三)电子数据的收集、提取过程及结果是否可以重现；

(四)电子数据有增加、删除、修改等情形的，是否附有说明；

(五)电子数据的完整性是否可以保证。

第三十一条 对电子数据是否完整，注重审查以下内容：

(一)原始存储介质的扣押、封存状态是否完好；

(二)比对电子数据完整性校验值是否发生变化；

(三)电子数据的原件与备份是否相同；

(四)冻结后的电子数据是否生成新的操作日志。

第三十二条 对电子数据的合法性，注重审查以下内容：

(一)电子数据的收集、提取、保管的方法和过程是否规范；

(二)查询、勘验、扣押、调取、冻结等的法律手续是否齐全；

(三)勘验笔录、搜查笔录、提取笔录等取证记录是否完备；

(四)是否由符合法律规定的取证人员、见证人、持有人(提供人)等参与，因

客观原因没有见证人、持有人(提供人)签名或者盖章的，是否说明原因；

(五)是否按照有关规定进行同步录音录像；

(六)对于收集、提取的境外电子数据是否符合国(区)际司法协作及相关法律规定的要求。

第三十三条 对电子数据的关联性，注重审查以下内容：

(一)电子数据与案件事实之间的关联性；

(二)电子数据及其存储介质与案件当事人之间的关联性。

第三十四条 原始存储介质被扣押封存的，注重从以下方面审查扣押封存过程是否规范：

(一)是否记录原始存储介质的品牌、型号、容量、序列号、识别码、用户标识等外观信息，是否与实物一一对应；

(二)是否封存或者计算完整性校验值，封存前后是否拍摄被封存原始存储介质的照片，照片是否清晰反映封口或者张贴封条处的状况；

(三)是否由取证人员、见证人、持有人(提供人)签名或者盖章。

第三十五条 对原始存储介质制作数据镜像予以提取固定的，注重审查以下内容：

(一)是否记录原始存储介质的品牌、型号、容量、序列号、识别码、用户标识等外观信息，是否记录原始存储介质的存放位置、使用人、保管人；

(二)是否附有制作数据镜像的工具、方法、过程等必要信息；

(三)是否计算完整性校验值；

(四)是否由取证人员、见证人、持有人(提供人)签名或者盖章。

第三十六条 提取原始存储介质中的数据内容并予以固定的，注重审查以下内容：

(一)是否记录原始存储介质的品牌、型号、容量、序列号、识别码、用户标识等外观信息，是否记录原始存储介质的存放位置、使用人、保管人；

(二)所提取数据内容的原始存储路径，提取的工具、方法、过程等信息， 是否一并提取相关的附属信息、关联痕迹、系统环境等信息；

(三)是否计算完整性校验值；

(四)是否由取证人员、见证人、持有人(提供人)签名或者盖章。

第三十七条 对于在线提取的电子数据，注重审查以下内容：

(一)是否记录反映电子数据来源的网络地址、存储路径或者数据提取时的进入步骤等；

(二)是否记录远程计算机信息系统的访问方式、电子数据的提取日期和时间、提取的工具、方法等信息， 是否一并提取相关的附属信息、关联痕迹、系统环境等信息；

(三)是否计算完整性校验值；

(四)是否由取证人员、见证人、持有人(提供人)签名或者盖章。

对可能无法重复提取或者可能出现变化的电子数据，是否随案移送反映提取过程的拍照、录像、截屏等材料。

第三十八条 对冻结的电子数据，注重审查以下内容：

(一)冻结手续是否符合规定；

(二)冻结的电子数据是否与案件事实相关；

(三)冻结期限是否即将到期、有无必要继续冻结或者解除；

(四)冻结期间电子数据是否被增加、删除、修改等。

第三十九条 对调取的电子数据，注重审查以下内容：

(一)调取证据通知书是否注明所调取的电子数据的相关信息；

(二)被调取单位、个人是否在通知书回执上签名或者盖章；

(三)被调取单位、个人拒绝签名、盖章的，是否予以说明；

(四)是否计算完整性校验值或者以其他方法保证电子数据的完整性。

第四十条 对电子数据进行检查、侦查实验，注重审查以下内容：

(一)是否记录检查过程、检查结果和其他需要记录的内容， 并由检查人员签名或者盖章；

(二)是否记录侦查实验的条件、过程和结果， 并由参加侦查实验的人员签名或者盖章；

(三)检查、侦查实验使用的电子设备、网络环境等是否与发案现场一致或者基本一致；

(四)是否使用拍照、录像、录音、通信数据采集等一种或者多种方式客观记录检查、侦查实验过程。

第四十一条 对电子数据进行检验、鉴定，注重审查以下内容：

(一)鉴定主体的合法性。包括审查司法鉴定机构、司法鉴定人员的资质， 委托鉴定事项是否符合司法鉴定机构的业务范围，鉴定人员是否存在回避等情形；

(二)鉴定材料的客观性。包括鉴定材料是否真实、完整、充分， 取得方式是否合法，是否与原始电子数据一致；

(三)鉴定方法的科学性。包括鉴定方法是否符合国家标准、行业标准， 方法标准的选用是否符合相关规定；

(四)鉴定意见的完整性。是否包含委托人、委托时间、检材信息、鉴定或者分析论证过程、鉴定结果以及鉴定人签名、日期等内容；

(五)鉴定意见与其他在案证据能否相互印证。

对于鉴定机构以外的机构出具的检验、检测报告， 可以参照本条规定进行审查。

第四十二条 行政机关在行政执法和查办案件过程中依法收集、提取的电子数据，人民检察院经审查符合法定要求的，可以作为刑事案件的证据使用。

第四十三条 电子数据的收集、提取程序有下列瑕疵，经补正或者作出合理解释的，可以采用；不能补正或者作出合理解释的，不得作为定案的根据：

(一)未以封存状态移送的；

(二)笔录或者清单上没有取证人员、见证人、持有人(提供人)签名或者盖章的；

(三)对电子数据的名称、类别、格式等注明不清的；

(四)有其他瑕疵的。

第四十四条 电子数据系篡改、伪造、无法确定真伪的，或者有其他无法保证电子数据客观、真实情形的，不得作为定案的根据。

电子数据有增加、删除、修改等情形， 但经司法鉴定、当事人确认等方式确定与案件相关的重要数据未发生变化，或者能够还原电子数据原始状态、查清变化过程的，可以作为定案的根据。

第四十五条 对于无法直接展示的电子数据，人民检察院可以要求公安机关提供电子数据的内容、存储位置、附属信息、功能作用等情况的说明， 随案移送人民法院。

第四章 出庭支持公诉

第四十六条 人民检察院依法提起公诉的网络犯罪案件，具有下列情形之一的，可以建议人民法院召开庭前会议：

(一)案情疑难复杂的；

(二)跨国(边)境、跨区域案件社会影响重大的；

(三)犯罪嫌疑人、被害人等人数众多、证据材料较多的；

(四)控辩双方对电子数据合法性存在较大争议的；

(五)案件涉及技术手段专业性强，需要控辩双方提前交换意见的；

(六)其他有必要召开庭前会议的情形。

必要时，人民检察院可以向法庭申请指派检察技术人员或者聘请其他有专门知识的人参加庭前会议。

第四十七条 人民法院开庭审理网络犯罪案件，公诉人出示证据可以借助多媒体示证、动态演示等方式进行。必要时， 可以向法庭申请指派检察技术人员或者聘请其他有专门知识的人进行相关技术操作，并就专门性问题发表意见。

公诉人在出示电子数据时，应当从以下方面进行说明：

(一)电子数据的来源、形成过程；

(二)电子数据所反映的犯罪手段、人员关系、资金流向、行为轨迹等案件事实；

(三)电子数据与被告人供述、被害人陈述、证人证言、物证、书证等的相互印证情况；

(四)其他应当说明的内容。

第四十八条 在法庭审理过程中，被告人及其辩护人针对电子数据的客观性、合法性、关联性提出辩解或者辩护意见的， 公诉人可以围绕争议点从证据来源是否合法，提取、复制、制作过程是否规范， 内容是否真实完整，与案件事实有无关联等方面，有针对性地予以答辩。

第四十九条 支持、推动人民法院开庭审判网络犯罪案件全程录音录像。对庭审全程录音录像资料，必要时人民检察院可以商请人民法院复制，并将存储介质附检察卷宗保存。

第五章 跨区域协作办案

第五十条 对跨区域网络犯罪案件，上级人民检察院应当加强统一指挥和统筹协调，相关人民检察院应当加强办案协作。

第五十一条 上级人民检察院根据办案需要，可以统一调用辖区内的检察人员参与办理网络犯罪案件。

第五十二条 办理关联网络犯罪案件的人民检察院可以相互申请查阅卷宗材料、法律文书，了解案件情况，被申请的人民检察院应当予以协助。

第五十三条 承办案件的人民检察院需要向办理关联网络犯罪案件的人民检察院调取证据材料的，可以持相关法律文书和证明文件申请调取在案证据材料，被申请的人民检察院应当配合。

第五十四条 承办案件的人民检察院需要异地调查取证的，可以将相关法律文书及证明文件传输至证据所在地的人民检察院，请其代为调查取证。相关法律文书应当注明具体的取证对象、方式、内容和期限等。

被请求协助的人民检察院应当予以协助，及时将取证结果送达承办案件的人民检察院；无法及时调取的，应当作出说明。被请求协助的人民检察院有异议的，可以与承办案件的人民检察院进行协商；无法解决的，由承办案件的人民检察院报请共同的上级人民检察院决定。

第五十五条 承办案件的人民检察院需要询问异地证人、被害人的，可以通过远程视频系统进行询问，证人、被害人所在地的人民检察院应当予以协助。远程询问的，应当对询问过程进行同步录音录像。

第六章 跨国(边)境司法协作

第五十六条 办理跨国网络犯罪案件应当依照《中华人民共和国国际刑事司法协助法》及我国批准加入的有关刑事司法协助条约， 加强国际司法协作，维护我国主权、安全和社会公共利益， 尊重协作国司法主权、坚持平等互惠原则， 提升跨国司法协作质效。

第五十七条 地方人民检察院在案件办理中需要向外国请求刑事司法协助的，应当制作刑事司法协助请求书并附相关材料，经报最高人民检察院批准后，由我国与被请求国间司法协助条约规定的对外联系机关向外国提出申请。没有刑事司法协助条约的，通过外交途径联系。

第五十八条 人民检察院参加现场移交境外证据的检察人员不少于二人，外

方有特殊要求的除外。

移交、开箱、封存、登记的情况应当制作笔录，由最高人民检察院或者承办案件的人民检察院代表、外方移交人员签名或者盖章，一般应当全程录音录像。有其他见证人的，在笔录中注明。

第五十九条 人民检察院对境外收集的证据，应当审查证据来源是否合法、手续是否齐备以及证据的移交、保管、转换等程序是否连续、规范。

第六十条 人民检察院办理涉香港特别行政区、澳门特别行政区、台湾地区的网络犯罪案件，需要当地有关部门协助的，可以参照本规定及其他相关规定执行。

第七章 附 则

第六十一条 人民检察院办理网络犯罪案件适用本规定，本规定没有规定的，适用其他相关规定。

第六十二条 本规定中下列用语的含义：

(一)信息网络，包括以计算机、电视机、固定电话机、移动电话机等电子设备为终端的计算机互联网、广播电视网、固定通信网、移动通信网等信息网络，以及局域网络；

(二)存储介质，是指具备数据存储功能的电子设备、硬盘、光盘、优盘、记忆棒、存储芯片等载体；

(三)完整性校验值，是指为防止电子数据被篡改或者破坏，使用散列算法等特定算法对电子数据进行计算，得出的用于校验数据完整性的数据值；

(四)数字签名，是指利用特定算法对电子数据进行计算，得出的用于验证电子数据来源和完整性的数据值；

(五)数字证书，是指包含数字签名并对电子数据来源、完整性进行认证的电子文件；

(六)生物识别信息，是指计算机利用人体所固有的生理特征(包括人脸、指纹、声纹、虹膜、 DNA 等)或者行为特征(步态、击键习惯等)来进行个人身份识别的信息；

(七)运行脚本，是指使用一种特定的计算机编程语言，依据符合语法要求编写的执行指定操作的可执行文件；

(八)数据镜像，是指二进制(0101 排序的数据码流)相同的数据复制件，与原件的内容无差别；

(九)MAC 地址，是指计算机设备中网卡的唯一标识，每个网卡有且只有一个 MAC 地址。

第六十三条 人民检察院办理国家安全机关、海警机关、监狱等移送的网络犯罪案件，适用本规定和其他相关规定。

第六十四条 本规定由最高人民检察院负责解释。

第六十五条 本规定自发布之日起施行。

最高人民法院关于审理使用人脸识别技术处理个人信息相关民事案件适用法律若干问题的规定

法释〔2021〕15 号

《最高人民法院关于审理使用人脸识别技术处理个人信息相关民事案件适用法律若干问题的规定》已于 2021 年 6 月 8 日由最高人民法院审判委员会第 1841 次会议通过，现予公布，自 2021 年 8 月 1 日起施行。

最高人民法院

2021 年 7 月 27 日

最高人民法院关于审理使用人脸识别技术处理个人信息相关民事案件适用法律若干问题的规定

(2021 年 6 月 8 日最高人民法院审判委员会第 1841 次会议通过，自 2021 年 8 月 1 日起施行)

为正确审理使用人脸识别技术处理个人信息相关民事案件，保护当事人合法权益，促进数字经济健康发展，根据《中华人民共和国民法典》《中华人民共和国网络安全法》《中华人民共和国消费者权益保护法》《中华人民共和国电子商务法》《中华人民共和国民事诉讼法》等法律的规定，结合审判实践，制定本规定。

第一条 因信息处理者违反法律、行政法规的规定或者双方的约定使用人脸识别技术处理人脸信息、处理基于人脸识别技术生成的人脸信息所引起的民事案件，适用本规定。

人脸信息的处理包括人脸信息的收集、存储、使用、加工、传输、提供、公开等。

本规定所称人脸信息属于民法典第一千零三十四条规定的“生物识别信息”。

第二条 信息处理者处理人脸信息有下列情形之一的，人民法院应当认定属于侵害自然人人格权益的行为：

(一)在宾馆、商场、银行、车站、机场、体育场馆、娱乐场所等经营场所、公共场所违反法律、行政法规的规定使用人脸识别技术进行人脸验证、辨识或者分析；

(二)未公开处理人脸信息的规则或者未明示处理的目的、方式、范围；

(三)基于个人同意处理人脸信息的，未征得自然人或者其监护人的单独同意，或者未按照法律、行政法规的规定征得自然人或者其监护人的书面同意；

(四)违反信息处理者明示或者双方约定的处理人脸信息的目的、方式、范围等；

(五)未采取应有的技术措施或者其他必要措施确保其收集、存储的人脸信息安全，致使人脸信息泄露、篡改、丢失；

(六)违反法律、行政法规的规定或者双方的约定，向他人提供人脸信息；

(七)违背公序良俗处理人脸信息；

(八)违反合法、正当、必要原则处理人脸信息的其他情形。

第三条 人民法院认定信息处理者承担侵害自然人人格权益的民事责任，应当适用民法典第九百九十八条的规定，并结合案件具体情况综合考量受害人是否为未成年人、告知同意情况以及信息处理的必要程度等因素。

第四条 有下列情形之一，信息处理者以已征得自然人或者其监护人同意为由抗辩的，人民法院不予支持：

(一)信息处理者要求自然人同意处理其人脸信息才提供产品或者服务的，但是处理人脸信息属于提供产品或者服务所必需的除外；

(二)信息处理者以与其他授权捆绑等方式要求自然人同意处理其人脸信息的；

(三)强迫或者变相强迫自然人同意处理其人脸信息的其他情形。

第五条 有下列情形之一，信息处理者主张其不承担民事责任的，人民法院依法予以支持：

(一)为应对突发公共卫生事件，或者紧急情况下为保护自然人的生命健康和

财产安全所必需而处理人脸信息的；

(二)为维护公共安全，依据国家有关规定在公共场所使用人脸识别技术的；

(三)为公共利益实施新闻报道、舆论监督等行为在合理的范围内处理人脸信息的；

(四)在自然人或者其监护人同意的范围内合理处理人脸信息的；

(五)符合法律、行政法规规定的其他情形。

第六条 当事人请求信息处理者承担民事责任的，人民法院应当依据民事诉讼法第六十四条及《最高人民法院关于适用〈中华人民共和国民事诉讼法〉的解释》第九十条、第九十一条，《最高人民法院关于民事诉讼证据的若干规定》的相关规定确定双方当事人的举证责任。

信息处理者主张其行为符合民法典第一千零三十五条第一款规定情形的，应当就此所依据的事实承担举证责任。

信息处理者主张其不承担民事责任的，应当就其行为符合本规定第五条规定的情形承担举证责任。

第七条 多个信息处理者处理人脸信息侵害自然人人格权益，该自然人主张多个信息处理者按照过错程度和造成损害结果的大小承担侵权责任的，人民法院依法予以支持；符合民法典第一千一百六十八条、第一千一百六十九条第一款、第一千一百七十条、第一千一百七十一条等规定的相应情形，该自然人主张多个信息处理者承担连带责任的，人民法院依法予以支持。

信息处理者利用网络服务处理人脸信息侵害自然人人格权益的，适用民法典第一千一百九十五条、第一千一百九十六条、第一千一百九十七条等规定。

第八条 信息处理者处理人脸信息侵害自然人人格权益造成财产损失，该自然人依据民法典第一千一百八十二条主张财产损害赔偿的，人民法院依法予以支持。

自然人为制止侵权行为所支付的合理开支，可以认定为民法典第一千一百八十二条规定的财产损失。合理开支包括该自然人或者委托代理人对侵权行为进行调查、取证的合理费用。人民法院根据当事人的请求和具体案情， 可以将合理的律师费用计算在赔偿范围内。

第九条 自然人有证据证明信息处理者使用人脸识别技术正在实施或者即将

实施侵害其隐私权或者其他人格权益的行为，不及时制止将使其合法权益受到难以弥补的损害，向人民法院申请采取责令信息处理者停止有关行为的措施的，人民法院可以根据案件具体情况依法作出人格权侵害禁令。

第十条 物业服务企业或者其他建筑物管理人以人脸识别作为业主或者物业使用人出入物业服务区域的唯一验证方式，不同意的业主或者物业使用人请求其提供其他合理验证方式的，人民法院依法予以支持。

物业服务企业或者其他建筑物管理人存在本规定第二条规定的情形，当事人请求物业服务企业或者其他建筑物管理人承担侵权责任的，人民法院依法予以支持。

第十一条 信息处理者采用格式条款与自然人订立合同，要求自然人授予其无期限限制、不可撤销、可任意转授权等处理人脸信息的权利， 该自然人依据民法典第四百九十七条请求确认格式条款无效的，人民法院依法予以支持。

第十二条 信息处理者违反约定处理自然人的人脸信息，该自然人请求其承担违约责任的，人民法院依法予以支持。该自然人请求信息处理者承担违约责任时，请求删除人脸信息的，人民法院依法予以支持；信息处理者以双方未对人脸信息的删除作出约定为由抗辩的，人民法院不予支持。

第十三条 基于同一信息处理者处理人脸信息侵害自然人人格权益发生的纠纷，多个受害人分别向同一人民法院起诉的，经当事人同意，人民法院可以合并审理。

第十四条 信息处理者处理人脸信息的行为符合民事诉讼法第五十五条、消费者权益保护法第四十七条或者其他法律关于民事公益诉讼的相关规定，法律规定的机关和有关组织提起民事公益诉讼的，人民法院应予受理。

第十五条 自然人死亡后，信息处理者违反法律、行政法规的规定或者双方的约定处理人脸信息，死者的近亲属依据民法典第九百九十四条请求信息处理者承担民事责任的，适用本规定。

第十六条 本规定自 2021 年 8 月 1 日起施行。

信息处理者使用人脸识别技术处理人脸信息、处理基于人脸识别技术生成的人脸信息的行为发生在本规定施行前的，不适用本规定。

最高人民法院 最高人民检察院 公安部关于办理信息网络犯罪案件适用刑事诉

讼程序若干问题的意见

法发〔2022〕23 号

为依法惩治信息网络犯罪活动，根据《中华人民共和国刑法》《中华人民共和国刑事诉讼法》以及有关法律、司法解释的规定，结合侦查、起诉、审判实践，现就办理此类案件适用刑事诉讼程序问题提出以下意见。

一、关于信息网络犯罪案件的范围

1.本意见所称信息网络犯罪案件包括：

(1)危害计算机信息系统安全犯罪案件；

(2)拒不履行信息网络安全管理义务、非法利用信息网络、帮助信息网络犯罪活动的犯罪案件；

(3)主要行为通过信息网络实施的诈骗、赌博、侵犯公民个人信息等其他犯罪案件。

二、关于信息网络犯罪案件的管辖

2.信息网络犯罪案件由犯罪地公安机关立案侦查。必要时， 可以由犯罪嫌疑人居住地公安机关立案侦查。

信息网络犯罪案件的犯罪地包括用于实施犯罪行为的网络服务使用的服务器所在地，网络服务提供者所在地，被侵害的信息网络系统及其管理者所在地，犯罪过程中犯罪嫌疑人、被害人或者其他涉案人员使用的信息网络系统所在地，被害人被侵害时所在地以及被害人财产遭受损失地等。

涉及多个环节的信息网络犯罪案件，犯罪嫌疑人为信息网络犯罪提供帮助的，其犯罪地、居住地或者被帮助对象的犯罪地公安机关可以立案侦查。

3.有多个犯罪地的信息网络犯罪案件，由最初受理的公安机关或者主要犯罪地公安机关立案侦查。有争议的，按照有利于查清犯罪事实、有利于诉讼的原则，协商解决；经协商无法达成一致的，由共同上级公安机关指定有关公安机关立案侦查。需要提请批准逮捕、移送审查起诉、提起公诉的， 由立案侦查的公安机关所在地的人民检察院、人民法院受理。

4.具有下列情形之一的，公安机关、人民检察院、人民法院可以在其职责范围内并案处理：

(1)一人犯数罪的；

(2)共同犯罪的;

(3)共同犯罪的犯罪嫌疑人、被告人还实施其他犯罪的;

(4)多个犯罪嫌疑人、被告人实施的犯罪行为存在关联,并案处理有利于查明全部案件事实的。

对为信息网络犯罪提供程序开发、互联网接入、服务器托管、网络存储、通讯传输等技术支持,或者广告推广、支付结算等帮助, 涉嫌犯罪的,可以依照第一款的规定并案侦查。

有关公安机关依照前两款规定并案侦查的案件,需要提请批准逮捕、移送审查起诉、提起公诉的,由该公安机关所在地的人民检察院、人民法院受理。

5.并案侦查的共同犯罪或者关联犯罪案件,犯罪嫌疑人人数众多、案情复杂的,公安机关可以分案移送审查起诉。分案移送审查起诉的, 应当对并案侦查的依据、分案移送审查起诉的理由作出说明。

对于前款规定的案件,人民检察院可以分案提起公诉,人民法院可以分案审理。

分案处理应当以有利于保障诉讼质量和效率为前提,并不得影响当事人质证权等诉讼权利的行使。

6.依照前条规定分案处理,公安机关、人民检察院、人民法院在分案前有管辖权的,分案后对相关案件的管辖权不受影响。根据具体情况, 分案处理的相关案件可以由不同审级的人民法院分别审理。

7.对于共同犯罪或者已并案侦查的关联犯罪案件,部分犯罪嫌疑人未到案,但不影响对已到案共同犯罪或者关联犯罪的犯罪嫌疑人、被告人的犯罪事实认定的,可以先行追究已到案犯罪嫌疑人、被告人的刑事责任。之前未到案的犯罪嫌疑人、被告人归案后, 可以由原办案机关所在地公安机关、人民检察院、人民法院管辖其所涉及的案件。

8.对于具有特殊情况,跨省(自治区、直辖市)指定异地公安机关侦查更有利于查清犯罪事实、保证案件公正处理的重大信息网络犯罪案件, 以及在境外实施的信息网络犯罪案件,公安部可以商最高人民检察院和最高人民法院指定侦查管辖。

9.人民检察院对于审查起诉的案件,按照刑事诉讼法的管辖规定,认为应当

由上级人民检察院或者同级其他人民检察院起诉的，应当将案件移送有管辖权的人民检察院，并通知移送起诉的公安机关。人民检察院认为需要依照刑事诉讼法的规定指定审判管辖的，应当协商同级人民法院办理指定管辖有关事宜。

10.犯罪嫌疑人被多个公安机关立案侦查的，有关公安机关一般应当协商并案处理，并依法移送案件。协商不成的，可以报请共同上级公安机关指定管辖。

人民检察院对于审查起诉的案件，发现犯罪嫌疑人还有犯罪被异地公安机关立案侦查的，应当通知移送审查起诉的公安机关。

人民法院对于提起公诉的案件，发现被告人还有其他犯罪被审查起诉、立案侦查的，可以协商人民检察院、公安机关并案处理， 但可能造成审判过分迟延的除外。决定对有关犯罪并案处理， 符合《中华人民共和国刑事诉讼法》第二百零四条规定的，人民检察院可以建议人民法院延期审理。

三、关于信息网络犯罪案件的调查核实

11.公安机关对接受的案件或者发现的犯罪线索，在审查中发现案件事实或者线索不明，需要经过调查才能够确认是否达到刑事立案标准的，经公安机关办案部门负责人批准，可以进行调查核实；经过调查核实达到刑事立案标准的，应当及时立案。

12.调查核实过程中，可以采取询问、查询、勘验、检查、鉴定、调取证据材料等不限制被调查对象人身、财产权利的措施， 不得对被调查对象采取强制措施，不得查封、扣押、冻结被调查对象的财产，不得采取技术侦查措施。

13.公安机关在调查核实过程中依法收集的电子数据等材料，可以根据有关规定作为证据使用。

调查核实过程中收集的材料作为证据使用的，应当随案移送，并附批准调查核实的相关材料。

调查核实过程中收集的证据材料经查证属实，且收集程序符合有关要求的，可以作为定案依据。

四、关于信息网络犯罪案件的取证

14.公安机关向网络服务提供者调取电子数据的，应当制作调取证据通知书，注明需要调取的电子数据的相关信息。调取证据通知书及相关法律文书可以采用数据电文形式。跨地域调取电子数据的， 可以通过公安机关信息化系统传输相关

数据电文。

网络服务提供者向公安机关提供电子数据的，可以采用数据电文形式。采用数据电文形式提供电子数据的，应当保证电子数据的完整性，并制作电子证明文件，载明调证法律文书编号、单位电子公章、完整性校验值等保护电子数据完整性方法的说明等信息。

数据电文形式的法律文书和电子证明文件，应当使用电子签名、数字水印等方式保证完整性。

15.询(讯)问异地证人、被害人以及与案件有关联的犯罪嫌疑人的，可以由办案地公安机关通过远程网络视频等方式进行并制作笔录。

远程询(讯)问的，应当由协作地公安机关事先核实被询(讯)问人的身份。办案地公安机关应当将询(讯)问笔录传输至协作地公安机关。询(讯)问笔录经被询(讯)问人确认并逐页签名、捺指印后，由协作地公安机关协作人员签名或者盖章，并将原件提供给办案地公安机关。询(讯)问人员收到笔录后，应当在首页右上方写明“于某年某月某日收到”，并签名或者盖章。

远程询(讯)问的，应当对询(讯)问过程同步录音录像，并随案移送。

异地证人、被害人以及与案件有关联的犯罪嫌疑人亲笔书写证词、供词的，参照执行本条第二款规定。

16.人民检察院依法自行侦查、补充侦查，或者人民法院调查核实相关证据的，适用本意见第 14 条、第 15 条的有关规定。

17.对于依照本意见第 14 条的规定调取的电子数据，人民检察院、人民法院可以通过核验电子签名、数字水印、电子数据完整性校验值及调证法律文书编号是否与证明文件相一致等方式，对电子数据进行审查判断。

对调取的电子数据有疑问的，由公安机关、提供电子数据的网络服务提供者作出说明，或者由原调取机关补充收集相关证据。

五、关于信息网络犯罪案件的其他问题

18.采取技术侦查措施收集的材料作为证据使用的，应当随案移送，并附采取技术侦查措施的法律文书、证据材料清单和有关说明材料。

移送采取技术侦查措施收集的视听资料、电子数据的， 应当由两名以上侦查人员制作复制件，并附制作说明，写明原始证据材料、原始存储介质的存放地点

等信息，由制作人签名，并加盖单位印章。

19.采取技术侦查措施收集的证据材料，应当经过当庭出示、辨认、质证等法庭调查程序查证。

当庭调查技术侦查证据材料可能危及有关人员的人身安全，或者可能产生其他严重后果的，法庭应当采取不暴露有关人员身份和技术侦查措施使用的技术设备、技术方法等保护措施。必要时，审判人员可以在庭外对证据进行核实。

20.办理信息网络犯罪案件，对于数量特别众多且具有同类性质、特征或者功能的物证、书证、证人证言、被害人陈述、视听资料、电子数据等证据材料，确因客观条件限制无法逐一收集的，应当按照一定比例或者数量选取证据，并对选取情况作出说明和论证。

人民检察院、人民法院应当重点审查取证方法、过程是否科学。经审查认为取证不科学的，应当由原取证机关作出补充说明或者重新取证。

人民检察院、人民法院应当结合其他证据材料， 以及犯罪嫌疑人、被告人及其辩护人所提辩解、辩护意见， 审查认定取得的证据。经审查， 对相关事实不能排除合理怀疑的，应当作出有利于犯罪嫌疑人、被告人的认定。

21.对于涉案人数特别众多的信息网络犯罪案件，确因客观条件限制无法收集证据逐一证明、逐人核实涉案账户的资金来源， 但根据银行账户、非银行支付账户等交易记录和其他证据材料，足以认定有关账户主要用于接收、流转涉案资金的，可以按照该账户接收的资金数额认定犯罪数额，但犯罪嫌疑人、被告人能够作出合理说明的除外。案外人提出异议的，应当依法审查。

22.办理信息网络犯罪案件，应当依法及时查封、扣押、冻结涉案财物，督促涉案人员退赃退赔，及时追赃挽损。

公安机关应当全面收集证明涉案财物性质、权属情况、依法应予追缴、没收或者责令退赔的证据材料，在移送审查起诉时随案移送并作出说明。其中， 涉案财物需要返还被害人的，应当尽可能查明被害人损失情况。人民检察院应当对涉案财物的证据材料进行审查，在提起公诉时提出处理意见。人民法院应当依法作出判决，对涉案财物作出处理。

对应当返还被害人的合法财产，权属明确的，应当依法及时返还；权属不明的，应当在人民法院判决、裁定生效后， 按比例返还被害人，但已获退赔的部分

应予扣除。

23.本意见自 2022 年 9 月 1 日起施行。《最高人民法院、最高人民检察院、公安部关于办理网络犯罪案件适用刑事诉讼程序若干问题的意见》(公通字〔2014〕10 号)同时废止。

最高人民法院 最高人民检察院

公安部

2022 年 8 月 26 日

最高人民法院关于为促进消费提供司法服务和保障的意见

法发〔2022〕35 号

消费对经济发展具有基础性作用，最终消费是经济增长的持久动力。促进消费对释放内需潜力、推动经济转型升级、保障和改善民生具有重要意义。为完整、准确、全面贯彻新发展理念、加快构建新发展格局、着力推动高质量发展，进一步发挥人民法院职能作用，服务保障全面促进消费、加快消费提质升级，助力实施扩大内需战略，提出如下意见。

一、加强消费者权益司法保护

1.以最严的举措保护食品、药品安全。严格贯彻落实“四个最严”要求，充分发挥审判职能，对食品和药品生产、运输、仓储、销售全链条所涉制假售假行为进行严厉打击，确保人民群众“舌尖上的安全”和“针尖上的安全”。严格依法适用首负责任制，避免生产者和经营者相互推诿，及时保护消费者合法权益。依法支持和监督行政机关管理生产经营不符合食品安全标准食品的食品生产经营者、违法生产经营行为造成严重后果的食品生产经营者，以及生产、销售、使用假药、劣药的生产经营者，维护市场秩序。依法严厉惩治生产、销售不符合安全标准的食品罪和生产、销售有毒、有害食品罪，以及生产、销售假药罪和生产、销售劣药罪，充分发挥刑罚对涉食品、药品安全犯罪行为的震慑作用。

2.以最严的手段斩断“黑作坊”生产经营链条。生产经营未依法标明生产者名称、地址、生产日期、保质期的预包装食品，消费者主张生产经营者承担惩罚性赔偿责任的，人民法院应当依法支持，但法律、行政法规、食品安全国家标准对标签标注事项另有规定的除外。未取得药品相关批准证明文件而生产

药品或者明知是该类药品而销售，药品的适应症、功能主治或者成分不明的，按妨害药品管理罪惩处；药品被依法认定为假劣药，生产经营者同时构成生产、销售假药罪或者生产、销售劣药罪的，依照处罚较重的规定定罪处罚。既要依法追究生产者责任，也要依法追究经营者责任，坚决斩断“黑作坊”食品、药品的生产经营链条。

3.以最严的赔偿责任遏制食品、药品制假售假行为。充分发挥惩罚性赔偿责任对制假售假行为的遏制作用。生产不符合食品安全标准的食品或者经营明知是不符合食品安全标准的食品，生产假药、劣药或者明知是假药、劣药仍然销售、使用，消费者、受害人或者其近亲属请求生产经营者承担惩罚性赔偿责任的，人民法院应当依法支持。

4.加强预付式消费中消费者权益保护。经营者以打折、低价吸引消费者预存费用、办卡消费后，不兑现承诺，随意扣费、任意加价、降低商品或者服务质量，消费者请求经营者承担违约责任的，人民法院应当依法支持。经营者收取消费者预付款后未与消费者签订书面合同，导致双方对合同内容产生争议的，可依据交易习惯和民法典第五百一十一条规定认定合同内容。经营者收取预付款后，终止营业却不通知消费者退款，导致消费者既无法继续获得商品或者服务也无法申请退款，构成欺诈的，对消费者请求经营者承担惩罚性赔偿责任的诉讼请求，人民法院应当依法支持。经营者的行为构成犯罪的，依法追究刑事责任。

5.依法整治消费领域“霸王条款”。提供格式条款的经营者未依法履行提示或者说明义务，致使消费者没有注意或者理解与其有重大利害关系的条款的，消费者有权主张该条款不成为合同的内容。消费者主张经营者提供的排除或者不合理地限制消费者主要权利的格式条款，以及不合理地免除或者减轻经营者责任的格式条款无效的，人民法院应当依法支持。对格式条款的理解发生争议，消费者主张依照民法典第四百九十八条规定进行解释，经营者以其享有最终解释权为由进行抗辩的，人民法院对其抗辩不予支持。

6.妥善审理直播电商、平台纠纷案件。结合直播间运营者是否尽到标明义务以及交易外观、直播间运营者与经营者的约定、与经营者的合作模式、交易过程以及消费者认知等因素认定直播间运营者责任。网络餐饮服务平台经营者

未尽实名登记、审查许可证等法定义务，消费者主张网络餐饮服务平台经营者与入网餐饮服务提供者承担连带责任的，人民法院应当依法支持。综合销售者出售商品的性质、来源、数量、价格、频率、是否有其他销售渠道、收入等因素，能够认定销售者系从事商业经营活动，在二手商品网络交易平台购买商品受到损害的消费者主张销售者依据消费者权益保护法承担经营者责任的，人民法院应当依法支持。

7.加强新业态下消费者权益保护。消费者通过网络购买商品，有权依法自收到商品之日起七日内退货，无需说明理由，但是法律另有规定的除外。消费者因检查商品的必要对商品进行拆封查验且不影响商品完好，电子商务经营者不得以商品已拆封为由主张不适用七日无理由退货制度。电子商务经营者作出更优承诺的，应当遵守。收到商品七日后符合法定或者约定的合同解除条件，消费者主张及时退货的，人民法院应当依法支持。

8.加强快递服务消费者权益保护。因快递人员擅自使用快递商品、违规打开快递包装、暴力分拣快递等故意或者重大过失行为导致快递商品丢失、毁损，消费者请求赔偿损失，快递服务提供者依据免责条款提出免责抗辩的，人民法院对其抗辩不予支持。经营者向消费者盲发快递，消费者请求无条件退货的，人民法院应当依法支持。

9.加强消费者个人信息保护。经营者处理敏感个人信息、跨境转移个人信息等行为应当取得消费者单独同意，经营者以其获得消费者概括同意为由进行免责抗辩的，人民法院对其抗辩不予支持。经营者过度收集消费者个人信息、在消费者撤回同意后未停止处理或者未及时删除消费者个人信息、未取得未成年消费者父母或者其他监护人的同意处理不满十四周岁未成年消费者个人信息，消费者请求经营者承担停止侵害等民事责任的，人民法院应当依法支持。经营者以消费者不同意处理个人信息为由拒绝提供商品或者服务，致使消费者被迫同意经营者处理个人信息，消费者请求经营者承担停止侵害等民事责任的，人民法院应当依法支持。经营者处理个人信息侵害个人信息权益造成损害，不能证明自己没有过错的，应当承担损害赔偿等侵权责任。

10.加强住房消费者权益保护。严格保护依法成立生效的房屋买卖合同，维护市场秩序，助力实施房地产市场平稳健康发展长效机制，积极保护居民合理

自住需求，遏制投资投机性需求，促进居住消费健康发展，推动实现稳地价、稳房价、稳预期。对当事人逾期付款、逾期交房、逾期办证等违约行为引起的商品房买卖合同纠纷，人民法院要加强调解，引导当事人协商解决纠纷；当事人请求违约方承担逾期付款、逾期交房、逾期办证的违约责任的，人民法院应当依照合同约定或者商品房买卖合同司法解释第十三条和第十四条规定处理。出卖人出售房屋后又与第三人恶意串通，另行订立商品房买卖合同并将已出售房屋交付第三人使用，导致原来的买受人无法取得房屋的，人民法院应当依法认定出卖人与第三人订立的商品房买卖合同无效。

11.妥善处理消费者出行纠纷。疫情或者疫情防控措施导致消费者不能履行旅游、客运、住宿等合同，消费者请求解除合同、退还定金和价款等费用的，人民法院应当依法支持。消费者请求变更经营者提供服务的时间等合同内容的，人民法院应当加强调解；调解不成的，人民法院可综合考虑交易习惯、合同目的、案件具体情况等因素作出裁判。经营者仅以消费者超出其公布的退款时间为由，主张拒退、少退定金和价款等费用的，人民法院不予支持。充分发挥旅游巡回法庭作用，就地、快速解决旅游纠纷，方便消费者景区维权。

12.妥善处理涉疫情消费购物纠纷。经营者明知口罩、护目镜、防护服、消毒液等防疫物品属于假冒伪劣商品仍然经营，构成欺诈，消费者请求经营者承担惩罚性赔偿责任的，人民法院应当依法支持。经营者的行为构成犯罪的，依法追究刑事责任。疫情期间，经营者利用消费者处于危困状态、缺乏判断能力等情形，哄抬物价、收取高额快递费等费用，致使所订立合同显失公平，消费者请求撤销合同的，人民法院应当依法支持。合同被撤销后，消费者不能返还或者没有必要返还合同标的物的，人民法院可根据相关法律规定、交易习惯和公平原则认定消费者应折价补偿的价款。

13. 妥善处理医疗健康服务和体育消费纠纷。依法审理医疗损害责任纠纷案件，积极保护患者等各方当事人的合法权益。依法惩处涉医违法犯罪，严惩“医闹”，维护正常医疗秩序，构建和谐医患关系。积极引导医疗机构等主体增加高质量的医疗、养生保健、康复、健康旅游等服务，助力推进健康中国建设。准确适用自甘风险等民事法律制度，妥善处理体育消费中产生的各类纠纷，促进群众体育消费，助力实施全民健身战略。

14.加强未成年消费者权益保护。妥善处理生育、托育、教育等服务合同纠纷，促进育幼服务消费发展，助力提升教育服务质量。学校、托幼机构等单位的食堂未严格遵守法律、行政法规和食品安全标准，未从取得食品生产经营许可的企业订餐，或者未按照要求对订购的食品进行查验，导致提供的食品不符合食品安全标准，消费者请求其承担赔偿责任的，人民法院应当依法支持。依法办理危害食品安全刑事案件，将“危害专供婴幼儿的主辅食品安全”作为加重处罚情节，加强对未成年人食品安全的特殊保护。网络游戏、网络直播服务提供者违反法律规定向未成年人提供网络游戏、网络直播服务，收取充值费用、接受直播打赏，消费者请求返还游戏充值费、打赏费的，人民法院应当依法支持。限制民事行为能力人未经其监护人同意，通过参与网络付费游戏或者网络直播平台打赏等方式支出与其年龄、智力不相适应的款项，消费者请求返还该款项的，人民法院应当依法支持。加大对网络违法行为整治力度，积极营造健康、清朗、有利于未成年人成长的网络环境。

15.加强老年消费者权益保护。通过夸大宣传、虚构商品或者服务的治疗、保健、养生等功能，向老年消费者销售质次价高的商品或者服务，构成欺诈，消费者请求生产经营者承担惩罚性赔偿责任的，人民法院应当依法支持。经营者诱导老年消费者购买不符合其需求或者明显超出其需求范围的保健食品等商品或者服务，致使合同显失公平，消费者请求撤销合同的，人民法院应当依法支持。经营者的行为构成诈骗罪的，依法追究刑事责任；同时构成生产、销售伪劣产品罪等其他犯罪的，依照处罚较重的规定定罪处罚。通过营造良好法治环境，服务养老事业和养老产业协同发展，助力发展银发经济。

16.加强农村消费者权益保护。依法严厉打击农村食品市场存在的假冒知名品牌、滥用食品添加剂、销售过期食品以及制售无生产厂家、无生产日期、无保质期、无食品生产许可的食品等违法行为。助推“快递进村”，为大型商贸流通企业、电子商务平台和现代服务企业向农村延伸、开拓农村消费市场提供优质司法服务，让农村消费者充分享受好商品、好服务、好价格。

二、加强生产经营者权益司法保护

17.依法保护生产经营者的产权和经营自主权。加强产权司法保护，全面依法平等保护各类产权，完善以公平为原则的产权保护制度，充分发挥产权保护

对激励商品和服务产出的作用，助力扩大消费供给。依法审理涉市场准入和经营自主权等行政案件，充分保障生产经营者依法自行组织生产经营的权利。对于行政机关违法限制生产经营者建设汽车充电设施、物业管理公司无理阻碍业主建设汽车充电设施的行为，应依法予以规范，助力解决电动汽车消费中的痛点、堵点问题。

18.依法保护农村各类市场主体权益。依法惩治生产销售假种子、假化肥、假农药等不符合国家强制性技术标准或者安全标准的农业生产资料、伪劣商品等违法犯罪行为，依法保护农村市场主体合法权益。严厉打击种子套牌侵权行为，切实维护种业创新主体合法权益，净化种业市场，维护粮食安全。助推实施“数商兴农”和“互联网+”农产品出村进城等工程，助力实现质量兴农、科技兴农和绿色发展目标，为实施乡村振兴战略提供有力司法服务和保障。

19.加强知识产权保护。严格实施知识产权侵权惩罚性赔偿制度，有效遏制知识产权侵权行为，通过加强司法保护促进科技创新成果的产出和运用，助力科技强国建设。依法整治知识产权领域虚假诉讼、恶意诉讼、滥用诉权等不诚信诉讼行为，积极为广大市场主体技术研发和科技创新创造良好法治环境。加大对“专精特新”中小企业关键核心技术和原始创新成果的司法保护力度，支持和引导市场主体通过技术进步和科技创新提升核心竞争力，积极发挥供给侧对消费升级的支撑引领作用。加强文化创意产品著作权保护，鼓励文化创意产品创作，助推优质文化资源开发和中华优秀传统文化创造性转化、创新性发展，助力增加优质文化产品和服务供给。

20.保障平台经济健康有序发展。准确认定电子商务平台经营者、平台内经营者以及货运物流服务提供者等主体的法律责任。依法保护、引导电子商务平台经营者、快递物流经营者等市场主体在疫情防控中做好防疫物资和重要民生商品保供“最后一公里”的线上线下联动。引导电子商务平台经营者等市场主体加快人工智能、云计算、区块链、操作系统、处理器等领域技术研发突破和商业模式创新，不断开拓新的消费市场。把握好平台经济发展中的“红绿灯”，稳定发展预期，激发投资活力，助力构建电子商务平台经营者、平台内经营者、消费者等各方权益均得到有效保护、各方积极性均得到充分激发的平台发展环境，让资本在促消费、稳增长、惠民生方面发挥更大更好的作用。

21．助力培育新型消费。依法支持线上线下商品消费融合发展。助推传统线下业态数字化改造和转型升级，助力智慧超市、智慧商店、智慧餐厅等新零售业态发展。依法保护 5G 网络和千兆光网应用，依法支持自动驾驶、无人配送等技术应用。妥善处理“互联网+社会服务”、“互联网+医疗健康”服务等新服务类型引发的纠纷，既要依法保护消费者合法权益，又要依法支持无接触交易服务等新类型消费模式发展。妥善处理共享出行、共享住宿、共享旅游等共享经济领域产生的纠纷，合理认定相关民事主体的注意义务和法律责任，支持和引导新的生活和消费方式健康发展。依法保护新个体经济，支持社交电商、网络直播等多样化经营模式。

22.妥善处理房屋租赁合同纠纷。疫情或者疫情防控措施导致小微企业、个体工商户等承租人没有收入或者收入明显减少，造成支付租金困难，出租人请求解除房屋租赁合同、由承租人承担违约责任的，人民法院应当加强调解，引导出租人和承租人合理分担损失，共克时艰。对国有房屋租金数额发生争议，承租人请求按照有关政府机关的规定减免租金的，人民法院应当依法支持。出租人减免租金后主张税务机关按照相关规定减免当年房产税、城镇土地使用税，符合法律规定或者国家税收政策的，人民法院应当依法支持。

三、维护诚信公平高效的市场秩序

23.营造诚实守信的市场环境。生产经营者虚构、夸大商品和服务的功效，构成欺诈，消费者请求生产经营者承担惩罚性赔偿责任的，人民法院应当依法支持。生产经营者的行为构成犯罪的，依法追究刑事责任。坚决打击电信网络诈骗等犯罪活动，遏制欺诈消费者的不诚信行为，引导生产经营者通过提高商品和服务质量获得竞争优势。促进经营者诚实守信经营，保障消费者明明白白消费。

24.维护有利于促进消费的公平竞争市场秩序。依法规制具有市场支配地位的电子商务平台经营者等市场主体实施收取垄断高价、强制“二选一”等滥用市场支配地位行为。积极营造有利于小微企业、个体工商户发展的营商环境，遏制因垄断、不正当竞争导致市场竞争环境恶化而损害消费者权益的行为，充分发挥小微企业、个体工商户在丰富商品和服务供给、增加群众收入、促进消费发展中的作用。依法规范歧视性待遇、虚假宣传、刷单炒信、强制搭售等直

接损害消费者权益的垄断和不正当竞争行为，积极营造公平竞争的市场环境。

25.推动构建有利于增强消费信心的社会信用体系。加强与行政机关等单位的信息沟通，积极对接市场监管部门消费领域失信名单制度，推动共建失信违法生产经营者信息披露平台。完善守信激励和失信惩戒机制，增加违法经营成本，营造不敢、不能、不愿违法经营的市场环境。依法支持、引导行业协会、电子商务平台经营者等主体构建协会内和平台内信用惩戒机制，通过行业自治、平台规制防范和减少欺诈等违法生产经营行为，助力加强消费信用体系建设。积极推动建设多力量参与、多渠道共建、多平台共促，有利于遏制欺诈、增强消费信心的社会信用体系。

26.依法保障安全高效的物流体系。进一步加强行政审判，妥善处理涉商品流通等行政案件，既要依法支持行政机关采取的必要防疫举措，又要依法纠正违法设卡、阻碍物流等不当干预微观经济活动的行政行为，保障商品正常流通，推动跨区域物资运输畅通有序，助力生活必需品“保供稳价”。按照“统筹疫情防控和经济社会发展”的要求，助力防疫、生产、消费统筹兼顾、有序开展，促进全国统一大市场建设。

四、进一步提升司法服务水平

27.提升消费纠纷在线化解质效。当事人及其诉讼代理人等因受疫情影响不能正常出庭参加诉讼，符合条件的，依法在线开展诉讼活动。推动完善电子认证等数字应用基础设施，主动适应互联网时代消费发展要求，回应人民群众公正、高效、便捷解纷的司法需求。准确适用在线诉讼规则等规定，充分发挥在线诉讼灵活、简便、全天候、易操作等优势。准确适用在线调解规则等规定，充分发挥在线调解多元化参与、全流程在线、开放式融合、一体化解纷等优势，实现提升消费纠纷在线化解质效与保障人民群众合法诉讼权益相统一。

28.完善消费者权益司法救济制度。进一步完善消费民事公益诉讼与私益诉讼衔接机制，探索建立食品安全民事公益诉讼惩罚性赔偿制度。依法办理消费公益诉讼案件，充分发挥公益诉讼保护消费者合法权益、遏制违法生产经营行为、维护诚信高效市场秩序的作用。探索建立消费者集体诉讼制度，充分利用小额诉讼制度，降低消费者维权成本，及时、高效保护消费者合法权益。不断增加对农村消费者的司法服务供给，积极引导和协调消费者组织、公益诉讼主

体、司法救助力量向农村地区倾斜。充分发挥人民法庭立足基层、面向群众、服务农村的优势，妥善处理涉休闲农业、乡村旅游、民宿经济等纠纷。

29.推动构建有利于促进消费的综合治理体系。坚持系统思维，综合治理。充分发挥一站式多元纠纷解决和诉讼服务体系作用，广泛邀请人民调解、行业专业调解、行政调解的调解员，以及人大代表、政协委员、行业专家、退休法律工作者等参与消费纠纷调解，多元化解纠纷。通过发出司法建议、交换信息、联合信用惩戒等方式，对制售假冒伪劣商品、侵害个人信息权益、虚假宣传等违法生产经营行为形成规制合力。积极构建司法机关、行政机关、消费者组织、行业协会等多方参与的多元治理体系，完善多元化消费维权机制和纠纷解决机制，为保护消费者权益、促进消费营造良好法治环境。

30.加强消费者权益司法保护宣传工作。充分发挥司法裁判的示范引领作用，通过以案说法、发布典型案例、开展巡回审判、送法进村进企进校等方式加强消费者权益司法保护宣传工作，普及消费者权益保护法律知识；依法保护新闻媒体对制售假冒伪劣商品等违法生产经营行为的舆论监督；引导生产经营者诚实守信经营，倡导节约集约的绿色生活方式，营造安全诚信放心的消费环境。

最高人民法院

2022 年 12 月 26 日

最高人民法院 最高人民检察院 公安部印发《关于依法惩治网络暴力违法犯罪的指导意见》的通知

法发〔2023〕14 号

各省、自治区、直辖市高级人民法院、人民检察院、公安厅(局)，解放军军事法院、军事检察院，新疆维吾尔自治区高级人民法院生产建设兵团分院、新疆生产建设兵团人民检察院、公安局：

现将《关于依法惩治网络暴力违法犯罪的指导意见》予以印发，请认真贯彻执行。执行中遇到的重大问题，请分别报告最高人民法院、最高人民检察院、公安部。

最高人民法院 最高人民检察院 公安部

2023 年 9 月 20 日

最高人民法院 最高人民检察院 公安部
关于依法惩治网络暴力违法犯罪的指导意见

为依法惩治网络暴力违法犯罪活动，有效维护公民人格权益和网络秩序，根据刑法、刑事诉讼法、民法典、民事诉讼法、个人信息保护法、治安管理处罚法及《最高人民法院、最高人民检察院关于办理利用信息网络实施诽谤等刑事案件适用法律若干问题的解释》等法律、司法解释规定，结合执法司法实践，制定本意见。

一、充分认识网络暴力的社会危害，依法维护公民权益和网络秩序

1.在信息网络上针对个人肆意发布谩骂侮辱、造谣诽谤、侵犯隐私等信息的网络暴力行为，贬损他人人格，损害他人名誉，有的造成了他人“社会性死亡”甚至精神失常、自杀等严重后果；扰乱网络秩序，破坏网络生态，致使网络空间戾气横行，严重影响社会公众安全感。与传统违法犯罪不同，网络暴力往往针对素不相识的陌生人实施，受害人在确认侵害人、收集证据等方面存在现实困难，维权成本极高。人民法院、人民检察院、公安机关要充分认识网络暴力的社会危害，坚持严惩立场，依法能动履职，为受害人提供有效法律救济，维护公民合法权益，维护公众安全感，维护网络秩序。

二、准确适用法律，依法严惩网络暴力违法犯罪

2.依法惩治网络诽谤行为。在信息网络上制造、散布谣言，贬损他人人格、损害他人名誉，情节严重，符合刑法第二百四十六条规定的，以诽谤罪定罪处罚。

3.依法惩治网络侮辱行为。在信息网络上采取肆意谩骂、恶意诋毁、披露隐私等方式，公然侮辱他人，情节严重，符合刑法第二百四十六条规定的，以侮辱罪定罪处罚。

4.依法惩治侵犯公民个人信息行为。组织“人肉搜索”，违法收集并向不特定多数人发布公民个人信息，情节严重，符合刑法第二百五十三条之一规定的，以侵犯公民个人信息罪定罪处罚；依照刑法和司法解释规定，同时构成其他犯罪的，依照处罚较重的规定定罪处罚。

5.依法惩治借网络暴力事件实施的恶意营销炒作行为。基于蹭炒热度、推广引流等目的，利用互联网用户公众账号等推送、传播有关网络暴力违法犯罪

的信息，符合刑法第二百八十七条之一规定的，以非法利用信息网络罪定罪处罚；依照刑法和司法解释规定，同时构成其他犯罪的，依照处罚较重的规定定罪处罚。

6.依法惩治拒不履行信息网络安全管理义务行为。网络服务提供者对于所发现的有关网络暴力违法犯罪的信息不依法履行信息网络安全管理义务，经监管部门责令采取改正措施而拒不改正，致使违法信息大量传播或者有其他严重情节，符合刑法第二百八十六条之一规定的，以拒不履行信息网络安全管理义务罪定罪处罚；依照刑法和司法解释规定，同时构成其他犯罪的，依照处罚较重的规定定罪处罚。

7.依法惩治网络暴力违法行为。实施网络侮辱、诽谤等网络暴力行为，尚不构成犯罪，符合治安管理处罚法等规定的，依法予以行政处罚。

8.依法严惩网络暴力违法犯罪。对网络暴力违法犯罪，应当体现从严惩治精神，让人民群众充分感受到公平正义。坚持严格执法司法，对于网络暴力违法犯罪，依法严肃追究，切实矫正“法不责众”的错误倾向。要重点打击恶意发起者、组织者、恶意推波助澜者以及屡教不改者。实施网络暴力违法犯罪，具有下列情形之一的，依法从重处罚：

(1)针对未成年人、残疾人实施的；

(2)组织“水军”、“打手”或者其他人员实施的；

(3)编造“涉性”话题侵害他人人格尊严的；

(4)利用“深度合成”等生成式人工智能技术发布违法信息的；

(5)网络服务提供者发起、组织的。

9.依法支持民事维权。针对他人实施网络暴力行为，侵犯他人名誉权、隐私权等人格权，受害人请求行为人承担民事责任的，人民法院依法予以支持。

10.准确把握违法犯罪行为的认定标准。通过信息网络检举、揭发他人犯罪或者违法违纪行为，只要不是故意捏造事实或者明知是捏造的事实而故意散布的，不应当认定为诽谤违法犯罪。针对他人言行发表评论、提出批评，即使观点有所偏颇、言论有些偏激，只要不是肆意谩骂、恶意诋毁的，不应当认定为侮辱违法犯罪。

三、畅通诉讼程序，及时提供有效法律救济

11.落实公安机关协助取证的法律规定。根据刑法第二百四十六条第三款的规定，对于被害人就网络侮辱、诽谤提起自诉的案件，人民法院经审查认为被害人提供证据确有困难的，可以要求公安机关提供协助。公安机关应当根据人民法院要求和案件具体情况，及时查明行为主体，收集相关侮辱、诽谤信息传播扩散情况及造成的影响等证据材料。网络服务提供者应当依法为公安机关取证提供必要的技术支持和协助。经公安机关协助取证，达到自诉案件受理条件的，人民法院应当决定立案；无法收集相关证据材料的，公安机关应当书面向人民法院说明情况。

12.准确把握侮辱罪、诽谤罪的公诉条件。根据刑法第二百四十六条第二款的规定，实施侮辱、诽谤犯罪，严重危害社会秩序和国家利益的，应当依法提起公诉。对于网络侮辱、诽谤是否严重危害社会秩序，应当综合侵害对象、动机目的、行为方式、信息传播范围、危害后果等因素作出判定。

实施网络侮辱、诽谤行为，具有下列情形之一的，应当认定为刑法第二百四十六条第二款规定的“严重危害社会秩序”：

(1)造成被害人或者其近亲属精神失常、自杀等严重后果，社会影响恶劣的；

(2)随意以普通公众为侵害对象，相关信息在网络上大范围传播，引发大量低俗、恶意评论，严重破坏网络秩序，社会影响恶劣的；

(3)侮辱、诽谤多人或者多次散布侮辱、诽谤信息，社会影响恶劣的；

(4)组织、指使人员在多个网络平台大量散布侮辱、诽谤信息，社会影响恶劣的；

(5)其他严重危害社会秩序的情形。

13.依法适用侮辱、诽谤刑事案件的公诉程序。对于严重危害社会秩序的网络侮辱、诽谤行为，公安机关应当依法及时立案。被害人同时向人民法院提起自诉的，人民法院可以请自诉人撤回自诉或者裁定不予受理；已经受理的，应当裁定终止审理，并将相关材料移送公安机关，原自诉人可以作为被害人参与诉讼。对于网络侮辱、诽谤行为，被害人在公安机关立案前提起自诉，人民法院经审查认为有关行为严重危害社会秩序的，应当将案件移送公安机关。

对于网络侮辱、诽谤行为，被害人或者其近亲属向公安机关报案，公安机

关经审查认为已构成犯罪但不符合公诉条件的，可以告知报案人向人民法院提起自诉。

14.加强立案监督工作。人民检察院依照有关法律和司法解释的规定，对网络暴力犯罪案件加强立案监督工作。

上级公安机关应当加强对下级公安机关网络暴力案件立案工作的业务指导和内部监督。

15.依法适用人格权侵害禁令制度。权利人有证据证明行为人正在实施或者即将实施侵害其人格权的违法行为，不及时制止将使其合法权益受到难以弥补的损害，依据民法典第九百九十七条向人民法院申请采取责令行为人停止有关行为的措施的，人民法院可以根据案件具体情况依法作出人格权侵害禁令。

16.依法提起公益诉讼。网络暴力行为损害社会公共利益的，人民检察院可以依法向人民法院提起公益诉讼。

网络服务提供者对于所发现的网络暴力信息不依法履行信息网络安全管理义务，致使违法信息大量传播或者有其他严重情节，损害社会公共利益的，人民检察院可以依法向人民法院提起公益诉讼。

人民检察院办理网络暴力治理领域公益诉讼案件，可以依法要求网络服务提供者提供必要的技术支持和协助。

四、落实工作要求，促进强化综合治理

17.有效保障受害人权益。办理网络暴力案件，应当及时告知受害人及其法定代理人或者近亲属有权委托诉讼代理人，并告知其有权依法申请法律援助。针对相关网络暴力信息传播范围广、社会危害大、影响消除难的现实情况，要依法及时向社会发布案件进展信息，澄清事实真相，有效消除不良影响。依法适用认罪认罚从宽制度，促使被告人认罪认罚，真诚悔罪，通过媒体公开道歉等方式，实现对受害人人格权的有效保护。对于被判处刑罚的被告人，可以依法宣告职业禁止或者禁止令。

18.强化衔接配合。人民法院、人民检察院、公安机关要加强沟通协调，统一执法司法理念，有序衔接自诉程序与公诉程序，确保案件顺利侦查、起诉、审判。对重大、敏感、复杂案件，公安机关听取人民检察院意见建议的，人民检察院应当及时提供，确保案件依法稳妥处理。完善行政执法和刑事司法衔接

机制，加强协调配合，形成各单位各司其职、高效联动的常态化工作格局，依法有效惩治、治理网络暴力违法犯罪。

19.做好法治宣传。要认真贯彻“谁执法谁普法”普法责任制，充分发挥执法办案的规则引领、价值导向和行为规范作用。发布涉网络暴力典型案例，明确传导“网络空间不是法外之地”，教育引导广大网民自觉守法，引领社会文明风尚。

20.促进网络暴力综合治理。立足执法司法职能，在依法办理涉网络暴力相关案件的基础上，做实诉源治理，深入分析滋生助推网络暴力发生的根源，通过提出司法建议、检察建议、公安提示函等方式，促进对网络暴力的多元共治，夯实网络信息服务提供者的主体责任，不断健全长效治理机制，从根本上减少网络暴力的发生，营造清朗网络空间。

第十八章 地方法规

北京市未成年人保护条例

(1988 年 10 月 20 日北京市第九届人民代表大会常务委员会第五次会议通过 根据 1992 年 2 月 14 日北京市第九届人民代表大会常务委员会第三十二次会议通过的《关于修改〈北京市未成年人保护条例〉的决定》修正 根据 1997 年 4 月 16 日北京市第十届人民代表大会常务委员会第三十六次会议通过的《关于修改〈北京市未成年人保护条例〉的决定》修正 2003 年 12 月 5 日北京市第十二届人民代表大会常务委员会第八次会议修订 根据 2016 年 11 月 25 日北京市第十四届人民代表大会常务委员会第三十一次会议通过的《关于修改部分地方性法规的决定》修正 2023 年 5 月 26 日北京市第十六届人民代表大会常务委员会第三次会议修订)

目 录

第一章 总 则

第一条 为了保护未成年人身心健康，保障未成年人合法权益，促进未成年人德智体美劳全面发展，培养有理想、有道德、有文化、有纪律的社会主义建设者和接班人，培养担当民族复兴大任的时代新人，根据《中华人民共和国未成年人保护法》等法律、行政法规，结合本市实际，制定本条例。

第二条 保护未成年人是全社会的共同责任，应当坚持最有利于未成年人的原则。

处理涉及未成年人事项，应当符合下列要求：

(一)给予未成年人特殊、优先保护；

(二)尊重未成年人人格尊严；

(三)保护未成年人隐私权和个人信息；

(四)适应未成年人身心健康发展的规律和特点；

(五)听取未成年人的意见；

(六)保护与教育相结合。

第三条 政府、家庭、学校、社会应当对未成年人进行理想教育、道德教育、科学教育、文化教育、法治教育、国家安全教育、健康教育、劳动教育，加强爱国主义、集体主义和中国特色社会主义的教育，培养爱祖国、爱人民、爱劳动、爱科学、爱社会主义的公德， 抵制腐朽思想的侵蚀，引导未成年人树立和践行社会主义核心价值观。

第四条 本市在党委领导下，建立政府统筹、司法联动、家庭学校社会协同的未成年人保护体系，发挥各方力量共同做好未成年人保护工作。

第五条 市、区人民政府应当将未成年人保护工作纳入本级国民经济和社会发展规划、计划，相关经费纳入本级政府预算。

市、区人民政府应当建立未成年人保护工作协调机制， 统筹、协调、督促和指导有关部门做好未成年人保护工作。

民政、教育、公安、卫生健康、网信、市场监督管理、商务、司法行政、文化和旅游、新闻出版、电影、广播电视、交通等有关部门按照职责做好未成年人保护工作。

乡镇人民政府、街道办事处设立未成年人保护工作站， 办理未成年人相关事务，并支持、指导、保障居民委员会、村民委员会做好未成年人保护工作。居民委员会、村民委员会应当设置专人专岗负责未成年人保护工作。

第六条 共产主义青年团、妇女联合会、工会、残疾人联合会、关心下一代工作委员会、青年联合会、学生联合会、少年先锋队以及其他人民团体、有关社会组织，应当协助各级人民政府及其有关部门、人民检察院、人民法院做好未成年人保护工作，发挥各自优势，开展有益于未成年人健康成长的活动，维护未成年人合法权益。

第七条 政府、家庭、学校、社会应当教育、帮助、指导未成年人树立自尊、自信、自立、自强意识， 引导未成年人增强自我保护意识，依法维护自身合法权益；关注未成年人身心健康，培养社会成员保护未成年人的责任意识和自觉行动，共同营造有利于未成年人身心健康的成长环境。

第八条 任何组织或者个人发现不利于未成年人身心健康或者侵犯未成年人合法权益的情形，都有权劝阻、制止或者向公安、民政、教育、卫生健康、网信等有关部门提出检举、控告。

国家机关、居民委员会、村民委员会、密切接触未成年人的单位及其工作人员，在工作中发现未成年人身心健康受到侵害、疑似受到侵害或者面临其他危险情形的，应当立即向公安、民政、教育、卫生健康、网信等有关部门报告。

第九条 对保护未成年人有显著成绩和突出贡献的组织和个人，按照国家和本市有关规定给予表彰和奖励。

第二章 家庭保护

第十条 未成年人的父母或者其他监护人应当承担家庭教育主体责任，学习家庭教育知识，接受家庭教育指导，积极参加家庭教育指导机构、学校、幼儿园、社区等提供的公益性家庭教育指导和实践活动，树立正确的家庭教育理念，以良好的言行和适当的方法，教育、影响和保护未成年人。

鼓励共同生活的其他成年家庭成员学习家庭教育知识，参加家庭教育指导和

实践活动，共同构建文明、和睦的家庭关系。

第十一条 未成年人的父母或者其他监护人应当教育未成年人养成良好的学习和生活习惯，指导、支持未成年人参加家庭劳动、文体活动、社会公益活动和健康的社会交往活动；为未成年人提供安全的家庭生活环境，及时排除引发触电、烧伤、烫伤、跌落、中毒等伤害的安全隐患；采取配备儿童安全座椅等措施，防止未成年人受到交通事故的伤害；对未成年人进行交通出行、健康上网和防溺水、防火灾、防欺凌、防性侵、防拐卖、防动物伤害等方面的安全知识教育， 关注未成年人的心理健康，增强其自我保护的意识和能力。

第十二条 未成年人的父母或者其他监护人应当依法承担监护职责，履行抚养、教育和保护未成年人的义务； 交由他人临时照护或者委托他人代为照护未成年人应当符合法律的规定。

未成年人的父母或者其他监护人，共同生活的其他成年家庭成员，以及临时照护人、代为照护的被委托人不得实施虐待、遗弃、非法送养、暴力伤害、性侵害等侵犯未成年人身心健康和合法权益的行为。

第十三条 未成年人的父母或者其他监护人，共同生活的其他成年家庭成员，以及临时照护人、代为照护的被委托人发现未成年人身心健康受到侵害、疑似受到侵害或者其他合法权益受到侵犯的，应当及时了解情况并采取保护措施；情况严重的，立即向公安、民政、教育、卫生健康、网信等有关部门报告。未履行报告义务的，任何组织或者个人都有权督促其履行，或者直接向有关部门报告。

第三章 学校保护

第十四条 学校、幼儿园应当健全并落实未成年人保护工作责任制，明确保护工作机构，建立、实施保护工作制度， 维护未成年人合法权益，保障未成年人健康成长、全面发展。

第十五条 学校、幼儿园应当提供必要的卫生保健条件，按照规定设立卫生保健机构，配备专职或者兼职保健工作人员，购置必需的药品和急救器材，协助卫生健康部门做好在校、在园未成年人的卫生保健工作。

未成年人在校内、园内或者本校、本园组织的校外、园外活动中发生突发疾病、人身伤害事故等， 学校、幼儿园应当立即救护， 妥善处理，及时通知未成年人的父母或者其他监护人，并向有关部门报告。

第十六条 学校、幼儿园应当建立健全校园安全管理制度，落实日常巡查、定期检查、技防监控等措施，加强安全保卫、场地设施、食品安全、校车运行、学生宿舍、文体活动、消防安全等方面的安全管理。

学校、幼儿园的教育教学和生活设施， 卫生环境和条件，以及为未成年人提供的食品、药品、服装、教具、餐具、体育运动器材等学习、生活用品， 应当符合质量和安全标准。

学校、幼儿园发现教职员工或者拟聘用人员存在国家规定的可能对未成年人造成不良影响的身心疾病等情形的，应当按照要求进行评估，并将评估结果作为是否聘用或者调整工作岗位的依据。

第十七条 学校应当按照规定配备专职心理健康教育教师，设立心理辅导室，建立学生心理健康问题的筛查和早期干预机制，开展社会生活指导、心理健康测评、青春期教育、生命教育等， 为未成年学生提供日常心理辅导与咨询，协同其父母或者其他监护人共同预防和解决学生心理、行为异常问题。

学校可以通过与社会工作服务机构、专业心理健康服务机构、精神卫生医疗机构等合作的方式，为未成年学生提供专业心理健康服务。

第十八条 学校应当建立学生体质监测制度，定期开展体检，发现未成年学生出现近视等倾向或者有影响体质的不良行为习惯的，应当进行必要的干预，并督促、指导其父母或者其他监护人及时给予健康保障。

第十九条 学校应当完善管理制度，保障未成年学生在课间、课后使用学校的体育运动场地、设施开展体育锻炼； 学校体育设施应当在国家法定节假日、休息日及寒暑假期向本校学生免费或者优惠开放，具体办法由市教育部门另行制定。

区人民政府应当采取措施，鼓励和支持有条件的学校在国家法定节假日、休息日及寒暑假期向非本校未成年人免费或者优惠开放校内体育设施。

第二十条 学校应当与未成年学生的父母或者其他监护人互相配合，按照国家和本市规定，合理安排学生的学习时间，减轻学习负担，保障其休息、娱乐、体育锻炼和社会实践的时间。

学校应当加强在校未成年学生使用手机等智能终端产品管理。未经学校允许，未成年学生不得将手机等智能终端产品带入课堂，带入学校的应当统一管理。

面向未成年学生开展的各类主题教育宣传活动确需纳入教学内容的，应当符

合法律、法规的规定，并与学生年龄、身心发展阶段、认知特点等相适应。

第二十一条 支持幼儿园对二至三周岁的幼儿提供保育、教育服务；鼓励学校在课后时间及寒暑假期提供未成年学生托管服务，丰富托管服务内容。教育部门应当对学校、幼儿园提供服务给予必要的指导、支持。

鼓励和支持社会力量举办婴幼儿照护服务机构。市、区人民政府及其有关部门可以通过提供场地、购买服务、给予市政公用服务优惠等方式， 提供必要的支持。

第二十二条 学校应当将法治教育纳入教育教学计划，结合未成年学生特点，采取多种方式进行法治教育，培育法治观念，指导其依法规范自身行为、维护合法权益。

学校应当从司法和执法机关、法学教育和法律服务机构等单位， 聘请符合条件的人员担任法治副校长或者校外法治辅导员，协助开展法治教育、学生保护、安全管理、预防犯罪等工作，并为其提供必要的工作便利。

学校应当在教育等部门的指导下建立法治副校长或者校外法治辅导员工作评价制度。

第二十三条 学校、幼儿园应当结合未成年人保护的需要，制定应对自然灾害、事故灾难、公共卫生事件等突发事件和意外伤害的预案， 配备相应设施，并定期开展必要的急救、自救等应急培训和演练。

学校、幼儿园应当建立预防性侵害、性骚扰未成年人工作制度， 对遭受性侵害、性骚扰的未成年人及时采取保护措施。

学校、幼儿园不得安排未成年人参加商业性活动， 不得向未成年人及其父母或者其他监护人推销或者要求其购买指定的商品和服务。

第二十四条 学校应当建立学生欺凌防控工作制度，对教职员工、学生等开展防治学生欺凌的教育和培训，提升教职员工、学生对学生欺凌的预防、识别和应对处理能力。

学校应当定期开展防治欺凌专项调查，采取多种方式及时了解学生欺凌情况。学校教职员工、未成年人的父母或者其他监护人发现学生受到欺凌或者疑似受到欺凌的，应当及时向学校报告。学生报告欺凌情况的， 学校应当采取必要的保护措施。

学校应当立即制止并依法认定、处理学生欺凌行为， 开展心理辅导、教育引导及家庭教育指导等工作，未成年学生的父母或者其他监护人应当积极配合。

第二十五条 学校、幼儿园应当加强与未成年学生、幼儿的父母或者其他监护人的联系，及时沟通其学习、生活、身心健康、安全等情况； 可以组织开展公益性家庭教育指导服务和实践活动，传授家庭教育的理念、知识和方法。

未成年学生、幼儿的父母或者其他监护人应当配合、支持学校、幼儿园开展教育、保育工作，参与校园治理，共同维护教学秩序，做好未成年人教育管理。

第四章 社会保护

第二十六条 全社会应当树立关心、爱护未成年人的良好风尚。

鼓励、支持和引导人民团体、企业事业单位、社会组织及其他组织和个人，开展有利于未成年人健康成长的社会活动和服务。

培育、引导和规范社会组织、社会工作者依法提供家庭教育指导服务， 提供心理辅导、康复救助和家庭监护能力评估、收养评估等专业服务， 参与涉及未成年人案件中未成年人的心理干预、法律援助、社会调查、社会观护、教育矫治、社区矫正等工作。

共产主义青年团、妇女联合会和未成年人保护组织可以设立未成年人服务热线，为未成年人提供心理健康咨询、法律维权等服务。鼓励、支持法律服务机构和律师协会为未成年人权益保护提供法律咨询服务。

第二十七条 鼓励科技工作者、艺术工作者、作家及其他人员，创作有利于未成年人健康成长的作品；鼓励出版、制作和传播有利于未成年人健康成长的图书、报刊、电影、广播电视节目、舞台艺术作品、音像制品、电子出版物和网络信息等。

第二十八条 有关单位应当按照国家和本市规定向未成年人提供便利、优惠或者免费的服务。任何组织或者个人不得违反有关规定， 限制未成年人应当享有的照顾或者优惠。

第二十九条 在学校、幼儿园周边开展生产、经营及其他活动的，应当符合法律、法规的规定。

在学校、幼儿园周边二百米范围内不得设置营业性娱乐场所、酒吧、互联网上网服务营业场所等不适宜未成年人活动的场所；在学校、幼儿园周边一百米范

围内不得设置售烟网点。

在学校、幼儿园周边一定范围内不得设置酒、彩票销售网点， 具体范围由市商务、民政、体育等部门确定并公布。

任何人不得在学校、幼儿园和其他未成年人集中活动的公共场所吸烟、饮酒。

第三十条 向未成年人销售商品、提供服务，应当与其年龄、智力发展状况相适应，不得侵害未成年人的身心健康和合法权益，并符合下列规定：

(一)剧本娱乐经营场所使用的剧本脚本应当设置适龄提示，标明适龄范围；设置的场景不适宜未成年人的，不得允许未成年人进入；除国家法定节假日、休息日及寒暑假期外，不得向未成年人提供剧本娱乐活动。

(二)未经未成年人的父母或者其他监护人同意，不得向未成年人提供医疗美容服务，紧急救治情况下无法取得其父母或者其他监护人同意的，按照国家规定办理。

(三)不得向未成年人提供文身服务。

(四)法律、法规的其他规定。

第三十一条 旅馆、宾馆、酒店、民宿等住宿经营者接待未成年人入住时，应当询问其父母或者其他监护人的联系方式、同住人员身份关系等情况， 并如实记录。发现下列可疑情形的， 应当立即向公安机关报告，及时联系未成年人的父母或者其他监护人，并采取相应的安全保护措施：

(一)未成年人单独入住、异性未成年人或者多名未成年人共同入住， 没有合理解释的；

(二)未成年人和成年人共同入住，不能说明身份关系或者身份关系有疑点的；

(三)未成年人身体受伤、醉酒、意识不清， 可能存在被殴打、麻醉、胁迫等情况的；

(四)其他可疑情形。

第三十二条 任何组织或者个人不得招用未满十六周岁未成年人，国家另有规定的除外。

营业性娱乐场所、酒吧、互联网上网服务营业场所等不适宜未成年人活动的场所，不得招用已满十六周岁的未成年人。

招用已满十六周岁未成年人的单位和个人应当执行国家在工种、劳动时间、

劳动强度和保护措施等方面的规定，不得安排其从事过重、有毒、有害等危害未成年人身心健康的劳动或者危险作业。

第三十三条 密切接触未成年人的单位招聘、录用工作人员，或者采用劳务派遣、劳务外包等用工形式的， 应当依法履行从业查询义务；不得录用具有性侵害、虐待、拐卖、暴力伤害等违法犯罪记录的人员。

第五章 网络保护

第三十四条 网信部门负责统筹协调未成年人网络保护工作。网信部门、新闻出版、教育、公安、民政、卫生健康、文化和旅游、市场监督管理、电影、广播电视等有关部门，以及学校、未成年人的父母或者其他监护人等， 依据各自职责和义务，采用适合未成年人身心健康特点的技术产品和服务，做好未成年人保护工作，保障未成年人在网络空间的合法权益。

网信部门会同公安、文化和旅游、新闻出版、电影、广播电视等部门， 根据不同年龄阶段未成年人的成长特点，确定可能影响未成年人身心健康的网络信息的种类、范围和判断标准；依法惩处利用网络从事危害未成年人身心健康的行为。

第三十五条 网络产品和服务提供者应当建立健全未成年人保护机制和网络合规制度，明确专门负责未成年人保护的人员及岗位职责，依法履行未成年人保护义务，并遵守下列规定：

(一)建立便捷、合理、有效的投诉和举报渠道， 向社会公开投诉、举报方式等信息，及时受理、处理涉及未成年人的投诉、举报；

(二)建立网络信息生产和传播自查、内部审核制度， 发现存在可能影响、危害未成年人身心健康或者利用网络对未成年人实施违法犯罪行为的，应当及时采取必要措施；

(三)设置防沉迷技术措施，不得向未成年人提供诱导沉迷的产品和服务，应当针对未成年人使用产品和服务设置时间管理、权限管理、消费管理等功能， 提示在上网服务设施和智能终端产品上安装未成年人网络保护软件；

(四)建立未成年人个人信息保护制度，发现未成年人通过网络发布私密信息的，应当及时提示，并采取必要的保护措施；

(五)建立未成年人网络欺凌预警预防机制，设立紧急防护功能；

(六)向未成年人提供人工智能产品和算法推荐服务的，应当便于未成年人获

取有益身心健康的信息，不得推送可能引发模仿不安全行为、诱导不良嗜好或者违反社会公德等影响未成年人身心健康的信息；

(七)法律、法规的其他规定。

第三十六条 以未成年人为服务对象的在线教育网络产品和服务提供者应当遵守内容审核规定，不得插入网络游戏链接，不得推送广告等与教学无关的信息。

线上直播类培训应当设置合理的时段、时长，保证未成年人休息时间。

第三十七条 网络游戏、网络直播、网络音视频、网络社交等网络服务提供者应当完善网络社区规则和用户公约，引导规范未成年人的网络行为；不得违反规定向未成年人提供现金充值、在线支付等打赏服务， 以及其他不适宜未成年人的服务。

网络游戏服务提供者应当对游戏产品进行分类，作出适龄提示，并采取技术措施，防止未成年人接触不适宜的游戏；要求未成年人以真实身份信息注册并登录网络游戏，并不得在每日二十二时至次日八时向未成年人提供网络游戏服务。

任何组织或者个人不得向未成年人提供网络游戏账号租售交易服务。以租售账号等方式规避未成年人网络游戏管理规定的，网络游戏服务提供者应当采取限制使用、终止服务或者封闭账号等措施予以处理。

网络直播服务提供者不得为未满十六周岁的未成年人提供网络直播发布者账号注册服务；为年满十六周岁的未成年人提供网络直播发布者账号注册服务时，应当对其身份信息进行认证，并征得其父母或者其他监护人同意。

第三十八条 网络行业组织应当加强行业自律，制定、实施未成年人网络保护行业规范，指导会员履行未成年人网络保护义务，加强对未成年人的网络保护。

网络产品和服务提供者可以成立未成年人保护联盟，通过建立健全、推广未成年人保护标准和行为准则等方式，履行未成年人保护的社会责任，提高未成年人保护水平。

第六章 政府保护

第三十九条 市、区人民政府及其有关部门应当保障校园安全，监督、指导学校、幼儿园等单位落实校园安全责任，建立突发事件报告、处置和协调机制，将安全、应急等知识和技能纳入校(园)长、教师培训和中小学公共安全教育内容。

公安机关和其他有关部门应当依法维护校园周边的治安和交通秩序，根据需

要开展联合执法、安全隐患排查、社会治安及交通综合治理等行动， 预防和制止侵害未成年人的违法犯罪行为。

第四十条 市、区人民政府应当建立和改善适合未成年人的活动场所和设施，支持公益性未成年人活动场所和设施的建设、运行， 鼓励社会力量兴办适合未成年人的活动场所和设施，并加强管理。

市、区人民政府按照有关规定， 统筹规划学校、幼儿园校车的配备和管理工作，组织有关部门为在校、在园未成年人提供安全、便利的校车服务。

本市推进儿童友好型城市创建，提升未成年人活动场所和设施的建设、运行水平。

第四十一条 市、区人民政府及其有关部门通过政府购买服务、孵化扶持、鼓励公益事业单位设置社会工作专业岗位等方式，培育和发展未成年人保护社会组织，加强社会工作专业队伍建设，支持开展有利于未成年人健康成长的社会活动和服务。

第四十二条 市、区人民政府应当将家庭教育指导服务纳入城乡公共服务体系和政府购买服务目录。

市民政部门会同教育、卫生健康、公安、网信等部门和妇女联合会、残疾人联合会等人民团体，制定家庭监护指引，为未成年人的父母或者其他监护人履行监护职责提供指导和帮助。

第四十三条 市、区人民政府及其有关部门应当对困境未成年人实施分类保障，采取措施满足其生活、教育、安全、医疗康复、住房等方面的基本需要。保障标准根据本市经济社会发展水平和困境未成年人生活需求等情况适时调整。

第四十四条 市、区人民政府及其有关部门应当建立健全残疾未成年人康复服务保障机制，开展残疾未成年人抢救性治疗和康复，丰富医疗、教育、社会融入等康复服务内容，满足残疾未成年人康复服务需求。

第四十五条 市、区人民政府及其教育等部门应当鼓励和支持学校、幼儿园开展融合教育，对具有接受普通教育能力、能适应校园生活的义务教育、学前教育阶段的残疾未成年人，在同等条件下，优先、就近安排在适宜的普通学校、幼儿园接受教育；保障不具有接受普通教育能力的残疾未成年人，在特殊教育学校、幼儿园接受学前教育、义务教育和职业教育。

市、区人民政府及其教育等部门应当保障特殊教育学校、幼儿园的办学、办园条件，鼓励和支持社会力量举办特殊教育学校、幼儿园。

第四十六条 民政部门、人民检察院、人民法院等可以根据需要，按照有关规范和标准，开展家庭监护能力评估。评估的具体办法由市民政部门会同人民检察院、人民法院等制定。

有关部门、乡镇人民政府、街道办事处等可以结合家庭监护能力评估结果和具体情况，对未成年人的父母或者其他监护人及其家庭给予监护指导、家庭教育指导、救助帮扶等支持和服务。有关组织和个人可以参考家庭监护能力评估结果，对具有法定情形、不适宜作为未成年人监护人的， 依法向人民法院申请撤销其监护人资格。

对由民政部门依法进行临时监护的未成年人，根据其家庭监护能力评估结果，未成年人的父母或者其他监护人重新具备履行监护职责条件的，民政部门可以将未成年人送回其父母或者其他监护人抚养。居民委员会、村民委员会应当对监护情况进行随访。

第四十七条 公安机关在办案过程中或者接受报告后，发现未成年人的父母或者其他监护人严重伤害未成年人或者实施其他严重侵犯未成年人合法权益行为，致使未成年人面临人身安全威胁、处于无人照料等危险状况的， 应当立即制止，将面临紧急危险的未成年人带离危险环境，并通知住所地民政部门、居民委员会或者村民委员会依法进行安置；对未成年人的父母或者其他监护人的违法犯罪行为，依法予以处理。

第四十八条 发生自然灾害、事故灾难、公共卫生事件等突发事件时，市、区人民政府及其有关部门，乡镇人民政府、街道办事处应当采取调查询问、摸底排查等方式及时了解未成年人监护情况。发现未成年人监护缺失的，由民政部门、未成年人住所地的居民委员会、村民委员会依法采取临时监护、临时生活照料及其他救助、保护措施。

第四十九条 民政部门应当对符合临时监护、长期监护法定条件的未成年人依法监护，及时作出安排，保障未成年人的合法权益。

民政部门应当会同相关部门加强对临时监护、长期监护的未成年人的保障，落实生活、教育、安全、医疗康复等保障措施， 对长期监护的未成年人在其成年

后按照规定给予就业扶持、住房保障、社会救助等。

第五十条 市、区人民政府及其民政部门应当规划建设儿童福利机构、未成年人救助保护机构，负责收留、抚养依法由民政部门监护的未成年人。

鼓励有条件的儿童福利机构、未成年人救助保护机构拓展社会服务功能， 发挥场地、资源等优势， 为残疾未成年人、困境未成年人等提供康复训练、托养照料、家庭教育指导等社会化服务。

第五十一条 民政、教育、市场监督管理、文化和旅游、商务、卫生健康、网信、公安等部门应当依法履行未成年人保护监督管理职责， 在开展监督检查工作时，可以依法采取下列措施：

(一)进入有关单位的场所实施现场检查；

(二)询问有关人员，了解落实法律、法规情况；

(三)要求有关单位就相关问题作出说明；

(四)查阅复制证照、营业账簿、交易记录、监控录像等资料；

(五)其他必要的监督检查措施。

有关部门应当密切协作，加强信息互通共享，根据实际开展联合执法、专项检查等行动，优化未成年人成长环境。

第五十二条 公安、民政、教育、卫生健康、网信等部门应当制定报告指引，细化报告情形，指导、督促相关的密切接触未成年人的单位依法履行报告义务。

负有报告义务的单位应当建立健全内部制度和流程，加强对本单位人员的培训，不得因工作人员履行报告义务作出处分、单方解除劳动关系等侵犯其合法权益的决定。

第五十三条 公安、民政、教育、卫生健康、网信、市场监督管理等部门接到检举、控告或者报告， 应当依法调查、处置， 对检举、控告或者报告的组织或者个人的信息予以保密并及时反馈处理情况；不属于本部门职权的，应当接受、记录，并按照规定移送有关部门处理。

有关部门应当明确接受检举、控告或者报告的渠道，并向社会公布。

第五十四条 本市依托 12345 市民服务热线建立未成年人保护热线，设置专席人员，负责受理、转介涉及未成年人合法权益的诉求， 收集意见建议，提供未成年人保护方面的咨询、帮助； 专席人员应当熟悉未成年人身心特点，定期接受

专门培训。

未成年人保护热线受理咨询、检举、控告和报告应当纳入本市接诉即办工作体系。

第七章 司法保护

第五十五条 公安机关、人民检察院、人民法院和司法行政部门应当确定专门机构或者指定专门人员，负责办理涉及未成年人案件。办理涉及未成年人案件，应当考虑未成年人身心特点和健康成长的需要，使用未成年人能够理解的语言和表达方式，听取未成年人的意见，保障未成年人的合法权益，依法提供法律援助或者司法救助。

第五十六条 公安机关、人民检察院、人民法院依托一站式综合办案中心，对受到性侵害、虐待、暴力伤害的未成年被害人开展一站式询问、取证、身体检查等工作，减轻对其身体、心理的不良影响。

一站式综合办案中心可以委托社会工作者、心理咨询师、律师等专业人员，驻场协助开展心理疏导、风险评估、法律咨询帮助等服务。

第五十七条 未成年犯罪嫌疑人、被告人没有委托辩护人的，公安机关、人民检察院、人民法院应当依法通知法律援助机构指派律师担任辩护人； 未成年当事人因经济困难申请法律援助，有证据证明无固定生活来源的，免予核查其经济困难状况。

法律援助机构应当指派熟悉未成年人身心特点的律师为未成年人提供法律援助；未成年被害人为女性的，应当指派女性律师。有条件的法律援助机构可以组建专门的未成年人法律援助服务团队。

法律援助机构、律师协会应当对办理未成年人法律援助案件的律师进行指导和培训。

第五十八条 人民检察院依法对涉及未成年人的诉讼活动进行监督。

未成年人合法权益受到侵犯，相关组织和个人未代为提起诉讼的，人民检察院可以督促、支持其提起诉讼， 并提供法律咨询、协助申请法律援助、协助收集证据、协助申请减免案件受理费等帮助；涉及公共利益的，依法提起公益诉讼。

第五十九条 人民法院发挥审判职能，依法保障未成年人人身权、财产权等合法权益。

人民法院审理继承案件，应当依法保护未成年人的继承权和受遗赠权；审理离婚案件，涉及未成年子女抚养问题的，应当尊重已满八周岁未成年子女的真实意愿，根据双方具体情况，按照最有利于未成年子女的原则依法处理。

人民法院开庭审理涉及未成年人案件，未成年被害人、证人一般不出庭作证；必须出庭的，应当采取保护其隐私的技术手段和心理干预等保护措施。

第六十条 公安机关、人民检察院、人民法院和司法行政部门发现有关单位未尽到未成年人教育、管理、救助、看护等保护职责的，应当向该单位提出建议，并可以采取询问、走访等方式督促落实。

被建议单位应当在一个月内书面回复建议落实情况；在规定期限内，经督促无正当理由不予落实或者落实不到位的，公安机关、人民检察院、人民法院和司法行政部门可以通报被建议单位的上级机关、行政主管部门或者行业自律组织等。

第六十一条 公安机关、人民检察院、人民法院、司法行政部门办理涉及未成年人的案件，可以会同民政部门、人民团体或者委托社会服务机构等， 开展家庭教育指导、社会调查、社会观护、教育矫治、安置帮教、救助帮扶等工作。

公安机关、人民检察院、人民法院、司法行政部门开展上述工作， 涉案未成年人住所地不在本市的，应当将有关情况通报至其住所地有关机关，按照最有利于未成年人的原则，综合考虑家庭情况、帮教条件等因素进行协调和安排； 未成年人无固定住所的，应当依托未成年人救助保护机构、专门学校、社会观护基地等实施。

第八章 法律责任

第六十二条 未成年人的父母或者其他监护人，共同生活的其他成年家庭成员，以及临时照护人、代为照护的被委托人违反本条例第十二条规定的， 由其居住地的居民委员会、村民委员会予以劝诫、制止； 情节严重的，应当及时向公安机关报告，公安机关应当依法处理。

第六十三条 相关经营者违反本条例第二十九条第二款、第三款规定的，由文化市场综合执法、市场监督管理、烟草专卖、公安等部门按照职责分工责令限期改正，给予警告，没收违法所得，可以并处五万元以下罚款；拒不改正或者情节严重的，责令停业整顿或者吊销营业执照、吊销相关许可证， 可以并处五万元以上五十万元以下罚款。

第六十四条 违反本条例第二十九条第四款规定的，由卫生健康、教育、市场监督管理等部门按照职责分工责令改正，给予警告，可以并处五百元以下罚款；场所管理者未及时制止的，由卫生健康、教育、市场监督管理等部门按照职责分工给予警告，并处一万元以下罚款。

第六十五条 违反本条例第三十条第(二)项规定，未经未成年人的父母或者其他监护人同意，向未成年人提供医疗美容服务的，由卫生健康部门责令改正，处一万元以上三万元以下罚款；拒不改正或者造成严重后果的，处三万元以上三十万元以下罚款，对有关医务人员可以责令暂停一个月以上六个月以下执业活动。未依法取得医疗机构执业许可证，向未成年人提供医疗美容服务的，按照国家有关规定处理。

第六十六条 违反本条例第三十条第(三)项规定，向未成年人提供文身服务的，由市场监督管理部门责令改正，处一万元以上三万元以下罚款；拒不改正或者造成严重后果的，责令停业整顿，可以并处三万元以上三十万元以下罚款；医疗美容机构向未成年人提供文身服务的，由卫生健康部门按照上述规定予以处罚。

第六十七条 密切接触未成年人的单位违反本条例第三十三条规定的，由教育、人力资源和社会保障、市场监督管理等部门按照职责分工责令限期改正， 给予警告，并处五万元以下罚款；拒不改正或者造成严重后果的，责令停业整顿或者吊销营业执照、吊销相关许可证， 并处五万元以上五十万元以下罚款，对直接负责的主管人员和其他直接责任人员依法给予处分。

第九章 附 则

第六十八条 本条例自 2023 年 6 月 1 日起施行。

北京地区电信领域数据安全管理实施细则

(2023 年 7 月 24 日)

第一章 总 则

第一条 为了加强北京地区电信领域数据安全管理工作，进一步提高数据安全保护水平，根据《中华人民共和国数据安全法》《中华人民共和国网络安全法》《中华人民共和国个人信息保护法》《工业和信息化领域数据安全管理办法(试行)》《关于更好发挥数据要素作用进一步加快发展数字经济的实施意见》等法律法规和有关规定，结合本市实际，制定本细则。

第二条 北京地区的电信领域数据处理者开展数据处理活动及其安全监管，应当遵守相关法律、行政法规和本细则的要求。

第三条 本细则所称电信领域数据是指在电信业务经营过程中产生和收集的数据，包括各类基础电信业务和增值电信业务数据。

电信领域数据处理者是指数据处理活动中自主决定处理目的、处理方式的取得电信业务经营许可证的电信业务经营者。

数据处理活动包括但不限于数据收集、存储、使用、加工、传输、提供、公开等活动。

第四条 在工业和信息化部统筹指导下，北京市通信管理局负责北京地区电信领域数据安全的组织协调、统筹规划和监督管理工作。

第五条 数据安全管理应当坚持总体国家安全观，统筹数据发展与安全，鼓励数据开发利用，加强数据治理，保证数据供给、流通、使用全过程安全合规。

第二章 基础性数据安全保护要求

第六条 电信领域数据处理者应当每年至少开展一次数据梳理工作，按照电信领域重要数据和核心数据识别标准识别重要数据和核心数据，相关工作开展情况按年度形成报告并报送北京市通信管理局，报告内容包括数据梳理工作开展情况、数据分类分级情况、数据分级防护措施等。

第七条 电信领域数据处理者应当按要求将识别出的重要数据和核心数据进行目录填报，并报北京市通信管理局备案。备案内容包括但不限于数据来源、类别、级别、规模、载体、处理目的和方式、使用范围、责任主体、对外共享、跨境传输、安全保护措施等基本情况，不包括数据内容本身。

备案内容发生重大变化的，电信领域数据处理者应当在发生变化的三个月内履行备案变更手续。重大变化是指某类重要数据和核心数据规模(数据条目数量或者存储总量等)变化 30%以上，重要数据或核心数据类别新增或减少，数据安全情况、责任主体信息发生变动，或者其他备案内容发生变化。

北京市通信管理局对备案信息完整性、重要数据和核心数据类别、级别、数据量等填报内容准确完备性进行审核，在电信领域数据处理者提交备案申请的二十个工作日内完成并反馈审核结果。备案未通过的申请人应当在收到反馈情况后的十五个工作日再次提交备案申请。

北京市通信管理局对重要数据和核心数据目录备案落实情况进行监督检查，电信领域数据处理者应当予以配合。

第八条 电信领域数据处理者应当根据实际工作需要配备数据安全管理人员，统筹负责数据处理活动的安全监督管理。

电信领域重要和核心数据处理者还应当建立覆盖本单位相关部门的数据安全工作体系，明确数据安全负责人和管理机构，负责牵头内部数据安全管理工作，明确数据处理关键岗位和岗位职责，要并配备具备相应技能水平的专职人员，定期参与行业认可的数据安全考核与培训。

第九条 电信领域数据处理者应加强权限审批管理，合理配置数据处理活动的权限，明确各部门和相关人员权限管理要求，包含但不限于数据处理活动平台系统账号权限分配原则、流程等，建立并定期更新权限分配表。

第十条 电信领域数据处理者应对数据处理、系统运行、权限管理、人员操作等日志进行留存管理，日志留存时间不少于六个月。日志记录信息应包括执行时间、操作账号、处理方式等，针对数据使用加工、关联分析、批量访问、批量复制等数据处理行为还应记录授权情况、登录信息等， 记录完整、准确、不可修改。

第十一条 电信领域数据处理者应定期开展数据安全审计，审计对象完整覆盖全部数据处理活动，审计发现问题需及时进行整改，并对审计及处置记录进行留存管理。

重要数据处理活动应至少每半年开展一次审计，核心数据处理活动应至少每季度开展一次审计。

第十二条 电信领域数据处理者应当开展数据安全风险监测，对数据安全风险隐患进行预警，并及时开展处置。对于可能造成较大及以上安全事件的风险，应及时向北京市通信管理局报告，报告内容包括但不限于风险类别和级别、涉及数据情况、产生时间、影响范围等信息。

第十三条 电信领域数据处理者应制定数据安全事件应急预案并开展应急演练。应急预案应充分结合数据泄露、数据滥用、数据篡改、数据损毁、数据违规使用等数据安全事件场景和等级明确应急响应工作责任分工、实施流程、保障措施等。

在数据安全事件发生后，电信领域数据处理者应当按照应急预案，及时开展应急处置。涉及重要数据和核心数据的安全事件， 第一时间向北京市通信管理局报告，事件处置完成后立即开展事件调查、问题整改、责任追究， 在处置完成七个工作日内形成总结报告并报送北京市通信管理局。对于发生过数据安全事件的电信领域数据处理者还应每年向北京市通信管理局报告数据安全事件处置情况。

第十四条 电信领域重要数据和核心数据处理者应当自行或委托第三方评估机构，每年对其数据处理活动至少开展一次风险评估，及时整改风险问题，并向北京市通信管理局报送风险评估报告。

重要数据和核心数据目录备案内容发生重大变化的，电信领域数据处理者应当在履行备案变更手续后及时启动风险评估，备案变更后三个月内向北京市通信管理局重新提交风险评估报告。

电信领域一般数据处理者应当自行或委托第三方评估机构，每年至少开展一次数据安全合规性评估，及时整改问题，并向北京市通信管理局报送评估报告。评估内容包括但不限于数据合规使用情况、数据安全保障措施配备情况与完善程度、合作方数据安全保护水平等。

第十五条 电信领域数据处理者应加强数据安全教育培训，鼓励企业通过积极参与本地区、本行业数据安全人才培养计划等方式， 提升相关岗位人员数据安全保护意识和技能水平。

电信领域数据处理者应定期组织开展内部数据安全教育培训，培训内容涵盖数据安全法律法规、标准规范、管理制度和工作要求、知识技能、保护意识等，培训对象覆盖数据安全岗位人员，年度培训时长不小于 30 学时。

电信领域重要数据和核心数据处理者还应针对处理重要数据和核心数据的重点岗位人员定期开展教育培训，培训内容包括但不限于重要数据和核心数据安全管理要求、安全操作规程、风险评估规范等，年度培训时长不少于 45 学时。

第十六条 电信领域数据处理者应当加强对合作方管理，通过签订合同协议等方式，明确数据委托处理、数据处理系统开发运维等合作方数据安全责任和义务。涉及重要数据和核心数据的，应当对合作方的数据安全保护能力、资质进行核验。

第三章 数据全生命周期安全保护要求

第十七条 电信领域数据处理者应当对数据处理活动负安全主体责任，建立健全全流程数据安全管理制度，针对不同级别数据，制定数据收集、存储、使用、加工、传输、提供、公开等环节的具体分级防护要求和操作规程。

第十八条 电信领域数据处理者收集数据应当遵循合法、正当的原则，不得窃取或者以其他非法方式获取数据。

数据收集过程中，采取规范化采集流程、方式、渠道和数据格式， 根据数据安全级别采取相应的安全措施，加强重要数据和核心数据收集人员、设备的管理，并对收集来源、时间、类型、数量、频度、流向等进行记录。

对直接采集或者通过间接渠道获得的数据负有同等的保护责任和义务。通过间接途径获取重要数据和核心数据的，电信领域数据处理者应当与数据提供方通过签署相关协议、承诺书等方式，明确双方法律责任。

通过移动应用程序或其他方式面向用户直接收集个人信息类数据的，应在业务用户协议或隐私政策文件中明确个人信息收集的目的、用途和范围， 按照公开透明原则将收集规则以通俗易懂、简单明了的文字向用户明示， 在获得授权或有其他合法性基础的前提下开展。

第十九条 电信领域数据处理者应当按照法律、行政法规规定和用户约定的方式、期限进行数据存储， 应结合数据分类分级策略明确差异化数据存储安全策略和操作规程。

存储重要数据和核心数据的，应当采用校验技术、密码技术等措施进行安全存储，并实施数据容灾备份和存储介质安全管理，定期开展数据恢复测试，对备份数据的有效性和可用性进行检查和恢复验证。

第二十条 电信领域数据处理者进行数据使用加工应遵循目的明确原则，制定不同目的下数据使用审批流程、数据脱敏处理使用规则， 明确数据使用结果发布和使用的安全保护规则。

利用数据进行自动化决策的，应当保证决策的透明度和结果公平合理。使用、加工重要数据和核心数据的，还应当加强访问控制。

第二十一条 电信领域数据处理者应当根据传输的数据类型、级别和应用场景，制定安全策略并采取保护措施。针对不同网络安全域之间的数据传输采取访问控制、监控等安全防护技术措施。传输重要数据和核心数据的， 应当采取校验

技术、密码技术、安全传输通道或者安全传输协议等措施。

第二十二条 电信领域数据处理者对外提供数据，应当明确提供的范围、类别、条件、程序等， 对数据提供形式、期限、涉及的业务或系统、数据安全保护措施等实施管理。提供重要数据和核心数据的， 应当与数据获取方签订数据安全协议，对数据获取方数据安全保护能力进行核验，采取校验技术、密码技术、安全传输通道、安全传输协议等必要的安全保护措施。

第二十三条 电信领域数据处理者应当在数据公开前分析研判可能对国家安全、公共利益产生的影响， 拟公开前十个工作日前向北京市通信管理局提交重要数据和核心数据公开申请，审批通过后予以公开，存在重大影响的不得公开。对于法律、行政法规要求公开的数据场景， 应采用静态脱敏等措施防止数据泄露或滥用。

第二十四条 电信领域数据处理者在中华人民共和国境内收集和产生的重要数据和核心数据，法律、行政法规有境内存储要求的， 应当在境内存储，确需向境外提供的，应当依法依规进行数据出境安全评估。

第二十五条 电信领域数据处理者应当建立数据销毁制度，明确销毁对象、规则、流程和技术等要求， 对销毁活动进行记录和留存。个人、组织按照法律规定、合同约定等请求销毁的，电信领域数据处理者应当销毁相应数据。

销毁重要数据和核心数据的，应当设置销毁相关监督角色并采用多人操作模式，单人不得拥有完整操作权限。重要数据和核心数据销毁后，不得以任何理由、任何方式进行恢复；引起重要数据和核心数据目录备案内容发生变化的，应当履行备案变更手续。

电信领域数据处理者发生重组、解散、宣告破产、业务撤销等情形的， 应当在有关情形发生前向北京市通信管理局报告，按照相关要求移交或销毁数据。

第二十六条 跨主体提供、转移、委托处理核心数据的，电信领域数据处理者应当评估安全风险，采取必要的安全保护措施，并报送北京市通信管理局。北京市通信管理局按照有关规定进行审查后报工业和信息化部。

第四章 支持与保障

第二十七条 加强数据安全人才培养和引进，推动北京地区高等院校和职业院校加强数据安全相关学科建设；创新教育培养模式，鼓励高等院校、职业院校、

优质企业和培训机构深化产教融合，培养实用型、复合型数据安全专业技术技能人才和优秀管理人才。

第二十八条 鼓励开展数据安全知识宣传普及、教育培训，增强全市公共数据安全保护意识，推动有关部门、行业组织、科研机构、企业和个人共同参与数据安全保护工作，提高数据安全风险管理能力。

第二十九条 加强投诉举报，北京市通信管理局健全数据安全违法行为投诉举报机制，依法接收、处理投诉举报， 根据工作需要开展执法调查。鼓励电信领域数据处理者建立用户投诉处理机制。

第五章 附 则

第三十条 本细则自印发之日起施行。

网络服务提供者未成年人用户账号管理指引

(北京互联网法院 中国社会科学院大学互联网法治研究中心 2023 年 5 月 25 日)

第一条 为在网络服务中充分保护未成年人身心健康，保障未成年人合法权益，支持网络服务健康有序发展，鼓励网络服务提供者完善未成年人用户账号管理机制，根据《中华人民共和国未成年人保护法》《中华人民共和国个人信息保护法》《中华人民共和国网络安全法》等法律法规及相关规定，制定本指引。

第二条 网络服务提供者在未成年人用户账号的注册、管理及未成年人用户账号信息的处理中，应当坚持最有利于未成年人的原则，遵守现行法律法规关于未成年人权益保护的规定，创设有利于未成年人健康成长的网络空间和环境，保障未成年人的生存权、发展权、受保护权和参与权。

第三条 网络服务提供者依法提供适宜未成年人使用的网络服务，应当面向未成年人开放用户账号的注册申请，并设置“未成年人模式”或其他专门的未成年人用户账号管理机制，保障未成年人用户正当、平等使用网络及享受网络服务的权利。

第四条 网络服务提供者针对未成年人用户账号的管理机制包括未成年人用户身份认证机制、未成年人用户信息发布的审核巡查机制、未成年人权益侵害风险监测防御机制、账号交易管理机制等。

第五条 网络服务提供者应当在账号注册、充值打赏、商品或服务消费等环

节依法设置相应的身份认证机制，鼓励网络服务提供者探索开发与未成年人年龄相应的消费管理模式和内容管理机制，在特定商品或服务的消费环节依法设置实名身份认证。

第六条 网络服务提供者在非注册环节或非支付场景通过个人信息合法收集、用户主动提供年龄等方式识别账号实际系未成年人使用的，应当同步将该用户纳入未成年人账号管理。鼓励网络服务提供者在充分平衡用户个人信息保护、未成年人权益保护的情况下，探索符合法律规定的未成年人用户识别机制。

第七条 电子商务类网络服务提供者应当明确是否允许未成年人作为经营者在平台上开设店铺或进行经营行为。如果允许， 应当就年满十六周岁不满十八周岁的未成年人开设网络店铺的行为能力建立相应地审核、提示、管理机制。

第八条 网络服务提供者应当针对已认证的未成年人用户涉个人信息尤其是涉人身、财产安全信息的内容发布进行安全提醒。网络服务提供者发现未成年人用户发布包含自杀、自残倾向或其他心理健康风险倾向信息内容的， 应当及时予以介入或疏导，或采取其他合理措施。

第九条 鼓励网络服务提供者通过算法推荐、数据监控等科学、合理方式，针对未成年人用户的个人账号落实“未成年人模式”或“青少年防沉迷系统”下的账号权限管理、时间管理、内容管理、消费管理等功能。

第十条 网络服务提供者应优先处理涉未成年人网络暴力行为举报，综合研判本平台涉未成年人网络暴力现象的风险，并依据本平台未成年人用户的需求情况提供针对未成年人用户的网络暴力阻断、防治、巡查机制； 对涉未成年人网络暴力的信息不予发布或及时删除，对参与和实施网络暴力的主体及时采取警告、断开链接、禁言、账号封禁等处理措施； 涉及违法犯罪行为的，应当立即停止向其提供网络服务，保存有关记录，并向公安机关报告。

第十一条 电子商务平台应当加强对账号买卖租赁、代充值服务的管理，充分研判此类业务的合法合规性，采取合理的资质审核机制。如继续允许相关业务存在，应结合平台的未成年人保护机制，要求商户针对购买、租赁账号和代充值服务等情况进行询问、提示，发现交易对方为未成年人的，应当按照法律规定，不与其订立合同或要求监护人追认。

第十二条 网络服务提供者面向未成年人提供直播秀场、电子商务类网络服

务，应当建立对平台内第三方服务主体及从业人员的管理、培训以及教育机制，对多次出现侵害未成年人权益行为或严重侵害未成年人权益的第三方服务主体及从业人员，应当视情况及时采取警告、关停店铺、断开链接、禁言、账号封禁等处理措施；涉及违法犯罪行为的，应当立即停止向其提供网络服务，保存有关记录，并向公安机关报告。

附则 本指引为网络服务提供者完善未成年人账号管理机制提供参考，法律法规另有规定的，从其规定。本指引未尽事宜， 网络服务提供者应当按照最有利于未成年人的原则提供服务。

网络服务提供者涉侵害未成年人权益投诉处理指引

（北京互联网法院 中国社会科学院大学互联网法治研究中心 2023 年 5 月 25 日）

第一条 为在网络服务中充分保护未成年人身心健康，保障未成年人合法权益，鼓励网络服务提供者针对涉侵害未成年人权益行为完善投诉处理机制，支持网络服务健康有序发展，根据《中华人民共和国未成年人保护法》《中华人民共和国个人信息保护法》《中华人民共和国网络安全法》等法律法规及相关规定，制定本指引。

第二条 网络服务提供者面向未成年人提供服务，应当坚持最有利于未成年人的原则，遵守现行法律法规关于未成年人权益保护的规定，设置科学合理的涉未成年人权益投诉申诉审核处理流程机制，创设有利于未成年人健康成长的网络空间和环境，保障未成年人的生存权、发展权、受保护权和参与权。

第三条 网络服务提供者面向未成年人提供网络社交、网络音视频、网络直播、电子商务等网络服务， 应当针对涉未成年人权益的投诉或平台申诉设置并公示专门的审核处理机制。

第四条 未成年人用户比例较高、在未成年人群体中具有较大影响力的网络服务提供者应当针对平台内公开发布违法或不良信息行为、网络暴力行为、违法披露未成年人个人信息或隐私等涉及侵害未成年人权益的情况设置平台层面的巡查机制，在平台内发现侵害未成年人权益线索时，应当及时核验是否存在相关情况，并采取必要措施。

第五条 网络服务提供者接到涉及未成年人权益的通知时，应综合研判是否

涉及未成年人人身安全或基本权利风险，通过适当扩大信息内容审核范围、涉未成年人权益内容专门处理等方式及时减弱影响，并视情况立即采取删除，断开链接，向网信、公安等部门报告等必要处理措施。

第六条 网络服务提供者应当在显著、便利的位置提供针对涉未成年人权益的违法或不良信息发布、个人信息披露、网络暴力行为等的投诉举报入口。

第七条 未成年人用户比例较高、在未成年人群体中具有较大影响力的网络服务提供者面向未成年人提供信息发布、即时通讯、新闻资讯等信息内容类服务，对于涉未成年人权益的违法信息以及可能引发未成年人模仿不安全行为或违反社会公德行为、诱导未成年人不良嗜好等的信息应当不予发布； 已经发布的，接到投诉或平台巡查发现线索后，应当及时核实并视情况采取删除，断开链接，向网信、公安等部门报告等必要处理措施。

第八条 未成年人用户比例较高、在未成年人群体中具有较大影响力的网络服务提供者应当对本平台上网络暴力、违法披露未成年人个人信息或隐私等可能侵害未成年人权益的行为设置阻断及处罚机制；对严重或多次侵害未成年人权益的用户以及被投诉包含以上侵害未成年人权益行为的信息内容，平台经审核核实后应当视情况及时采取警告，删除，断开链接，禁言，账号封禁，向网信、公安等部门报告等必要处理措施。

第九条 非未成年人账号主体提出账号系未成年人使用并支出与其年龄、智力不相适应的款项要求退款时，网络服务提供者可要求申诉人提供身份信息、监护关系证明等材料并作情况说明，网络服务提供者可根据用户在平台的消费特点综合判断，对疑似为未成年人消费的，可通过电话回访等方式，核实相关问题，并对退款的帐户采取合理措施限制充值打赏功能。确认为未成年人消费的， 应积极与监护人协商处理退款事宜。

第十条 未成年人用户比例较高、在未成年人群体中具有较大影响力的网络服务提供者应当明确平台上信息内容生产者的行为规范并作为平台规则公开发布，保护和激励优质内容生产者。针对被投诉存在诱导未成年人充值打赏、发布可能影响未成年人身心健康信息的信息内容生产者，视情况及时采取警告、断开链接、禁言、账号封禁等处理措施。

第十一条 网络服务提供者提供生成式人工智能服务，应当对人工智能的生

成内容进行伦理审查，不得生成、提供、发布侵害未成年人权益的信息内容。

第十二条 网络服务提供者面向未成年人提供服务，设置涉未成年人权益投诉申诉审核处理机制，应当积极配合行政机关、司法机关的管理监督与调查取证，在涉未成年人权益投诉申诉审核处理中承担留证义务。

附则 本指引为网络服务提供者完善涉侵害未成年人权益投诉处理机制提供参考，法律法规另有规定的，从其规定。未尽事宜， 网络服务提供者应当按照最有利于未成年人的原则提供服务。

浙江省汽车数据处理管理规定

(2023 年 11 月 4 日)

第一条 为了规范省内汽车数据处理活动，保护个人、组织的合法权益，维护国家安全和社会公共利益，促进汽车数据合理开发利用，根据《中华人民共和国网络安全法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》《汽车数据安全管理若干规定(试行)》等法律法规和国家有关规定， 结合本省实际情况，制定本规定。

第二条 在本省行政区域内开展汽车数据处理活动，应当遵守本规定。

第三条 本规定所称汽车数据，包括汽车设计、生产、销售、使用、运维等过程中涉及的个人信息和重要数据。

汽车数据处理，包括汽车数据的收集、存储、使用、加工、传输、提供、公开等。

汽车数据处理者，是指开展汽车数据处理活动的组织，包括汽车制造商、零部件和软件供应商、经销商、维修机构以及出行服务企业等。

个人信息，是指以电子或者其他方式记录的与已识别或者可识别的车主、驾驶人、乘车人、车外人员等有关的各种信息，不包括匿名化处理后的信息。

敏感个人信息，是指一旦泄露或者非法使用，可能导致车主、驾驶人、乘车人、车外人员等受到歧视或者人身、财产安全受到严重危害的个人信息， 包括车辆行踪轨迹、音频、视频、图像和生物识别特征等信息。

重要数据是指一旦遭到篡改、破坏、泄露或者非法获取、非法利用， 可能危害国家安全、公共利益或者个人、组织合法权益的数据，包括：

(一)军事管理区、国防科工单位以及县级以上党政机关等重要敏感区域的地

理信息、人员流量、车辆流量等数据；

(二)车辆流量、物流等反映经济运行情况的数据；

(三)汽车充电网的运行数据；

(四)包含人脸信息、车牌信息等的车外视频、图像数据；

(五)涉及个人信息主体超过 10 万人的个人信息；

(六)国家网信部门和国务院发展改革、工业和信息化、公安、交通运输等有关部门确定的其他可能危害国家安全、公共利益或者个人、组织合法权益的数据。

座舱数据，是指通过摄像头、红外传感器、指纹传感器或传声器等部件从汽车座舱采集的可能包含个人信息的数据，以及对其进行加工后产生的数据。

个人信息主体，是指个人信息所标识或者关联的自然人。

匿名化，是指通过对个人信息的技术处理，使得个人信息主体无法被识别或者关联，且处理后的信息不能被复原的过程。

去标识化，是指通过对个人信息的技术处理，使其在不借助额外信息的情况下，无法识别或者关联个人信息主体的过程。

第四条 汽车数据处理必须具有明确、合理的目的，处理的汽车数据类型应与实现产品或服务的业务功能直接关联，同时应遵守对重要数据处理的相关规定。

直接关联指的是没有上述汽车数据的参与，产品或服务的功能无法实现。

第五条 汽车数据处理者处理个人信息前，应通过用户手册、车载显示面板、语音、汽车使用相关应用程序等显著方式， 告知处理个人信息的具体情境和必要性、各类个人信息的保存期限、精确到设区市的保存地点、用户权益事务联系人的姓名和联系方式等事项。

除法律法规另有规定外，汽车数据处理者处理个人信息前，应获得个人信息主体的授权同意，并向个人信息主体提供查阅、复制、删除等个人信息管理的方式和途径。

第六条 汽车数据处理者处理敏感个人信息，对每项敏感个人信息应取得个人信息主体单独同意，且不得一次性针对多项敏感个人信息取得同意，个人信息主体可自主选择同意期限。

汽车数据处理者收到敏感个人信息删除的请求，应当在十个工作日内删除。

第七条 汽车数据处理者通过车辆收集的车外视频、图像数据，如需向车外

提供，应在车内对数据中的人脸、车牌等信息进行匿名化处理。

除法律法规另有规定和下列情况外，未经个人信息主体单独同意，汽车不得向车外传输包含个人信息的数据。

(一)道路运输车辆依据相关规定向所属运输企业监控平台、公共管理平台和监管机构传输数据。

(二)出租汽车、公共汽车和教练车辆等营运车辆向监管机构传输数据。

(三)道路交通事故发生后按执法部门要求传输数据。

第八条 除非个人信息主体主动选择，汽车应默认设定为不收集座舱数据的状态，包括不打开车内的摄像头、传声器、红外传感器和指纹传感器等部件。

为保证行车安全及人身安全，正在提供公路营运服务的道路运输车辆，以及提供出行服务的公共汽车，可不关闭传声器、摄像头等收集座舱数据的部件。

第九条 汽车数据处理者持续收集敏感个人信息，应通过车载显示面板图标或信号装置指示灯的闪烁或长亮等方式提示收集状态。

个人信息主体要求终止收集敏感个人信息的，汽车数据处理者应提供实体按键、语音控制、虚拟按键等多种方式，确保收集终止。

第十条 汽车数据处理者不得存储原始个人生物识别信息，使用个人生物识别特征信息完成身份识别、认证等功能后， 应以不可逆方式删除可提取个人生物识别信息的原始图像。

第十一条 汽车数据处理者停止运营其产品或服务时，应通知个人信息主体，并及时停止继续收集个人信息，对其所持有的个人信息进行销毁或匿名化处理。

第十二条 汽车数据处理者进行商业营销推送，应取得个人信息主体授权同意，并提供拒绝接收商业营销推送的便捷方式。

第十三条 汽车数据处理者接入具备收集个人信息功能的第三方产品或服务时，应核验其实现方式，落实数据安全管理责任。

第十四条 汽车数据处理者未取得个人信息主体单独同意之前，不得公开其处理的个人信息和敏感个人信息。

除非个人信息主体拒绝，汽车数据处理者可以在合理的范围内处理已公开的个人信息。

第十五条 涉及显示屏幕、纸面等界面展示个人信息的，汽车数据处理者应

对需展示的个人信息采取去标识化处理等措施。

第十六条 汽车数据处理者设置个人信息保护方面的用户权益事务联系人，应对外告知联系人准确有效的姓名和联系方式，联系方式包括电话号码、邮箱地址、网址或即时通信平台账号等。

第十七条 汽车数据处理者因合并、分立、解散、被宣告破产等原因，需要转移个人信息，应向个人信息主体告知接收方的名称或者姓名和联系方式。

接收方变更原先的处理目的、处理方式的，应当重新取得个人信息主体同意。

第十八条 汽车数据处理者向境外提供汽车数据，应根据《数据出境安全评估办法》通过省网信部门向国家网信部门申报数据出境安全评估。

第十九条 汽车数据处理者不得公开披露个人生物识别特征信息，以及我国公民的种族、民族、政治观点、宗教信仰等敏感个人信息的分析结果。

第二十条 汽车数据处理者处置个人信息安全事件，个人信息泄露事件可能会给个人信息主体的合法权益造成严重危害的，应及时将事件相关情况以邮件、信函、电话、推送通知等方式告知受影响的个人信息主体。

第二十一条 汽车数据处理者应制定数据安全事件应急预案，并每年至少组织一次内部人员的应急响应培训和应急演练，内容包括记录事件内容、采取控制措施、上报事件情况等。

第二十二条 汽车数据处理者开展数据处理活动，应与行业组织、教育和科研机构、有关专业机构等在数据安全风险评估、防范、处置等方面开展协作， 组织数据安全教育培训，落实数据安全管理责任。

第二十三条 汽车数据处理者开展重要数据处理活动，应当按照规定开展风险评估，并向省网信部门和有关部门报送风险评估报告。

风险评估报告应当包括处理的重要数据的种类、目的、数量、范围、保存地点与期限、使用方式， 开展数据处理活动情况以及是否向第三方提供，面临的数据安全风险及其应对措施等。

第二十四条 开展重要数据处理活动的汽车数据处理者，应当在每年十二月十五日前向省网信部门和有关部门报送年度汽车数据安全管理情况。

第二十五条 汽车数据处理者违反本规定的， 由省级网信、经信、公安、交通运输等有关部门依照《中华人民共和国网络安全法》《中华人民共和国数据安

全法》《中华人民共和国个人信息保护法》等法律、行政法规的规定进行处罚；构成犯罪的，依法追究刑事责任。

第二十六条 本规定自 2023 年 11 月 1 日起施行。

上海市数据条例

上海市人民代表大会常务委员会公告〔十五届〕第九十四号

《上海市数据条例》已由上海市第十五届人民代表大会常务委员会第三十七次会议于 2021 年 11 月 25 日通过，现予公布，自 2022 年 1 月 1 日起施行。

上海市人民代表大会常务委员会

2021 年 11 月 25 日

上海市数据条例

(2021 年 11 月 25 日上海市第十五届人民代表大会常务委员会第三十七次会议通过)

第一章 总 则

第一条 为了保护自然人、法人和非法人组织与数据有关的权益，规范数据处理活动，促进数据依法有序自由流动，保障数据安全，加快数据要素市场培育，推动数字经济更好服务和融入新发展格局，根据《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》等法律、行政法规， 结合本市实际，制定本条例。

第二条 本条例中下列用语的含义：

(一)数据，是指任何以电子或者其他方式对信息的记录。

(二)数据处理，包括数据的收集、存储、使用、加工、传输、提供、公开等。

(三)数据安全，是指通过采取必要措施，确保数据处于有效保护和合法利用的状态，以及具备保障持续安全状态的能力。

(四)公共数据，是指本市国家机关、事业单位， 经依法授权具有管理公共事务职能的组织，以及供水、供电、供气、公共交通等提供公共服务的组织(以下统称公共管理和服务机构)，在履行公共管理和服务职责过程中收集和产生的数据。

第三条 本市坚持促进发展和监管规范并举，统筹推进数据权益保护、数据流通利用、数据安全管理， 完善支持数字经济发展的体制机制，充分发挥数据在

实现治理体系和治理能力现代化、推动经济社会发展中的作用。

第四条 市人民政府应当将数据开发利用和产业发展、数字经济发展纳入国民经济和社会发展规划，建立健全数据治理和流通利用体系，促进公共数据社会化开发利用，协调解决数据开发利用、产业发展和数据安全工作中的重大问题，推动数字经济发展和城市数字化转型。

区人民政府应当按照全市总体要求和部署，做好本行政区域数据发展和管理相关工作，创新推广数字化转型应用场景。

乡镇人民政府、街道办事处应当在基层治理中， 推进数据的有效应用，提升治理效能。

第五条 市政府办公厅负责统筹规划、综合协调全市数据发展和管理工作，促进数据综合治理和流通利用，推进、指导、监督全市公共数据工作。

市发展改革部门负责统筹本市新型基础设施规划建设和数字经济发展，推进本市数字化重大体制机制改革、综合政策制定以及区域联动等工作。

市经济信息化部门负责协调推进本市公共数据开放、社会经济各领域数据开发应用和产业发展，统筹推进信息基础设施规划、建设和发展，推动产业数字化、数字产业化等工作。

市网信部门负责统筹协调本市个人信息保护、网络数据安全和相关监管工作。

市公安、国家安全机关在各自职责范围内承担数据安全监管职责。

市财政、人力资源社会保障、市场监管、统计、物价等部门在各自职责范围内履行相关职责。

市大数据中心具体承担本市公共数据的集中统一管理，推动数据的融合应用。

第六条 本市实行数据工作与业务工作协同管理，管区域必须管数字化转型、管行业必须管数字化转型，加强运用数字化手段，提升治理能力和治理水平。

本市鼓励各区、各部门、各企业事业单位建立首席数据官制度。首席数据官由本区域、本部门、本单位相关负责人担任。

第七条 市人民政府设立由高校、科研机构、企业、相关部门的专家组成的数据专家委员会。数据专家委员会开展数据权益保护、数据流通利用、数据安全管理等方面的研究、评估，为本市数据发展和管理工作提供专业意见。

第八条 本市加强数字基础设施规划和布局，提升电子政务云、电子政务外

网等的服务能力，建设新一代通信网络、数据中心、人工智能平台等重大基础设施，建立完善网络、存储、计算、安全等数字基础设施体系。

第九条 市、区有关部门应当将数据领域高层次、高学历、高技能以及紧缺人才纳入人才支持政策体系；完善专业技术职称体系，创新数据人才评价与激励机制，健全数据人才服务和保障机制。

本市加强数据领域相关知识和技术的宣传、教育、培训， 提升公众数字素养和数字技能，将数字化能力培养纳入公共管理和服务机构教育培训体系。

第十条 市标准化行政主管部门应当会同市政府办公厅、市有关部门加强数据标准体系的统筹建设和管理。

市数据标准化技术组织应当推动建立和完善本市数据基础性、通用性地方标准。

第十一条 本市支持数据相关行业协会和组织发展。行业协会和组织应当依法制定并推动实施相关团体标准和行业规范，反映会员合理诉求和建议，加强行业自律，提供信息、技术、培训等服务， 引导会员依法开展数据处理活动，配合有关部门开展行业监管，促进行业健康发展。

第二章 数据权益保障

第一节 一般规定

第十二条 本市依法保护自然人对其个人信息享有的人格权益。

本市依法保护自然人、法人和非法人组织在使用、加工等数据处理活动中形成的法定或者约定的财产权益，以及在数字经济发展中有关数据创新活动取得的合法财产权益。

第十三条 自然人、法人和非法人组织可以通过合法、正当的方式收集数据。收集已公开的数据，不得违反法律、行政法规的规定或者侵犯他人的合法权益。法律、行政法规对数据收集的目的和范围有规定的， 应当在法律、行政法规规定的目的和范围内收集。

第十四条 自然人、法人和非法人组织对其合法取得的数据，可以依法使用、加工。法律、行政法规另有规定或者当事人另有约定的除外。

第十五条 自然人、法人和非法人组织可以依法开展数据交易活动。法律、行政法规另有规定的除外。

第十六条 市、区人民政府及其有关部门可以依法要求相关自然人、法人和非法人组织提供突发事件处置工作所必需的数据。

要求自然人、法人和非法人组织提供数据的，应当在其履行法定职责的范围内依照法定的条件和程序进行，并明确数据使用的目的、范围、方式、期限。收集的数据不得用于与突发事件处置工作无关的事项。对在履行职责中知悉的个人隐私、个人信息、商业秘密、保密商务信息等应当依法予以保密，不得泄露或者非法向他人提供。

第十七条 自然人、法人和非法人组织开展数据处理活动、行使相关数据权益，应当遵守法律、法规，尊重社会公德和伦理，遵守商业道德，诚实守信，不得危害国家安全和公共利益，不得损害他人的合法权益。

第二节 个人信息特别保护

第十八条 除法律、行政法规另有规定外，处理个人信息的，应当取得个人同意。个人信息的处理目的、处理方式和处理的个人信息种类发生变更的，应当重新取得个人同意。

处理个人自行公开或者其他已经合法公开的个人信息，应当依法在合理的范围内进行；个人明确拒绝的除外。处理已公开的个人信息，对个人权益有重大影响的，应当依法取得个人同意。

第十九条 基于个人同意处理个人信息的，应当保证个人在充分知情的前提下自愿、明确作出同意，不得通过误导、欺诈、胁迫等违背其真实意愿的方式取得同意。法律、行政法规规定处理个人信息应当取得个人单独同意或者书面同意的，从其规定。

处理者在提供产品或者服务时，不得以个人不同意处理其个人信息或者撤回同意为由，拒绝提供产品或者服务；处理个人信息属于提供产品或者服务所必需的除外。

第二十条 处理个人信息前，应当向个人告知下列事项：

(一)处理者的名称或者姓名和联系方式；

(二)处理个人信息的目的、方式；

(三)处理的个人信息种类、保存期限；

(四)个人依法享有的权利以及行使权利的方式和程序；

(五)法律、行政法规规定应当告知的其他事项。

处理者应当以显著方式、清晰易懂的语言真实、准确、完整地告知前款事项。

第二十一条 个人发现其个人信息不准确或者不完整的，有权请求处理者更正、补充。

有下列情形之一的，处理者应当主动删除个人信息；处理者未删除的，个人有权请求删除：

(一)处理目的已实现、无法实现或者为实现处理目的不再必要；

(二)处理者停止提供产品或者服务，或者保存期限已届满；

(三)个人撤回同意；

(四)处理者违反法律、行政法规或者违反约定处理个人信息；

(五)法律、行政法规规定的其他情形。

对属于本条第一款、第二款情形的，处理者应当分别予以更正、补充、删除。法律、行政法规另有规定的，从其规定。

第二十二条 处理自然人生物识别信息的，应当具有特定的目的和充分的必要性，并采取严格的保护措施。处理生物识别信息应当取得个人的单独同意； 法律、行政法规另有规定的，从其规定。

第二十三条 在本市商场、超市、公园、景区、公共文化体育场馆、宾馆等公共场所，以及居住小区、商务楼宇等区域，安装图像采集、个人身份识别设备，应当为维护公共安全所必需，遵守国家有关规定，并设置显著标识。

所收集的个人图像、身份识别信息， 只能用于维护公共安全的目的，不得用于其他目的；取得个人单独同意的除外。

本条第一款规定的公共场所或者区域，不得以图像采集、个人身份识别技术作为出入该场所或者区域的唯一验证方式。

第二十四条 利用个人信息进行自动化决策，应当遵循合法、正当、必要、诚信的原则，保证决策的透明度和结果的公平、公正， 不得对个人在交易价格等交易条件上实行不合理的差别待遇。

通过自动化决策方式向个人进行信息推送、商业营销的， 应当同时提供不针对其个人特征的选项，或者向个人提供便捷的拒绝方式。

通过自动化决策方式作出对个人权益有重大影响的决定，个人有权要求处理

者予以说明，并有权拒绝处理者仅通过自动化决策的方式作出决定。

第三章 公共数据

第一节 一般规定

第二十五条 本市健全公共数据资源体系，加强公共数据治理，提高公共数据共享效率，扩大公共数据有序开放，构建统一协调的公共数据运营机制，推进公共数据和其他数据融合应用，充分发挥公共数据在推动城市数字化转型和促进经济社会发展中的驱动作用。

第二十六条 负责本系统、行业公共数据管理的市级部门(以下简称市级责任部门)应当依据业务职能，制定本系统、行业公共数据资源规划，完善管理制度和标准规范，组织开展本系统、行业数据的收集、归集、治理、共享、开放、应用及其相关质量和安全管理。公共数据管理涉及多个部门或者责任不明确的， 由市政府办公厅指定市级责任部门。

区人民政府明确的公共数据主管部门，负责统筹开展本行政区域公共数据管理工作，接受市政府办公厅的业务指导。

第二十七条 市大数据资源平台和区大数据资源分平台(以下统称大数据资源平台)是本市依托电子政务云实施全市公共数据归集、整合、共享、开放、运营的统一基础设施，由市大数据中心负责统一规划。

本市财政资金保障运行的公共管理和服务机构不得新建跨部门、跨层级的公共数据资源平台、共享和开放渠道；已经建成的，应当按照有关规定进行整合。

第二十八条 本市建立全市统一的公共数据目录管理体系。公共管理和服务机构在依法履行公共管理和服务职责过程中收集和产生的数据，以及依法委托第三方收集和产生的数据，应当纳入公共数据目录。

市政府办公厅负责制定目录编制规范。市级责任部门应当按照数据与业务对应的原则，编制本系统、行业公共数据目录，明确公共数据的来源、更新频率、安全等级、共享开放属性等要素。区公共数据主管部门可以根据实际需要， 对未纳入市级责任部门公共数据目录的公共数据编制区域补充目录。

第二十九条 本市对公共数据实行分类管理。市大数据中心应当根据公共数据的通用性、基础性、重要性和数据来源属性等制定公共数据分类规则和标准，明确不同类别公共数据的管理要求，在公共数据全生命周期采取差异化管理措施。

市级责任部门应当按照公共数据分类规则和标准确定公共数据类别，落实差异化管理措施。

第三十条 公共管理和服务机构收集数据应当符合本单位法定职责，遵循合法、正当、必要的原则。可以通过共享方式获取的公共数据，不得重复收集。

需要依托区有关部门收集的视频、物联等数据量大、实时性强的公共数据，由区公共数据主管部门根据市级责任部门需求统筹开展收集，并依托区大数据资源分平台存储。

第三十一条 通过市大数据资源平台治理的公共数据，可以按照数据的区域属性回传至大数据资源分平台，支持各区开展数据应用。

第三十二条 本市财政资金保障运行的公共管理和服务机构为依法履行职责，可以申请采购非公共数据。市政府办公厅负责统筹市级公共管理和服务机构的非公共数据采购需求，市大数据中心负责统一实施。区公共数据主管部门负责统筹本行政区域个性化采购需求，自行组织采购。

第三十三条 本市国家机关、事业单位以及经依法授权具有管理公共事务职能的组织应当及时向大数据资源平台归集公共数据。其他公共管理和服务机构的公共数据可以按照逻辑集中、物理分散的方式实施归集， 但具有公共管理和服务应用需求的公共数据应当向大数据资源平台归集。

市大数据中心根据公共数据分类管理要求对相关数据实施统一归集，保障数据向大数据资源平台归集的实时性、完整性和准确性。

已归集的公共数据发生变更、失效等情形的， 公共管理和服务机构应当及时更新。

第三十四条 市大数据中心应当统筹规划并组织实施自然人、法人、自然资源和空间地理等基础数据库建设。

市级责任部门应当按照本市公共数据管理要求，规划和建设本系统、行业业务应用专题库，并会同相关部门规划和建设重点行业领域主题库。

第三十五条 市级责任部门应当建立健全本系统、行业公共数据质量管理体系，加强数据质量管控。

市大数据中心应当按照市政府办公厅明确的监督管理规则，组织开展公共数据的质量监督，对数据质量进行实时监测和定期评估，并建立异议与更正管理制

度。

第三十六条 市政府办公厅应当建立日常公共数据管理工作监督检查机制，对公共管理和服务机构的公共数据目录编制工作、质量管理、共享、开放等情况开展监督检查。

市政府办公厅应当对市级责任部门和各区开展公共数据工作的成效情况定期组织考核评价，考核评价结果纳入各级领导班子和领导干部年度绩效考核。

第三十七条 本市财政资金保障运行的公共管理和服务机构开展公共数据收集、归集、治理、共享、开放及其质量和安全管理等工作涉及的经费，纳入市、区财政预算。

第二节 公共数据共享和开放

第三十八条 公共管理和服务机构之间共享公共数据，应当以共享为原则，不共享为例外。公共数据应当通过大数据资源平台进行共享。

公共管理和服务机构应当根据履职需要，提出数据需求清单；根据法定职责，明确本单位可以共享的数据责任清单；对法律、法规明确规定不能共享的数据，经市政府办公厅审核后，列入负面清单。

市政府办公厅应当建立以共享需求清单、责任清单和负面清单为基础的公共数据共享机制。

第三十九条 公共管理和服务机构提出共享需求的，应当明确应用场景，并承诺其真实性、合规性、安全性。对未列入负面清单的公共数据，可以直接共享，但不得超出依法履行职责的必要范围；对未列入公共数据目录的公共数据，市级责任部门应当在收到共享需求之日起十五个工作日内进行确认后编入公共数据目录并提供共享。

公共管理和服务机构超出依法履行职责的必要范围，通过大数据资源平台获取其他机构共享数据的，市大数据中心应当在发现后立即停止其获取超出必要范围的数据。

第四十条 公共管理和服务机构向自然人、法人和非法人组织提供服务时，需要使用其他部门数据的，应当使用大数据资源平台提供的最新数据。

公共管理和服务机构应当建立共享数据管理机制，通过共享获取的公共数据，应当用于本单位依法履行职责的需要，不得以任何形式提供给第三方，也不得用

于其他任何目的。

第四十一条 本市以需求导向、分级分类、公平公开、安全可控、统一标准、便捷高效为原则，推动公共数据面向社会开放，并持续扩大公共数据开放范围。

公共数据按照开放类型分为无条件开放、有条件开放和非开放三类。涉及个人隐私、个人信息、商业秘密、保密商务信息，或者法律、法规规定不得开放的，列入非开放类；对数据安全和处理能力要求较高、时效性较强或者需要持续获取的公共数据，列入有条件开放类；其他公共数据列入无条件开放类。

非开放类公共数据依法进行脱密、脱敏处理，或者相关权利人同意开放的，可以列入无条件开放或者有条件开放类。对有条件开放类公共数据， 自然人、法人和非法人组织可以通过市大数据资源平台提出数据开放请求，相关公共管理和服务机构应当按照规定处理。

第四十二条 本市依托市大数据资源平台向社会开放公共数据。

市级责任部门、区人民政府以及其他公共管理和服务机构分别负责本系统、行业、本行政区域和本单位的公共数据开放， 在公共数据目录范围内制定公共数据开放清单，明确数据的开放范围、开放类型、开放条件和更新频率等， 并动态调整。

公共数据开放具体规则，由市经济信息化部门制定。

第四十三条 本市制定相关政策，组织开展公共数据开放和开发利用的创新试点，鼓励自然人、法人和非法人组织对公共数据进行深度加工和增值使用。

第三节 公共数据授权运营

第四十四条 本市建立公共数据授权运营机制，提高公共数据社会化开发利用水平。

市政府办公厅应当组织制定公共数据授权运营管理办法，明确授权主体，授权条件、程序、数据范围， 运营平台的服务和使用机制，运营行为规范，以及运营评价和退出情形等内容。市大数据中心应当根据公共数据授权运营管理办法对被授权运营主体实施日常监督管理。

第四十五条 被授权运营主体应当在授权范围内，依托统一规划的公共数据运营平台提供的安全可信环境，实施数据开发利用，并提供数据产品和服务。

市政府办公厅应当会同市网信等相关部门和数据专家委员会，对被授权运营

主体规划的应用场景进行合规性和安全风险等评估。

授权运营的数据涉及个人隐私、个人信息、商业秘密、保密商务信息的， 处理该数据应当符合相关法律、法规的规定。

市政府办公厅、市大数据中心、被授权运营主体等部门和单位， 应当依法履行数据安全保护义务。

第四十六条 通过公共数据授权运营形成的数据产品和服务，可以依托公共数据运营平台进行交易撮合、合同签订、业务结算等；通过其他途径签订合同的，应当在公共数据运营平台备案。

第四章 数据要素市场

第一节 一般规定

第四十七条 市人民政府应当按照国家要求，深化数据要素市场化配置改革，制定促进政策，培育公平、开放、有序、诚信的数据要素市场，建立资产评估、登记结算、交易撮合、争议解决等市场运营体系，促进数据要素依法有序流动。

第四十八条 市政府办公厅应当制定政策，鼓励和引导市场主体依法开展数据共享、开放、交易、合作，促进跨区域、跨行业的数据流通利用。

第四十九条 本市制定政策，培育数据要素市场主体，鼓励研发数据技术、推进数据应用，深度挖掘数据价值，通过实质性加工和创新性劳动形成数据产品和服务。

第五十条 本市探索构建数据资产评估指标体系，建立数据资产评估制度，开展数据资产凭证试点，反映数据要素的资产价值。

第五十一条 市相关主管部门应当建立健全数据要素配置的统计指标体系和评估评价指南，科学评价各区、各部门、各领域的数据对经济社会发展的贡献度。

第五十二条 市场主体应当加强数据质量管理，确保数据真实、准确、完整。

市场主体对数据的使用应当遵守反垄断、反不正当竞争、消费者权益保护等法律、法规的规定。

第二节 数据交易

第五十三条 本市支持数据交易服务机构有序发展，为数据交易提供数据资产、数据合规性、数据质量等第三方评估以及交易撮合、交易代理、专业咨询、数据经纪、数据交付等专业服务。

本市建立健全数据交易服务机构管理制度，加强对服务机构的监管，规范服务人员的执业行为。

第五十四条 数据交易服务机构应当建立规范透明、安全可控、可追溯的数据交易服务环境，制定交易服务流程、内部管理制度， 并采取有效措施保护数据安全，保护个人隐私、个人信息、商业秘密、保密商务信息。

第五十五条 本市鼓励数据交易活动，有下列情形之一的，不得交易：

(一)危害国家安全、公共利益，侵害个人隐私的；

(二)未经合法权利人授权同意的；

(三)法律、法规规定禁止交易的其他情形。

第五十六条 市场主体可以通过依法设立的数据交易所进行数据交易，也可以依法自行交易。

第五十七条 从事数据交易活动的市场主体可以依法自主定价。

市相关主管部门应当组织相关行业协会等制订数据交易价格评估导则，构建交易价格评估指标。

第五章 数据资源开发和应用

第五十八条 本市支持数据资源开发和应用，发挥海量数据和丰富应用场景优势，鼓励和引导全社会参与经济、生活、治理等领域全面数字化转型， 提升城市软实力。

第五十九条 本市通过标准制定、政策支持等方式，支持数据基础研究和关键核心技术攻关，发展高端数据产品和服务。

本市培育壮大数据收集存储、加工处理、交易流通等数据核心产业， 发展大数据、云计算、人工智能、区块链、高端软件、物联网等产业。

第六十条 本市促进数据技术与实体经济深度融合，推动数据赋能经济数字化转型，支持传统产业转型升级，催生新产业、新业态、新模式。本市鼓励各类企业开展数据融合应用，加快生产制造、科技研发、金融服务、商贸流通、航运物流、农业等领域的数据赋能，推动产业互联网和消费互联网贯通发展。

第六十一条 本市促进数据技术和服务业深度融合，推动数据赋能生活数字化转型，提高公共卫生、医疗、教育、养老、就业等基本民生领域和商业、文娱、体育、旅游等质量民生领域的数字化水平。本市制定政策， 支持网站、手机应用

程序、智慧终端设施、各类公共服务设施面向残疾人和老年人开展适应性数字化改造。

第六十二条 本市促进数据技术与政府管理、服务、运行深度融合，推动数据赋能治理数字化转型，深化政务服务“一网通办”、城市运行“一网统管”建设，推进经济治理、社会治理、城市治理领域重点综合场景应用体系构建， 通过治理数字化转型驱动超大城市治理模式创新。

第六十三条 本市鼓励重点领域产业大数据枢纽建设，融合数据、算法、算力，建设综合性创新平台和行业数据中心。

本市推动国家和地方大数据实验室、产业创新中心、技术创新中心、工程研究中心、企业技术中心，以及研发与转化功能型平台、新型研发组织等建设。

第六十四条 本市建设数字化转型示范区，支持新城等重点区域同步规划关键信息基础设施，完善产业空间、生活空间、城市空间等领域数据资源的全生命周期管理机制。

市、区人民政府应当根据本市产业功能布局， 推动园区整体数字化转型，发展智能制造、在线新经济、大数据、人工智能等数字产业园区。

第六章 浦东新区数据改革

第六十五条 本市支持浦东新区高水平改革开放、打造社会主义现代化建设引领区，推进数据权属界定、开放共享、交易流通、监督管理等标准制定和系统建设。

第六十六条 本市支持浦东新区探索与海关、统计、税务、人民银行、银保监等国家有关部门建立数据共享使用机制，对浦东新区相关的公共数据实现实时共享。

浦东新区应当结合重大风险防范、营商环境提升、公共服务优化等重大改革创新工作，明确数据应用场景需求。

浦东新区应当健全各区级公共管理和服务机构之间的公共数据共享机制。

第六十七条 本市按照国家要求，在浦东新区设立数据交易所并运营。

数据交易所应当按照相关法律、行政法规和有关主管部门的规定， 为数据交易提供场所与设施，组织和监管数据交易。

数据交易所应当制订数据交易规则和其他有关业务规则，探索建立分类分层

的新型数据综合交易机制，组织对数据交易进行合规性审查、登记清算、信息披露，确保数据交易公平有序、安全可控、全程可追溯。

浦东新区鼓励和引导市场主体依法通过数据交易所进行交易。

第六十八条 本市根据国家部署，推进国际数据港建设，聚焦中国(上海)自由贸易试验区临港新片区(以下简称临港新片区)，构建国际互联网数据专用通道、功能型数据中心等新型基础设施，打造全球数据汇聚流转枢纽平台。

第六十九条 本市依照国家相关法律、法规的规定，在临港新片区内探索制定低风险跨境流动数据目录，促进数据跨境安全、自由流动。在临港新片区内依法开展跨境数据活动的自然人、法人和非法人组织，应当按照要求报送相关信息。

第七十条 本市按照国家相关要求，采取措施，支持浦东新区培育国际化数据产业，引进相关企业和项目。

本市支持浦东新区建立算法评价标准体系，推动算法知识产权保护。

本市支持在浦东新区建设行业性数据枢纽，打造基础设施和平台，促进重大产业链供应链数据互联互通。

第七十一条 本市支持浦东新区加强数据交易相关的数字信任体系建设，创新融合大数据、区块链、零信任等技术， 构建数字信任基础设施，保障可信数据交易服务。

第七章 长三角区域数据合作

第七十二条 本市按照国家部署，协同长三角区域其他省建设全国一体化大数据中心体系长三角国家枢纽节点，优化数据中心和存算资源布局，引导数据中心集约化、规模化、绿色化发展， 推动算力、数据、应用资源集约化和服务化创新，全面支撑长三角区域各行业数字化升级和产业数字化转型。

第七十三条 本市与长三角区域其他省共同开展长三角区域数据标准化体系建设，按照区域数据共享需要，共同建立数据资源目录、基础库、专题库、主题库、数据共享、数据质量和安全管理等基础性标准和规范， 促进数据资源共享和利用。

第七十四条 本市依托全国一体化政务服务平台建设长三角数据共享交换平台，支撑长三角区域数据共享共用、业务协同和场景应用建设， 推动数据有效流动和开发利用。

本市与长三角区域其他省共同推动建立以需求清单、责任清单和共享数据资源目录为基础的长三角区域数据共享机制。

第七十五条 本市与长三角区域其他省共同推动建立跨区域数据异议核实与处理、数据对账机制， 确保各省级行政区域提供的数据与长三角数据共享交换平台数据的一致性，实现数据可对账、可校验、可稽核，问题可追溯、可处理。

第七十六条 本市与长三角区域其他省共同促进数字认证体系、电子证照等的跨区域互认互通，支撑政务服务和城市运行管理跨区域协同。

第七十七条 本市与长三角区域其他省共同推动区块链、隐私计算等数据安全流通技术的利用，建立跨区域的数据融合开发利用机制，发挥数据在跨区域协同发展中的创新驱动作用。

第八章 数据安全

第七十八条 本市实行数据安全责任制，数据处理者是数据安全责任主体。

数据同时存在多个处理者的，各数据处理者承担相应的安全责任。

数据处理者发生变更的，由新的数据处理者承担数据安全保护责任。

第七十九条 开展数据处理活动，应当履行以下义务，保障数据安全：

(一)依照法律、法规的规定， 建立健全全流程数据安全管理制度和技术保护机制；

(二)组织开展数据安全教育培训；

(三)采取相应的技术措施和其他的必要措施，确保数据安全，防止数据篡改、泄露、毁损、丢失或者非法获取、非法利用；

(四)加强风险监测，发现数据安全缺陷、漏洞等风险时， 应当立即采取补救措施；

(五)发生数据安全事件时，应当立即采取处置措施，按照规定及时告知用户并向有关主管部门报告；

(六)利用互联网等信息网络开展数据处理活动，应当在网络安全等级保护制度的基础上，履行上述数据安全保护义务；

(七)法律、法规规定的其他数据安全保护义务。

第八十条 本市按照国家要求，建立健全数据分类分级保护制度，推动本地区数据安全治理工作。

本市建立重要数据目录管理机制，对列入目录的数据进行重点保护。重要数据的具体目录由市政府办公厅会同市网信等部门编制，并按照规定报送国家有关部门。

第八十一条 重要数据处理者应当明确数据安全责任人和管理机构，按照规定定期对其数据处理活动开展风险评估，并依法向有关主管部门报送风险评估报告。

处理重要数据应当按照法律、行政法规及国家有关规定执行。

第八十二条 市级责任部门应当制定本系统、行业公共数据安全管理制度，并根据国家和本市数据分类分级相关要求对公共数据进行分级，在数据收集、使用和人员管理等业务环节承担安全责任。

属于市大数据中心实施信息化工作范围的，市大数据中心应当对公共数据的传输、存储、加工等技术环节承担安全责任，并按照数据等级采取安全防护措施。

第八十三条 本市按照国家统一部署，建立健全集中统一的数据安全风险评估、报告、信息共享、监测预警机制， 加强本地区数据安全风险信息的获取、分析、研判、预警工作。

第八十四条 本市按照国家统一部署，建立健全数据安全应急处置机制。发生数据安全事件，市网信部门应当会同市公安机关依照相关应急预案，采取应急处置措施，防止危害扩大，消除安全隐患，并及时向社会发布与公众有关的警示信息。

第八十五条 本市支持数据安全检测评估、认证等专业机构依法开展服务活动。

本市支持有关部门、行业组织、企业、教育和科研机构、有关专业机构等在数据安全风险评估、防范、处置等方面开展协作。

第九章 法律责任

第八十六条 违反本条例规定，法律、行政法规有规定的，从其规定。

第八十七条 国家机关、履行公共管理和服务职责的事业单位及其工作人员有下列行为之一的，由本级人民政府或者上级主管部门责令改正；情节严重的，由有权机关对直接负责的主管人员和其他直接责任人员依法给予处分：

(一)未按照本条例第十六条第二款规定收集或者使用数据的；

(二)违反本条例第二十七条第二款规定，擅自新建跨部门、跨层级的数据资源平台、共享、开放渠道，或者未按规定进行整合的；

(三)未按照本条例第二十八条规定编制公共数据目录的；

(四)未按照本条例第三十条、第三十三条、第三十八条、第三十九条、第四十条、第四十二条规定收集、归集、共享、开放公共数据的；

(五)未按照本条例第三十五条第一款规定履行公共数据质量管理义务的；

(六)未通过公共数据开放或者授权运营等法定渠道，擅自将公共数据提供给市场主体的。

第八十八条 违反本条例规定，依法受到行政处罚的，相关信息纳入本市公共信用信息服务平台，由有关部门依法开展联合惩戒。

第八十九条 违反本条例规定处理个人信息，侵害众多个人的权益的，人民检察院、市消费者权益保护委员会， 以及由国家网信部门确定的组织，可以依法向人民法院提起诉讼。

第十章 附 则

第九十条 除本条例第二条第四项规定的公共管理和服务机构外，运行经费由本市各级财政保障的单位、中央国家机关派驻本市的相关管理单位以及通信、民航、铁路等单位在依法履行公共管理和服务职责过程中收集和产生的各类数据，参照公共数据的有关规定执行。法律、行政法规另有规定的，从其规定。

第九十一条 本条例自 2022 年 1 月 1 日起施行。

上海市杨浦区企业数据合规指引

(2022 年 1 月 27 日)

为贯彻落实习近平总书记重要讲话精神和党中央重大决策部署，根据最高人民检察院关于企业合规改革试点的工作要求，充分发挥检察职能作用，深入探索督促企业数据合规管理，及时有效惩治预防数据违法犯罪，进一步优化营商环境，为数字经济高质量发展提供更加优质的法治保障，结合本区经济发展情况制定本指引，为相关企业建立数据合规管理体系提供参考。

第一章 总 则

第一条【目的和依据】为引导企业加强数据合规管理， 保护个人信息，保障数据安全，规范数据处理活动，根据《中华人民共和国个人信息保护法》《中华

人民共和国网络安全法》《中华人民共和国数据安全法》等法律法规(以下统称为数据法规)，制定本指引。

第二条【适用范围和效力】本区各类所有制企业进行数据处理活动均可参照本指引开展数据合规管理。

本指引不具有强制性，法律法规对数据合规另有专门规定的，从其规定。

第三条【数据分类分级保护】企业应当建立数据分类分级保护制度。按照数据对国家安全、公共利益或者个人、组织合法权益的影响和重要程度进行分类分级，针对不同类别级别的数据采取相应的保护措施。

第四条【数据权益保障】鼓励数据处理者按照《上海市数据条例》的规定开发和利用数据资源。数据处理者依法在数据处理活动中形成的法定或者约定的财产权益，以及在数字经济发展中有关数据创新活动取得的合法财产权益受法律保护。

第五条【数据合规管理的重要性】引导各类企业开展数据合规管理是降低企业及其员工涉数据类违法犯罪风险的重要举措，对于建立现代化的企业合规管理制度和文化具有重要意义，有利于促进企业合规守法经营，推动企业在市场竞争的道路上行稳致远。

第二章 数据合规管理体系

第六条【合规责任人】企业的最高管理者是数据合规的第一责任人。最高管理者应当承担以下职责：

(一)分配足够和适当的资源来建立、发展、实施、评估、维护和改进数据合规管理体系；

(二)确保建立举报数据违规的有效机制；

(三)确保战略和运营目标与履行数据合规义务之间的一致性；

(四)建立和维护问责机制，包括纪律处分和后果；

(五)确保将数据合规落实情况和效果纳入企业内部人员绩效考核体系。

第七条【数据合规管理部门】鼓励各类企业设置专门的数据合规管理部门，或者将数据合规管理职能融入现有的企业合规管理体系，但是不建议由法务部门履行合规管理职能。

企业应当向数据合规管理部门负责人提供足够的授权、人力、财力来支持数

据合规管理体系的运行。一般由董事会直接设立企业合规部门，下设数据合规管理部门等各类专业合规部门。

第八条【数据合规计划】数据合规部门负责人应结合企业自身的经营范围、行业特征、监管政策、风险识别等因素制定并不断完善数据合规计划。

数据合规计划应当根据企业内部环境和外部环境的变化不断调整，以帮助企业应对各种风险的挑战。

第九条【数据合规管理部门管理职责】数据合规管理部门应履行以下职责：

(一)制定数据合规管理整体方针策略，协调建立数据合规技术保障措施，牵头做好数据风险识别、风险评估、风险处置等工作；

(二)制定、完善数据合规计划，并推动其有效实施；

(三)审核评估企业的经营管理和业务行为，确保企业与供应商、代理商、经销商、关联企业、分支机构的业务活动， 以及处理个人信息等活动符合数据法规的要求，并制定数据风险应对措施；

(四)组织或协助管理部门、业务部门等开展数据合规教育培训， 并向管理层和各部门员工提供数据合规咨询；

(五)建立数据合规举报记录台账，对数据合规举报制定调查方案并开展调查；

(六)推动将数据合规责任纳入企业岗位职责和员工绩效考核评价体系，培养数据合规文化；

(七)持续关注国内和业务所涉国家(地区)数据法规的发展动态，及时提供数据合规建议。

第十条【数据合规管理协调】数据合规管理部门应加强与业务部门的分工协作。相关业务部门应主动进行日常数据合规管理工作， 识别业务范围内的合规要求，制定并落实业务管理制度和风险防范措施，配合数据合规管理部门进行合规风险审查、评估和调查、处置、整改工作。

数据合规管理部门应与其他具有合规管理职能的监督部门 (如法务部门、审计部门、监察部门等)建立明确的合作和信息交流机制，加强协调配合。

企业应积极与数据监管部门建立沟通渠道，了解数据监管部门期望的数据合规体系，并制定符合其要求的数据合规制度；对于复杂或专业性强且存在重大数据风险的事项，可以向数据监管部门咨询；面对数据监管部门的调查，企业应积

极沟通并予以配合。

第三章 数据风险识别

第十一条【风险识别】企业开展数据合规管理应当准确识别风险。常见的数据风险包括数据全生命周期各阶段中可能存在的未授权访问、数据滥用、数据泄漏等风险，以及侵犯个人信息、非法获取计算机信息系统数据、传播违法信息、侵犯知识产权、非法跨境提供数据等刑事犯罪风险， 企业应根据识别出的风险评估相关经营管理和业务行为是否合规。

本章所列的风险内容并非数据风险的全面指引，企业应当根据自身实际情况建立必要的数据合规计划，通过内部反馈、外部咨询、持续跟踪数据立法、执法、司法的最新进展等方式准确识别数据风险。

第十二条【禁止从事的数据活动】企业及其员工开展数据处理活动应当遵守法律、行政法规，尊重社会公德和伦理，不得从事以下活动：

(一)危害国家安全、荣誉和利益，泄露国家秘密和工作秘密；

(二)侵害他人人格权、知识产权和其他合法权益等；

(三)通过窃取或者以其他非法方式获取数据；

(四)非法出售或者非法向他人提供数据；

(五)制作、发布、复制、传播违法信息；

(六)法律、行政法规禁止的其他行为。

任何个人和组织知道或者应当知道他人从事前款活动的，不得为其提供技术支持、工具、程序和广告推广、支付结算等服务。

第十三条【数据安全】数据处理者处理个人信息等数据应当符合数据法规的规定，遵循合法、正当、必要和诚信的原则。

数据处理者开展影响或者可能影响国家安全的数据处理活动，应当按照国家有关规定，申报网络安全审查。

第十四条【自动化工具】数据处理者在采用网络爬虫等自动化工具访问、收集数据时，应当评估对网络服务的性能、功能带来的影响， 不得干扰网络服务的正常功能。

自动化工具访问、收集数据违反法律、行政法规或者行业自律公约、影响网络服务正常功能，或者侵犯他人知识产权等合法权益的，数据处理者应当停止访

问、收集数据行为并采取相应补救措施。

第十五条【软件开发工具包】企业在应用程序开发和运营过程中使用第三方软件开发工具包时，应当通过合同等形式明确第三方的数据安全责任义务，并督促第三方采取必要的数据安全保护措施，加强数据合规管理。

企业可以使用经相关部门审核合规的开源软件开发工具包进行程序开发活动，不得使用风险不可控的开源软件开发工具包等工具。

第十六条【个人信息的处理规则】数据处理者处理个人信息， 应当依据《个人信息保护法》的规定遵守以下规则：

(一)按照服务类型分别向个人申请处理个人信息的同意，不得使用概括性条款取得同意；

(二)处理个人生物识别、宗教信仰、特定身份、医疗健康、金融账户、行踪轨迹等敏感个人信息应当取得个人单独同意；

(三)处理不满十四周岁未成年人的个人信息，应当取得其监护人同意；

(四)不得以改善服务质量、提升用户体验、研发新产品等为由， 强迫个人同意处理其个人信息；

(五)不得通过误导、欺诈、胁迫等方式获得个人的同意；

(六)不得通过捆绑不同类型服务、批量申请同意等方式诱导、强迫个人进行批量个人信息同意；

(七)不得超出个人授权同意的范围处理个人信息；

(八)不得在个人明确表示不同意后，频繁征求同意、干扰正常使用服务。

个人信息的处理目的、处理方式和处理的个人信息种类发生变更的， 数据处理者应当重新取得个人同意，并同步修改个人信息处理规则。依法无需取得个人同意的除外。

第十七条【个人信息的处理】数据处理者应当采取必要的安全保护措施收集、传输、存储、加工、使用、提供、公开个人信息数据。

数据处理者应按照《个人信息保护法》的规定及时删除个人信息或者进行匿名化处理。

第十八条【个人生物特征信息】数据处理者利用生物特征进行个人身份认证的，应当对必要性、安全性进行风险评估，不得强制个人同意收集人脸、步态、

指纹、虹膜、声纹等生物特征信息。

在宾馆、商场、银行、车站、机场、体育场馆、娱乐场所等经营场所、公共场所收集使用人脸等生物特征信息应当严格遵守法律、行政法规的规定。

数据处理者应当采取严格的保护措施确保其依法收集、存储的人脸等生物特征信息安全，防止泄露、篡改和丢失。

第十九条【向第三方提供数据的规则】数据处理者向第三方提供个人信息，或者共享、交易、委托处理重要数据的，应当遵守以下规则：

(一)向个人告知提供个人信息的目的、类型、方式、范围、存储期限、存储地点，并取得个人单独同意，符合法律、行政法规规定的不需要取得个人同意的情形或者经过匿名化处理的除外；

(二)与数据接收方约定处理数据的目的、范围、处理方式， 数据安全保护措施等，通过合同等形式明确双方的数据安全责任义务，并对数据接收方的数据处理活动进行监督；

(三)留存个人同意记录及提供个人信息的日志记录，共享、交易、委托处理重要数据的审批记录、日志记录至少五年。

数据处理者为订立、履行个人作为一方当事人的合同所必需向第三方提供个人信息的，在采取适当的数据保护措施后无需取得个人单独同意。

第二十条【接收方处理数据的规则】数据接收方应当履行约定的义务， 不得超出约定的目的、范围、处理方式处理个人信息和重要数据， 且不得从事数据法规禁止的行为。

第二十一条【跨境提供个人信息等数据】数据处理者因业务等需要， 确需向中华人民共和国境外提供数据的，应当符合法律法规关于跨境提供数据的规定，事先开展数据出境风险自评估。

数据处理者跨境提供个人信息的，应当向个人等告知境外数据接收方的名称、联系方式、处理目的、处理方式、个人信息的种类以及个人向境外数据接收方行使个人信息权利的方式等事项，并取得个人的单独同意。

第二十二条【个人权利保障】数据处理者在个人信息处理活动中， 应当保障《个人信息保护法》规定的个人对其个人信息处理活动享有的知情权、决定权、查阅权、复制权、更正、补充权、删除权等权利。

第四章 数据风险评估与处置

第二十三条【风险评估】企业在识别数据风险内容的基础上，可根据自身经营规模、组织体系、业务内容以及市场环境，分析和评估数据风险的来源、发生的可能性、后果的严重性等，并对数据风险进行分级。

数据合规部门负责人应当根据风险评估结果对不同职级、不同工作范围的管理层与员工进行风险提示，降低管理层和员工的违法犯罪风险。

第二十四条【风险处置机制】企业应建立健全数据安全事件应急预案与风险处置机制，对识别和评估的各类数据风险设置恰当的控制和应对措施来降低风险，必要时停止相关风险行为。

发生个人信息等数据泄露、篡改、丢失等事件的，数据处理者应当立即采取补救措施，并通知所在地区的数据监管部门。安全事件涉嫌犯罪的，应当及时向公安机关报案。

第二十五条【立即停止违法行为】经评估发现可能已经发生数据违法行为，或者数据监管部门已立案并启动调查程序的，企业应当立即停止违法行为并与执法机构合作。

企业积极配合调查或者主动消除、减轻违法行为危害后果的，可能会获得数据监管部门从轻或者减轻处罚。

第二十六条【积极应对数据监管部门的调查】当企业受到数据监管部门调查时，应通知管理层、法务负责人、数据合规负责人和相关业务工作负责人等，按照企业内部受调查操作流程妥善应对，进行内部初步调查，分析相关法律法规并评估数据违法行为成立的可能性与法律后果。

企业应积极配合数据监管机构调查。不得拒绝提供有关材料、信息，或者提供虚假材料、信息，或者隐匿、销毁、转移证据，或者有其他拒绝、阻碍调查的行为。

第二十七条【投诉举报渠道】

数据处理者应当建立便捷的数据安全投诉举报渠道，及时受理、处置数据安全投诉举报。

数据处理者应当公布接受投诉、举报的联系方式、责任人信息，每年公开披露受理和收到的数据安全投诉数量、投诉处理情况、平均处理时间情况，接受社

会监督。

第五章 数据合规运行与保障

第二十八条【合规咨询】企业可建立数据合规咨询机制， 管理层和各部门员工在工作中可以向数据合规管理部门咨询数据合规问题。数据合规管理部门应当不断学习、提升合规管理水平，也可以同外部机构开展数据合规咨询合作。

第二十九条【发现机制】发现机制是数据合规管理部门通过日常监测和定期评估发现数据不合规行为的机制，可以通过设置日常的流程监控、内部审核、重点核查以及定期评等方式发现企业及员工的违规行为，并及时按照合规计划采取相应的处置措施。

数据合规管理部门应定期向合规负责人汇报数据合规管理情况。当发生可能给企业带来重大数据合规风险的违规行为时，应当及时向合规负责人汇报，并提出相应的解决方案。

第三十条【举报机制】举报机制是员工根据合规计划举报企业内部违规行为的机制，应当允许员工实名或者匿名通过内部举报系统举报数据违规行为，并严格保护实名举报者和匿名举报者不受打击和报复，尤其是保护匿名举报者的个人信息安全。

第三十一条【激励和纪律】企业应当建立数据合规考核机制， 数据合规考核结果作为企业绩效考核的重要依据，与员工的评优评先、职务任免、职务晋升以及薪酬待遇等挂钩。

对于严格遵守数据合规的管理层和员工，制定适当的激励措施使合规计划得到一致遵守和执行。

对于不严格执行甚至违反合规计划的管理层和员工，采取适当的纪律措施进行惩戒，并根据违规程度采取不同的风险处置措施。

第三十二条【培训与承诺】数据合规管理部门应当建立培训机制， 定期为管理层、员工培训数据合规， 使其充分了解数据法规、数据合规计划、岗位角色与职责等。

鼓励企业管理层和其他员工作出并履行明确、公开的数据合规承诺， 内容主要是知悉、愿意遵守数据合规计划，愿意承担违反数据合规承诺的后果。

第三十三条【数据合规管理信息化建设】企业可通过数据合规管理信息化建

设，并运用大数据分析等工具，加强对经营管理行为中的数据合规的实时监控和风险分析。

第三十四条【数据合规文化培育】鼓励企业将数据合规文化作为企业文化建设的重要内容，践行合规经营的价值观，不断增强员工的数据合规意识。

鼓励行业协会在本行业内积极倡导数据合规文化，强化行业的数据合规意识。

第六章 附 则

第三十五条【基本概念】本指引所称的概念含义如下：

(一)数据，是指任何以电子或者其他方式对信息的记录；

(二)数据合规，是指企业及其员工的经营管理行为符合个人信息保护、网络安全、数据安全等数据法规的要求；

(三)数据合规管理，是指以预防和降低涉数据违法犯罪为目的，以企业及其员工经营管理行为为对象，开展包括合规管理体系、风险识别、风险评估与处置、合规运行与保障等有组织、有计划的管理活动；

(四)个人信息，是以电子或者其他方式记录的与已识别或者可识别的自然人有关的各种信息，不包括匿名化处理后的信息。个人信息的处理包括个人信息的收集、存储、使用、加工、传输、提供、公开、删除等；

(五)数据安全，是指通过采取必要措施，确保数据处于有效保护和合法利用的状态，以及具备保障持续安全状态的能力；

(六)重要数据，重要数据是指一旦遭到篡改、破坏、泄露或者非法获取、非法利用，可能危害国家安全、公共利益的数据；

(七)数据处理，包括数据的收集、传输、存储、加工、使用、提供、公开等。

(八)自动化工具，自动化工具是按照一定规则能够自动实现某些功能的程序。

第三十六条【法律责任】数据处理者违反数据法规规定处理个人信息等数据的，被侵权者可以要求数据处理者承担民事责任；数据监管部门可以追究数据处理者的行政责任。

数据处理者违反《刑法》规定， 可能被追究以下刑事责任：侵犯公民个人信息罪、破坏计算机信息系统罪、非法侵入计算机信息系统罪、非法获取计算机信息系统数据、非法控制计算机信息系统罪、提供侵入、非法控制计算机信息系统程序、工具罪、拒不履行信息网络安全管理义务罪、非法利用信息网络罪、帮助

信息网络犯罪活动罪、侵犯商业秘密罪等。

第三十七条 指引的解释

本指引由上海市杨浦区人民检察院、上海市杨浦区工商业联合会、上海市信息服务业行业协会、上海数据合规与安全产业发展专家工作组负责解释。

第三十八条 施行日期

本指引自发布之日起施行。

附录一：

企业可参考的相关法律法规与标准

序号	类型	层级	名称
1	数据安全	法律	《国家安全法》
2		法律	《网络安全法》
3		法律	《数据安全法》
4		司法解释	《最高人民法院关于审理使用人脸识别技术处理个人信息相关民事案件适用法律若干问题的规定》
5		行政法规	《网络数据安全管理条例(征求意见稿)》
6		部门规章	《网络安全审查办法》
7		部门规范性文件	《网络数据安全标准体系建设指南(征求意见稿)》
8		标准	《网络数据处理安全规范(征求意见稿)》
9	重要数据保护	标准	《重要数据识别指南》（征求意见稿）
10		标准	《基础电信企业重要数据识别指南》 2019-0217T-YD CCSA 草案
11	个人信息保护	法律	《个人信息保护法》
		标准	《信息安全技术 个人信息安全规范》 (GB/T 35273—2020)
12	数据出境安全评估	部门规章	《数据出境安全评估办法(征求意见稿)》
13		标准	《信息安全技术 数据出境安全评估指南》 (征求意见稿)
14	电信领域	部门规章	《工业和信息化领域数据安全管理办法(试行)》（征求意见稿）

15		标准	《基础电信企业数据分类分级方法》
16		标准	《基础电信企业重要数据识别指南》
17		标准	《电信网和互联网数据安全评估规范》
18		标准	《电信网和互联网数据安全通用要求》
19	金融领域	标准	《金融数据安全 数据安全分级指南》(JR/T 0197—2020)
20		标准	《金融数据安全 数据生命周期安全规范》(JR/T 0223—2021)
21		标准	《金融数据安全 数据安全评估规范》(征求意见稿)
22		标准	《金融数据跨境安全要求》(征求意见稿)
23		标准	《证券期货业数据分类分级指引》(JR/T 0158-2018)
24	汽车领域	部门规章	《汽车数据安全管理若干规定(试行)》
25		部门工作文件	《工业和信息化部关于加强车联网网络安全和数据安全工作的通知(工信部网安〔2021〕134 号)》
26	医疗领域	部门规范性文件	《国家健康医疗大数据标准、安全和服务管理办法(试行)》
27		标准	《信息安全技术 健康医疗数据安全指南》

关于印发《上海市电信和互联网行业首席数据官制度建设指南(试行)》的通知

本市各电信和互联网企业，各相关单位：

为贯彻《数据安全法》《工业和信息化领域数据安全管理办法(试行)》《上海市数据条例》有关规定精神， 健全电信和互联网行业数据治理体系，根据“浦江护航”数据安全专项行动任务要求，我局研究编制了《上海市电信和互联网行业首席数据官制度建设指南(试行)》，现印发给你们，请遵照执行。

特此通知。

上海市通信管理局

2023 年 5 月 31 日

上海市电信和互联网行业首席数据官制度建设指南(试行)

一、总则

为深入贯彻落实《数据安全法》《中共中央 国务院关于构建更加完善的要素市场化配置体制机制的意见》《数字中国建设整体布局规划》《工业和信息化领域数据安全管理办法(试行)》《上海市数据条例》等文件精神，着力营造开放、健康、安全的数字生态， 坚持数据发展与安全并重，深化上海市电信和互联网行业数据治理，健全电信和互联网企业数据安全管理组织，明晰上海市电信和互联网行业首席数据官管理职责和边界，制定本建设指南。

二、工作目标

以习近平新时代中国特色社会主义思想为指导，全面贯彻党的二十大精神，深入落实习近平总书记关于“发展数字经济，抢占未来发展制高点”重要指示精神，以上海全面推进城市数字化转型为契机，加快数据要素市场建设，营造良好数字生态，打造优势数字产业，护航数字经济安全。通过在本市电信和互联网行业试点建立首席数据官(以下简称CDO)制度，将数据战略引入自身的日常管理运营，指导行业全面统筹数据开发、利用和安全， 引导企业构建、激活数据管理能力。

三、适用对象

本指南的适用对象为在本市行政区域内取得电信业务经营许可证的电信和互联网企业，包括基础电信业务经营者和互联网数据中心、互联网接入服务、在线数据处理与交易处理、互联网信息服务等增值电信业务经营者以及域名注册管理和服务机构等。

四、职责分工

上海市通信管理局及有关主管部门。在工业和信息化部的领导下， 根据市政府办公厅的统筹指导，市通信管理局部署推进电信和互联网行业 CDO 制度建设工作、指导开展 CDO 培训和研讨等相关活动、施行 CDO 备案制度等管理工作。市通信管理局与相关部门建立通报协调机制，定期通报电信和互联网行业 CDO 制度建设与管理情况。

电信和互联网企业。负责企业 CDO 制度建设工作，设立 CDO 岗位，明确其工作职责，坚持企业发展与数据安全并重，将数据战略引入自身的日常管理运营中，协调企业整体范围内数据管理和运用，构建、激活并保持企业的数据管理能力。

行业协会组织、相关专业机构。支撑与服务上海市电信和互联网行业 CDO 制

度建设工作，组织开展 CDO 培训和研讨等相关活动、建立 CDO 人才库、遴选并推广 CDO 制度建设优秀案例等相关工作。

五、主要任务

(一)企业 CDO 制度的建立

CDO 应设置在企业最高管理层，应为高级管理团队中分管数据治理的管理人员。CDO 负责和实施企业数据相关战略工作，审批数据安全整体策略，统筹保障数据发展与安全工作所需人、财、物等资源， 促进企业数据与公共数据融合与发展，壮大数据要素市场，并确保数据安全各项工作有序开展。

CDO 制度的组织架构设计应职责清晰、分工明确， 组织重点职责包括制定数据安全和数据发展利用相关制度、规范、标准， 明确数据责任归属，建设数据安全技术防护架构，健全数据治理考核机制。

企业需配置专职岗位负责本单位数据处理、流通利用等具体工作， 以及与数据工作相关的沟通协调和日常联络工作，例如数据产业政策宣贯、数据利用制度实施、辖内数据安全管理等。企业还需配备相关岗位配合开展本单位的数据收集、管理和运营，协助内设业务机构负责人开展具体应用场景的规划设计，本岗位可由单位内设关键业务机构中既熟悉业务又具备一定信息化技能的人员兼任。

企业各内设部门需要全力支持 CDO 及其管理组织的相关工作，有效保障数据管理各项措施切实执行。

(二)企业 CDO 的职责

1.制定企业数据治理战略并推动实施

制定企业数据治理战略，在保障企业数据战略目标与业务战略目标的一致的前提下，持续跟踪市场竞争环境、信息化发展动向、数据安全技术发展等最新趋势，将数据作为战略资产来管理落实数据治理、完善企业数据成熟度， 全面推动企业数字化转型变革；积极构建企业数据资产文化，推进开展培训教育，引导员工建立正确的数据资产意识和价值观，增强全员的数据治理意识。

2.优化企业数据治理与发展

加强与政府部门的沟通，在符合我国现行法律法规监管要求下，以保障合法权利和权益为前提，探索开放数据策略，强化数据管控、分析和使用， 充分发掘数据价值，全方位协调数据资源促成交换共享、应用集成和职能协调， 实现降本

增效、各项业务的良性循环效应， 积极促进企业各部门以及外部组织间的数据开放共享，加快完善数据要素市场化配置。

3.加强数据合规与安全保障

落实《数据安全法》《工业和信息化领域数据安全管理办法(试行)》等法律法规和规范性文件要求，密切关注数据安全监管动向和发展趋势，根据自身实际情况健全以重要数据和核心数据保护为基础的数据安全保障体系，健全完善数据分类分级、目录管理以及风险评估等核心制度机制，加强管理和技术能力储备，以确保数据处于有效保护和合法利用的状态，以及具备保障持续安全状态的能力。

(三)企业 CDO 的能力要求

CDO 需具有良好的职业道德和敬业精神，诚实守信、履职尽责； 熟悉并遵守国家相关法律法规和标准，具有正确的数据价值观，有强烈的大数据意识和广阔的大数据视野，熟悉本企业的业务状况和所处的行业背景，有较强的创新、组织和协调能力；能够定期参加主管部门组织或指导的 CDO 专业能力培训。

CDO 核心能力和素质应包括：

1.战略思维与规划能力

具有对企业数据工作进行全局的战略规划和布局、合理配置企业内外部资源、制定发展目标和工作计划的能力。

2.领导力与执行能力

建立工作团队、指挥和带领团队成员围绕数据战略规划开展工作、实现数据发展目标的能力。支持、整合企业内外部资源、协调各方面的关系以促成合作的能力。

3.对数据的深刻理解和对行业的洞察力

深刻理解所在行业的数据资产价值以及技术发展趋势，准确判断数据及新技术带来机遇和风险的能力；深度了解数据安全相关法律和监管部门工作机制，具有良好的数据合规风险防控与应对的能力。

(四)企业 CDO 备案机制

施行企业 CDO 备案机制。企业需填写《企业首席数据官备案表(试行)》(详情见附件)，由企业法人签字，并加盖公章后报上海市通信管理局备案。如遇人员变动等情况，需在 5 个工作日内重新备案。

企业名称	

注册地址			组织机构代码	
经营范围			员工人数	
首席数据官基本信息	姓名		电子邮件	
	手机		最高学历	
	专业		专业资质	
主要工作经历及数据治理领域取得的业绩				
数据治理组织架构及数据专职岗位人员信息				
企业意见	法人签字： （单位盖章） 年　月　日			

关于印发《中国(上海)自由贸易试验区临港新片区数据跨境流动分类分级管理办法(试行)》的通知

沪自贸临管规范〔2024〕3 号

管委会各部门、各直属单位，临港新片区各镇、各开发公司、各有关单位：

为加快更大力度先行先试、更高水平对外开放、更大程度促进发展， 在数据跨境流动、跨境离岸金融等领域率先开展更大程度的压力测试， 加快推动国际数据经济产业园建设，管委会组织制定《中国(上海)自由贸易试验区临港新片区数据跨境流动分类分级管理办法(试行)》，并经 2024 年 1 月 30 日第 2 次管委会主任办公会审议通过，现予印发，请认真执行。

附件：中国(上海)自由贸易试验区临港新片区数据跨境流动分类分级管理办法(试行)

中国(上海)自由贸易试验区临港新片区管理委员会

2024 年 2 月 8 日

中国(上海)自由贸易试验区临港新片区数据跨境流动分类分级管理办法(试行)

第一章 总 则

第一条 指导思想

以习近平新时代中国特色社会主义思想为指导，以“五个重要”指示精神为

统领，对标最高标准、最高水平， 实行更大程度的压力测试，深化“五自由一便利”制度型开放，充分发挥国际数据要素价值赋能实体经济发展。全面深入对接国际高标准经贸规则，制定数据跨境流动分类分级管理办法，推动数据安全、高效、自由有序跨境流动， 实现高水平对外开放，打造国际一流营商环境，提升数字经济的国际影响力。

第二条 目的和依据

为进一步指导和帮助数据处理者高效合规地开展数据跨境流动，中国(上海)自由贸易试验区临港新片区管理委员会(以下简称“临港新片区管委会”)根据《网络安全法》《数据安全法》《个人信息保护法》《国务院关于进一步优化外商投资环境加大吸引外商投资力度的意见》《全面对接国际高标准经贸规则推进中国(上海)自由贸易试验区高水平制度型开放总体方案》《数据出境安全评估办法》以及《上海市数据条例》等文件，制定本办法。

第三条 适用范围

本办法适用于在临港新片区范围内登记注册的，或在临港新片区开展数据跨境流动相关活动的企业、事业单位、机构协会和组织等数据处理者。

第四条 基本原则

(一)安全有序：统筹发展与安全，保障国家安全、公共利益，释放数据价值，促进数据产业国际化发展。

(二)正当必要：数据处理者开展数据跨境流动时需遵守法律法规的规定，采取对数据主体影响最小的方式处理数据，不得损害数据主体的合法权益。

(三)需求导向：以问题为导向，案例为样本，通过清单化方式管理，增强数据跨境流动的便利性和实用性。

(四)分类分级：遵循国家数据分类分级保护要求，按照数据所属行业领域进行分类分级管理，通过建立数据跨境流动重要数据目录、一般数据清单的模式，分类施策，分级管理。

(五)动态更新：根据有关法律、法规、规章和政策的要求， 对清单进行动态更新。

第二章 职责及分工

第五条 管理部门职责

临港新片区管委会负责建立数据跨境流动工作统筹推进协调机制，具体工作包括：

(一)建立数据跨境流动分类分级管理体系并统筹协调相关事宜；

(二)协调各行业主管部门，推动制定和更新数据跨境流动清单；

(三)对数据处理者的数据跨境流动进行日常监管，开展风险防范工作；

(四)接受市委网信办及各行业主管部门对数据跨境流动工作进行指导、监督。

第六条 数据处理者职责

数据处理者应当按照相关规定，做好自身的数据分类分级管理，并积极参与临港新片区相关数据跨境流动清单的研究制定。

数据处理者在开展数据跨境活动过程中，应开展数据出境风险自评估，主动识别申报重要数据。

第三章 数据跨境分类分级管理

第七条 数据跨境分类管理

结合上海“五个中心”建设，围绕汽车、金融、航运、生物医药等重点领域以及临港新片区相关行业的发展要求，以跨境需求最迫切的典型场景为切入口，对跨境数据进行分类管理。

第八条 数据跨境分级管理

按照《数据安全法》要求， 跨境数据分级从高到低依次分为核心数据、重要数据、一般数据 3 个级别，核心数据禁止跨境，重要数据形成重要数据目录，一般数据形成一般数据清单。

第四章 重要数据目录管理

第九条 重要数据目录制定

临港新片区管委会负责制定纳入数据出境安全评估管理范围的重要数据目录，并报相关部门备案。同时按照要求制定纳入数据出境安全评估、个人信息出境标准合同、个人信息保护认证管理范围的数据清单， 报经市委网络安全和信息化委员会批准后，报相关部门备案。

第十条 重要数据目录应用

数据处理者对重要数据目录内的数据，可通过临港新片区数据跨境服务中心申报数据出境安全评估。

第十一条 重要数据目录更新机制

临港新片区管委会负责对重要数据目录进行更新，并报相关部门备案，经批准后及时告知数据处理者。

第五章 一般数据清单管理

第十二条 一般数据清单制定

在确保国家安全、公共利益和个人隐私的前提下， 临港新片区管委会负责制定一般数据清单。

第十三条 一般数据清单应用

数据处理者对在一般数据清单内的数据，可向临港新片区管委会申请登记备案，并在满足相关管理要求下自由流动。

第十四条 一般数据清单更新机制

临港新片区管委会负责对一般数据清单进行更新，并及时告知数据处理者。若相关领域出台场景化重要数据目录，则该领域的一般数据清单自动失效。

第六章 监督管理及违规处置

第十五条 管理要求

开展数据跨境活动的数据处理者可向临港新片区管委会申请备案，对纳入临港新片区管委会备案管理的数据跨境活动，临港新片区管委会依托“临港新片区数据便捷流通公共服务管理平台”，提供数据跨境流动合规服务。相关数据清单调整后，数据处理者应及时更新备案。

第十六条 监督检查

临港新片区管委会负责对数据处理者的数据跨境活动进行日常监督检查以及抽查，数据处理者应予以积极配合。

第十七条 违规处置

若数据处理者在数据跨境流动过程中未严格履行相关承诺，或出现其他违规行为的，临港新片区管委会可立即暂停或终止数据跨境流动。数据处理者需继续开展数据跨境流动的，应按照要求整改，整改完成后重新备案。

第十八条 违规追责

数据处理者对自身所提交材料的真实性、安全性、合规性等承担法律责任，若发现故意违反有关法律、法规的行为，由相关单位依法追究其法律责任。

第七章 附 则

第十九条 法律适用

(一)本办法未明确规定的，若法律、行政法规或者国家网信部门、行业主管部门等有关部门和上海市出台新的规定，从其规定；

(二)我国缔结或者参加的国际条约、协定有不同规定的，适用该国际条约、协定，但我国声明保留的条款除外。

第二十条 鼓励与支持

临港新片区管委会鼓励企业、科研院所、高等院校以及行业协会等各方参与制定相关领域的重要数据目录和一般数据清单，给予相应支持。

第二十一条 办法解释及试行日期

本办法由临港新片区管委会负责解释，自 2024 年 2 月 8 日起试行，有效期至 2025 年 2 月 7 日。

附录 A

相关名词解释

1.核心数据：对领域、群体、区域具有较高覆盖度或达到较高精度、较大规模、一定深度的重要数据，一旦被非法使用或共享，可能直接影响政治安全。主要包括关系国家安全重点领域的数据，关系国民经济命脉、重要民生、重大公共利益的数据，经国家有关部门评估确定的其他数据；

2.重要数据：特定领域、特定群体、特定区域或达到一定精度和规模的数据，一旦被泄露或篡改、损毁， 可能直接危害国家安全、经济运行、社会稳定、公共健康和安全。仅影响组织自身或公民个体的数据，一般不作为重要数据；

3.一般数据：核心数据、重要数据外的其他数据；

4.数据分类：按照数据具有的某种共同属性或特征，采用一定原则和方法进行区分和归类，以便于管理和使用数据；

5.数据分级：数据分级的目的是差异性保护数据安全，按照数据一旦遭到篡改、破坏、泄露或者非法获取、非法利用后对国家安全、公共利益、个人合法权益和组织合法权益的危害程度对跨境数据进行分级，为数据全生命周期管理的安全策略制定和分级监管提供支撑。

关于印发《中国(上海)自由贸易试验区临港新片区智能网联汽车领域数据跨境

场景化一般数据清单(试行)》的通知

沪自贸临管委〔2024〕50 号

管委会各部门、各有关单位：

为促进数据跨境安全有序流动，发挥临港新片区先行先试作用，依据《国务院关于进一步优化外商投资环境 加大吸引外商投资力度的意见》《全面对接国际高标准经贸规则推进中国(上海)自由贸易试验区高水平制度型开放总体方案》《促进和规范数据跨境流动规定》《中国(上海)自由贸易试验区临港新片区数据跨境流动分类分级管理办法(试行)》等规定，临港新片区管委会研究形成《中国(上海)自由贸易试验区临港新片区智能网联汽车领域数据跨境场景化一般数据清单(试行)》，主要包括跨境场景、数据类别、典型示例和说明、传输要求等内容。数据处理者可向临港新片区管委会申请咨询一般数据清单各数据类别项下的数据字段，并按照《中国(上海)自由贸易试验区临港新片区数据跨境流动一般数据清单操作指南(试行)》的管理要求开展数据跨境流动。本清单试行期限为自发布之日起后一年整，试行结束后将依据实际情况作出调整更新。

本清单由临港新片区管理委员会负责解释。

特此通知。

附件：中国(上海)自由贸易试验区临港新片区智能网联汽车领域数据跨境场景化一般数据清单(试行)

中国(上海)自由贸易试验区临港新片区管理委员会

2024 年 5 月 16 日

关于印发《中国(上海)自由贸易试验区临港新片区生物医药领域数据跨境场景化一般数据清单(试行)》的通知

沪自贸临管委〔2024〕51 号

管委会各部门、各有关单位：

为促进数据跨境安全有序流动，发挥临港新片区先行先试作用，依据《国务院关于进一步优化外商投资环境 加大吸引外商投资力度的意见》《全面对接国际高标准经贸规则推进中国(上海)自由贸易试验区高水平制度型开放总体方案》《促进和规范数据跨境流动规定》《中国(上海)自由贸易试验区临港新片区数据跨境流动分类分级管理办法(试行)》等规定，临港新片区管委会研究形成

《中国(上海)自由贸易试验区临港新片区生物医药领域数据跨境场景化一般数据清单(试行)》，主要包括跨境场景、数据类别、典型示例和说明、传输要求等内容。数据处理者可向临港新片区管委会申请咨询一般数据清单各数据类别项下的数据字段，并按照《中国(上海)自由贸易试验区临港新片区数据跨境流动一般数据清单操作指南(试行)》的管理要求开展数据跨境流动。本清单试行期限为自发布之日起后一年整，试行结束后将依据实际情况作出调整更新。本清单由临港新片区管理委员会负责解释。

特此通知。

附件：中国(上海)自由贸易试验区临港新片区生物医药领域数据跨境场景化一般数据清单(试行)

中国(上海)自由贸易试验区临港新片区管委会

2024 年 5 月 16 日

关于印发《中国(上海)自由贸易试验区临港新片区公募基金领域数据跨境场景化一般数据清单(试行)》的通知

沪自贸临管委〔2024〕52 号

管委会各部门、各有关单位：

为促进数据跨境安全有序流动，发挥临港新片区先行先试作用，依据《国务院关于进一步优化外商投资环境 加大吸引外商投资力度的意见》《全面对接国际高标准经贸规则推进中国(上海)自由贸易试验区高水平制度型开放总体方案》《促进和规范数据跨境流动规定》《中国(上海)自由贸易试验区临港新片区数据跨境流动分类分级管理办法(试行)》等规定，临港新片区管委会研究形成《中国(上海)自由贸易试验区临港新片区公募基金领域数据跨境场景化一般数据清单(试行)》，主要包括跨境场景、数据类别、典型示例和说明、传输要求等内容。数据处理者可向临港新片区管委会申请咨询一般数据清单各数据类别项下的数据字段，并按照《中国(上海)自由贸易试验区临港新片区数据跨境流动一般数据清单操作指南(试行)》的管理要求开展数据跨境流动。本清单试行期限为自发布之日起后一年整，试行结束后将依据实际情况作出调整更新。本清单由临港新片区管理委员会负责解释。

特此通知。

附件：中国(上海)自由贸易试验区临港新片区公募基金领域数据跨境场景化一般数据清单(试行)

中国(上海)自由贸易试验区临港新片区管理委员会

2024 年 5 月 16 日

关于印发《中国(天津)自由贸易试验区企业数据分类分级标准规范》的通知

津商自贸〔2024〕1 号

各有关单位：

为促进和规范中国(天津)自由贸易试验区企业数据安全有序流动，提升数据安全保护能力，依据《中华人民共和国数据安全法》《中华人民共和国网络安全法》《中华人民共和国个人信息保护法》和《天津市促进大数据发展应用条例》等法律法规和政策规定，市商务局、自贸试验区管委会研究制定了《中国(天津)自由贸易试验区企业数据分类分级标准规范》，现予印发，请认真执行。

市商务局

自贸试验区管委会

2024 年 2 月 5 日

中国(天津)自由贸易试验区企业数据分类分级标准规范

为促进和规范中国(天津)自由贸易试验区(以下简称天津自贸试验区)企业数据安全有序流动，提升数据安全保护能力，依据《中华人民共和国数据安全法》《中华人民共和国网络安全法》《中华人民共和国个人信息保护法》和《天津市促进大数据发展应用条例》等法律法规和政策规定，制定本规范。

一、实施目的

加快高水平对外开放，落实自贸试验区提升战略，在天津自贸试验区开展先行先试，对接国际高标准经贸规则，探索数据领域规则创新，建立天津自贸试验区数据分类分级保护制度，鼓励数据依法依规、安全有序流动。通过构建天津自贸试验区数据跨境流动管理新模式，解决企业数据跨境流动政策诉求，为企业数据出境提供便利，保障商业数据安全顺畅流动，有效提升天津自贸试验区营商环境。

二、总体要求

坚持以习近平新时代中国特色社会主义思想为指导，以总体国家安全观为根

本遵循，贯彻落实党中央、国务院对数据安全工作的重大决策部署， 推动天津自贸试验区对接国际高标准经贸规则，统筹发展和安全，在国家数据分类分级总体框架下开展天津自贸试验区企业数据分类分级工作，制定天津自贸试验区企业重要数据目录，促进商业数据自由流动，消费者权益充分保障，天津自贸试验区企业数据跨境流动安全有序，数据汇聚融合、共享开放、开发利用和安全保障能力进一步增强，制度型开放进一步加快，发挥天津自贸试验区先行先试的示范带动作用。

三、适用范围

本规范适用于天津自贸试验区内企业在生产经营过程中产生、收集、存储、传输和处理的数据的分类分级。涉及国家秘密的数据、政务数据的分类分级不包含在本规范适用范围之内，按照有关法律、法规和规定执行。

四、总体原则

遵循国家数据分类分级保护要求，按照数据所属行业领域进行分类分级管理，依据以下原则对数据进行分类分级。

(一)合法合规原则

天津自贸试验区企业开展数据分类分级应按照有关法律法规，遵循行业主管部门数据分类分级标准规范，优先对国家或行业主管部门有明确要求的数据进行识别和管理，满足相应数据安全管理要求。

(二)统筹兼顾原则

统筹发展和安全，既维护国家安全、保护数据安全， 又有利于促进数据开发利用，推动数字经济和数字贸易加快发展。发挥政策创新优势， 探索支持有序流动并有效保障安全的企业数据管理模式，促进天津自贸试验区内商业数据安全顺畅流动，构筑数字贸易发展新生态。

(三)通用性和隐私保护相统一原则

数据分类分级标准规范适用范围立足天津自贸试验区，面向更广泛对外开放场景，充分考虑通用性，力争覆盖天津自贸试验区的各类企业、各项业务， 兼顾长远对外开放需求。注重个人信息隐私保护， 在从国家安全角度考虑数据自身重要性的同时，关注并防范海量个人信息、个人隐私数据汇聚后可能对国家安全、公共利益和公民权益带来的影响。

(四)就高从严原则

采用就高原则确定数据级别，当多个因素可能影响数据分级时，按照可能造成的各个影响对象的最高影响程度确定数据级别。

(五)动态更新原则

根据数据的业务属性、重要性和可能造成的危害程度的变化， 对数据分类分级、重要数据目录等进行定期审核更新。

五、术语和定义

(一)核心数据

对领域、群体、区域具有较高覆盖度或达到较高精度、较大规模、 一定深度的重要数据，一旦被非法使用或共享，可能直接影响政治安全。主要包括关系国家安全重点领域的数据，关系国民经济命脉、重要民生、重大公共利益的数据，经国家有关部门评估确定的其他数据。

(二)重要数据

特定领域、特定群体、特定区域或达到一定精度和规模的数据，一旦被泄露或篡改、损毁， 可能直接危害国家安全、经济运行、社会稳定、公共健康和安全等的数据。仅影响组织自身或公民个体的数据，一般不作为重要数据。

(三)一般数据

核心数据、重要数据之外的其他数据。

(四)数据分类

按照数据具有的某种共同属性或特征(包括数据对象共享属性、开放属性、应用场景等)，采用一定原则和方法进行区分和归类，以便于管理和使用数据。

(五)数据分级

数据分级目的是差异化保护数据安全，按照数据遭到破坏(包括攻击、泄露、篡改、非法使用等)后对国家安全、社会稳定、公共利益以及个人、法人和其他组织的合法权益(受侵害客体)的危害程度对数据进行定级，为数据全生命周期管理的安全策略制定提供支撑。

(六)天津自贸试验区

天津自贸试验区于 2014 年 12 月由国务院批准设立，2015 年 4 月正式挂牌运行，是全国第二批、北方第一个自贸试验区。规划面积 119.9 平方公里，包括

天津机场片区、天津港东疆片区、滨海新区中心商务片区三个片区。其中， 天津机场片区是天津先进制造业和研发转化的重要集聚区，重点发展航空航天、装备制造、新一代信息技术等高端制造业和研发设计、航空物流等生产性服务业。天津港东疆片区是中国北方国际航运中心和国际物流中心的核心功能区，重点发展航运物流、国际贸易、融资租赁等现代服务业。滨海新区中心商务片区是天津市金融改革创新集聚区，重点发展金融创新、总部经济、跨境电子商务、科技信息服务、文化传媒创意等现代服务业。

六、数据分类机制

按照国家部委关于各领域数据分类分级标准规范要求，结合天津自贸试验区企业应用需求和数据管理实际，将自贸试验区内企业在生产经营过程中收集、存储、使用、加工、传输、提供、公开的数据按照所属行业性质分类，依次分为三层，每个层级又分成若干类目管理。同一层级的类目构成并列关系，不同层级类目构成隶属关系。

一层分类划分为战略物资和大宗商品类、自然资源和环境类、工业类、国防科技工业类、电信类、广电视听传媒类、金融类、交通运输类、卫生健康和食品药品类、公共安全类、互联网服务和电子商务类、科学技术类以及其他数据类共十三类。

二层分类是在一层分类的基础上，将十三类数据细分为四十个子类别。

(一)战略物资和大宗商品类

1.石油、石化和天然气。包括存储与交易数据、国际贸易数据、战略储备数据等。

2.农产品。包括国际合作数据、国际贸易数据、战略储备数据等。

(二) 自然资源和环境类

3.地理信息。包括基础地理信息数据， 可细分为定位基础数据、地名地址数据、地形地貌数据、其他基础地理信息数据； 遥感影像数据，可细分为原始影像数据、影像产品数据和其他遥感影像数据等； 专题地理信息数据，可细分为自然资源、生态环境等领域的专题地理信息。

4.气象。包括气象监测数据、空间大气监测数据、气象保障数据、区域气象数据、雷达基数据、气象台站元数据等。

5.海洋。包括海洋环境数据、海洋资源数据。

6.环保。包括反映污染物排放水平的自行监测、接受行政处罚或其他污染物排放等数据。

7.水利。包括水利业务数据、水利工程建筑信息模型等水利基础数据， 水旱灾害灾情综合分析评价等数据。

(三)工业类

8.钢铁、有色金属。包括储量、产量、采购量等数据，国际合作数据、国际贸易数据等。

9.稀土。包括储量与开采数据、行业使用数据、出口数据等。

10.其他矿产。包括储量数据、国际合作数据、国际贸易谈判数据、与矿产有关的产业发展布局情况。

11.化学工业。包括生产作业场所和运输信息、生产销售信息、制作方法信息，民用爆炸物品行业相关数据信息。

12.电力。包括发电厂生产数据、输配电数据、建设运维数据。

13.电子信息。包括基础电子信息产品(关键芯片、操作系统、大型软件等)参数，源代码、集成电路布图等数据， 产品测试数据，产品面向国防军工、政务等领域销售和服务情况。

14.民用核设施。包括民用核设施科研中的试验或测试数据，核设施相关设计和制造工艺信息，核设施运行监控数据。

15.工业装备。包括工业装备研发、应用、生产、销售、运维、管理数据。

16.智能汽车。包括智能汽车运行过程中获取的地理信息、人员流量、车辆流量等数据，智能汽车用户用车数据。

17.其他。包括工业互联网的网络、平台、安全保障相关数据，工业控制系统的参数、控制、运行维护、测试数据。

(四)国防科技工业类

18.国防科技工业类。包括经营管理、研发设计、生产制造、试验验证、维修保障等数据。

(五)电信类

19.电信。包括网络规划运维数据、安全保障数据、经济运行和业务发展数

据、关键技术成果数据、用户注册信息等。

(六)广电视听传媒类

20.广播电视。包括广电网络规划建设类数据，广电安全播出运维、应急保障、调度指挥等信息，广电监测监管系统数据，用户注册信息等。

21.新媒体。包括未公开或限制公开媒体资源类文件，用户数字画像、推送地址等数据。

(七)金融类

22.银行。包括银行客户数据、业务数据、经营管理数据、系统运行和安全管理数据等。

23.保险。包括保险机构客户数据、业务数据、经营管理数据、系统运行和安全管理数据等。

24.证券期货。包括投资者类数据、技术类数据、业务类数据等。

25.融资租赁。包括客户数据、企业交易数据、经营管理数据等。

(八)交通运输类

26.交通。包括铁路交通、公路交通、道路运输、城市交通、水路交通、民用航空、邮政管理、综合管理等数据。

(九)卫生健康和食品药品类

27.遗传资源。包括自然人基因数据、人类遗传资源信息等与种族、群体健康相关的数据。

28.健康医疗。包括医疗服务、电子病历、电子健康档案、医学研究等各类数据，健康数据、医疗救援保障数据、特定药品实验数据等， 或对患者健康医疗数据的开发利用结果。

29.食品。包括食品安全溯源标识数据，食品生产中自动控制系统的参数和控制类数据。

30.药品。包括药品供应、药品审批过程中提交的实验数据，以及与药品生产流程、生产设施有关的试验数据。

31.生物安全。包括病毒研究或生物实验室相关数据。

32.疾控数据。包括突发公共卫生事件及与传染病相关的疫情、治疗、疫苗、死因等数据。

(十)公共安全类

33.物理安全。包括建筑基础数据、安保装备数据等。

34.网络安全。包括自贸试验区企业信息系统设计运行数据、网络设施拓扑架构数据、安全保障数据等。

(十一)互联网服务和电子商务类

35.服务外包。包括境外客户委托境内企业提供服务过程中收集、产生的数据或与重要服务客户有关的数据。开展数字贸易、跨境电商业务中收集、产生的数据或与重要服务客户有关的数据。

36.互联网平台服务。包括提供互联网服务过程中产生的各类数据。

(十二)科学技术类

37.属于出口管制法管制的相关数据。包括列入国家出口管制清单的相关物项数据。

38.知识产权和重大发现。包括涉及国防、国家安全或其他非公开的知识产权，其他能显著提升国家安全能力或直接影响国家安全的科研论文、观测数据、产业化成果等。

(十三)其他数据类

39.禁止出口限制出口技术。包括列入《中国禁止出口限制出口技术目录》所列技术有关的数据。

40.其他可能影响国家政治、国土、军事、经济、文化、社会、科技、网络、生态、资源、核、海外利益、太空、极地、深海、生物等安全的数据。

三层分类由数据处理者自行决定。

七、数据分级机制

数据分级旨在对数据要素进行全面梳理并确立适当级别。数据分级通过定量与定性结合方式开展，是数据安全管理和依法有序流动的基础工作。

天津自贸试验区企业数据从高到低分为核心数据、重要数据、 一般数据 3 个级别。经综合判定， 数据要素符合核心数据定义时，优先识别为核心数据；不符合核心数据定义时，优先识别为重要数据；依次判定不符合核心数据和重要数据定义时，识别为一般数据。

重要数据判定参照相关法律、法规和规定， 结合本标准规范开展。如果行业

主管部门已公开发布或已在行业内部发布本行业本领域数据分类分级标准规范，优先按照行业规范识别重要数据，行业主管部门未明确判定标准时，按照以下标准识别重要数据：

(一)统一识别规则

1.天津自贸试验区企业掌握的 1000 万人以上个人信息；100 万人以上个人敏感信息；10 万人以上且包含个人银行账户、个人保险账户、个人注册账户、个人诊疗数据等的个人敏感信息。

2.被国家认定为关键信息基础设施的运营者掌握的个人信息。

3.天津自贸试验区企业在研发设计过程、生产制造过程、经营管理过程中收集和产生的与行业竞争力、行业生产安全相关的高价值敏感数据。涉及国家安全的企业供应链相关数据。

4.天津自贸试验区企业掌握的关系国计民生领域的自动控制系统参数以及控制、运行维护、测试数据。

(二)战略物资和大宗商品类

石油、石化、天然气领域可能推算出涉及国家重大战略的重要领域运行状况、发展态势、增长速度等的产品产量数据、国际贸易数据等。粮食、棉花、食用植物油、食糖、肉类、乳制品等大宗农产品国际合作数据、国际贸易数据、战略储备数据，达到一定精度或未公开农产品地理信息数据。

(三)自然资源和环境类

达到国家规定的覆盖度、精度和尺度等， 或表现敏感区域和目标的基础地理信息数据和遥感影像数据。服务军事、国防科研、高科技领域的各类气象监测数据。不宜公开发布的具有军事价值的海洋环境监测数据、灾害防御数据等。

(四)工业类

1.具有重要军用、民用价值的有色金属储量、产量、采购量等数据， 国家钢铁、有色金属战略储备数据或战略性有色金属矿床的重要地质数据， 富含重要伴生矿资源的矿区数据。我国独特掌握的稀土开采、冶炼等生产技术数据。大宗原材料信息，以及能够左右原材料采购定价权的数据。

2.天津自贸试验区企业掌握的重点危险化学品检测监控、关键工艺、设备运行、产量储量等数据。民用核设施领域科研试验数据，运行监控数据(核事故应

急准备和响应所需数据除外)等。

3.电子信息行业先进技术、集成电路先进设计和制造技术、重大计算装备设计数据、算法和软硬件架构以及重要电子元器件设备国产化率等信息。智能汽车领域汽车 OTA 参数。规上工业企业使用的工业互联网或工业控制系统安全运行保障数据。

(五)国防科技工业类

与国家军事、经济、科技、网络安全相关的数据， 综合反映国防科技工业重要企事业单位科研与生产能力的数据，汇总后能反映国防科技工业整体情况的数据，国防科技工业领域相关特色重要数据。

(六)电信类

基础电信骨干网络、应急通信部署类数据。

(七)广电视听传媒类

天津自贸试验区企业掌握的广电网络的规划建设、运行维护、关键资源(如 IP 地址、接入网资源等)以及被滥用可能导致意识形态安全、公共安全的新媒体数据。

(八)金融类

银行、保险、证券期货及融资租赁领域的机构安保信息， 以及其处理的重要企事业单位业务数据，包括国防军工企业、关系国家安全企业的相关信息。

(九)交通运输类

铁路交通、公路交通、道路运输、城市交通、水路交通、民用航空、邮政管理等领域影响生产安全的控制类数据、施工建设过程中获取的自然资源类数据、未公开的线路图、关键站点等数据， 以及被泄露、篡改可能造成重大交通事故的数据。

(十)卫生健康和食品药品类

反映种族整体情况或关系生物安全的遗传资源数据，关系国家安全、生命安全、人类自身安全的食品、药品、生物安全和疾控数据。

(十一)公共安全类

给社会稳定造成严重危害的重要目标基础数据、安保装备数据、敏感场所安保部署数据；关键信息基础设施或重要网络规划、安全运行数据。

(十二)互联网服务和电子商务类

在提供互联网服务过程中产生的可用来实施社会动员的数据，相关退伍人员等敏感人群数字画像数据，对军工、政府类客户记录和跟踪的数据。

(十三)科学技术类

与国家安全和利益、履行防扩散等国际义务相关属于出口管制法管制的数据。涉及国防、国家安全的知识产权数据。

(十四)其他数据类

其他可能影响国家政治、国土、军事、经济、文化、社会、科技、网络、生态、资源、核、海外利益、太空、极地、深海、生物等安全， 符合重要数据定义的数据。

核心数据的确定，由国家有关部门在重要数据目录的基础上认定并书面通知企业和有关部门。

八、数据分类分级程序

(一)企业开展数据分类分级。企业根据本规范开展内部数据分类分级工作，形成企业数据目录，明确本企业重要数据，并向天津自贸试验区网络数据安全工作主管部门报送重要数据目录。

(二)汇总形成重要数据目录汇总表。天津自贸试验区网络数据安全工作主管部门梳理汇总企业报送的重要数据目录，形成天津自贸试验区重要数据目录汇总表，并报送天津市数据安全工作协调机制。

(三)审核确认重要数据。由天津市数据安全工作协调机制对天津自贸试验区重要数据目录汇总表进行确认，形成天津自贸试验区企业重要数据目录，并按程序报送国家数据安全工作协调机制办公室。相关认定结果及时反馈企业作为开展数据安全保护和跨境流动等工作的基础。

(四)数据分类分级变更。当企业因应用场景、业务调整导致数据发生较大变化时，要及时调整数据目录，涉及重要数据变化的，按程序重新报送重要数据目录。对于企业未报备，但经有关主管、监管部门评估达到核心数据、重要数据的，及时将相关数据纳入目录，并通知涉及企业加强数据安全保护。

(五)定期检查评估。天津自贸试验区网络数据安全工作主管部门定期评估本规范的有效性和应用情况，并根据实际需要适时调整修订本规范。

关于印发《中国(天津)自由贸易试验区数据出境管理清单(负面清单)(2024版)》的通知

津自贸发〔2024〕3 号

各有关单位：

为推动自贸试验区企业数据跨境流动更加便利，依据《促进和规范数据跨境流动规定》等有关文件规定， 中国(天津)自由贸易试验区管理委员会、天津市商务局会同有关部门制定了《中国(天津)自由贸易试验区数据出境管理清单(负面清单)(2024 版)》，现正式印发，请遵照执行。

中国(天津)自由贸易试验区管理委员

天津市商务局

2024 年 5 月 8 日

中国(天津)自由贸易试验区数据出境管理清单(负面清单)(2024 年版)

为促进中国(天津)自由贸易试验区(以下简称“天津自贸试验区”)企业数据依法有序跨境流动，推进高水平对外开放，更好服务加快构建新发展格局，制定《中国(天津)自由贸易试验区数据出境管理清单(负面清单)(2024 年版)》(以下简称《负面清单》)。

一、目的意义

落实《中华人民共和国网络安全法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》和《数据出境安全评估办法》《个人信息出境标准合同办法》《促进和规范数据跨境流动规定》等法律规章，对接国际高标准经贸规则，探索数字领域制度型开放，通过构建数据跨境流动管理新模式，为企业数据依法有序高效出境提供便利，有效提升营商环境和企业国际竞争力。

二、基本原则

1.坚持统筹兼顾。统筹发展和安全， 坚守国家数据安全底线，在保障重要数据安全和维护个人信息权益的基础上，促进数据资源有序流动和开发利用，推动数字经济和数字贸易高质量发展。

2.坚持便捷合规。发挥天津自贸试验区先行先试政策优势， 研究建立依法有序的数据跨境流动管理模式，探索形成数据跨境流动的便利化管理机制。

3.坚持简明实用。按照数据出境安全评估、个人信息出境标准合同、个人信息保护认证等国家数据出境管理制度要求，结合天津自贸试验区企业、机构数据出境的实际需求，制定可操作、可落地的《负面清单》，便于企业掌握和执行。

4.坚持动态调整。根据国家数据安全形势和天津自贸试验区企业主体、数据出境场景等变化，动态调整《负面清单》内容，实现保障安全与促进发展相统一。

三、适用范围

《负面清单》列明了天津自贸试验区企业向境外提供数据需要申报数据出境安全评估、订立个人信息出境标准合同、通过个人信息保护认证的情形。天津自贸试验区企业向境外提供《负面清单》外的数据免予申报数据出境安全评估、订立个人信息出境标准合同、通过个人信息保护认证。涉及国家秘密的数据、核心数据、政务数据不纳入《负面清单》管理， 相关数据出境按照有关法律、法规和规定执行。

《负面清单》在使用过程中出现的新情况、新问题，由市网信办、市商务局、市数据局、天津自贸试验区管委会会同有关部门协商沟通， 共同研究制定对策措施，并做好解释说明。国家行业主管部门相关政策规定发生变化，《负面清单》内容与其不一致的，从其规定。

四、主要考虑因素

1.落实数据分类分级管理要求。严格遵循法律法规和国家行业主管部门数据分类分级要求，国家行业主管部门或本市认定的重要数据纳入本清单管理，遵守国家相关数据出境管理要求。

2.加强个人信息保护。围绕保护个人信息权益、规范个人信息处理活动、促进个人信息合理利用，将不同规模、不同类型个人信息出境纳入《负面清单》管理。

3.服务企业高质量发展。根据企业国际贸易、对外交流的数据出境需要， 明确了出境数据管理的类别、基本特征与描述等内容， 降低企业、机构数据出境合规成本，提升竞争力。

4.规范数据出境行为。加强天津自贸试验区数据出境安全风险监测能力建设，从机构队伍、技术手段等方面提升数据出境事中事后监管能力， 及时发现处置违法违规数据出境行为。加强对天津自贸试验区数据出境政策制度标准的宣传解读，

提升企业合规意识。

本清单将根据相关法律法规和本市实际需要进行适时修订。

附件：中国(天津)自由贸易试验区数据出境管理清单(负面清单)(2024 年版).pdf

关于印发《广东省企业首席数据官建设指南》的通知

粤工信数字产业函〔2022〕32 号

各地级以上市人民政府，省有关单位：

为建设数据管理高端人才队伍，充分挖掘数据资源价值，促进企业数字化转型，推动我省数字经济高质量发展，经省人民政府同意，现将《广东省企业首席数据官建设指南》印发给你们， 请各地、各有关单位认真组织实施， 执行中遇到的问题，请及时向我厅反映。

广东省工业和信息化厅

2022 年 8 月 24 日

广东省企业首席数据官建设指南

党的十八大以来，党中央高度重视发展数字经济，作出了一系列重大决策部署。数据作为数字经济的关键生产要素和基础资源， 蕴藏着巨大价值，数据的深度挖掘应用将促进资源优化配置、提高全要素生产率，是重塑企业竞争优势、推动经济社会转型发展的重要引擎，对于提升数字经济发展水平意义重大。

企业拥有丰富的数据资源，是培育发展数据要素市场的重要力量。企业首席数据官(Chief Data Officer，以下简称“CDO”)是源于数字化转型需要而产生的一个新型管理者。企业设立 CDO，有利于加强数据管理，推进数据资产化和数据驱动决策，有利于完善数据标准制度，推动数据价值深度挖掘和应用，有利于推进数据资源市场化配置，建立健全数据要素市场体制机制。

广东省数据资源富集、产业基础雄厚、融合应用场景丰富， 目前部分企业已设立 CDO，开展数据管理能力成熟度评估模型(DCMM)贯标评估，实现数据管理体系革新、生产模式优化、运行效率提升。为加快培育数据要素市场体系， 建设数据管理高端人才队伍，充分挖掘数据资源市场价值，促进企业数字化转型，在全省建立企业 CDO 工作机制，推动企业设立 CDO，助力广东数字经济高质量发展。

一、建设原则

鼓励数字化基础较好、拥有较大规模数据资源、数据产品和服务能力较突出的各行业企业设立 CDO，按照企业主导、政府推动、价值优先、多方协同的原则，参考本建设指南组织实施。

(一)企业主导。充分发挥市场在资源配置中的决定性作用，强化企业在数据要素市场上的主体地位，支持企业自主设立职位并遴选聘任 CDO，充分发挥 CDO 在数据资产管理、数据人才、数据文化、数据安全等方面的领导作用。

(二)政府推动。省市工业和信息化主管部门鼓励各种类型企业设立CDO，组织 CDO 培训交流平台，宣传推广企业优秀案例，帮助CDO 提升业务水平和工作能力。鼓励各地人才管理部门将企业 CDO 列入产业人才政策范围。

(三)价值优先。鼓励企业 CDO 充分发现挖掘企业内外部数据价值，推动数据资源开发利用和数据资产化运营，培育数据创新生态，促进数据资源交易流通，释放数据要素活力，完善数据要素市场体制机制。

(四)多方协同。省市工业和信息化主管部门、省级相关部门、企业、 社会组织加强企业 CDO 宣传引导，推动社会和企业认识企业 CDO 在数据要素市场培育和数字化转型过程中的作用和意义，营造有利于企业 CDO 发挥才能的良好工作环境。

二、建设内容

企业 CDO 是有效管理和运用企业数据资产、充分挖掘数据价值、驱动业务创新和业务转型变革的企业负责人。企业 CDO 需具备宽广视野和战略眼光，要熟悉企业的各项业务流程，具有业务数据价值洞察力，要及时掌握各类数字化技术发展动态，能够围绕企业信息系统产生的大规模数据资源进行数字化运营，通过数据支撑引领业务创新和商业模式创新，提升内外部客户的满意度和应用体验，帮助企业降本增效创新增长。

(一)岗位设置

企业 CDO 应设置在企业决策层，是企业对数据资产的使用管理和安全全面负责的高层管理人员，由企业自主聘任并授权其开展工作。企业应当按照公开、公平、公正、择优的原则，参照副职负责人的选聘任用程序设置 CDO，直接向企业负责人汇报。企业应当对照 CDO 的职责要求，为 CDO 提供组织机构、岗位职务、人员编制、资金保障等各种必要条件。企业应当以制度形式赋予 CDO 对企业重大

事务的知情权、参与权和决策权。

鼓励大型企业以业务驱动设立数据资产管理委员会和数据资产管理部门。数据资产管理委员会由企业负责人、CDO、部门负责人等中高层管理人员组成，负责确立数据资产管理的目标、资源和重大事项的协调和决策， 指导审批数据资产管理工作规划和年度目标，审定数据资产管理相关的政策、组织建设、管理流程。数据资产管理部门负责数据资产工作的战略规划、目标举措以及实施落地，负责数据资产从产生、消费到消亡全生命周期管理的治理框架、流程规范、方法和 IT 工具的制定与推行，推动数据资产管理项目和以数据为核心的数字化转型，设计数据资产质量度量模型、执行数据资产质量监控及重大数据问题披露，统筹建设完善数据安全保障体系，负责企业数据资产管理能力提升和数据文化建立传播。

(二) 岗位能力素质要求

1.数据资产管理领导能力。CDO 需具有良好的职业道德和敬业精神，熟悉并遵守国家数据领域相关法律法规和标准，具有正确的数据价值观，依法依规组织实施企业内外部数据的收集、存储、使用、加工、传输、提供、公开等处理活动。

2.数据规划和执行能力。精通数据收集、管理、分析等方面的业务理论和技术，具备对数据资产管理运用工作进行全局战略规划和布局、配置企业内外部数据资源、制定发展目标和工作计划的战略思维与规划执行能力。

3.数据价值行业洞察能力。熟悉企业的业务流程与工艺流程以及行业发展情况，能够洞察所在行业和企业的数据资产价值，具备判断分析数据及数字技术带来机遇和风险的能力。

4.数据资产运营和增值能力。具备管理和推动大规模、跨职能、多层级的项目管理整合能力，带领和指挥团队成员围绕数据战略规划开展工作，充分挖掘企业内部数据资源优势，整合外部数据资源，提供具有经济价值和社会价值的数据，熟悉数据交易情况，以数据赋能推动企业生产经营和投资决策创新发展。

5.数据基础平台自研建设能力。带领团队完成数据存储监控、数据处理任务调度、数据指标监控等关键大数据基础平台能力建设， 能有效避开海外开源大数据平台框架技术屏蔽、卡脖子，为数据增值和数据价值洞察提供良好的基础保证。

(三)岗位职责

1.数据治理。建立数据治理的组织架构和专门团队，健全业务驱动数据治理

的体制机制，改善数据资产管理体系架构和管理方法，加强统一数据治理平台建设，攻克多渠道数据来源统一管控的难关，规范数据处理的流程和标准，推进实施《数据管理能力成熟度评估模型》(DCMM)等国际国内标准、团体标准、企业标准，推动数据治理平台的规划、设计、建设及运营，保障数据资产质量和提升企业数据资产管理水平，优化企业业务运营模式。

2.数据增富。关注数据资产的战略价值和应用场景，组织制订和实施企业数据战略，获取数据中内涵的价值，建立数据驱动生产经营管理的体制机制，打破数据壁垒，使数据可以便捷地跨部门及跨职能流通，推动数据在企业内更好的消费和利用，通过数据分析主动支持业务，优化现有业务，挖掘潜在客户和市场需求，调整产品结构、提升产品和服务质量水平、创新商业模式， 为企业创造新的商业利润。

3.数字增值。适应数据市场的需要，按相关法律法规要求，组织推进企业数据资产的数据清洗、数据变换、数据集成、数据脱敏、数据规约、数据标注等数据处理，推动上下游、跨行业的数据共享开发利用， 推动数据资产评估，探索形成数据产品，采用合法交易方式，为市场提供企业数据服务，实现数据资产的市场价值。

4.数据安全。贯彻执行国家数据等方面的法律、法规和政策， 建立企业数据资产安全保障制度和分类分级安全管理制度，组织制定并实施企业数据安全防护方案，提升数据全生命周期安全防护能力。定期组织数据安全评估， 组织基于供应链的数据安全监测，提高企业数据风险管控能力，确保企业数据隐私与安全。

5.数据人才。加强企业数据管理人才队伍建设，组织开展培训教育，培育企业 CDO 后备人才、数字化管理师等人才团队，打造高素质的人才梯队。

6.数据文化。加强企业数据文化建设，提升企业员工数据资产意识，建立正确的企业数据价值观，增强企业的数据安全意识。引入互联网数据思维，围绕“大中台+小前台”数据战略推进传统企业数据落地和应用，形成员工新型工作思维和工作方式。

三、保障措施

(一)加强组织引导。省工业和信息化厅将企业 CDO 建设作为各地数字经济发展情况评估的重要内容，鼓励地市将企业 CDO 建设作为制定数字经济领域相关扶

持政策的重要参考。省市工业和信息化主管部门建立常态化 CDO 工作沟通机制，加强跟踪服务指导，为 CDO 高效履职提供强有力工作保障。完善企业与业务主管部门的沟通机制，了解各行业企业的数据现状与需求，探索企业数据与公共数据资源综合利用场景及模式，推进政企数据资源融合增值。

(二)建立人才资源库。省工业和信息化厅组织建立全省企业 CDO 人才资源库，鼓励支持企业 CDO 积极主动加入，形成 CDO 人才资源汇聚、交流、合作、提升的重要平台，实现 CDO 与市场的高效对接和合理配置，探索支持企业 CDO 人才的政策。

(三)强化企业培训。省市工业和信息化主管部门建立健全企业 CDO 培训机制，组织实施企业 CDO 交流培训，开展相关研讨活动，组织有经验的专家为设立 CDO 的企业提供政策宣讲、咨询答疑等贴心服务， 帮助企业 CDO 提升业务水平和工作能力。

(四)开展示范建设。省工业和信息化厅支持广州、深圳、珠海、佛山、惠州、东莞、中山及其他有意愿且数字化基础条件较好的地市工业和信息化局组织开展企业市级 CDO 示范建设工作，指导各地制定完善工作程序和建设标准，2022 年至 2024 年每年培养一批既懂数字技术又懂生产经营的 CDO，适时开展省级企业 CDO 示范建设工作。

(五)形成优秀案例推广。省工业和信息化厅指导有关地市工业和信息化局依托企业 CDO 组织开展企业 CDO 优秀案例建设工作。围绕数据开发利用、数据管理、数据文化、数据安全等领域，省工业和信息化厅定期归纳总结出一批作用突出、成效显著、可复制推广的 CDO 优秀案例，树立先进标杆宣传典型经验，省市联合进行宣传推广。

(六)加强社会多方协同引导。充分发挥新闻媒体的作用，大力宣传企业 CDO 的目的、作用、成效和典型事例， 营造 CDO 建设的良好氛围。发挥 CIO、大数据领域社会组织作用，依法依规开展 CDO 交流、互动、培训等活动，提高各行业、各领域数据管理水平。

关于印发《广州市国资委监管企业数据安全合规管理指南(试行 2021 年版)》的通知

穗国资法〔2021〕13 号

各监管企业，各受托监管部门：

为加快推动监管企业全面加强合规管理，有效提升监管企业全面加强数据安全合规管理，规范监管企业数据处理活动，保障企业数据安全，促进企业健康发展，保护个人、组织的合法权益，维护国家经济安全和社会稳定，我委制定了《广州市国资委监管企业数据安全合规管理指南(试行 2021 年版)》，现印发给你们，请结合实际，认真遵照执行。工作中的问题和建议请及时反馈。

特此通知。

广州市人民政府国有资产监督管理委员会

2021 年 12 月 20 日

广州市国资委监管企业数据安全合规管理指南

(试行 2021 年版)

第一章 总 则

第一条 为推动广州市国资委监管企业全面加强数据安全合规管理，规范监管企业数据处理活动，保障企业数据安全，促进企业健康发展，保护个人、组织的合法权益，维护国家经济安全和社会稳定，提升监管企业数据治理能力及数据安全保护水平，根据《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》《中华人民共和国网络安全法》《关键信息基础设施保护条例》《广州市市属企业合规管理指引(试行)》等有关法律法规规定，制定本指南。

第二条 本指南适用于广州市人民政府国有资产监督管理委员会(以下简称“市国资委”)直接履行出资人职责的国有及国有控股企业、国有实际控制企业(以下称“监管企业”)。

第三条 市国资委负责监督指导监管企业数据安全合规管理工作。

第四条 监管企业应当对本企业工作中收集和产生的数据和数据安全承担主体责任。

数据安全合规管理是合规管理体系的专项重点领域，已建立合规管理体系的监管企业，应在现有合规管理体系的基础上，进行专项深化管理。

数据安全风险较高的监管企业，必须将数据安全合规作为重点领域进行专项管理。达到以下条件之一的，视为数据安全风险较高：

(一)主要业务涉及公共通信和信息服务、能源、交通、水利、金融、公共服

务、电子政务等重要行业和重要领域的；

(二)主要业务涉及个人信息处理，且从业人员规模大于 200 人；

(三)处理超过 100 万人的个人信息，或预计在 12 个月内处理超过 100 万人的个人信息；

(四)处理超过 10 万人的个人敏感信息的；

(五)从事国家秘密载体制作、复制、维修、销毁，涉密信息系统集成或者武器装备科研生产等涉及国家秘密的业务的；

(六)法律法规规定的其他情形。

第五条 监管企业应当按照以下原则提升数据安全合规管理：

(一)高度重视。数据是重要的战略性资源， 监管企业要将数据安全合规管理提升到事关国家安全、经济安全、社会稳定和人民群众切实合法权益的高度， 始终把国家主权、安全、发展利益放在首位，加强安全能力建设，重视企业、员工、股东及合作方数据安全及个人信息保护，以发展促安全、以安全保发展。

(二)推进落实。监管企业要坚持将数据安全合规要求逐步覆盖各业务领域，各部门，各级全资、控股或实际控制的子企业、分支机构及其员工。数据应当全面包括电子或其他方式对信息的记录。数据安全合规管控措施及技术应用覆盖所有数据资产及数据处理全流程。

(三)强化责任。监管企业要切实加强对数据安全合规管理的组织领导， 明确职责，建立健全分工负责、协作配合的工作机制， 明确管理人员和各岗位员工的数据合规责任并督促有效落实。

(四)协同融合。监管企业认真贯彻落实数据安全合规的相关要求， 将数据安全合规工作纳入企业数字化转型整体布局中，将数据安全合规管理通过企业数字化技术的应用及升级进行有效落地。

第二章 管理职责

第六条 监管企业应将数据安全合规管理的职责纳入现有合规管理组织体系。通过建立专项制度或文件的形式，在原有合规管理组织体系合规职责范围内，进一步细化及明确各层级合规管理机构及相关部门的数据安全合规管理职责。

第七条 董事会合规委员会或承担合规管理职责的专业委员会应在职责范围内推动企业数据安全合规管理，以完善企业合规管理体系，合理配置数据安全合

规管理工作所需的相关资源和奖惩机制，审批重大数据安全合规事项，确保工作有效推行及落地。

第八条 经理层及合规管理负责人应在原有合规管理职责的范围内，指导及监督企业数据安全合规管理相关制度规范建设、相关管理措施的设计与执行、数据安全技术应用等，确保企业数据安全合规。

第九条 监管企业承担数据管理、信息系统管理或 IT 技术等部门和其它各职能部门分别作为各业务范围内数据安全合规管理的责任部门，作为数据安全合规管理的第一道防线，主要职责包括：

(一)制定企业数据管理的相关标准，包括数据分类分级、权限管理等工作；

(二)制定企业数据管理的相关制度及规范，包括数据全生命周期管理的相关制度；

(三)负责统一规范企业数据收集、存储、使用、加工、传输、提供、公开等工作机制；

(四)负责数据安全技术的应用及更新；

(五)负责数据管理能力建设；

(六)其他规章制度规定的数据管理工作。

第十条 监管企业各职能部门负责本领域的日常数据安全合规管理工作，规范数据收集、存储、使用、加工、传输、提供、公开等工作， 妥善应对数据安全合规风险事件，组织或配合进行违规问题调查并及时整改。

第十一条 监管企业合规管理牵头部门作为数据合规管理第二道防线，在数据安全合规管理方面的职责包括：

(一)参与对企业涉及数据安全事项的合规审查；

(二)对数据安全合规管理的情况进行评估与检查；

(三)组织或协助数据安全合规责任部门、人事部门开展数据安全合规培训，为公司其他部门提供数据安全合规咨询与支持；

(四)合规委员会或合规管理负责人交办的其他工作。

第十二条 监管企业可视情况通过建立联合的数据合规管理办公室或工作组，开展数据安全合规管理标准、制度及规范的建立工作，可由相关业务、信息系统、技术、合规、风险管理、内部审计等部门人员组成， 在经理层及合规管理负责人

的领导下，有效推动数据安全合规管理工作的开展及实施。

第十三条 内部审计部门负责定期对数据安全进行审计，可根据风险评估和审计资源铺排，在审计工作中涵盖数据安全合规的内容，并出具相关审计报告，为公司数据安全风险管理的有效性提供合理保障。

纪检监察部门负责职权范围内的违规事件的监督、执纪、问责等工作。

第三章 制度规范建设

第十四条 监管企业应建立健全数据安全合规管理的相关标准、制度和规范，建立重大数据安全合规审批清单、数据分类分级管理、权限管理、数据安全合规风险评估及审计、重大数据安全合规风险事件报告、应急处置机制、教育培训等管理事项，并根据法律法规变化和监管动态，及时将外部合规要求落实到内部规章制度。

第十五条 监管企业重大数据安全合规事项实施清单管理。由数据安全合规管理的责任部门牵头编制本企业重大数据安全合规事项清单，提交党委会审议通过后，由董事会合规委员会或承担合规管理职责的专业委员会负责审批清单涉及的重大数据合规事项。

数据安全合规管理的责任部门应根据法律法规及企业的实际运营情况的变化进行及时更新清单。

第十六条 监管企业应建立数据分类分级管控标准和管控要求。企业应优先根据所属行业相关标准对核心业务数据进行分类分级[详情可参考工业和信息化部《工业数据分类分级指南(试行)》，中国人民银行《金融数据安全数据安全分级指南》等。]，无明确标准的企业可自行建立相关分类及分级标准。其中数据分级标准应参考及遵循国家数据安全等相关法律法规。

关系国家安全、国民经济命脉、重要民生、重大公共利益等数据需要实施更加严格的管理制度，包括涉及国家保密范围的产业规划、战略规划、重大项目、核心技术等，应根据相关法律法规的具体要求进行重点保护和管理。上述相关数据的交易、出境及共享等业务， 应列入企业“三重一大”事项进行管理，不得向境外司法或执法机构提供存储于境内的数据。

监管企业应根据标准对现有数据进行全面分类分级，并通过技术手段落实安全管理要求，定期对新增数据进行梳理，确保所有数据分类及分级管控。同时，

应根据相关法律法规或行业标准的变化，及时更新企业内部数据分类分级的相关标准。

第十七条 监管企业应规范数据处理的权限管理，建立适当的用户权限管理机制，根据岗位设置相关账户权限，明确相关数据所涉及的账户管理流程，减少数据滥用情况，提高数据安全合规水平。

第十八条 数据安全风险较高的监管企业，应建立数据安全合规评估及审计机制，应自行或委托有相关信息安全检查评估资质的机构，每年至少进行一次全面的网络安全监测和风险评估，定期或不定期对企业整体数据使用情况、数据全生命周期安全及合规性、基础安全等情况进行评估及审计， 并对发现的问题及时整改。

第十九条 数据安全风险较高的监管企业，应建立数据安全应急响应机制，明确数据安全事故管理和应急响应职责，制定各类数据安全事故的处置流程及应急预案，并定期进行演练，对各类安全事件进行及时响应和处置，降低企业因数据安全事故而引发的损失。

第二十条 数据安全风险较高的监管企业，应建立重大数据安全合规风险事件报告制度，对影响或可能影响国家安全的数据处理活动，发现数据安全威胁时，应按规定向公安机关、国家安全机关报告， 可能关系到重大经营风险的应同步及时向市国资委报告，并积极采取措施防止危害，减少损失。

第二十一条 监管企业应积极配合公安机关、国家安全机关依法维护国家安全或者侦查犯罪需要及时配合提供相关数据。

第二十二条 监管企业应建立有效的管控模式，对其下属全资、控股和实际控制子企业在数据安全合规工作内容和职责分工，可根据实际情况，分批推进各单位数据安全合规管理工作，并结合集团合规管理管控模式进行差异化管理。

第二十三条 监管企业应全面评估企业本部及下属各级全资、控股和实际控制子企业的数据安全风险。针对数据安全风险较高的企业应尽快开展数据安全合规管理相关工作，建立数据安全合规的相关标准、制度及规范。监管企业可根据相关子企业的工作成果及经验，逐步在其他子企业进行推广及实施。

第二十四条 数据安全风险较高的监管企业，可基于企业的原有的战略规划、IT 规划等制定本企业的数据安全三年滚动工作规划，确保监管企业按照既定路

线达成数据安全合规目标，并在执行过程中，根据数据安全合规和企业 IT 战略目标下不断优化、提升数据安全合规管理的各项制度和信息系统。

第四章 数据安全合规管理措施

第二十五条 监管企业在数据安全合规管理过程中，应对数据采集、数据传输、数据储存、数据使用、数据开放共享、数据销毁等数据全生命周期管理的要素，制定必要的管控措施及标准，依法保护企业数据基础设施免受攻击、侵入、干扰和破坏，防范数据处理的违规风险，确保数据安全合规。

第二十六条 规范数据采集的管理，明确数据采集渠道，确定数据格式标准，制定各类数据采集流程及方式，定期开展数据采集合规性审查，确保数据采集合法合规。

第二十七条 加强数据传输安全管理，划分企业网络系统安全域，区分域内、域间等不同数据传输场景，明确数据传输安全策略和操作规程。

第二十八条 监管企业应梳理数据出境情况的业务，建立企业内部数据出境合规审查的流程及规范，针对境外并购、赴境外上市等情况， 应充分评估数据出境的相关风险，按相关规定进行内部审核审批，并根据法律法规要求，履行监管机构数据出境的审查申报。非经相关部门批准， 不得向外国司法或执法机构提供存储与中华人民共和国境内的数据

监管企业境外分支机构在当地设立服务器，并通过该服务器储存及使用监管企业数据的，应按数据出境的管理要求实施数据安全管理。境外分支机构通过远程访问使用数据的，应加强访问权限控制及数据传输安全管理，确保数据安全。

第二十九条 规范并加强数据储存的管理，加强对数据储存介质的管理，包括提升对服务器及离线储存介质的物理安全及加密管理，规范带数据储存功能的可移动设备的管控，加强对本地数据储存系统平台接入移动储存介质的管控，实施对储存在第三方云平台数据的风险评估，对数据下载到本地终端行为进行审核及日志记录等管控措施，提升数据储存的安全性。

第三十条 规范数据使用的管理，根据不同类别、级别的数据，明确不同场景的数据使用审批流程，制定数据脱敏处理规则，提升数据使用的安全性；建立数据开发利用的相关流程及规范，完善数据开发利用的风险评估机制。

具有数据交易相关业务的监管企业，应按国家相关法律法规的相关要求进行

交易，法律法规尚未规定的，应进行充分的风险评估，确保数据安全。

第三十一条 加强数据开放及共享的管理，根据数据使用目的、共享对象，明确数据可进行开放及共享的范围，建立数据共享的申请及授权审批的流程及权限设置，明确数据共享过程的传输方式。

第三十二条 针对企业向外部单位共享数据的情况，监管企业应充分评估相关数据安全风险，涉及重大敏感的数据提供要按审批权限逐级审批。并在相关合同中明确数据安全及保密义务，明确相关违约责任，必要时可单独签订保密协议。相关事项结束后，应进行内部总结汇报，对数据共享情况进行说明，加强数据共享的管理。监管企业应尽量依托国资国企信息安全“云”监管平台，积极支持配合国资国企一体化网络安全信息大数据平台的建立，促进数据安全信息联动和能力共享。

第三十三条 建立员工数据安全合规行为规范，针对员工日常工作中数据储存、数据处理、数据传输、数据共享等事项明确相关合规管理要求。

第三十四条 规范数据销毁的过程管理，建立数据销毁的申请审批机制及流程，规范数据销毁过程的监督及记录，明确存储介质销毁策略及操作规范，委托第三方进行数据销毁的，应委托具有相关资质的单位，确保数据销毁的安全可靠。

第五章 与商业伙伴合作中的数据保护

第三十五条 监管企业应加强及规范与商业伙伴合作中的数据安全管理，明确合作方准入、日常管理、数据安全评估、变更及退出等环节的合规管理要求。

第三十六条 监管企业应明确信息系统开发及运维、数据储存、数据处理等数据服务相关合作方的准入标准，并在合作方选择时进行资格审查。同等条件下应优先采购境内安全可信的网络产品和数据服务。必要时， 应对数据服务的合作方进行数据安全合规方面的尽职调查。

第三十七条 对于合作方能接触到企业非公开数据的合作项目，监管企业应加强合同管理，通过制定相应的示范文本在相关合同中明确数据安全合规相关条款。

对于为企业提供数据服务的合作方，企业应结合实际情况将服务标准、数据备份和恢复、数据泄露预防、业务连续性计划等内容在合同中进行明确。

涉及委托处理个人信息的合作方，企业应结合实际情况将委托处理的目的、

期限、处理方式、个人信息种类、保护措施以及双方的权利和义务等内容在合同中进行明确，并对合作方的个人信息处理活动进行监督。

第三十八条 监管企业应明确与合作方对接部门的数据安全管理责任。涉及公司资料及数据分享的，应按实现合作目的最小数据获取原则，对部分非必要数据进行脱敏，并对数据分享过程进行记录。

涉及合作方提供驻场服务，链接企业信息系统，或直接接触重要数据的，相关项目负责人应采取适当措施对其合作方的工作进行管控，确保数据安全。

第三十九条 监管企业应建立数据服务合作方定期的数据安全监测、检测和评估机制，明确数据安全监测、检测和评估的范围及具体内容， 并将相关评估结果与合作方的变更及退出进行挂钩，发现合作方存在数据滥用、盗卖数据、预留“后门”等违法违规行为的，应及时终止合作并永久禁止合作，并按合同约定进行索赔。确保合作方数据安全合规。

第六章 个人信息保护

第四十条 监管企业应进一步规范及完善个人信息保护机制，加强企业员工、访客个人信息的保护。

监管企业应梳理集团本部及下属各级全资、控股或实际控制子企业涉及大规模处理个人信息的业务，加强及完善相关部门及企业个人信息保护的管理，针对个人信息分类、个人信息获取、个人信息储存、个人信息使用及处理等管理过程中，按法律法规建立相关标准及规范，并满足下述相关管理要求。

第四十一条 建立企业内部个人信息分类标准，明确个人敏感信息定义范围及处理规则，明确处理不满十四周岁未成年人个人信息处理规则。个人敏感信息及未成年人个人信息处理规则应遵循法律法规的相关规定。

第四十二条 个人信息的收集应满足法定的相关原则，不得过度收集个人信息，确保个人信息采集及处理前取得个人同意。优化取得个人同意的方式， 确保由个人在充分知情的前提下自愿、明确作出同意。针对法定要求需取得个人单独同意的情形，确保取得个人的单独同意。并且当个人信息的处理目的、处理方式和处理的个人信息种类发生变更时，可以及时有效重新取得个人同意，同时能够为个人提供便捷的撤回同意的方式。

第四十三条 建立个人信息储存的相关规范，明确个人信息的保存期限，结

合个人信息删除的相关机制，确保信息保存期限为实现处理目的所必要的最短时间。同时完善相关技术应用， 采取使用加密及去标识化等安全技术措施，确保个人信息的储存安全。

第四十四条 梳理内部进行个人信息处理的各类场景，对于向他人提供企业处理的个人信息，利用个人信息进行自动化决策，在公共场所安装图像采集、个人身份识别设备、针对法定要求需取得个人单独同意的情形， 等情形，应依据相关法律法规的要求，明确处理流程并制定规范要求。

第四十五条 建立完善的个人信息处理规则，确保在处理个人信息前，按照相关法律法规的要求， 向个人告知个人信息处理者的名称或者姓名和联系方式，个人信息的处理目的、处理方式， 处理的个人信息种类、保存期限， 个人行使法定权利的方式和程序等内容，并建立便捷的个人行使权利的申请受理和处理机制。并且当上述内容有变更的，能够及时将变更部分告知个人。

建立个人信息处理事前影响评估机制，监管企业应结合实际情况根据法律法规要求梳理须进行事前个人信息保护影响评估的具体场景，制定评估的标准及规范，明确个人信息保护影响评估报告及处理情况记录保存的相关要求。

建立个人信息主动删除的相关机制，明确个人信息删除的流程及规范，确保当个人信息处理目的已实现、无法实现或者为实现处理目的不再必要， 企业停止提供产品或者服务，或者保存期限已届满，以及个人撤回同意时，相关个人信息得到及时删除。

第四十六条 属于相关主管部门认定为关键信息基础设施运营者的监管企业，应依法依规履行关键信息基础设施安全保护的责任义务。提供重要互联网平台服务、用户数量巨大、业务类型复杂的监管企业， 应对其个人数据信息处理活动负责，并应通过制定及优化内部管理，履行基础互联网平台的法定合规义务，包括建立独立的监督机构、制定平台个人信息保护规则及定期发布个人信息保护社会责任报告等相关事项。

第七章 数据安全技术应用

第四十七条 监管企业应通过相关技术的应用及更新，提升企业在数据识别、敏感信息保护、数据操作审计、接口安全管理、数据防泄露等方面的技术能力，提升数据安全保障能力。

第四十八条 监管企业可采用定期数据资产扫描，脱敏效果验证等技术，深入到具体业务场景，精准识别重要敏感数据、敏感人群、特权操作等， 持续提升企业数据识别能力，从数据检测能力维度保障企业数据能够按照既定的分类标准及规则进行处理，确保企业数据分类分级安全合规。

第四十九条 监管企业应通过加强个人信息去标识化、数据关键字段隐藏、扰乱等技术的应用，提升个人敏感信息保护能力，保障大规模个人数据在储存及传输过程中的安全。采用校验或加密技术保证重要数据在传输过程中的完整性和安全性，采用密码技术保证重要数据在存储过程中的保密性。

第五十条 监管企业应通过对涉及储存、处理个人敏感信息和企业重要数据系统平台的防泄漏技术的应用，提升数据防泄露的能力，防范数据泄露风险，确保数据安全。

第五十一条 监管企业可通过数据操作审计系统的部署应用，实现对企业重要敏感业务系统的数据操作实施监控及审计，防范操作性风险。

第五十二条 监管企业可通过建立面向互联网及合作方数据接口的安全认证机制及加强数据接口安全监控技术的应用，对数据出口进行集中化管理，提升接口安全管理的能力，防范数据传输合规风险。

第八章 责任与监督

第五十三条 市国资委对监管企业数据安全合规管理情况进行监督检查，发现数据处理活动存在较大安全风险的，可以按照规定的权限和程序对有关企业、个人进行约谈，并要求有关企业、个人采取措施进行整改，消除隐患。

第五十四条 监管企业在日常数据处理中，企业或员工违反法律、行政法规规定，窃取或者以其他非法方式获取数据，开展数据处理活动排除、限制竞争，或者损害个人、组织合法权益的， 除依法承担相应法律责任外，市国资委应视情况启动对相关企业的合规调查，责令相关企业整改，并监督其完善数据安全合规管理。

第五十五条 监管企业在日常数据处理中，企业或员工违反法律、行政法规规定，未履行数据安全保护义务、向境内外调查咨询和中介机构提供重要数据、拒不配合数据调取、未经主管机关批准向外国司法或者执法机构提供数据的， 依法承担相应法律责任。

属于关键信息基础设施运营者的监管企业违法违规向境外提供重要数据的，依法承担相应法律责任。

监管企业因违反相关法律法规受到责令整改、警告、罚款、责令暂停相关业务、停业整顿、吊销相关业务许可证或者吊销营业执照、追究刑事责任的， 市国资委应视情况对相关企业及主要负责人进行违规问责。

其中出现属于关键信息基础设施运营者的监管企业违法违规向境内外调查咨询和中介机构提供重要数据，或监管企业拒不配合数据调取、未经主管机关批准向外国司法或者执法机构提供数据的情形，市国资委应立即启动相应的违规问责，并监督相关企业实施整改。

第九章 附 则

第五十六条 监管企业应根据本指南，结合实际制定数据安全合规管理制度或在现有数据管理制度中增加数据安全合规的相关内容。

委托监管企业的数据安全合规管理工作，参照本指南操作。

第五十七条 本指南将结合相关领域立法更新情况变更和调整。

第五十八条 本指南由市国资委负责解释。

第五十九条 本指南自公布之日起施行。

深圳市企业数据合规指引

（深圳市人民检察院 深圳市互联网信息办公室 深圳市发展和改革委员会 深圳市司法局 深圳数据交易所 2023 年 9 月 11 日）

目 录

第一章 总 则

第一条【目的和依据】为引导企业加强数据合规管理，促进企业数据合规利用，保障企业数据安全，根据《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》《中华人民共和国网络安全法》等法律法规，制定本指引。

第二条【适用范围和效力】深圳市各类企业进行数据处理活动可参照本指引开展数据合规管理。

本指引不具有强制性，法律、法规及有关国家、行业标准另有专门规定的，从其规定。

第三条【涉案企业合规从宽】企业参照本指引建立并严格实施数据合规管理制度，履行数据合规义务，积极配合监管，主动采取措施有效减轻、消除危害后果，符合涉案企业合规适用条件的，检察机关可根据具体情况开展合规考察。

对于涉案企业合规建设经评估符合有效性标准的，检察机关可以参考评估结论依法作出不批准逮捕、变更强制措施、不起诉的决定，或提出从宽处罚的量刑建议；符合行政处罚法规定条件的，可以向有关主管机关提出从轻或者减轻行政处罚等建议、意见。

第四条【数据合规指引的必要性】引导各类企业开展数据合规管理是提高企业数据合规意识，提高数据保护水平，降低企业及其员工涉数据类违法犯罪风险的重要举措。企业可以通过建立完善的数据合规管理体系，有效预防数据安全风险事件。

第五条【职责明确原则】企业应当通过建立完善的数据合规管理组织体系和制度体系，明确企业内部各部门数据安全管理职责，落实数据合规主体责任。

第六条【合法、正当和诚信原则】企业处理数据应当符合法律、法规和强制性标准的规定，遵循合法、正当和诚信原则，不得从事危害国家安全、公共利益的数据处理活动，不得非法收集、使用、加工、传输、买卖、提供、公开他人个人信息，不得通过误导、欺诈、胁迫等方式处理个人信息。

第七条【数据质量保障原则】企业应当采取适当措施保证数据质量，并定期

对数据进行更新，避免因数据不准确、不完整、不及时产生的不利影响。

第八条【负责原则】企业应当对其数据处理活动负责，并采取必要措施保障所处理数据的安全。

第九条【分类分级保护原则】企业应当建立数据分类分级保护制度，按照数据对国家安全、公共利益或者个人、组织合法权益的影响和重要程度进行分类分级，针对不同类别级别的数据采取相应的管理和保护措施。

第十条【风险导向原则】企业应当采取必要措施对国家核心数据、重要数据、敏感个人信息等存在较高合规风险的数据予以重点保护，加强合规管理。

第十一条【可追溯原则】企业对数据进行修改、查询、导出、删除等处理时，应当记录相应操作，确保操作记录可追溯、可审查。

第二章 数据合规管理组织体系建设

第十二条【一般要求】企业开展数据处理活动应当依照法律、法规的规定，建立健全数据合规管理组织体系和常态化沟通协作机制，明确数据合规责任主体，组织开展数据合规教育培训，加强人力资源考核与保障，强化数据合规意识。

第十三条【数据合规决策层的职责】数据合规第一负责人由企业法定代表人或主要负责人担任，对数据合规负领导责任。数据合规第一负责人与董事会应当承担以下职责：

(一)为企业数据合规管理制度体系的建构和运行提供必要的资源保障和条件支持，确保合规管理制度体系有效运转并持续改进；

(二)确立数据合规方针和合规目标，并确保企业战略方向与合规方针和目标保持一致；

(三)保障数据合规管理部门具备独立履行职责的能力与权限；

(四)审批企业重大数据合规事项；

(五)确保将数据合规管理要求融入企业的业务过程；

(六)确保建立有效的数据违规举报与惩处机制；

(七)引导培育企业数据合规自主性，促成数据合规企业文化。

第十四条【数据合规管理层的职责】企业应当设立专门的数据合规管理部门，或由合规管理、法务等相关部门承担数据合规管理职能，并配备数据合规专员。数据合规管理部门在部门负责人的指导下开展工作，承担以下职责：

(一)组织制定企业数据合规管理制度规范与合规计划，并推动其有效实施；

(二)统筹实施数据合规管理工作，并对数据合规管理情况进行评估与检查；

(三)建立数据合规举报与调查机制，对数据合规举报制定调查方案并开展调查；(四)定期组织或协助人事部门开展数据安全合规培训，为企业相关内部职能部门提供数据合规咨询与支持；

(五)向数据合规第一负责人与董事会报告数据合规重大风险和数据合规工作落实情况。

第十五条【数据合规执行层的职责】企业内部开展数据处理工作的各职能部门负责本部门业务范围内的数据合规工作，并承担以下职责：

(一)结合企业数据合规管理制度和合规指引，明确本部门日常数据处理活动的全生命周期合规要求和具体工作机制；

(二)确保本部门员工遵守企业合规制度规范，履行数据合规义务；

(三)配合数据合规管理负责人和合规管理部门开展合规风险审查、评估、整改等各项合规工作；

(四)密切监测日常数据处理工作中的数据安全合规风险，并采取适当的安全保护措施；

(五)当发现数据处理活动存在较大合规风险或者发生数据安全事件时，及时向数据合规管理负责人和合规管理部门报告，并配合采取应急处置和整改措施。

第十六条【个人信息保护负责人的指定及责任】处理个人信息达到国家网信部门规定数量的企业应当指定专门的个人信息保护负责人，并承担以下职责：

(一)统筹实施企业内部的个人信息合规工作；

(二)组织制定个人信息合规方面的内部制度和操作规程，并督促落实；

(三)组织开展个人信息安全影响评估，督促整改安全隐患；

(四)定期组织开展合规审计；

(五)及时受理相关投诉、举报；

(六)与监管部门保持沟通，通报或报告个人信息保护和事件处置等情况。企业应当公开个人信息保护负责人的姓名、联系方式等情况， 并报送履行个人信息保护职责的部门。

第十七条【数据合规教育和培训】企业应当定期组织开展数据合规教育培训

及考核，确保内部人员充分了解数据法规、数据合规计划、数据合规义务与举报程序等，提升内部人员数据合规意识，促进企业合规守法经营。

第十八条【人力资源管理与保障】企业应当在数据合规管理制度规范中明确员工的数据合规义务，鼓励将数据合规落实效果纳入考核体系，作为决定评优评先、职务晋升与薪酬待遇的重要依据。

企业应当将遵守数据合规要求和履行数据合规义务作为人员聘用条件。对于数据处理关键岗位的员工应当开展必要的背景调查，了解其犯罪记录，诚信状况等相关信息，并通过签署合规承诺书、保密协议等方式明确其应遵守的数据合规要求和履行的数据合规义务，并建立相应的奖惩机制督促落实。关键岗位员工离岗后，应当按照数据合规管理要求执行离岗交接、审计、脱密等措施。

第十九条【合规承诺制度】企业应当建立数据合规承诺制度， 明确违反数据合规承诺的后果与问责机制，数据合规第一犬负责人，数据合规管理部门负责人以及其他数据处理关键岗位员工应作出并严格履行数据合规承诺。

第二十条【举报与调查机制】企业应当建立内部数据合规举报机制，鼓励、支持内部人员对试图、涉嫌或实际存在的数据不合规行为进行举报， 并采取必要措施保护内部举报人信息，不得因此对举报人采取不利措施。

收到举报后，数据合规管理部门应当结合举报线索的真实性、有效性及时启动调查程序，确保调查过程的独立性、公正性， 形成调查结果报告并采取相应处理和改进措施，持续完善数据合规管理制度体系。

第二十一条【文件化信息】企业应当以适当的形式和载体记录数据合规管理体系运行产生的文件化信息。文件化信息应当以清晰、易读和易检索的方式保存，并采取必要措施防止泄密、不当使用或完整性受损。

第三章 数据合规管理制度体系建设

第二十二条【一般要求】企业应当依照法律、法规规定， 结合自身业务，建立健全覆盖数据全生命周期的数据合规管理制度体系，明确企业内部数据合规管理的相关标准、规范和操作规程， 坚持安全和发展并重，确保数据合规管理制度与生产运营、业务发展同步规划、同步建设、同步运行。

第二十三条【数据分类分级保护制度】企业应当根据自身业务内容定期对企业数据资产进行全面梳理，并结合所属行业、地区的相关标准， 对数据进行分类

分级，经数据合规管理部门审批后，形成数据分类分级清单。对无明确分类分级标准的数据，可根据数据的重要程度、对国家安全、公共利益或者个人、组织合法权益造成的危害程度等因素，按照就高从严原则进行分类分级。

企业应确立数据分类分级管控标准，明确不同类别级别数据的操作要求和保护措施。同时处理不同级别数据且难以分别采取保护措施的， 企业应当按照其中级别最高的要求给予保护。

第二十四条【重要数据、核心数据保护制度】企业应当结合相关法律、法规和主管部门、所属行业重要数据具体目录等标准规范， 识别和确定自身业务活动中涉及的重要数据与核心数据，形成数据清单。

企业应当对重要数据与核心数据实施更加严格的合规管理制度，明确重要数据、核心数据的管理职责、操作规范、审批要求、备案机制等事项， 建立重要数据和核心数据的日常记录和容灾备份机制，强化重要数据与核心数据的安全保障。

第二十五条【采取安全技术保护措施】企业应当根据数据分类分级情况， 采取适当的匿名化、备份、加密、访问控制、入侵防范等数据安全保护措施，加强对数据处理系统、数据传输网络、数据存储环境、数据访问接口等物理和网络环境的安全防护，将数据安全技术保护覆盖到数据处理的全过程。

处理重要数据的系统应满足三级以上网络安全等级保护和关键信息基础设施安全保护要求，处理核心数据的系统依照有关规定从严保护。

第二十六条【权限控制机制】企业应当按照最小授权原则合理确定数据访问与操作权限，仅在完成职责所需的范围内授予特定人员最小必要的数据操作权限，并采取技术措施，避免出现越权访问、下载、复制、修改数据等行为。针对重要数据和核心数据，企业应当通过设置严格的数据处理权限、配备风险阻断机制、明确安全审计流程、落实访问和操作留痕等方式，实现权限最小化管控。

第二十七条【依法申报数据安全审查】鼓励企业主动审查其数据处理活动是否影响或者可能影响国家安全，符合法律法规规定条件的，应当按照国家有关规定，申报网络安全审查。

掌握超过 100 万用户个人信息的网络平台运营者赴国外上市，必须向网络安全审查办公室申报网络安全审查。

第二十八条【建立合规风险评估机制】企业应当建立数据合规风险评估机制，

每年至少开展一次数据合规风险评估，对数据分类分级保护情况、数据安全技术保护措施有效性、关键基础设施安全水平、数据处理合规情况、法律法规变化和监管动态落实情况、数据安全预警和应急事件处置能力、数据安全问题整改和监管执法响应情况等内容进行评估，并形成数据合规风险评估报告。涉及处理重要数据的，还应对重要数据的处理情况作出评估，并向有关主管部门报送风险评估报告。对新上线业务、第三方数据合作业务以及重点存量业务， 企业可以不定期开展合规风险评估。

企业应当根据数据合规风险评估报告对相关职能部门、岗位员工作出风险提示，并要求其采取相应的风险处置和整改措施，必要时应暂停或取消具有较高合规风险的业务活动。

第二十九条【定期合规审计】企业内部应当定期开展数据合规审计， 或委托具有相关资质的外部机构进行，并形成、保存相应的数据合规审计报告。对于审计过程中发现的合规问题与安全隐患应及时采取整改措施。

企业可以针对风险较高的数据处理行为进行不定期审计，确保及时发现问题隐患并予以改正。

第三十条【监测预警与存在安全缺陷、漏洞的补救措施】企业应当建立数据安全风险监测预警机制，及时监测日常数据处理活动中的异常情况和安全风险，并进行预警。当发现数据安全缺陷、漏洞等风险时， 应当立即采取预防、补救措施；造成或者可能造成严重后果的，应当及时告知可能受到影响的主体，并向有关主管部门报告。

企业应当建立针对数据不合规行为的监测机制，及时发现日常数据处理活动中的不合规行为，采取相应的处置和惩戒措施，并对类似问题进行排查。发生可能对企业带来重大数据合规风险的违规行为时，应当及时向数据合规负责人汇报，并确定相应的解决方案。

第三十一条【数据安全应急预案、演练和处置机制】企业应当制定数据安全应急预案，按照危害程度、影响范围等因素对数据安全事件进行分级， 并结合分级情况确定应急处置的方针策略、人员职责、具体措施、流程规范、物资保障等事项。企业应当每年至少组织一次应急响应培训和应急预案演练，使相关人员掌握熟悉应急处置策略和规程。

当发生数据安全事件时，企业应当按照应急预案及时采取处置措施，防止危害扩大，消除安全隐患，记录事件内容，保留相关证据，并向有关主管部门报告。安全事件对个人、组织造成实质性危害的， 企业还应及时以电话、短信、邮件等方式向所涉主体告知安全事件情况、危害后果、已采取的补救措施等信息。无法逐一告知的，可采取公告方式告知。

第三十二条【积极配合监管】企业应当建立监管执法配合机制， 受到监管部门调查时应立即通知数据合规负责人、数据合规管理部门负责人和相关职能部门负责人等人员，启动必要的内部调查程序并明确监管调查对接人员，必要时应当暂停相应的数据处理活动。

企业应当对监管部门的监管执法予以协助、配合， 不得拒绝、阻挠， 不得提供虚假材料、信息或隐匿、销毁、转移证据。

企业积极配合监管并主动开展合规整改采取措施有效减轻、消除危害后果的，可以向监管部门申请酌情从轻或减轻行政处罚。

第三十三条【建立监管响应和整改机制】企业应当按照监管部门提出的监管建议及时采取整改措施，优化、更新数据合规管理制度， 建立健全数据合规长效机制，有效消除安全隐患。

第三十四条【外部投诉机制】企业应当建立便捷的数据合规外部投诉机制，公布受理部门或人员联系方式、受理流程等信息， 鼓励受到数据不合规行为影响的主体进行投诉，并在合理时间内向投诉人回复处理情况。

第四章 数据全生命周期合规

第一节 数据收集和使用

第三十五条【以爬虫等手段抓取数据的合法标准】企业采用网络爬虫等自动化工具收集数据的，应当遵守法律法规、行业自律公约， 尊重爬取对象网站的爬虫协议及规则，事前评估对网络服务的性能、功能可能带来的影响， 避免干扰网络服务的正常功能或妨碍计算机信息系统正常运行。

企业收集涉及他人知识产权、商业秘密或非公开的个人信息的数据， 应事前征得所涉主体同意。企业不得以下列不正当的方式获取他人持有的数据：

(一)以盗窃、胁迫、欺诈，电子侵入等方式，未经授权或超越授权获取数据；

(二)违反国家规定，侵入国家事务、国防建设、尖端科学技术领域的计算机

信息系统获取数据；

(三)以非法获取内部访问、操作权限等方式，未经授权或超越授权获取数据；

(四)以提供替代性产品或服务为目的，违反约定或者合理、正当的数据抓取协议，或以其他违反诚实信用和商业道德的方式获取数据；

(五)以其他违反法律禁止性规定或可能导致不正当竞争的方式获取数据。

第三十六条【以购买、交换等手段收集数据的合法标准】企业通过向第三方购买、交换、共享等方式收集数据的， 应当符合法律、法规要求， 对第三方的资质以及获取和持有数据的合规性进行必要审查，要求其作出数据来源合法性承诺并提供必要证明。

对从第三方获取的数据，企业应当承担与直接收集的数据同等的安全保护责任与合规义务。

第三十七条【在提供产品、服务过程中收集数据的合法标准】企业在提供产品、服务过程中收集个人信息， 应当符合最小必要原则，仅收集与实现产品或服务的业务功能直接相关的个人信息。不得因个人不同意提供非必要个人信息， 而拒绝向其提供基本功能或服务。

企业基于开发新型业务功能、提升服务体验等目的， 超出必要范围收集用户个人信息的，应当征得个人同意。

企业如需使用在提供产品、服务过程中收集到的数据， 应当事先获得相关数据主体的授权同意。

第三十八条【自动化决策场景的合规义务】企业利用数据进行自动化决策的，应当保证自动化决策的透明度，并以适当方式公示其自动化决策的基本原理、目的意图和主要运行机制等信息。自动化决策的结果可能对个人权益造成显著影响的，应当对此种影响及可能产生的后果予以说明，并为个人提供拒绝自动化决策的选项。

通过自动化决策方式进行信息推送、商业营销的， 应当同时提供不针对个人特征的选项，并向个人提供便捷的拒绝方式。

企业不得利用数据分析，对交易条件相同的交易相对人实施差别待遇，但是有下列情形之一的除外：

(一)根据交易相对人的实际需求，且符合正当的交易习惯和行业惯例，实行

不同交易条件的；

(二)针对新用户在合理期限内开展优惠活动的；

(三)基于公平、合理、非歧视规则实施随机性交易的；

(四)法律、法规规定的其他情形。

前款所称交易条件相同，是指交易相对人在交易安全交易成本、信用状况、交易环节、交易持续时间等方面不存在实质性差别。

第三十九条【分类管理】企业应当建立个人信息分类管理制度，结合个人信息的主体属性、具体种类、敏感程度、处理方式、应用场景、对个人权益的影响、可能存在的安全风险等因素明确个人信息分类标准，并分别确定针对不同类型个人信息的处理规则、合规义务和保护标准。敏感个人信息及未成年人个人信息处理规则应当遵循法律、法规的相关规定。

第四十条【个人信息保护影响评估】企业应当针对业务中涉及的对个人权益有重大影响的数据处理活动开展个人信息保护影响评估，持续检验、监控个人信息处理活动的合法合规程度、对个人合法权益造成损害的各种风险以及相关保护措施的有效性，形成和保存个人信息保护影响评估报告和处理情况记录，并采取相应改进措施。

第四十一条【建立个人信息权利行使的响应机制】企业应当为用户行使《中华人民共和国个人信息保护法》赋予的各项权利提供便捷的申请受理和响应机制，明确合理的响应时限。

第二节 数据存储

第四十二条【分级分域管理】企业应当根据分类分级等内部规范对不同类型、风险等级和重要、敏感程度的数据进行分级分域管理，对不同数据进行物理隔离或强逻辑隔离，并采取相适应的安全保护措施和访问控制机制，维护数据的完整性、保密性、可用性。

企业应当通过加密存储、访问控制、校验技术等措施强化对重要数据和敏感个人信息的保护。

第四十三条【数据存储介质管理】企业应当根据数据类型、风险等级和重要、敏感程度等因素选择安全性能、防护级别与安全等级相适应的存储设备和介质，制定数据存储设备和介质清单，建立数据存储设备和介质管理制度，规范存储设

备和介质的使用、操作、维修和故障处理， 并对传递、使用数据存储设备和介质的行为建立审批和日志记录等管控机制，强化存储设备和介质的物理安全和加密管理。

第四十四条【云平台存储】企业使用第三方云平台进行数据存储的， 应当要求云服务提供商定期报告云平台运行状态、安全状况等信息， 并定期对第三方云平台的稳定性和采取的安全保护措施等进行审计，确保其具备充分的数据安全保护能力。

企业终止使用云平台存储服务的，有权取回数据、文档等资料并对其完整性、有效性进行验证。云服务提供商应当按照约定方式删除、销毁云平台存储的数据及副本。

第四十五条【技术保护措施：去标识化、匿名化】企业在存储数据时应当采取加密、去标识化、匿名化处理等安全技术措施，降低个人信息被篡改、破坏、泄露或者非法获取、非法利用等风险。经过去标识化处理的个人信息应当与其他个人信息分开存储，并严格控制访问权限。

第四十六条【数据备份及恢复】企业应当建立重要数据和个人信息的备份与恢复机制，确定数据备份的范围、频率、方法和流程， 并定期对备份数据进行恢复测试和完整性校验，防范数据意外损毁、丢失等风险。

第三节 数据传输和提供

第四十七条【数据传输的合规要求】企业应当采取加密等安全保护措施确保数据传输介质和环境安全，保障重要数据和敏感个人信息传输过程的安全性，防范未经授权访问和数据泄露。

第四十八条【向第三方提供数据的合规要求】企业因业务需要等正当理由向第三方提供或共享、委托处理数据的， 应当对数据接收方进行事前资格审查并评估其数据安全保护能力。涉及提供重要数据、敏感数据的， 应当留存相应的日志记录。

企业应当通过合同等形式与数据接收方约定处理数据的目的、范围、方式、限制与应采取的安全保护措施等事项，明确双方权利和义务，并对数据接收方的处理活动进行必要监督。发现数据接收方违反法律、法规规定或双方约定处理数据的，应当立即要求其停止相关行为并采取必要的补救措施：必要时应当暂停或

终止向其提供数据，并监督数据接收方及时返还、删除、销毁已获得的数据。

第四十九条【向第三方提供个人信息的合规要求与豁免】企业向第三方提供或共享、委托处理个人信息的， 应当向个人告知接收方的名称或者姓名、联系方式、处理目的、处理方式和个人信息的种类，并按照法律规定征得个人单独同意。

第五十条【共同处理场合下的合规要求】两个以上的企业共同决定个人信息的处理目的和处理方式的，应当约定各自的权利和义务、应采取的安全保护措施、发生数据安全事件时的补救与应急处置措施以及责任承担等事项。

第五十一条【合作方管理】企业应当加强对合作方的合规管理， 明确信息系统开发及运维、数据存储、数据处理等合作方的准入标准和资格审查机制， 并通过签订合规协议等形式明确双方的权利和义务，以及合作方的数据处理权限、应采取的安全保护措施等事项。

企业应当定期对合作方进行合规检查和审计，并结合风险特征对合作方进行合规分级、分类管控， 对不同风险级别的合作方采取相适应的合规管理措施。发现合作方存在严重违法、违规、违约行为或发生重大数据安全事故、丧失数据安全保障能力、故意不履行数据安全保护职责等情形的，应及时终止与其合作。

第五十二条【第三方接入场景／SDK 的合规义务】企业在其产品或服务中接入由第三方提供的软件开发工具包的，应当事前对接入第三方进行安全检测，评估是否存在已知的安全漏洞以及可能引起数据泄露等安全事件的行为，并建立相应的接入第三方合规管理机制，通过签署开发者服务协议等形式明确双方的权利和义务、应采取的安全保护措施、发生数据安全事件时的补救与应急处置措施以及责任承担等事项，并留存第三方接入日志记录。

第三方软件开发工具包具备收集、处理个人信息功能的， 企业应当要求该第三方如实、完整披露收集、处理个人信息的具体情况， 并应将相关情况及时、准确告知所涉个人，并按照法律规定征得个人同意。

企业应当对第三方软件开发工具包进行持续安全监测，发现接入第三方存在违反法律、法规规定或双方约定处理数据， 或未落实数据安全保护责任造成较大安全风险的，应当及时切断接入，并督促其采取整改措施。对于存在流量劫持、资费消耗、隐私窃取等恶意行为的第三方软件开发工具包应当取消其接入权限。

第五十三条【合并、重组、分立、解散、破产场合下的合规要求】企业因兼

并、重组、破产等原因需要转移数据的， 应当制定数据转移方案，明确数据承接方及其应当履行的数据安全保护责任等事项，并以合适的方式通知受影响的个人。

作为数据承接方的企业应当继续承担数据合规义务和数据安全责任。因业务需要等正当理由确需改变数据处理目的、范围、方式的， 应当重新征得所涉个人同意。

第四节 数据交易

第五十四条【数据交易场所的合规义务】数据交易场所应当建立数据来源可确认、使用范围可界定、交易过程可追溯、安全风险可防范的可信数据交易环境，制定平台准入、数据质量评估、交易管理、合规审查、信息披露、自律监管等规则，对场内交易进行管理，交易参与主体应当予以配合。

数据交易场所应当对场内交易进行合法性与合规性评估，并履行以下义务：

(一)要求数据提供方说明数据来源，并审核相关信息；

(二)审核数据交易双方身份和数据交易合同；

(三)留存相关审核、交易记录；

(四)监督数据交易、结算和交付；

(五)采取必要技术手段确保数据交易安全，保护个人信息、个人隐私、商业秘密、保密商务信息和重要数据；

(六)法律、法规规定的其他义务。

第五十五条【数据来源合规】开展数据交易的企业应当建立针对数据来源的合规审查机制，确保数据获取手段合法合规、数据来源链路清晰， 并经过所涉主体明确授权同意，不存在侵犯国家、公共利益或其他组织、个人合法权益的情况。

第五十六条【数据内容合规】开展数据交易的企业应当建立针对数据内容的合规审查机制，不得交易含有以下内容的数据产品或服务：

(一)含有未经授权的个人信息的；

(二)含有侵犯他人知识产权或商业秘密的内容的；

(三)含有未经依法开放的公共数据的；

(四)含有国家核心数据或国家秘密的；

(五)含有法律、法规规定禁止交易的其他数据的。

第五十七条【数据质量合规】开展数据交易的企业应当建立必要的数据质量

校验机制，提升交易数据的准确性、完整性和及时性， 并通过数据复核、交叉验证等方式强化重要数据、敏感数据的质量审查。

第五十八条【反馈修改机制】开展数据交易的企业应当建立问题反馈和修改机制，对证明存在错误或侵权的数据及时采取更正、删除等补救措施。

第五十九条【交易数据的使用监测】开展数据交易的企业应当通过与交易相对方签订数据使用协议等方式，明确交易数据的使用目的、范围、方式、处理限制与应采取的安全保护措施等事项，以及发生违约、侵权行为时的法律责任， 并在合理范围内对数据使用行为进行监督。

数据购买方应当按照约定的目的、场景和方式合规使用数据， 不得将通过交易获取的数据用于违反法律法规或双方约定的其他用途。

第六十条【免责事由 / 容错机制】开展数据交易的企业对超出其可预见范围和技术控制能力的数据错误等质量瑕疵，在及时采取补救措施后仍造成损失的，应当允许其通过事前约定等方式减轻或免除相应责任，但对损失的发生存在故意或重大过失的除外。

开展数据交易的企业参照本指引数据交易合规要求，履行数据合规义务，其销售的交易标的已按照深圳数据交易所的上市合规评估流程完成合法性与合规性评估的，检察机关可视情况适用涉案企业合规程序。

第五节 数据删除和销毁

第六十一条【应当删除、销毁数据的情形】企业应当建立数据存储冗余管理策略，定期对存储数据进行盘点，对于对实现处理目的不再必要的数据，应当及时进行删除或匿名化处理。

当出现以下情形时，企业应当对其持有的全部数据或相关数据进行删除、销毁：

(一)企业终止运营、解散或破产，且没有数据承接方的；

(二)约定的数据存储期限已经届满的，或发生约定的数据删除、销毁事由的；

(三)根据法律、法规规定应当删除、销毁数据的其他情形。

第六十二条【数据删除与销毁的合规要求】企业应当建立数据删除和销毁的操作规程和管理制度，明确删除和销毁的对象、权限、流程和技术等要求， 确保被销毁数据不可恢复，并对相关活动进行记录和留存。

企业对数据存储设备和介质进行报废处理的，应当事先采取格式化、重复删除、介质消磁等方式删除其中存储的数据， 并采取物理损毁等方式对介质进行彻底销毁。

第六十三条【删除个人信息的情形】符合下列情形之一的，企业应当在十五个工作日之内对相关个人信息进行删除或匿名化处理，并遵循可审计原则记录删除时间、操作人、数据内容等相关信息。个人信息处理者未删除的， 个人有权请求删除：

(一)处理目的已实现、无法实现或者为实现处理目的不再必要；

(二)企业停止提供产品或者服务，或者保存期限已届满；

(三)个人撤回同意；

(四)企业违反法律、行政法规或者违反约定处理个人信息；

(五)法律、行政法规规定的其他情形。

法律、行政法规规定的保存期限未届满， 或者删除个人信息从技术上难以实现的，企业当停止除存储和采取必要的安全保护措施之外的处理。

第五章 数据出境合规

第六十四条【适用数据出境安全评估的情形】企业向境外提供数据， 有下列情形之一的，应当通过所在地省级网信部门向国家网信部门申报数据出境安全评估：

(一)企业向境外提供重要数据；

(二)关键信息基础设施运营者和处理 100 万人以上个人信息的企业向境外提供个人信息；

(三)自上年 1 月 1 日起累计向境外提供 10 万人个人信息或者 1 万人敏感个人信息的企业向境外提供个人信息；

(四)国家网信部门规定的其他需要申报数据出境安全评估的情形。

第六十五条【数据出境风险自评估的开展】企业在申报数据出境安全评估前，应当开展数据出境风险自评估，重点评估以下事项：

(一)数据出境和境外接收方处理数据的目的、范围、方式等的合法性、正当性、必要性；

(二)出境数据的规模、范围、种类、敏感程度，数据出境可能对国家安全、

公共利益、个人或者组织合法权益带来的风险；

(三)境外接收方承诺承担的责任义务，以及履行责任义务的管理和技术措施、能力等能否保障出境数据的安全；

(四)数据出境中和出境后遭到篡改、破坏、泄露、丢失、转移或者被非法获取、非法利用等的风险，个人信息权益维护的渠道是否通畅等；

(五)与境外接收方拟订立的数据出境相关合同或者其他具有法律效力的文件等是否充分约定了数据安全保护责任义务；

(六)其他可能影响数据出境安全的事项。

第六十六条【需要重新评估的情形】在数据出境安全评估的结果有效期内出现以下情形之一的，企业当重新申报评估：

(一)向境外提供数据的目的、方式、范围、种类和境外接收方处理数据的用途、方式发生变化影响出境数据安全的， 或者延长个人信息和重要数据境外保存期限的；

(二)境外接收方所在国家或者地区数据安全保护政策法规和网络安全环境发生变化以及发生其他不可抗力情形、数据处理者或者境外接收方实际控制权发生变化、数据处理者与境外接收方法律文件变更等影响出境数据安全的；

(三)出现影响出境数据安全的其他情形。通过数据出境安全评估的结果有效期为 2 年，自评估结果出具之日起计算。有效期届满， 需要继续开展数据出境活动的，数据处理者应当在有效期届满 60 个工作日前重新申报评估。

第六十七条【明确约定数据安全保护责任义务】企业应当在与境外接收方订立的法律文件中明确约定数据安全保护责任义务，至少包括以下内容：

(一)数据出境的目的、方式和数据范围， 境外接收方处理数据的用途、方式等；

(二)数据在境外保存地点、期限， 以及达到保存期限、完成约定目的或者法律文件终止后出境数据的处理措施；

(三)对于境外接收方将出境数据再转移给其他组织、个人的约束性要求；(四)境外接收方在实际控制权或者经营范围发生实质性变化，或者所在国家、地区数据安全保护政策法规和网络安全环境发生变化以及发生其他不可抗力情形导致难以保障数据安全时，应当采取的安全措施；

(五)违反法律文件约定的数据安全保护义务的补救措施、违约责任和争议解决方式;

(六)出境数据遭到篡改、破坏、泄露、丢失、转移或者被非法获取、非法利用等风险时,妥善开展应急处置的要求和保障个人维护其个人信息权益的途径和方式。

第六十八条【向境外提供个人信息的条件】企业因业务等需要,确需向中华人民共和国境外提供个人信息的,应当具备下列条件之一:

(一)依照《个人信息保护法》第四十条的规定通过国家网信部门组织的安全评估;

(二)按照国家网信部门的规定经专业机构进行个人信息保护认证;

(三)按照国家网信部门制定的标准合同与境外接收方订立合同,约定双方的权利和义务;

(四)法律、行政法规或者国家网信部门规定的其他条件。

中华人民共和国缔结或者参加的国际条约、协定对向中华人民共和国境外提供个人信息的条件等有规定的,可以按照其规定执行。

企业应当采取必要措施,保障境外接收方处理个人信息的活动达到法律规定的个人信息保护标准。

第六十九条【个人数据出境场景下的告知同意要求】企业向中华人民共和国境外提供个人信息的,应当向个人告知境外接收方的名称或者姓名、联系方式、处理目的、处理方式、个人信息的种类以及个人向境外接收方行使《个人信息保护法》规定的各项权利的方式和程序等事项,并取得个人的单独同意。

第七十条【个人信息出境场景下的个人信息保护影响评估】企业向境外提供个人信息的,应当事前进行个人信息保护影响评估,并对处理情况进行记录。个人信息保护影响评估应当包括下列内容:

(一)个人信息的处理目的、处理方式等是否合法、正当、必要;

(二)对个人权益的影响及安全风险;

(三)所采取的保护措施是否合法、有效并与风险程度相适应。个人信息保护影响评估报告和处理情况记录应当至少保存三年。

第七十一条【适用个人信息保护认证的情形】企业通过经专业机构进行个人

信息保护认证的方式向境外提供个人信息的，应当符合 TC260－PG－20222A《个人信息跨境处理活动安全认证规范》、GB / T35273《信息安全技术个人信息安全规范》的要求。

第七十二条【适用出境标准合同的情形】企业通过订立标准合同的方式向境外提供个人信息的，应当同时符合下列情形：

(一)非关键信息基础设施运营者；

(二)处理个人信息不满 100 万人的；

(三)自上年 1 月 1 日起累计向境外提供个人信息不满 10 万人的；

(四)自上年 1 月 1 日起累计向境外提供敏感个人信息不满 1 万人的。

法律、行政法规或者国家网信部门另有规定的， 从其规定。企业不得采取数量拆分等手段，将依法应当通过出境安全评估的个人信息通过订立标准合同的方式向境外提供。

第七十三条【遵守出口管制要求的合规义务】国家对与维护国家安全和利益、履行国际义务相关的属于管制物项的数据依法实施出口管制，企业向境外提供涉及出口管制的数据的，应当依法向有关部门申请出口许可证：可能危害国家安全和利益的，不得向境外提供。

第七十四条【境外司法或执法机构调取数据场景下的合规义务】非经中华人民共和国主管机关批准，企业不得向外国司法或者执法机构提供存储于中华人民共和国境内的数据。

第六章 附 则

第七十五条【基本概念】本指引所称的概念含义如下：

(一)数据，是指任何以电子或者其他方式对信息的记录；

(二)个人信息，是指以电子或者其他方式记录的与已识别或者可识别的自然人有关的各种信息，不包括匿名化处理后的信息；

(三)敏感个人信息，是指一旦泄露或者非法使用，容易导致自然人的人格尊严受到侵害或者人身、财产安全受到危害的个人信息，包括生物识别、宗教信仰、特定身份、医疗健康、金融账户、行踪轨迹等信息， 以及不满十四周岁未成年人的个人信息。

(四)重要数据，是指一旦遭到篡改、破坏、泄露或者非法获取、非法利用等，

可能危害国家安全、经济运行、社会稳定、公共健康和安全等的数据；

(五)国家核心数据，是指关系国家安全、国民经济命脉、重要民生、重大公共利益等的数据：

(六)数据处理，包括数据的收集、传输、存储、加工、使用、提供、公开等；

(七)数据安全，是指通过采取必要措施，确保数据处于有效保护和合法利用的状态，以及具备保障持续安全状态的能力；

(八)数据合规，是指企业通过采取必要措施，确保其在日常经营活动中的数据处理行为达到个人信息保护、网络安全、数据安全等方面的法律要求的状态：

(九)数据合规管理，是指以预防和降低涉数据违法犯罪和数据安全风险为目的，以企业及其员工行为为管理对象，开展的一系列管理活动；

(十)自动化决策，是指通过计算机程序自动分析、评估个人的行为习惯、兴趣爱好或者经济、健康、信用状况等，并进行决策的活动；

(十一)数据交易场所，是指经深圳市政府批准成立的，组织开展数据交易活动的交易场所。

第七十六条【指引的解释】本指引由深圳市人民检察院、深圳市互联网信息办公室、深圳市司法局、深圳市发展和改革委员会、深圳数据交易所负责解释。

第七十七条【施行日期】本指引自发布之日起施行。

附录：

企业可参考的相关法律法规与标准

序号	类型	层级	名称
1	数据安全	法律	《中华人民共和国国家安全法》
2		法律	《中华人民共和国网络安全法》
3		法律	《中华人民共和国数据安全法》
4		部门规章	《网络安全审查办法》
5		标准	《信息安全技术 大数据安全管理指南》(GB/T 37973—2019)
6		标准	《网络安全标准实践指南——网络数据分类分级指引(v1.0-202112)》(TC260-PG-20212A)
7		标准	《合规管理体系 要求及使用指南》(GB/T 35770—2022)
8	重要数据保护	法律	《中华人民共和国个人信息保护法》
9	个人信息保护	法律	《中华人民共和国民法典》
10		法律	《中华人民共和国消费者权益保护法》

11		法律	《中华人民共和国电子商务法》
12		法律	《中华人民共和国未成年人保护法》
13		司法解释	《最高人民法院、最高人民检察院关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释》
14		司法解释	《最高人民法院、最高人民检察院关于办理危害计算机信息系统安全刑事案件应用法律若干问题的解释》
15		司法解释	《最高人民法院 最高人民检察院关于办理非法利用信息网络、帮助信息网络犯罪活动等刑事案件适用法律若干问题的解释》
16		司法解释	《最高人民法院关于审理利用信息网络侵害人身权益民事纠纷案件适用法律若干问题的规定》
17		行政法规	《互联网信息服务管理办法》
18		行政法规	《计算机信息网络国际联网安全保护管理办法》
19		行政法规	《互联网上网服务营业场所管理条例》
20		部门规章	《儿童个人信息网络保护规定》
21		部门规章	《电信和互联网用户个人信息保护规定》
22		部门规章	《网络信息内容生态治理规定》
23		标准	《信息安全技术 个人信息去标识化指南》(GB/T 37964-2019)
24		标准	《信息安全技术 移动智能终端个人信息保护技术要求》(GB/T 34978-2017)
25		标准	《信息安全技术 网络安全等级保护基本要求》(GB/T 22239+2019)
26		标准	《信息安全技术 个人信息安全规范》(GB/T 35273—2020)
27	数据出境	部门规章	《数据出境安全评估办法》
28		部门规章	《个人信息出境标准合同办法》
29		部门规范性文件	《个人信息保护认证实施规则》
30		标准	《网络安全标准实践指南—个人信息跨境处理活动安全认证规范 V2.0》
31	电信领域	部门规章	《工业和信息化领域数据安全管理办法(试行)》
32		标准	《基础电信企业数据分类分级方法》(YD/T 3813-2020)
33		标准	《基础电信企业重要数据识别指南》(YD/T 3867-2021)
34		标准	《电信网和互联网数据安全评估规范》(YD/T 3956-2021)
35		标准	《电信网和互联网数据安全通用要求》(YD/T 3802-2020)
36		行政法规	《征信业管理条例》
37	金融领域	标准	《金融数据安全 数据安全分级指南》(JR/T 0197—2020)

38		标准	《金融数据安全 数据生命周期安全规范》(JR/T 0223—2021)
39		标准	《证券期货业数据分类分级指引》(JR/T 0158-2018)
40	汽车领域	部门规章	《汽车数据安全管理若干规定(试行)》
41		部门工作文件	《工业和信息化部关于加强车联网网络安全和数据安全工作的通知》(工信部网安(2021)134 号)
42	医疗领域	行政法规	《中华人民共和国人类遗传资源管理条例》
43		部门规范性文件	《国家健康医疗大数据标准、安全和服务管理办法(试行)》
44		标准	《信息安全技术 健康医疗数据安全指南》(GB/T 39725-2020)

湖南省网络安全和信息化条例

湖南省第十三届人民代表大会常务委员会公告第 81 号

《湖南省网络安全和信息化条例》于 2021 年 12 月 3 日经湖南省第十三届人民代表大会常务委员会第二十七次会议通过，现予公布，自 2022 年 1 月 1 日起施行。

湖南省人民代表大会常务委员会

2021 年 12 月 3 日

湖南省网络安全和信息化条例

(2021 年 12 月 3 日湖南省第十三届人民代表大会常务委员会第二十七次会议通过)

第一章 总 则

第一条 为了保障网络安全，促进信息化发展，提高数字化水平，推进经济社会高质量发展，根据有关法律、行政法规，结合本省实际，制定本条例。

第二条 本省行政区域内的网络安全保障和信息化促进等活动适用本条例。

第三条 网络安全和信息化工作应当贯彻总体国家安全观，遵循统筹规划、创新引领、开放共享、保障安全的原则。

第四条 省网络安全和信息化议事协调机构负责研究制定本省网络安全和信息化发展战略、宏观规划和重大政策， 统筹协调本省网络安全和信息化重大事项和重要工作，推进本省网络安全和信息化法治建设。

第五条 县级以上负责网络安全和信息化工作的部门(以下简称网信部门)负责本行政区域网络安全和信息化统筹协调、督促落实和相关监督管理工作。

县级以上人民政府工业和信息化、发展改革、科技、公安、财政、政务等部门和国家安全机关、省通信管理机构按照各自职责做好网络安全和信息化相关工作。

第六条 县级以上人民政府应当将网络安全和信息化发展纳入国民经济和社会发展规划，安排网络安全和信息化专项资金，引导和支持社会资金投资网络安全和信息化建设。

鼓励企业、科研机构、高等院校、行业组织和个人参与网络安全共同治理与信息化发展工作。

第七条 县级以上网信部门应当根据上一级网络安全和信息化发展规划以及本行政区域国民经济和社会发展规划，编制本行政区域网络安全和信息化发展规划，经本级人民政府批准后发布实施，并报上一级网信部门备案。

县级以上人民政府有关部门应当根据实际需要，编制本系统、本部门的网络安全和信息化专项规划，并与本行政区域网络安全和信息化发展规划相衔接。

第八条 编制网络安全和信息化发展规划、专项规划，应当组织专家论证，广泛征求意见，坚持安全可控、合理前瞻、科学布局、绿色集约、开放共享的原则，防止重复建设和资源浪费。

第九条 省人民政府标准化部门应当会同有关部门制定完善本省网络安全和信息化地方标准并监督实施。

鼓励有关单位参与制定修订网络安全和信息化国际标准、国家标准、行业标准、地方标准，自主制定高于国家强制性标准的团体标准、企业标准。

第十条 县级以上人民政府应当加强网信人才的培养和引进。

省人民政府及其有关部门应当支持高等院校建设计算机科学与技术、网络空间安全、集成电路科学与工程等学科， 建设重点网络安全和信息化研究基地，支持建设国家一流网络安全学院和网信人才培养基地，加强高等院校与实务部门的人才交流。

省人民政府人力资源和社会保障部门应当会同有关部门，建立健全网信人才职称评价制度和职称评聘制度。

第十一条 县级以上人民政府应当组织有关部门、教育机构、公众传媒、村(居)民委员会开展网络安全和信息化宣传活动，提高全社会网络安全意识和信息

技术应用能力。

县级以上人民政府及其有关部门应当将网络安全教育和信息化内容纳入国家工作人员培训和普法考核，普及中小学信息技术教育，发展信息技术职业教育。

第十二条 县级以上人民政府应当将网络安全和信息化工作纳入经济社会发展考核体系，建立绩效评估指标，对本行政区域各部门和下级人民政府进行网络安全和信息化工作考核。

第二章 网络安全保障

第十三条 县级以上人民政府及其有关部门应当按照谁主管谁负责、属地管理原则，落实网络安全责任制，建立健全网络安全保障体系，提升网络安全保护能力，实现网络、关键信息基础设施、重要信息系统和数据的安全可控。

第十四条 县级以上网信、工业和信息化、公安、保密、密码管理等部门和国家安全机关、省通信管理机构依照有关法律、行政法规的规定， 在各自职责范围内负责网络安全、数据安全、个人信息保护和相关监督管理工作。

第十五条 省人民政府对本省行政区域内未列入关键信息基础设施的重要信息系统，在网络安全等级保护制度的基础上，实行重点保护。

重要信息系统的具体范围和识别指南由省网信部门会同公安等部门制定。

第十六条 重要信息系统的行业主管或者监督管理部门指导和监督本行业、本领域的重要信息系统运行安全保护工作，负责编制和组织实施本行业、本领域重要信息系统安全规划，建立健全网络安全监测预警和网络安全事件应急预案，定期组织开展网络安全检查监测、应急演练， 对重要信息系统进行识别并向省网信部门、公安机关报送识别结果。

第十七条 重要信息系统运营者应当履行下列安全保护义务：

(一)明确专门安全管理机构和安全管理负责人，并对该负责人和关键岗位的人员进行安全背景审查；

(二)对从业人员进行网络安全教育、职业道德教育和技术培训；

(三)对重要系统和数据库进行容灾备份；

(四)制定网络安全事件应急预案，并定期进行演练；

(五)法律、行政法规规定的其他义务。

第十八条 重要信息系统运营者应当采购安全可信的网络硬件、软件产品和

服务，并与网络产品和服务提供者签订安全保密协议，明确提供者的技术支持和安全保密义务与责任。

第十九条 省和设区的市、自治州网信部门应当统筹协调有关部门对重要信息系统的安全保护采取下列措施：

(一)建立网络安全信息共享机制，促进有关部门、运营者以及网络安全服务机构等之间的网络安全信息共享；

(二)对重要信息系统安全风险进行抽查检测，提出改进措施，必要时可以委托网络安全服务机构对网络存在的安全风险进行检测评估；

(三)定期组织重要信息系统运营者进行网络安全应急演练；

(四)对网络安全事件应急处置与网络功能的恢复等，提供技术支持和协助。

第二十条 县级以上网信部门应当建立本行政区域网络安全监测预警和信息通报制度，统筹协调有关部门定期开展网络安全检查，加强网络安全信息收集、分析和通报工作，协调有关部门建立健全风险评估和网络安全应急工作机制，制定网络安全事件应急预案，组织网络安全应急演练。

第二十一条 发生网络安全事件或者接到预警信息后，有关单位应当立即启动应急预案，及时处置、消除隐患。发生较大以上网络安全事件， 有关单位应当及时向同级网信、公安部门报告。

省和设区的市、自治州网信部门会同有关部门对发生的较大以上网络安全事件开展调查。

能源、电信、交通等行业应当为网络安全事件应急处置与网络功能恢复提供电力供应、网络通信、交通运输等方面的重点保障和支持。

第二十二条 县级以上网信部门和有关部门依法履行网络信息安全监督管理职责，发现法律、行政法规禁止发布或者传输的信息的， 应当要求网络运营者停止传输，采取消除等处置措施，防止信息扩散，保存有关记录。

第二十三条 网络运营者应当加强对其用户发布的信息的管理，发现法律、行政法规禁止发布或者传输的信息的，应当立即停止传输该信息，采取消除等处置措施，防止信息扩散，保存有关记录，并向网信、公安、通信等有关部门报告。

第二十四条 网络运营者应用算法推荐技术提供互联网信息服务，应当落实算法安全主体责任，建立健全用户注册、信息发布审核、算法机制机理审核、安

全评估监测等管理制度，不得利用算法推荐服务传播法律、行政法规禁止的信息，不得设置诱导用户沉迷或者高额消费等违背公序良俗的算法模型。

第二十五条 省人民政府有关部门应当按照国家数据分类分级保护要求制定数据分类分级指南，对本部门以及相关行业、领域的数据进行分类分级管理。

省人民政府有关部门应当按照国家有关要求和标准，组织制定本部门以及相关行业、领域重要数据目录，对列入目录的数据进行重点保护。

本条例所称重要数据，是指一旦遭到篡改、破坏、泄露或者非法获取、非法利用，可能危害国家安全、公共利益的数据。

第二十六条 网络运营者开展数据处理活动应当按照网络安全等级保护制度的要求，履行下列数据安全保护义务：

(一)建立健全全流程数据安全管理制度，组织开展数据安全教育培训，采取相应的技术措施和其他必要措施，保障数据安全；

(二)加强风险监测，发现数据安全缺陷、漏洞等风险时， 应当立即采取补救措施；发生数据安全事件时，应当立即采取处置措施，按照规定及时告知用户并向网信、公安等有关部门报告；

(三)法律、行政法规规定的其他义务。

第二十七条 开展重要数据处理的网络运营者应当明确数据安全负责人和管理机构，制定实施数据安全保护方案和数据安全事件应急预案，自行或者委托数据安全服务机构每年开展一次数据安全风险评估，并向网信、公安等有关部门报送风险评估报告。

第二十八条 实施数据收集、存储、加工、使用、提供、交易、公开等活动，有关单位和个人应当落实数据安全保护责任，采取必要措施确保数据安全，不得实施以下行为：

(一)窃取或者以其他非法方式获取数据；

(二)泄露或者篡改收集、存储的个人数据；

(三)未经相关权利人同意，向他人出售或者提供个人数据；

(四)违反法律、行政法规或者约定的其他数据活动。

因数据开发利用需要，在合法收集个人数据后应当进行去标识化处理，并确保无法识别到特定个人。但是，依法需要信息溯源的除外。

第二十九条 为应对紧急状态或者重大突发事件，需要收集、交换、共享个人数据的，由突发事件处置部门按照有关法律法规处理，不得用于与应对紧急状态或者重大突发事件无关的目的。

第三十条 互联网公众账号信息服务平台应当履行信息内容和公众账号管理主体责任，配备与业务规模相适应的管理人员和技术能力，明确内容安全负责人岗位，建立健全并严格落实账号注册、信息内容安全、应急处置等管理制度。

互联网公众账号生产运营者应当履行信息内容生产和公众账号运营管理主体责任，建立健全全过程信息内容安全审核机制，维护网络传播秩序。

第三十一条 县级以上网信部门依法对互联网用户公众账号信息服务进行监督管理，管辖范围包括公众账号信息服务平台的工商登记地、主营业地， 以及公众账号生产运营者的账号注册地、账号实际运营地位于本行政区域的所有信息服务提供者。

互联网用户公众账号生产运营者的账号注册地、账号实际运营地不一致的，按照相关规定处理。

第三十二条 县级以上网信部门统筹协调有关部门完善个人信息保护投诉、举报工作机制，接受、处理与个人信息保护有关的投诉、举报， 开展个人信息保护宣传教育，指导、监督个人信息处理者开展个人信息保护工作， 组织对应用程序等个人信息保护情况进行测评，调查、处理违法个人信息处理活动， 支持有关机构开展个人信息保护评估、认证服务。

第三十三条 县级以上网信部门以及有关部门在履行网络安全和信息化监督管理职责中，发现网络或者数据处理活动存在较大安全风险或者可能发生安全事件的，可以按照法定的权限和程序对有关单位和个人进行约谈，指出存在的问题，提出整改要求。被约谈的单位和个人应当及时整改。

第三章 信息化促进

第三十四条 县级以上人民政府及其有关部门应当推进新一代移动通信网建设、光纤网优化布局和互联网升级， 推动物联网、工业互联网、卫星互联网等新基础设施建设，推进生产生活、城乡治理、应急预警等领域的场景应用。

省人民政府及其有关部门应当统筹建设卫星导航定位基准服务系统和配套基础设施，提供卫星导航定位基准信息公共服务。

第三十五条 省人民政府应当加强大型云平台、大数据中心等算力基础设施的统筹规划和优化布局，促进超级计算中心算力资源利用，避免重复建设和资源浪费。

县级以上人民政府及其有关部门、省通信管理机构应当推进智能计算中心、数据中心等算力基础设施建设。

第三十六条 县级以上人民政府及其有关部门应当协同推进人工智能、云计算、区块链等新技术基础设施建设， 支持关键核心技术突破，推动新技术及其产品、服务和解决方案的广泛应用。

第三十七条 省和设区的市、自治州人民政府应当明确本行政区域管理公共数据的责任部门。县级以上人民政府有关部门根据职责分工负责相关公共数据管理工作。

本条例所称公共数据，是指国家机关、事业单位和其他依法管理公共事务的组织以及提供教育、卫生健康、社会福利、供水、供电、供气、环境保护、公共交通等公共服务的组织(以下统称公共管理和服务机构)在依法履行职责或者提供公共服务过程中获取、产生、处理的数据。

第三十八条 省人民政府公共数据管理部门负责建立健全本省统一的公共数据资源目录，制定公共数据资源目录编制规范和公共数据共享、开放的具体办法。

省和设区的市、自治州人民政府公共数据管理部门应当组织公共管理和服务机构，按照编制规范编制公共数据资源目录、处理各类公共数据， 明确公共数据来源部门和管理职责。

第三十九条 省和设区的市、自治州人民政府公共数据管理部门应当建立和完善本行政区域的公共数据共享交换平台和开放平台，促进公共数据共享和开发利用。

公共数据应当按照规定在公共管理和服务机构之间实现共享或者协同应用。通过共享获得的公共数据，应当用于履行本单位职责，不得用于其他目的。

公共管理和服务机构应当按照需求导向、分类分级、统一标准、安全可控、便捷高效的原则共享和开放公共数据。鼓励使用公共数据从事科学技术研究、咨询服务、产品开发等活动。

公共数据采集单位对所采集数据的真实性、准确性、完整性负责。公共数据

管理部门发现公共数据不准确、不完整或者不同采集单位提供的数据不一致的，可以要求采集单位限期核实、更正。采集单位应当在要求的期限内核实、更正。

第四十条 向社会开放的公共数据，应当按照以下方式分类：

(一)涉及商业秘密、个人隐私， 或者法律法规规定不得开放的公共数据，列入非开放类；

(二)对数据安全和处理能力要求较高、时效性较强或者需要持续获取的公共数据，列入有条件开放类；

(三)其他公共数据列入无条件开放类。

非开放类公共数据依法进行脱密、脱敏处理或者相关权利人同意开放的， 可以列入无条件开放类或者有条件开放类。

第四十一条 县级以上人民政府应当明确本行政区域信息技术推广应用的目标和重点领域，推进信息技术与经济社会各领域深度融合。

省人民政府科技、工业和信息化、农业农村等部门应当在有关专项资金中安排一定比例用于引导和扶持相关领域信息技术的推广应用。

第四十二条 县级以上人民政府应当制定和完善促进信息产业发展的政策，优化信息技术与信息产业发展环境，支持新一代信息技术产业基地和园区建设，促进区域信息产业集群和产业链发展，培育产业新生态。

鼓励建立产学研用合作机制，联合研究、开发、推广信息技术产品和服务，推进创新成果的产业化。

第四十三条 县级以上人民政府及其有关部门应当结合本地区实际，推动新一代移动通信、信息技术应用创新、集成电路、移动互联网、区块链、数字文化创意等产业发展。

省人民政府工业和信息化部门应当会同有关部门编制和更新本省信息产业发展目录，定期公布信息产业关键技术和产品指南。

第四十四条 省网信部门应当会同有关部门引导和支持企业、科研机构、高等院校等围绕网络安全和信息化重点领域开展联合攻关，突破关键核心技术，加强知识产权布局，提升信息产业链、供应链的安全性和自主性。

省人民政府科技部门应当会同有关部门，编制和更新本省网络安全和信息化领域关键核心技术目录，安排关键核心技术研发资金。

第四十五条 省人民政府及其有关部门应当推动国家和省实验室、重点实验室、技术创新中心、制造业创新中心、工程研究中心等科技创新平台、文化创意平台、公共技术服务平台和大科学装置建设， 支持企业、科研机构、高等院校参与建设有关平台和设施，支持建设面向细分领域的创新平台。

第四十六条 信息产业领域社会组织应当加强行业服务，依法开展信息交流、企业合作、产业研究、人才培训、咨询评估等活动。

第四十七条 县级以上人民政府及其工业和信息化部门应当推动制造业数字化转型，针对先进制造业重点行业和领域，推动智能制造单元、智能生产线、智能车间、智能工厂建设， 支持企业在研发设计、生产制造、运营管理、营销服务等环节加强数字化改造、网络化协同、智能化升级。

县级以上人民政府及其有关部门应当推进工业互联网的应用，降低中小企业使用工业互联网成本，培育众创设计、网络众包、个性化定制、服务型制造等新模式。

第四十八条 县级以上人民政府及其农业农村、工业和信息化、商务等部门应当推动新一代信息技术与种植业、林业、畜牧业和渔业等深度融合， 加强数字乡村建设，推动农村仓储、物流、冷链设施的数字化建设，促进大数据、物联网、人工智能、区块链在农业生产、加工、经营中的运用。

支持大宗粮食和战略性经济作物生产过程使用智能农机装备，促进信息化与农机装备、作业生产、管理服务深度融合， 提高农机装备信息收集、智能决策和精准作业能力，保障粮食安全和重要农产品有效供给。

第四十九条 县级以上人民政府及其文化和旅游、市场监督管理等部门应当推进文化、旅游、餐饮、娱乐、家政等生活性服务业和数字技术深度融合， 整合利用线上线下资源，发展体验式消费、个性需求定制服务等新业态。

推进现代金融、快递物流、检验检测、法律服务、商务咨询、人力资源等生产性服务业数字化转型，支持行业内数字技术应用场景的开发和创新。

第五十条 县级以上人民政府及其商务、工业和信息化、农业农村等部门应当引导和支持电子商务平台、电子商务服务体系发展， 推动工业电子商务普及应用，发展农业电子商务，培育社交电子商务、直播电子商务等新业态新模式。

省人民政府及其有关部门应当加强跨境数字贸易交流合作，促进跨境电商综

合试验区、数字服务出口基地建设， 依托中国(湖南)自由贸易试验区建设数据跨境通道，依法开展数据跨境流动安全评估。

第五十一条 县级以上人民政府及其有关部门应当深化数字化改革，推动数字技术与政府履职全面深度融合，推进政务服务全流程“一网通办”，实现数据共享和业务协同，推进政府数字化转型。

省人民政府应当统筹全省政务网络基础设施建设，推动建设全省统一的政务基础网络，提升政务网络承载能力，统筹规划全省统一的政务云平台和政务大数据中心。

第五十二条 县级以上人民政府及其有关部门应当加强智慧城市建设，依托省和设区的市、自治州公共数据平台， 促进新一代信息技术在城市交通、生态环境保护、应急管理等领域的综合应用， 通过数据资源整合共享，实现城市运行态势监测、公共资源配置、宏观决策、统一指挥调度和事件分拨处置数字化，提升城市治理水平。

第五十三条 县级以上人民政府及其有关部门、残疾人联合会应当推进新一代信息技术在教育、医疗、养老、抚幼、助残等领域的应用，为学生、患者、老年人、残疾人等提供适用的数字化、智能化产品和服务， 促进基本公共服务均等化、便利化。

教育部门应当加强教育领域数字基础设施和数字校园建设，加强数字教育资源开发与应用。

卫生健康、医疗保障等部门和医疗机构应当加强智慧医疗健康体系建设， 促进和规范互联网医疗行业发展，实行医疗诊断、检验、检查和治疗信息共享， 拓展医疗保障数字化平台便民应用。

民政、卫生健康等部门应当加强智慧养老体系建设， 建立全省统一的智慧养老服务平台，提供简便快捷的养老服务。

第四章 法律责任

第五十四条 网络运营者违反本条例第二十三条规定，对法律、行政法规禁止发布或者传输的信息未停止传输、采取消除等处置措施、防止信息扩散、保存有关记录的，由县级以上网信部门或者有关部门根据管理权限责令改正，给予警告，没收违法所得；拒不改正或者情节严重的，处十万元以上五十万元以下罚款，

并可以责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证， 对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。

第五十五条 网络运营者不履行本条例第二十六条规定的数据安全保护义务的，由县级以上网信、公安等有关部门根据管理权限责令改正， 给予警告，可以并处五万元以上五十万元以下罚款，对直接负责的主管人员和其他直接责任人员可以处一万元以上十万元以下罚款；拒不改正或者造成大量数据泄露等严重后果的，处五十万元以上二百万元以下罚款，并可以责令暂停相关业务、停业整顿、吊销相关业务许可证，对直接负责的主管人员和其他直接责任人员处五万元以上二十万元以下罚款。

第五十六条 违反本条例第二十八条、第三十条规定，构成违反治安管理行为的，依法给予治安管理处罚；构成犯罪的，依法追究刑事责任。

第五十七条 县级以上人民政府及其有关部门有下列行为之一的，由上一级人民政府或者主管部门责令改正；情节严重的，对直接负责的主管人员和其他直接责任人员依法给予处分：

(一)未按规定履行公共数据共享开放职责的；

(二)未及时落实约谈整改要求的；

(三)未履行网络安全保护义务，发生网络安全事件的。

第五十八条 县级以上网信部门和其他有关部门工作人员玩忽职守、滥用职权、徇私舞弊的，依法给予处分；构成犯罪的，依法追究刑事责任。

第五章 附 则

第五十九条 本条例自 2022 年 1 月 1 日起施行。2004 年 7 月 30 日湖南省第十届人民代表大会常务委员会第十次会议通过、2012 年 5 月 31 日湖南省第十一届人民代表大会常务委员会第二十九次会议修订的《湖南省信息化条例》同时废止。

河南省网络安全条例

河南省第十三届人民代表大会常务委员会公告第 92 号

《河南省网络安全条例》已经河南省第十三届人民代表大会常务委员会第三十六次会议于 2022 年 11 月 26 日审议通过，现予公布，自 2023 年 6 月 1 日起施行。河南省人民代表大会常务委员会 2022 年 11 月 26 日附：《河南省网络安全条

例》

河南省网络安全条例

(2022 年 11 月 26 日河南省第十三届人民代表大会常务委员会第三十六次会议通过)

第一章 总 则

第一条 为了保障网络安全，维护国家安全和社会公共利益，保护自然人、法人和非法人组织的合法权益，促进经济社会高质量发展，根据《中华人民共和国网络安全法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》等有关法律、行政法规，结合本省实际，制定本条例。

第二条 本省行政区域内网络安全的建设、保障、监管，以及网络使用、网络数据处理等活动，适用本条例。

涉密网络及其数据的安全保护，按照国家法律、行政法规的规定执行。

第三条 网络安全工作应当贯彻总体国家安全观，坚持网络安全与信息化发展并重，遵循统筹规划、综合治理、科学发展、确保安全的原则。

第四条 县级以上人民政府应当将网络安全纳入国民经济和社会发展规划，加大对网络安全建设维护的投入，建立健全网络安全机构，加强网络安全执法队伍建设，完善网络安全工作综合协调机制，解决网络安全重大问题，提升网络安全保障能力。

第五条 县级以上网信部门是网络安全工作的主管部门，负责统筹协调网络安全工作和相关监督管理工作。

县级以上工业和信息化、公安、保密管理、密码管理部门和国家安全机关、省电信管理机构等，应当在各自职责范围内负责网络安全保护和监督管理工作。

第六条 网络相关行业组织应当按照章程，加强行业自律，指导会员落实国家网络安全制度，加强网络安全保护，促进行业健康发展。

第七条 网络运营者、网络数据处理者和个人信息处理者应当遵守法律、法规，尊重社会公德和伦理，遵守商业道德和职业道德，诚实守信，履行网络安全保护义务，承担社会责任，接受政府和社会监督。

第八条 任何个人或者组织使用网络不得违反法律、法规，不得危害网络安全，不得利用网络危害国家安全和社会公共利益，不得利用网络扰乱经济秩序和

社会秩序，不得利用网络侵害他人合法权益。

任何个人或者组织对危害网络安全的行为，有权投诉、举报。收到投诉、举报的部门应当及时处理。

第九条 国家机关、人民团体、企业事业单位、新闻媒体应当以社会主义核心价值观为导向，倡导健康文明的网络行为，引导全社会依法办网、文明上网、安全用网，提高网络安全防范意识，营造共同维护网络安全的良好环境。

第十条 县级以上人民政府应当对在网络安全工作中做出突出贡献的个人和组织，按照有关规定给予表彰和奖励。

第二章 网络安全建设

第十一条 县级以上网信部门应当会同有关部门，根据上级网络安全规划以及本行政区域国民经济和社会发展规划，编制网络安全规划，报同级网络安全和信息化委员会同意后实施，并报上一级网信部门备案。

第十二条 省人民政府标准化部门和省网信、行政审批政务信息管理等部门应当根据各自职责，组织网络安全标准的宣传、推广和应用。

鼓励高等院校、科研机构、企业、行业组织等参与网络安全国家标准、行业标准的制定工作。

第十三条 县级以上人民政府应当安排网络安全专项资金，扶持重点网络安全技术产业和项目。

省人民政府设立的互联网产业发展基金，应当支持网络安全建设运营。

鼓励金融机构支持网络安全技术创新和产业发展。

第十四条 省人民政府及有关部门应当支持省实验室和省级以上工程技术研究中心、技术创新中心、重点实验室等， 开展网络安全技术研究，加强网络安全平台建设。

鼓励和支持高等院校、科研机构、企业参与网络安全技术创新项目和网络安全平台建设。

第十五条 省人民政府应当支持网络安全技术的研发和应用，重点支持安全芯片设计制造、网络安全态势感知、网络安全自主防御等关键技术攻关； 推动网络安全技术产品升级，支持新技术在网络安全领域的应用，推广安全可信的网络产品和服务。

省人民政府及有关部门应当支持网络安全相关企业、高等院校、科研机构协同开展关键技术攻关，引导网络安全产业集聚，推动网络安全技术应用与网络安全产业融合发展。

第十六条 省人民政府及有关部门应当指导支持高等院校、职业学校开设网络安全相关专业、课程， 建设国家一流网络安全学院；鼓励高等院校、科研机构与企业共建网络安全实训基地，加强人才交流。

县级以上人民政府及有关部门应当将网络安全高层次、高技能以及紧缺人才纳入人才体系，在住房、职称评定以及配偶就业、子女入学等方面提供支持。

第十七条 县级以上人民政府及有关部门应当组织开展经常性网络安全宣传教育活动，指导支持教育机构、大众传媒、行业组织、专业机构等做好网络安全宣传工作，提高全社会网络安全意识和防护能力。

国家机关、人民团体、企业事业单位应当建立健全网络安全培训制度。鼓励社会力量、网络安全企业开展网络安全培训。

县级以上人民政府教育部门、学校应当加强青少年网络安全教育， 推进网络安全知识技能进校园、进课堂，增强青少年网络安全意识。

第十八条 省、设区的市人民政府应当推进网络安全社会化服务体系建设。

鼓励支持符合条件的企业、机构依法开展网络安全规划咨询、安全集成、安全认证、产品检测、风险评估、应急响应、容灾备份等网络安全服务。

第三章 网络安全保障

第十九条 县级以上网信、公安等有关部门应当指导督促网络运营者落实关键信息基础设施安全保护、网络安全等级保护、数据安全保护、个人信息保护、密码应用安全性评估、云计算服务安全评估、网络信息安全投诉举报等制度， 落实相关国家标准的强制性要求，制定网络安全事件应急预案。

第二十条 本省对国家关键信息基础设施按照有关法律、行政法规，予以重点保护。

县级以上人民政府应当在网络安全等级保护制度的基础上，对本行政区域内未列入国家关键信息基础设施的重要信息系统加强保护。重要信息系统的范围和识别指南由省网信部门会同公安等部门制定。省人民政府行业主管部门负责制定本行业、本领域的重要信息系统认定规则， 根据认定规则识别本行业、本领域的

重要信息系统，通知网络运营者，并向省网信、公安部门报送识别结果。

第二十一条 网信部门应当统筹协调有关部门建立重要信息系统网络安全信息共享机制，会同行业主管部门检查、检测重要信息系统安全风险， 对重要信息系统领域的网络安全事件应急处置与网络功能恢复等，提供技术支持和指导。

行业主管部门负责指导和监督本行业、本领域重要信息系统安全保护工作，建立健全网络安全监测预警机制和网络安全事件应急预案，定期组织开展网络安全检查监测、应急演练。

第二十二条 重要信息系统建设应当确保具有支持业务稳定、持续运行的性能；网络安全技术措施应当与重要信息系统同步规划、同步设计、同步建设、同步验收、同步使用，确保网络安全、数据安全和信息安全。

第二十三条 重要信息系统运营者应当履行下列安全保护义务：

(一)建立健全网络安全管理制度，明确安全管理负责人；

(二)对重要信息系统设计、建设、运行、维护等服务实施安全管理；

(三)对重要信息系统和数据库采取容灾备份和加密等措施；

(四)编制网络安全事件应急预案，定期开展应急演练；

(五)法律、法规规定的其他义务。重要信息系统运营者应当履行网络安全保护主体责任。运营者采购网络产品和服务， 应当按照规定与提供者签订协议，明确提供者的技术支持、网络安全运行维护和安全保密责任，并对其履行监督责任。

第二十四条 省人民政府有关部门应当根据国家数据分类分级保护制度要求，对本行业、本领域的网络数据实行分类分级管理， 确定本行业、本领域重要数据具体目录，对列入目录的网络数据进行重点保护。

省人民政府行业主管部门确定的重要数据具体目录应当报省网信部门备案。省网信部门应当及时和公安、国家安全等有关部门共享备案信息。

第二十五条 网络数据处理者开展网络数据处理活动应当履行下列安全保护义务：

(一)制定管理制度和操作规程，合理确定网络数据处理的操作权限；

(二)采取安全技术措施和其他必要措施保障网络数据安全以及网络数据处理系统、存储环境等安全；

(三)加强风险监测，发现存在网络数据安全缺陷、漏洞时， 应当立即采取补

救措施；

(四)发生网络数据安全事件时，应当立即采取处置措施，及时告知利害关系人，并按照规定向设区的市级以上行业主管部门和网信、公安部门报告；

(五)法律、法规规定的其他义务。

第二十六条 网络运营者应当加强对用户发布信息内容的管理，建立健全用户注册、信息发布审核机制， 发现法律、行政法规禁止发布或者传输的信息， 应当立即停止传输，采取消除等处置措施，防止信息扩散，保存有关记录，并向属地网信、公安等有关部门报告。

网络运营者应用算法推荐技术提供互联网信息服务，应当履行算法安全主体责任，不得利用算法推荐服务传播法律、行政法规禁止的信息， 不得设置违反法律、行政法规或者违背公序良俗、公平竞争的算法模型。

第二十七条 提供平台服务的网络运营者应当建立保障数据安全的平台规则和隐私保护制度，不得损害公平竞争，不得侵害用户合法权益。

第二十八条 任何个人或者组织应当对其使用网络的行为负责，在网络上发布信息应当遵守法律法规、社会公德和公序良俗， 不得利用网络制作、发布、传播法律、行政法规禁止发布或者传输的信息。

第二十九条 利用网络收集、使用个人信息，应当遵循合法、正当、必要和诚信等原则，明示收集、使用信息的目的、方式和范围等事项，履行告知义务，并取得本人或者监护人同意；法律、行政法规另有规定的除外。

处理的个人信息应当为履行法定职责或者提供服务、产品所必需， 不得过度收集个人信息；不得因个人不同意提供非必需的个人信息，拒绝提供服务或者产品。

第三十条 利用网络处理个人信息应当采取下列措施，确保个人信息处理活动符合法律、行政法规的规定：

(一)制定管理制度和操作规程；

(二)对个人信息实行分类管理；

(三)采取相应的加密、去标识化、匿名化等安全技术措施；

(四)发生个人信息泄露、篡改、丢失的， 应当立即采取补救措施，通知当事人，并向设区的市级以上行业主管部门和网信、公安部门报告；

(五)法律、行政法规规定的其他措施。

第三十一条 任何个人或者组织不得非法侵入、干扰、攻击、破坏网络，不得实施窃取、泄露、篡改以及非法获取、公开、交易网络数据等危害网络安全的行为。

第四章 网络安全监管

第三十二条 县级以上网信部门和有关部门依法在各自职责范围内负责网络运行安全、网络数据安全、网络信息安全工作。

第三十三条 县级以上网信部门负责统筹协调本行政区域内网络安全保障体系建设、网络安全监测预警和应急处置工作； 统筹协调关键信息基础设施和重要信息系统安全保护、网络数据和个人信息安全保护工作； 依法组织开展网络运行安全、网络数据安全、网络信息安全的监督管理和执法工作。

县级以上网信部门根据需要，可以会同有关部门开展网络安全联合执法、案件督办等工作。

第三十四条 县级以上人民政府工业和信息化部门负责工业领域网络安全的监督管理工作。

无线电管理机构负责无线电干扰查处相关工作。

第三十五条 县级以上人民政府公安部门负责指导、监督、检查网络安全等级保护、关键信息基础设施安全保护和重要信息系统保护工作； 依法查处涉及网络安全的违法犯罪行为。

第三十六条 保密管理部门负责指导监督机关、单位网络保密工作；负责对涉密网络及关键信息基础设施运营者采购保密设备、产品和服务的保密监管； 负责涉密信息系统的测评审查和风险评估等安全保密工作；负责对各类网络进行保密监测预警和保密检查；负责各类网络失泄密案件的查处及危害评估和密级鉴定。

第三十七条 密码管理部门会同有关部门查处网络信息系统密码失泄密事件和违法违规研制、使用密码行为； 负责全省涉密网络密码规划管理；负责关键信息基础设施、重要信息系统密码应用推进和监督管理； 负责管理全省商用密码应用安全性评估工作；会同有关部门建立密码安全监测预警、风险评估、信息通报、重大事项会商和分级响应等协作机制。

第三十八条 省、设区的市国家安全机关负责开展网络反间谍安全防范指导、

检查及反间谍技术防范检查检测、处置等相关工作。

第三十九条 省电信管理机构负责指导督促电信企业和互联网企业落实网络与信息安全管理责任，依据职责权限组织开展电信网和互联网网络安全监督检查、监测预警、风险评估、威胁治理、信息通报、应急管理与处置等工作。

第四十条 县级以上行业主管部门指导监督本行业、本领域的网络安全保障工作，负责本行业、本领域的关键信息基础设施和重要信息系统安全保护， 承担本行业、本领域网络数据安全监管职责， 依法定期开展网络安全检查，开展网络安全隐患排查，处置网络安全事件，并及时将情况通报同级网信部门。

第四十一条 各级国家机关应当按照属地管理和谁主管谁负责的原则，落实网络安全工作责任制，建立健全网络安全工作体系，提升网络安全保障能力，确保关键信息基础设施、重要信息系统、网络运行、网络数据和网络信息的安全可控。

第四十二条 网信、公安、国家安全及有关主管部门依法履行网络安全监管职责时，网络运营者、网络数据处理者、个人信息处理者应当予以配合。

第四十三条 县级以上网信部门应当按照网络安全监测预警和信息通报制度要求，统筹协调有关部门加强网络安全信息收集、分析和通报工作， 按照规定统一发布网络安全监测预警信息。

行业主管部门应当建立健全本行业、本领域的网络安全监测预警和信息通报制度，与同级网信部门共享本行业、本领域的网络安全信息。

第四十四条 省、设区的市网信部门负责统筹协调本行政区域内网络安全事件应急处置工作，建立健全跨区域、跨部门、跨行业的联动处置机制。公安、电信管理等部门在职责范围内负责相关网络安全事件处置工作。能源、电信、交通等行业应当为网络安全事件应急处置与网络功能恢复提供重点保障和支持。

第四十五条 县级以上网信部门发现网络存在较大安全风险或者发生网络安全事件的，可以依法约谈相关网络运营者、网络数据处理者、个人信息处理者的法定代表人或者主要负责人。被约谈者应当按照有关要求及时消除网络安全风险、妥善处置网络安全事件，及时处置法律、行政法规禁止发布或者传输的信息。

第四十六条 省、设区的市网信部门应当建立健全网络安全投诉、举报制度，建立投诉举报平台，公开投诉举报电话，接受社会各界对危害网络安全行为的投

诉举报。对属于本部门职权范围内的，应当在三十日内办结并答复；情况复杂的，经单位负责人同意可以延长三十日。对不属于本部门职权范围内的投诉举报， 应当在三日内转有关部门办理。有关部门应当在上述时间内办结并答复投诉人、举报人，并向网信部门反馈办理结果。

网信部门及其他有关部门应当为投诉人、举报人保密， 保护投诉人、举报人的合法权益。

第四十七条 省、设区的市人民政府应当将网络安全工作纳入高质量发展综合绩效考核体系，建立绩效考核指标，对下级人民政府进行网络安全工作考核。

第五章 法律责任

第四十八条 违反本条例规定的行为，法律、行政法规已有法律责任规定的，从其规定。

第四十九条 违反本条例第二十三条第一款规定，重要信息系统运营者未履行安全保护义务的，由县级以上网信、公安部门根据管理权限责令改正， 给予警告；拒不改正或者导致危害网络安全等后果的，处五万元以上十万元以下罚款，对直接负责的主管人员处一万元以上五万元以下罚款。

第五十条 违反本条例第二十九条第一款规定，利用网络收集、使用个人信息未依法履行告知义务，未依法取得本人或者监护人同意的，由县级以上网信部门责令改正，给予警告，没收违法所得，对违法收集、使用个人信息的应用程序，责令暂停提供服务；拒不改正的，责令终止提供服务，并处十万元以上一百万元以下罚款；对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。

有前款规定的违法行为，情节严重或者造成严重后果的，由省网信部门责令改正，没收违法所得，并处一百万元以上五千万元以下或者上一年度营业额百分之五以下罚款；对直接负责的主管人员和其他直接责任人员处十万元以上一百万元以下罚款，并可以禁止其在五年内担任相关企业的董事、监事、高级管理人员和个人信息保护负责人。

第五十一条 违反本条例第三十条第一项至三项规定的，由县级以上网信部门责令改正；拒不改正的，处一万元以上五万元以下罚款。

违反本条例第三十条第四项规定，发生个人信息泄露、篡改、丢失事件， 未

立即采取补救措施的，由县级以上网信部门责令改正，并处十万元以上一百万元以下罚款，对直接负责的主管人员和其他直接责任人员处一万元以上五万元以下罚款；情节严重或者造成严重后果的，按照本条例第五十条第二款规定执行。未通知当事人并向设区的市级以上行业主管部门和网信、公安部门报告的， 由县级以上网信部门责令改正；拒不改正的，处一万元以上五万元以下罚款。

第五十二条 国家机关及其工作人员有下列情形之一的，由其上级机关或者网信部门责令改正；对直接负责的主管人员和其他直接责任人员，按照管理权限依法给予处分；构成犯罪的，依法追究刑事责任：

(一)未按照要求受理投诉举报或者反馈办理结果的；

(二)未履行网络安全保护义务，发生较大以上网络安全事件的；

(三)收集与履行法定职责无关的个人信息的；

(四)将履行工作职责中获取的信息用于其他不当用途的。

第六章 附 则

第五十三条 本条例自 2023 年 6 月 1 日起施行。

贵州省大数据安全保障条例

贵州省人民代表大会常务委员会公告 2019 第 9 号

《贵州省大数据安全保障条例》已于 2019 年 8 月 1 日经贵州省第十三届人民代表大会常务委员会第十一次会议通过，现予公布，自 2019 年 10 月 1 日起施行。

贵州省人民代表大会常务委员会

2019 年 8 月 1 日

贵州省大数据安全保障条例

(2019 年 8 月 1 日贵州省第十三届人民代表大会常务委员会第十一次会议通过)

目 录

第六章 附 则

第一章 总 则

第一条 为了保障大数据安全和个人信息安全，明确大数据安全责任，促进大数据发展应用，根据《中华人民共和国网络安全法》和有关法律、法规的规定，结合本省实际，制定本条例。

第二条 本省行政区域内大数据安全保障及相关活动，应当遵守本条例。

涉及国家秘密的大数据安全保障，还应当遵守《中华人民共和国保守国家秘密法》等法律、法规的规定。

第三条 本条例所称大数据安全保障，是指采取预防、管理、处置等策略和措施，防范大数据被攻击、侵入、干扰、破坏、窃取、篡改、删除和非法使用以及意外事故，保障大数据的真实性、完整性、有效性、保密性、可控性并处于安全状态的活动。

本条例所称大数据是指以容量大、类型多、存取速度快、应用价值高为主要特征的数据集合，是对数量巨大、来源分散、格式多样的数据进行采集、存储和关联分析，发现新知识、创造新价值、提升新能力的新一代信息技术和服务业态。

本条例所称大数据安全责任人，是指在大数据全生命周期过程中对大数据安全产生或者可能产生影响的单位和个人，包括大数据所有人、持有人、管理人、使用人以及其他从事大数据采集、存储、清洗、开发、应用、交易、服务等的单位和个人。

第四条 大数据安全保障工作坚持总体国家安全观，树立正确的网络安全观，按照政府主导、责任人主体，统筹规划、突出重点，预防为主、综合治理，包容审慎、支持创新， 安全与发展、监管与利用并重的原则， 维护大数据总体和动态安全。

第五条 大数据安全保障工作应当围绕国家大数据战略和省大数据战略行动实施，建立健全大数据安全管理制度，建设大数据安全地方标准体系、大数据安全测评体系、大数据安全保障体系等，采取大数据安全攻防演练等安全保障措施，推动大数据安全技术、制度、管理创新和发展。

第六条 省人民政府负责全省大数据安全保障工作，市、州和县级人民政府负责本行政区域内大数据安全保障工作。

开发区、新区管理机构根据设立开发区、新区的人民政府的授权， 负责本辖区大数据安全保障的具体工作。

第七条 县级以上有关部门按照下列规定，履行大数据安全保障职责：

(一)网信部门负责统筹协调、检查指导和相关监督管理等工作；

(二)公安机关负责安全保护和管理、风险评估、监测预警、应急处置和违法行为查处等监督管理工作；

(三)大数据发展管理部门负责与大数据安全相关的数据管理、产业发展、技术应用等工作；

(四)通信管理部门负责电信网、公共互联网运行安全监督管理等工作；

(五)保密行政管理部门负责保密监督管理等工作；

(六)密码管理部门负责密码监督管理等工作；

(七)其他部门按照有关法律、法规的规定和各自职责做好大数据安全保障工作。

第八条 省人民政府应当根据大数据发展应用总体规划，编制大数据安全保障规划；网信、公安、大数据发展管理等部门应当根据大数据安全保障规划， 编制本部门、本行业大数据安全保障专项规划。

第九条 县级以上人民政府应当建立大数据安全保障工作领导协调机制和责任机制，协调和指导本行政区域内大数据安全保障有关事项。

公安机关应当按照网络安全等级保护要求，会同有关部门制定大数据风险测评、应急防范等安全制度， 加强对大数据安全技术、设备和服务提供商的风险评估和安全管理。

第十条 任何单位和个人都有维护大数据安全的义务，不得从事危害大数据安全的活动，不得利用大数据从事危害国家安全以及损害国家利益、社会公共利益和他人合法权益的活动。

对危害大数据安全或者利用大数据从事违法犯罪活动的行为，任何单位和个人都有权劝阻、制止、投诉、举报。收到投诉举报的部门应当依法及时查处， 保护举报人的合法权益；不属于本部门职责的，应当及时移送有权处理的部门。

第十一条 鼓励开展大数据安全知识宣传普及、教育培训，增强全社会大数据安全意识，提高大数据安全风险防范能力。

第十二条 鼓励、支持成立大数据安全联盟、行业协会等社会组织，开展行业自律、交流合作和安全技术研究等大数据安全工作。

第二章 安全责任

第十三条 实行大数据安全责任制，保障大数据全生命周期安全。

大数据安全责任，按照谁所有谁负责、谁持有谁负责、谁管理谁负责、谁使用谁负责以及谁采集谁负责的原则确定。

大数据基于复制、流通、交换等同时存在的多个安全责任人， 分别承担各自安全责任。

第十四条 大数据安全责任人是单位的(以下简称单位大数据安全责任人)，应当履行下列职责：

(一)依法成立安全管理机构或者明确安全管理负责人，定期对从业人员进行安全教育、技术培训和技能考核；

(二)制定安全管理制度、操作规程、应急预案，明确不同岗位安全管理责任；

(三)加强数据采集、使用、处理权限管理， 对批量导出、复制、脱敏、销毁数据等实行审查批准；

(四)加强网络运行、访问监测管理，定期开展数据安全检查；

(五)采取数据分类、备份和加密等安全措施；

(六)按照规定期限留存相关的网络日志；

(七)发生数据安全事件时，立即采取措施，保存证据，并及时向行业主管部门和公安机关报告；

(八)发现违法发布或者传输信息的，立即停止发布、传输或者采取阻断、拦截等措施，保留有关记录，并及时向行业主管部门和公安机关报告；

(九)法律、法规规定的其他职责。

大数据安全责任人是个人的(以下简称个人大数据安全责任人)，应当依法采取安全管理措施，妥善存储、保管，合理使用，保障大数据安全。

第十五条 单位大数据安全责任人采集、存储、传输、处理、交换、应用、销毁大数据等，应当根据网络安全等级保护要求，建立大数据安全防护管理制度、大数据安全审计制度，制定大数据安全应急预案，落实安全管理责任，并定期开展安全评测、风险评估和应急演练； 采取安全保护技术措施，防止数据丢失、毁

损、泄露和篡改。

前款规定活动涉及个人信息的，还应当遵守法律、法规关于个人信息保护的规定。

第十六条 采集数据应当具有合法目的和用途，遵循最小且必要和正当原则，禁止过度采集；科学确定采集对象、范围、内容、方式， 依法进行采集，并保证数据的真实性、完整性、保密性。

国家机关采集数据应当经被采集人同意，法律、法规另有规定的除外。

采集数据不得侵犯国家秘密、商业秘密和个人信息， 不得损害被采集人和他人合法权益。

除法律、法规另有规定外， 向不特定公众提供普遍信息、接入、浏览、访问、营销、推广等网络服务的经营者， 不得采集与其提供服务无关的数据，不得以使用人拒绝提供相关信息而限制或者拒绝其享受普遍服务。

第十七条 除法律、法规另有规定外，任何单位和个人在公共场所设置数据采集设施、设备采集信息的， 应当设置明显标识，并报当地公安机关备案。留存的数据应当用于合法目的，不得非法向他人提供、查阅、复制和传播。

第十八条 存储数据应当根据数据类型、规模、用途、安全等级、重要程度等因素，选择相应安全性能和防护级别的系统、介质、设施设备， 采取技术和管理措施，保障存储系统和数据安全。

公共数据平台、企业数据中心等集中式大数据存储中心， 应当根据国家相关技术标准、规范要求和保障数据安全需要，科学选址，规范建设，建立容灾备份、安全评价、日常巡查管理、防火防盗等安全管理制度， 加强存储环境、供电、通信和存储系统、介质、设施设备安全审查。

第十九条 传输数据应当合理选择传输渠道，采取必要的安全措施，防止数据被窃取、泄露、篡改。

第二十条 处理数据应当保护原始数据，不得随意更改、伪造，不得通过恶意处理导致数据毁灭性更改和永久性丢失。

第二十一条 交换数据应当维护数据的完整性、可用性。交换数据应当合法进行，交换双方不得假冒他人或者以其他方式骗取数据交换。

第二十二条 使用数据不得用于非法目的和用途。明知是通过攻击、窃取、

恶意访问等非法方式获取的数据，不得使用。

使用数据开展广告宣传、营销推广等活动，不得干扰被采集人正常生产生活，不得损害被采集人及他人合法权益。

第二十三条 销毁数据应当根据大数据安全保护管理需要，合理确定销毁方式和销毁要求。销毁公共数据、涉及商业秘密和个人信息等重要数据的， 应当进行安全风险评估。

第二十四条 单位大数据安全责任人应当加强数据内容管理，定期清理、审查数据内容，发现其持有、管理、发布的数据含有违法内容的， 应当及时予以处理，并采取相关补救措施；超出自身处理权限的，应当立即停止使用，告知数据提供人并向公安机关报告。

第二十五条 为他人提供基础网络、互联网数据中心或者系统服务的网络运营者，应当建立安全监测预警平台，加强对服务对象的数据安全管理，督促其建立安全管理制度，落实安全监测保护技术措施。

开展互联网平台和数据空间等租赁业务的，出租人应当将租赁信息依法报通信管理部门备案，通信管理部门应当将备案信息与公安机关共享。未经出租人同意，承租人不得擅自转租。涉及互联网数据中心业务和互联网接入服务业务的，应当遵守有关法律、法规的规定。

第二十六条 各级人民政府及有关部门和公共机构、公共服务企业因信息公开、数据开放以及公示、公告等需要公布企业、个人数据的， 应当采取脱密、脱敏等措施，防止泄露国家秘密、商业秘密和个人信息。

第二十七条 银行、保险、房地产、航空、铁路、公路、供电、供水、供气、邮政、通信、快递、电子商务、旅游服务等经营者和学校、医疗机构、社保、户籍管理、车辆登记、公积金、社会信用管理等单位， 应当加强内部管理，建立数据接触、访问审查等制度，明确数据提供、调用、分析、处理等权限。

前款规定单位在经营、服务活动中获取的用户数据， 除依法共享开放外，单位及其工作人员不得泄露，不得出售或者非法向他人提供。

第二十八条 禁止发布、传播下列信息：

(一)危害国家主权、安全和发展利益；

(二)损害社会公共利益和他人合法权益；

(三)煽动民族仇恨、民族歧视;

(四)黄、赌、毒等违法犯罪信息;

(五)法律、法规禁止的其他信息。

第二十九条 禁止非法采集、窃取、存储、传输、使用、买卖个人信息。

第三十条 采集、存储、使用、处理人脸、指纹、基因、疾病等生物特征数据，应当遵守法律、法规的规定， 不得危害国家安全、公共安全， 不得侵犯个人合法权益。

第三十一条 单位大数据安全责任人因公共数据共享开放提供数据，基于提供时的合理预见无安全风险的，提供人不承担相关责任。

通过大数据分析、挖掘、整合等取得的数据或者得出的结论， 可能危害国家安全、损害国家利益、社会公共利益的， 不得使用、传播， 并应当立即停止相关活动，报公安机关依法予以处理。

第三章 监督管理

第三十二条 省人民政府应当建立统一的大数据安全监管平台，负责大数据安全信息收集、分析评估和通报， 监测大数据安全状况，发布大数据安全监测预警信息，统筹协调大数据安全事件处置。

行业主管部门负责监测本行业、本领域大数据安全状况， 发布相关信息，督促、指导本行业、本领域的大数据监测预警处置工作。

关键信息基础设施运营者、公共数据平台、企业数据中心等集中式大数据存储中心以及其他重要大数据安全责任单位，应当建立大数据安全监测预警平台，负责监测本单位大数据安全状况，发布相关信息。

第三十三条 县级以上公安机关应当加强大数据安全风险分析、预测、评估，收集相关信息；发现可能导致较大范围黑客攻击、病毒蔓延等大数据安全事件的，应当及时发布预警信息，提出防范应对措施，指导、监督大数据安全责任人做好安全防范工作。

第三十四条 行业主管部门、关键信息基础设施和重要信息系统运营单位发现本行业、本单位大数据安全事件发生的风险增大时， 应当加强监测，及时收集相关信息，开展安全风险分析评估，发布风险预警，并采取避免、减轻危害的措施。

第三十五条 单位大数据安全责任人的应急预案应当包括大数据安全事件应急处置的组织机构及其职责、安全事件分级、应急响应程序、处置措施等内容，并定期组织演练。

关键信息基础设施运营者、公共数据平台、企业数据中心等集中式大数据存储中心以及其他重要单位大数据安全责任人的应急预案，应当报行业主管部门和县级以上公安机关备案。

第三十六条 发生大数据安全事件时，安全责任人应当及时启动应急预案，采取相应处置措施，防止危害扩大，告知可能受到影响的用户，并向行业主管部门和县级以上公安机关报告。行业主管部门和县级以上公安机关应当根据事件的性质和特点，及时予以处置并依法发布相关信息。

处置大数据安全事件时应当保护现场，记录并留存相关数据信息。

第三十七条 县级以上公安机关应当建立大数据安全日常监测制度，加强对大数据安全责任人履行安全职责情况的巡查、检查， 指导、监督安全责任人建立安全管理制度，加强安全风险防范，落实安全保障责任。

县级以上公安机关发现有关单位和个人安全管理责任落实不到位，存在较大安全风险或者可能发生安全事件的，应当及时提出整改意见并督促落实。

第三十八条 建立大数据安全情况报告制度。关键信息基础设施经营者、公共数据平台、企业数据中心等集中式大数据存储中心以及其他重要单位大数据安全责任人，应当定期向行业主管部门和县级以上公安机关报告大数据安全情况。

第三十九条 有关部门因履行职责需要，按照有关法律、法规的规定要求提供掌握的宏观经济、社会管理、网络安全等数据的， 有关单位和个人应当及时提供。

除依法共享开放外，有关部门不得将前款规定的数据用于与履行职责无关的用途。

第四十条 大数据安全责任人应当协助公安机关、国家安全机关依法查处危害国家安全、公共安全及其他犯罪行为， 为预防、侦查危害国家安全、公共安全及其他犯罪活动提供相关资料、数据和技术接口等支持。

大数据安全责任人按照前款规定或者公安机关、国家安全机关的要求采集的数据，未经公安机关、国家安全机关同意，不得自行处理、使用或者向他人提供。

第四十一条 县级以上社会信用管理部门应当建立大数据安全诚信档案，记录大数据安全责任人数据采集、管理、使用等信用信息， 并按照有关规定纳入社会信用体系。

第四章 支持与保障

第四十二条 省人民政府应当支持大数据安全技术创新，推进大数据安全产业基地、园区和大数据安全城市建设， 推动形成大数据安全产品研发、生产、应用的大数据安全产业链。

市、州和县级人民政府应当采取相应措施， 引导、扶持、推动大数据安全相关产业、技术、产品发展应用。

鼓励高等院校、科研机构和企业事业单位加大大数据安全技术研发投入， 开展大数据安全技术创新研究和大数据安全关键技术攻关，形成自主知识产权，推动科技成果转化。

第四十三条 省人民政府标准化部门应当会同有关部门制定并适时修订有关大数据安全以及大数据产品、服务和运行安全的地方标准， 建立和完善大数据安全地方标准体系。

鼓励和支持企业、科研机构、高等院校和相关行业组织开展大数据安全相关标准的研究、制定和协同攻关，推动形成国家、行业和地方标准。

第四十四条 县级以上人民政府设立的大数据发展应用专项资金、大数据发展基金、科技成果转化资金等， 对大数据安全技术研发及成果转化应用、安全规范和安全标准制定、安全监测预警平台建设、安全保障体系建设、容灾备份体系建设、安全意识培训等，应当给予支持。

符合国家税收优惠政策规定的大数据安全企业，依法享受税收优惠。

鼓励金融机构创新金融产品，完善金融服务，支持大数据安全相关产业、技术、产品发展应用。

第四十五条 县级以上人民政府应当加强大数据安全监督管理人才队伍建设，鼓励和支持大数据安全及相关领域专业人才的培养、引进。

支持高等院校、科研机构大数据安全学科、专业等建设， 开设大数据安全相关课程；创新教育培养模式，开展校企合作办学，实行订单式培养，为大数据安全提供人才支撑。

第四十六条 县级以上人民政府应当加强实体经济企业大数据安全体系建设引导，支持实体经济企业与大数据深度融合，加强实体经济企业信息化、大数据应用系统的安全保障能力和安全防护意识。

第四十七条 县级以上人民政府推进大数据安全社会化服务体系建设，鼓励和支持企业开展安全测评、电子认证、数据加密、容灾备份等数据安全服务。

第四十八条 鼓励企业事业单位使用符合大数据安全要求的产品、技术、服务，并依法享受优惠政策。

第四十九条 鼓励和支持建立大数据安全实验室、大数据安全靶场、技术验证基地等，开展大数据及网络安全攻防演练，对大数据安全新技术、新应用、新产品进行测试、检验。

第五章 法律责任

第五十条 违反本条例第十四条第一款、第十五条第一款、第二十四条、第二十七条第一款、第三十一条第二款的，由有关部门或者县级以上公安机关责令改正，给予警告；拒不改正或者导致危害大数据安全等后果的，处以 1 万元以上 10 万元以下罚款，对直接负责的主管人员处以 5000 元以上 5 万元以下罚款。

第五十一条 违反本条例第十六条第一款、第二款规定，过度采集数据或者采集数据未经被采集人同意的，由有关部门或者县级以上公安机关责令改正，给予警告；拒不改正的，处以 5000 元以上 5 万元以下罚款，对直接负责的主管人员处以 1000 元以上 1 万元以下罚款；造成损失的，依法予以赔偿。

违反本条例第十六条第三款规定的，由有关部门或者县级以上公安机关责令改正，给予警告；拒不改正的，处以 1 万元以上 10 万元以下罚款，对直接负责的主管人员处以 5000 元以上 5 万元以下罚款。

第五十二条 违反本条例第十七条规定的，由有关部门或者县级以上公安机关责令改正，给予警告；拒不改正，或者擅自向他人提供、查阅、复制、传播留存的数据且情节严重的，可处以 5000 元以上 5 万元以下罚款，对直接负责的主管人员处以 1000 元以上 1 万元以下罚款。

第五十三条 违反本条例第十八条、第十九条、第二十条、第二十一条规定的，由有关部门或者县级以上公安机关责令改正，给予警告。

违反本条例第十八条第二款规定，拒不改正或者导致危害大数据安全等后果

的，由有关部门或者县级以上公安机关处以 10 万元以上 100 万元以下罚款，对直接负责的主管人员处以 1 万元以上 10 万元以下罚款。

第五十四条 违反本条例第二十二条规定的，由有关部门或者县级以上公安机关责令改正，给予警告，没收违法所得，可处以违法所得 1 倍以上 5 倍以下罚款；没有违法所得的，处以 5 万元以上 50 万元以下罚款。

第五十五条 违反本条例第二十三条规定，销毁数据未进行安全风险评估的，由有关部门或者县级以上公安机关责令改正，给予警告，可处以 5000 元以上 5 万元以下罚款。

第五十六条 违反本条例第二十五条第二款规定未备案或者擅自转租的，由通信管理部门责令改正，给予警告；拒不改正的，可处以 5000 元以上 5 万元以下罚款。

第五十七条 违反本条例第二十七条第二款、第二十九条规定的，由有关部门或者县级以上公安机关责令改正，给予警告，没收违法所得，并可处以违法所得 1 倍以上 10 倍以下罚款；没有违法所得的，处以 100 万元以下罚款，对直接负责的主管人员和其他直接责任人员处以 1 万元以上 10 万元以下罚款；情节严重的，责令暂停相关业务、停业整顿，或者吊销相关业务许可证、营业执照。

第五十八条 违反本条例第四十条规定的，由县级以上公安机关责令改正；拒不改正或者情节严重的，处以 5 万元以上 50 万元以下罚款，对直接负责的主管人员和其他直接责任人员，处以 1 万元以上 10 万元以下罚款。

第五十九条 国家机关及其工作人员违反本条例规定，或者玩忽职守、滥用职权、徇私舞弊， 妨碍大数据安全保障工作，尚不构成犯罪的，由其上级主管部门或者监察机关对直接负责的主管人员和其他直接责任人员依法予以处分。

第六十条 违反本条例规定的其他行为，法律、法规有处罚规定的，从其规定。

第六章 附 则

第六十一条 本条例自 2019 年 10 月 1 日起施行。

贵阳市大数据安全管理条例

（2018 年 6 月 5 日贵阳市第十四届人民代表大会常务委员会第十三次会议通过 2018 年 8 月 2 日贵州省第十三届人民代表大会常务委员会第四次会议批准 根

据 2020 年 10 月 30 日贵阳市第十四届人民代表大会常务委员会第三十二次会议通过 2021 年 5 月 27 日贵州省第十三届人民代表大会常务委员会第二十六次会议批准的《贵阳市人民代表大会常务委员会关于修改和废止部分地方性法规的决定》修正)

第一章 总 则

第一条 为了加强大数据安全管理，维护国家安全、社会公共利益，保护公民、法人和其他组织的合法权益，促进大数据发展应用，推动实施大数据战略，根据《中华人民共和国网络安全法》等有关法律法规的规定， 结合本市实际，制定本条例。

第二条 本条例适用于本市行政区域内大数据发展应用中的安全保护、监督管理以及相关活动。

涉及国家秘密的大数据安全管理，按照有关保密法律法规的规定执行。

本条例所称大数据安全，是指大数据发展应用中，数据的所有者、管理者、使用者和服务提供者(以下简称安全责任单位)采取保护管理的策略和措施，防范数据伪造、泄露或者被窃取、篡改、非法使用等风险与危害的能力、状态和行动。

本条例所称大数据，是指以容量大、类型多、存取速度快、应用价值高为主要特征的数据集合，是对数量巨大、来源分散、格式多样的数据进行采集、存储和关联分析，发现新知识、创造新价值、提升新能力的新一代信息技术和服务业态。

本条例所称数据，是指通过计算机或者其他信息终端及相关设备组成的系统收集、存储、传输、处理和产生的各种电子化的信息。

第三条 实施大数据安全管理，应当坚持正确的网络安全观，遵循统一领导、政府管理、行业自律、社会监督、风险防控、权责统一、包容审慎、支持创新的原则。

第四条 市人民政府统一领导本市大数据安全管理工作。县级人民政府领导本辖区大数据安全管理工作。

第五条 市级网信部门负责统筹协调全市大数据安全监督管理工作，组织开展全市关键信息基础设施监管等工作。县级网信部门按照职责负责综合协调本辖区大数据安全监督管理工作。

市级公安机关负责开展大数据安全的等级保护、日常巡查、执法检查、信息通报、应急处置等监督管理工作。县级公安机关按照职责负责本辖区大数据安全监督管理工作。

市级大数据主管部门统筹协调本市大数据安全保障体系建设。县级大数据主管部门按照职责负责本辖区大数据安全管理的相关工作。

保密、国家安全、密码管理、通信管理等主管部门按照各自职责， 做好大数据安全管理的相关工作。

第六条 安全责任单位应当加强大数据安全能力建设，履行大数据安全保护职责，接受有关主管部门监督管理和社会监督。

第七条 县级以上人民政府以及网信、公安、大数据等主管部门和安全责任单位、大众传播媒介按照各自职责，做好大数据安全宣传教育工作。

第八条 市人民政府设立统一的大数据安全监管服务、投诉举报平台，建立相应的工作机制。

任何单位和个人都有权投诉举报危害大数据安全的行为；有关部门应当对投诉举报予以保密。

第二章 安全保障

第九条 安全责任单位应当根据职责明确、意图合规、质量保障、数据最小化、最小授权操作、分类分级保护和可审计的原则， 采取有效措施保护数据的保密性、完整性、真实性、可控性、可靠性和可核查性。

第十条 安全责任单位的法定代表人或者主要负责人是本单位大数据安全的第一责任人。

安全责任单位应当根据数据的生命周期、规模、重要性和本单位的性质、类别、规模等因素，建立安全管理内控制度和支撑保障机制，明确安全管理负责人，落实不同岗位的安全管理职责；关键信息基础设施的运营者还应当设置专门安全管理机构。

第十一条 安全责任单位应当根据数据类型、级别、敏感程度以及数据安全能力成熟度等要求，制定安全规则、管理规范和操作规程， 采取相应的安全管理策略、管理措施和技术手段实施有效管理。

第十二条 安全责任单位应当按照大数据安全等级保护要求进行系统安全功

能配置，制定实施系统配置技术管理规程、软件采购使用限制策略和外部组件使用安全策略，规定配置管理的审批、操作流程，提供符合规范标准的管理与服务，对系统重要配置进行及时更新。

第十三条 安全责任单位应当制定完善访问控制策略，采取授权访问、身份认证等技术措施，防止未经授权查询、复制、修改或者传输数据。对个人信息和重要数据实行加密等安全保护，对涉及国家安全、社会公共利益、商业秘密、个人信息的数据依法进行脱敏脱密处理。

第十四条 安全责任单位应当建立大数据安全审计制度，规定审计工作流程，记录并保存数据分类、采集、清洗、转换、加载、传输、存储、复制、备份、恢复、查询和销毁等操作过程，定期进行安全审计分析。

第十五条 存储数据，应当选择安全性能、防护级别与其安全等级相匹配的存储载体，并且依法进行管理和维护。

销毁数据，应当按照数据分类分级建立审查机制，明确销毁对象、流程和技术等要求，设置相关监督角色，以不可逆方式销毁数据内容。

第十六条 安全责任单位服务外包业务涉及收集、存储、传输或者应用数据的，应当依法与外包服务提供商签订安全保护协议，采取安全保护措施，并对导出、复制、销毁数据等行为进行监督。

第十七条 支持依法成立的大数据行业组织依照法律、法规和章程的规定，制定行业安全规范和服务标准，对其会员的大数据安全行为进行自律管理，组织开展大数据安全教育、业务培训， 推进大数据安全合作、交流， 提高大数据安全管理水平和从业人员素质。

第十八条 市人民政府应当建立联席会议制度，研究、解决大数据安全工作的重大事项、重点工作和重要问题。

县级以上人民政府应当整合大数据安全防范、保障等资源， 建立重点领域工作联动、会商、约谈、通报、巡查和决策咨询等机制， 统筹有关职能部门履行大数据安全监督管理职责，防范安全风险。

第十九条 市人民政府建立大数据安全靶场和产品检验场地，对大数据安全新技术、新应用、新产品进行测试、检验， 定期开展攻防演练，促进大数据安全城市建设。

第二十条 县级以上人民政府应当采取资金扶持、开设绿色通道等措施，支持大数据安全技术产业发展、安全技术研发应用和安全管理方式创新。

鼓励企业、科研机构、高等院校、职业学校和相关行业组织建立教育实践和培训基地，开设相关专业课程，加强人才交流，多形式培养、引进和使用大数据安全人才。

第二十一条 市级公安机关负责大数据安全投诉举报平台的运行、维护和管理工作，公布投诉举报方式等信息，即时受理投诉举报，按照规定时限回复；对不属于本部门职责的，移送有关部门处理。有关部门处理后， 应当按照规定时限反馈市级公安机关。

安全责任单位应当建立大数据安全投诉举报制度，公布投诉举报方式等信息，接受和处理用户及相关利害关系人的投诉举报。

第二十二条 网信、公安、大数据、标准化、工业和信息化等主管部门应当加强大数据安全的国家标准、行业标准和地方标准的宣传、培训， 引导、鼓励安全责任单位采用大数据安全国家推荐标准、行业标准和地方标准。

鼓励支持教育、科研机构和企业参与大数据安全的国家标准、行业标准和地方标准的研究、制定。

鼓励安全责任单位运用区块链等新技术手段，优化数据聚通用架构，强化信任认证和防篡改设计，提升大数据安全防护水平。

第二十三条 市大数据主管部门应当配合制定大数据安全保护标准体系，指导数据资源分类分级、数据安全能力成熟度认定和数字认证等相关工作。

第二十四条 县级以上人民政府以及有关部门应当通过报刊杂志、电台电视台、门户网站、微信微博等途径，运用安全宣传周、主题日、专题会、研讨班、应用场景展示、竞赛等形式， 经常性地对公众以及大数据安全重点领域、重点行业、重点单位、重点人群等组织开展大数据安全法律法规、形势政策和知识技能的宣传培训。

安全责任单位应当制定计划，对员工、用户以及本单位的重点部位、重点设施、重点岗位安全工作人员开展大数据安全法律法规、知识技能等教育、培训和考核，提升大数据安全意识和防护技能水平。

第三章 监测预警与应急处置

第二十五条 市级公安机关负责大数据安全监管服务平台的日常维护管理，加强对平台监测信息、监督检查信息和上级通报信息的分析、安全形势研判和风险评估，按照规定发布安全风险预警或者信息通报。

县级公安机关应当及时落实上级公安机关通过大数据安全监管服务平台发布的各项指令。

第二十六条 县级以上人民政府应当根据国家和省的规定，落实大数据安全应急工作机制，明确工作责任、程序和规范； 制定大数据安全事件应急预案，明确应急处置组织机构及其职责、事件分级、响应程序、保障手段和处置措施； 定期组织演练，评估演练效果，分析存在问题，总结处置经验，提出改进和完善应急预案的意见。

发生大数据安全事件时，县级以上人民政府应当依法按程序启动应急预案，组织网信、公安、大数据等主管部门针对事件的性质和特点，采取应急措施处置。

第二十七条 安全责任单位应当制定大数据安全事件预警通报制度和应急预案，建立和实施安全事件预警、舆情监控、风险评估和应急响应的策略、规程，保持与有关主管部门、设备设施及软件服务提供商、安全机构、新闻媒体和用户的联络、协作。

发生大数据安全事件时，安全责任单位应当依法按程序启动应急预案，采取相应措施防止危害扩大，保存相关记录，告知可能受到影响的用户，按照规定向有关主管部门报告。

第四章 监督检查

第二十八条 县级以上人民政府应当将大数据安全管理工作纳入年度目标绩效考核。

第二十九条 县级以上人民政府应当建立健全大数据安全工作监督检查机制，明确监督检查的牵头部门、责任分工、内容、重点、目标、方式和标准。

监督检查的情况，应当在有关主管部门之间互通和共享。

第三十条 公安机关应当监督、检查、指导安全责任单位建立、落实大数据安全管理的各项制度和技术措施，依法查处大数据安全违法案件。

第三十一条 大数据主管部门应当结合监督检查大数据安全责任落实的情况，定期组织开展大数据安全风险评估，发布评估报告。

第三十二条 有关主管部门在监督检查、风险评估和攻防演练中，发现安全责任单位存在安全问题的，应当及时提出改进建议，发出整改意见并且督促整改。

安全责任单位应当根据有关主管部门的整改意见进行整改，并且反馈整改情况。

第三十三条 公安、大数据主管部门应当建立大数据安全管理诚信档案，记录违法信息，纳入统一的信用共享平台管理。

第五章 法律责任

第三十四条 安全责任单位不履行本条例第十条、第十一条、第十二条、第十三条、第十四条和第二十七条规定的数据安全保护义务的， 由有关主管部门责令改正，给予警告；拒不改正或者导致危害大数据安全等后果的，处以 1 万元以上 10 万元以下罚款，对直接负责的主管人员处以 5000 元以上 5 万元以下罚款。

第三十五条 违反本条例规定的其他行为，依据《中华人民共和国网络安全法》等法律、法规的相关规定处理。

第三十六条 安全责任单位中的国家机关不履行本条例规定的大数据安全保护职责的，由其上级机关或者有关机关责令改正；对直接负责的主管人员和其他直接责任人员依法给予处分。

大数据安全监督管理有关主管部门的工作人员玩忽职守、滥用职权、徇私舞弊，尚不构成犯罪的，依法给予处分。

第六章 附 则

第三十七条 本条例自 2018 年 10 月 1 日起施行。

西藏自治区网络信息安全管理条例

西藏自治区人民代表大会常务委员会公告〔2023〕2 号

《西藏自治区网络信息安全管理条例》已由西藏自治区第十一届人民代表大会常务委员会第四十三次会议于 2022 年 12 月 9 日审议通过，现予公布，自 2023 年 2 月 1 日起施行。

特此公告。

西藏自治区人民代表大会常务委员会

2023 年 1 月 18 日

西藏自治区网络信息安全管理条例

(2022 年 12 月 9 日西藏自治区第十一届人民代表大会常务委员会第四十三次会议通过)

第一条 为了维护国家安全和社会公共利益，反对分裂，促进民族团结进步，保障网络信息安全，保护公民、法人和其他组织的合法权益，根据《中华人民共和国网络安全法》《中华人民共和国国家安全法》等有关法律、行政法规，结合自治区实际，制定本条例。

第二条 自治区行政区域内利用计算机网络制作、复制、发布、传播信息等活动及其监督管理工作，适用本条例。

第三条 网络信息安全工作坚持中国共产党的领导，坚持总体国家安全观，坚持社会主义核心价值观，坚持铸牢中华民族共同体意识，坚持积极利用、科学发展、依法管理、确保安全的原则。

第四条 自治区实行网络信息安全综合治理，建立党委领导、政府管理、部门负责、企业履责、社会监督、网民自律等多主体参与的网络信息安全综合治理体系

第五条 自治区网络安全和信息化领导机构负责研究制定、指导实施自治区网络信息安全重要政策和举措，协调落实网络信息安全重大事项和重要工作。

第六条 自治区网信部门负责统筹协调自治区网络信息安全和监督管理工作，建立协调联动、资源共享、高效处置的网络信息安全工作机制，加强互联网信息内容管理、网络安全防护和网络执法监督。

地(市)、县(区)网信部门负责统筹协调本行政区域内的网络信息安全和监督管理工作。

自治区通信部门负责通信行业监督管理和通信安全防护工作，拟定通信管制措施。

县级以上公安机关负责打击网络违法犯罪活动，查处网络违法犯罪行为。

县级以上国家安全机关在网络领域依法行使维护国家安全的职责。

县级以上经信部门根据职责承担相关网络安全防护工作。

第七条 县级以上人民政府应当加大对网络信息安全的投入，支持保障网络信息安全的技术防护、监测预警、风险评估、应急响应、宣传教育等工作。

第八条 各级人民政府及其有关部门，应当依法组织开展网络信息安全宣传

教育，加强网络文明建设，净化网络空间，将治理网络违法、不良信息纳入群众性精神文明创建内容。

工会、共青团、妇联、社科联、科协、佛协等社会团体，应当发挥各自优势，有针对性地依法开展网络信息安全宣传教育。

广播电视等媒体应当开展网络信息安全宣传，营造全社会安全健康文明上网的氛围。

学校应当将科学、文明、安全、依法合理使用网络纳入教育教学内容，对学生有针对性地开展网络安全法律、法规、网络文明教育，将依法用网、文明上网纳入校纪校规。

宗教事务部门应当引导宗教教职人员自觉遵守国家网络信息安全法律、法规，文明上网、文明用网。

村(居)民委员会应当教育引导村(居)民遵守网络安全法律、法规，倡导将网络信息安全相关内容纳入村规民约、居民公约。

第九条 任何公民、法人和其他组织都有维护网络信息安全的义务，有权举报危害网络信息安全的行为。

网信、通信、公安、国家安全等有关部门应当设置举报平台，公示举报方式。接到举报的部门应当依法及时作出处理，不属于本部门职责的，应当及时转交有管辖权的部门。

有关部门应当对举报人的相关信息予以保密，并对举报属实且发挥积极作用的人员进行奖励。

第十条 自治区鼓励公民、法人和其他组织制作、传播下列信息：

(一)宣传习近平新时代中国特色社会主义思想，宣传党的理论、路线、方针、政策和新时代党的治藏方略的；

(二)宣传中国共产党党史、新中国史、改革开放史、社会主义发展史、中华民族发展史、西藏地方与祖国关系史的；

(三)弘扬社会主义核心价值观，宣传中华优秀传统文化、革命文化和社会主义先进文化的；

(四)铸牢中华民族共同体意识，建设中华民族共有精神家园的；

(五)展示真实、立体、全面的西藏，反映西藏新发展、新生活、新面貌

的；

(六)展现各族人民昂扬向上的精神风貌，宣传模范典型和先进事迹的；

(七)有效回应社会关切，解疑释惑，析事明理，有助于引导各族人民形成共识的；

(八)宣传法律、法规，普及科学文化知识，倡导科学文明健康生活方式的；

(九)其他讴歌真善美、促进民族团结进步等弘扬正气、传播正能量的。

第十一条 任何公民、法人和其他组织不得利用网络制作、复制、发布、下载、传播、转发下列信息：

(一)反对宪法所确定的基本原则的；

(二)危害国家安全，泄露国家秘密，颠覆国家政权，反对社会主义制度，分裂国家、破坏国家统一的；

(三)损害国家荣誉和利益的；

(四)宣扬“藏独”组织的标识、成员的图像、言论、活动以及通过书籍、漫画、音乐、影像、游戏、地图等其他形式宣扬分裂主义、支持分裂势力的，宣扬恐怖主义、极端主义或者煽动实施分裂活动、恐怖活动、极端活动的；

(五)煽动非法结社、集会、游行、示威和其他扰乱社会秩序活动的；

(六)歪曲、诋毁西藏人权、文化、历史和生态环境、自然资源等领域状况，诋毁、抵制使用国家通用语言文字的；

(七)歪曲、诋毁国家民族政策、民族状况，煽动民族仇恨、民族歧视，破坏民族团结的；

(八)歪曲、诋毁宗教事务管理相关法律法规、国家宗教政策、宗教状况、藏传佛教活佛转世宗教仪轨和历史定制，或者宣扬邪教、非法宗教活动和封建迷信的；

(九)侵害英雄烈士的姓名、肖像、名誉、荣誉的；

(十)制作、散布虚假险情、疫情、灾情、警情等，扰乱社会秩序和经济秩序的；

(十一)散布淫秽、色情、赌博、暴力、凶杀、恐怖或者教唆犯罪的；

(十二)侮辱或者诽谤他人，侵害他人合法权益的；

(十三)法律、行政法规禁止的其他内容。

第十二条 从事互联网宗教信息服务，应当经自治区人民政府宗教事务部门审核同意后，按照国家互联网信息服务管理有关规定办理。

互联网宗教信息服务内容应当符合有关法律、法规、规章和宗教事务管理的相关规定。

第十三条 任何公民、法人和其他组织不得擅自建立或者使用非法定信道进行国际联网。

第十四条 任何公民、法人和其他组织不得浏览明知含有分裂国家、破坏国家统一内容的网站平台，不得下载、使用明知用于分裂国家、破坏国家统一活动的应用程序。

任何公民、法人和其他组织不得组建策划实施分裂、恐怖、极端活动和非法结社、集会、游行、示威等扰乱社会秩序活动以及其他违法犯罪活动的网站、通讯群组。

任何公民、法人和其他组织不得加入策划实施分裂、恐怖、极端活动和非法结社、集会、游行、示威等扰乱社会秩序活动以及其他违法犯罪活动的通讯群组；不得组建、加入明知有分裂势力成员的通讯群组。

第十五条 网络运营者应当落实网络安全防范措施，建立健全网络信息内容发布审核监督制度，加强对其用户发布信息的管理，发现法律、法规和本条例禁止的信息和活动的，应当依法立即停止传输该信息，采取警示提醒、限制账号功能、暂停信息更新、关闭注销账号、列入负面清单、禁止重新注册等处置措施，防止信息扩散，保存有关记录，并立即向有关主管部门报告。

第十六条 网信部门和有关部门发现法律、法规和本条例禁止的信息和活动的，应当要求网络运营者停止传输，采取消除等处置措施，保存有关记录；对来源于中华人民共和国境外的上述信息，应当通知有关机构采取技术措施和其他必要措施阻断传播。

任何公民、法人和其他组织持有的移动通信终端、计算机、存储介质等设备含有法律、法规和本条例禁止的信息的，应当立即删除。

第十七条 网络运营者为用户办理网络接入、域名注册服务，办理固定电话、移动通信终端等入网手续，或者为用户提供信息发布、即时通讯等服务，

在与用户签订协议或者确认提供服务时，应当要求用户提供真实身份信息，确保人证信息一致。用户不提供真实身份信息的，网络运营者不得与其签订协议或者为其提供相关服务。

第十八条 网络运营者依法保护用户个人信息，收集、使用个人信息，应当遵循合法、正当、必要的原则，公开收集、使用规则，明示收集、使用信息的目的、方式和范围，并经被收集者同意。

网络运营者不得收集与其提供的服务无关的个人信息，不得违反法律、行政法规的规定和双方的约定收集、使用个人信息，并应当依照法律、行政法规的规定和与用户的约定，处理其保存的个人信息。

网络运营者不得泄露、篡改、毁损其收集的个人信息；未经被收集者同意，不得向他人提供个人信息。但是，经过处理无法识别特定个人且不能复原的除外。

网络运营者应当采取技术措施和其他必要措施，确保其收集的个人信息安全，防止信息泄露、毁损、丢失。发生或者可能发生个人信息泄露、毁损、丢失的，应当立即采取补救措施，按照规定及时告知用户并向有关主管部门报告。

第十九条 通讯群组、论坛社区版块的建立者、管理者应当加强对其成员发布信息的管理，发现传播法律、法规和本条例禁止的信息，应当立即采取有效的限制措施，保存有关记录，并向有关主管部门举报。

第二十条 互联网站、应用程序、论坛、博客、公众账号、即时通信工具、网络直播、短视频社交软件等网络信息服务提供者应当在显著位置开设网上有害信息举报专区，公示举报方式。接到举报的网络信息服务提供者，应当采取核查、删除、阻断等处置措施，保存有关记录，并向有关主管部门报告。

第二十一条 自治区建立网络信息安全监测预警和信息通报制度。自治区网信部门应当统筹协调有关部门加强网络信息收集、分析、研判和通报工作。

自治区网信部门应当会同有关部门建立健全网络信息安全风险评估和应急处置工作机制，制定网络信息安全事件应急预案，定期组织开展跨部门、跨行业网络信息安全应急演练。

发生网络信息安全事件，应当立即启动网络信息安全事件应急预案。

第二十二条 发现网络重要信息安全隐患、线索或者发生网络信息安全事件，网信部门可以向有关单位发出预警通报。有关单位应当及时采取核查处置、执法监管、积极回应等措施，并将处置情况反馈网信部门；发现违法犯罪活动线索，应当同时报告公安机关。

处置重大网络信息安全事件时，网信、通信、公安、国家安全和有关单位应当密切配合，遵循依法处置、舆论引导、社会面管控三同步原则，及时采取线上线下联动处置措施。

第二十三条 网信部门应当会同公安、国家安全等有关部门建立健全跨部门、跨区域执法联动响应和协作机制，推动实现信息共享、联合执法、监管互认，协同开展网络信息安全监管工作。

第二十四条 网信部门会同有关主管部门建立健全网络信息安全联合惩戒机制，对严重违反本条例规定的公民、法人和其他组织，实施限制从事网络信息服务、网上行为限制、行业禁入等惩戒措施。

第二十五条 违反本条例第十一条，法律、行政法规没有处罚规定的，由网信部门给予警告，情节严重的，处五千元以下罚款。

第二十六条 违反本条例第十四条第一款、第三款规定的，由公安机关给予警告或者通报批评，可以并处五千元以下罚款。

违反本条例第十四条第二款规定尚不构成犯罪的，由公安机关处五日以下拘留，可以并处一万元以上十万元以下罚款；情节较重的，处五日以上十五日以下拘留，可以并处五万元以上五十万元以下罚款。关闭用于实施违法犯罪活动的网站、通讯群组。

单位有前款行为的，由公安机关处十万元以上五十万元以下罚款，并对直接负责的主管人员和其他直接责任人员依照前款规定处罚。

第二十七条 违反本条例第十九条规定的，由公安机关给予警告；情节严重，造成恶劣影响的，处五千元以下罚款，并关闭通讯群组、论坛社区版块。

第二十八条 网信、通信、公安、国家安全等有关部门的工作人员在网络信息安全监督管理工作中玩忽职守、滥用职权、徇私舞弊，尚不构成犯罪的，依法给予处分。

第二十九条 网络运营者或者公民、法人和其他组织违反本条例规定的行

为，法律、行政法规已有处罚规定的，从其规定。

第三十条 本条例自 2023 年 2 月 1 日起施行。

浙江省公共数据条例

（2022年1月21日浙江省第十三届人民代表大会第六次会议通过）

目 录

第一章 总则

第一条 为了加强公共数据管理，促进公共数据应用创新，保护自然人、法人和非法人组织合法权益，保障数字化改革，深化数字浙江建设，推进省域治理体系和治理能力现代化，根据有关法律、行政法规，结合本省实际，制定本条例。

第二条 本省行政区域内公共数据收集、归集、存储、加工、传输、共享、开放、利用等数据处理活动，以及公共数据安全等管理活动，适用本条例。

涉及国家秘密的公共数据及相关处理活动，不纳入本条例管理，按照有关法律、法规的规定执行。

第三条 本条例所称公共数据，是指本省国家机关、法律法规规章授权的具有管理公共事务职能的组织以及供水、供电、供气、公共交通等公共服务运营单位（以下统称公共管理和服务机构），在依法履行职责或者提供公共服务过程中收集、产生的数据。

根据本省应用需求，税务、海关、金融监督管理等国家有关部门派驻浙江管理机构提供的数据，属于本条例所称公共数据。

第四条 公共数据发展和管理工作坚持中国共产党的领导，遵循统筹规划、依法有序、分类分级、安全可控的原则。

第五条　县级以上人民政府应当将公共数据发展和管理工作纳入国民经济和社会发展规划以及数字政府建设等相关专项规划，建立健全工作协调机制，完善政策措施，保障公共数据发展和管理工作所需经费。

县级以上人民政府应当建立健全公共数据发展和管理工作考核评价机制，将公共数据发展和管理工作作为年度政府目标责任制考核的重要内容。

第六条　县级以上人民政府大数据发展主管部门或者设区的市、县（市、区）人民政府确定的负责大数据发展工作的部门（以下简称公共数据主管部门），负责本行政区域内公共数据发展和管理工作，指导、协调、督促其他有关部门按照各自职责做好公共数据处理和安全管理相关工作。

公共管理和服务机构负责本部门、本系统、本领域公共数据处理和安全管理工作。

网信、公安、国家安全、保密、密码等部门按照各自职责，做好公共数据安全的监督管理工作。

第七条　公共数据主管部门应当会同有关部门建立健全监督检查工作机制，加强对公共数据平台建设、数据标准实施、数据质量、数据共享开放、数据安全保障等情况的监督检查，并督促落实。

第八条　县级以上人民政府应当按照长江三角洲区域一体化发展国家战略要求，加强公共数据发展和管理工作跨省域合作，推动公共数据标准统一，促进公共数据共享利用，发挥公共数据在区域一体化协同治理和跨区域协同发展中的驱动作用。

第二章　公共数据平台

第九条　省公共数据主管部门应当会同省有关部门，统筹规划和建设以基础设施、数据资源、应用支撑、业务应用体系为主体，以政策制度、标准规范、组织保障、网络安全体系为支撑的一体化智能化公共数据平台（以下简称公共数据平台），促进省域整体智治、高效协同。

设区的市公共数据主管部门应当会同同级有关部门，按照省有关标准和指导规范的要求建设本级公共数据平台。县（市、区）应当按照互联互通、共建共享原则，依托设区的市公共数据平台建设本级公共数据平台；确有必要的，可以单独建设。

省、设区的市公共数据平台应当按照地方实际需要，及时向下级公共数据平台返回数据。

第十条　公共数据主管部门应当依托公共数据平台建立统一的数据共享、开

放通道。公共管理和服务机构应当通过统一的共享、开放通道共享、开放公共数据。

公共管理和服务机构不得新建公共数据共享、开放通道；已建共享、开放通道的，应当并入统一的共享、开放通道。

第十一条　省公共数据主管部门应当统筹建设全省一体化数字资源系统，推动全省公共数据、应用、组件、算力等数字资源集约管理，促进数字资源高效配置供给，实现公共数据跨层级、跨地域、跨系统、跨部门、跨业务有序流通和共享。

第十二条　县级以上人民政府应当建立使用财政资金的数字化项目管理机制，加强对数字化项目的统筹、整合和共享管理，避免重复建设。

使用本省财政资金的数字化项目有下列情形之一的，不予立项、审查验收或者不予安排运行和维护经费：

（一）未经县级以上人民政府指定的部门同意，新建业务专网或者新建、扩建、改建独立数据平台的；

（二）未经县级以上人民政府指定的部门同意，在公共数据平台外开发、升级改造应用系统的；

（三）未按照规定纳入一体化数字资源系统管理的；

（四）未按照要求共享、开放数据或者重复收集数据的；

（五）不符合密码应用和安全管理要求的。

第十三条　公共数据实行目录化管理。省公共数据主管部门应当统筹推进省、设区的市、县（市、区）三级公共数据目录一体化建设，制定统一的目录编制标准，组织编制全省公共数据目录。

设区的市、县（市、区）公共数据主管部门应当按照统一标准，组织编制本级公共数据子目录，并报上一级公共数据主管部门审核。

公共管理和服务机构应当按照统一标准，编制本部门公共数据子目录，并报同级公共数据主管部门审核。

第十四条　省公共数据主管部门应当会同省标准化主管部门和其他有关部门，推进本省公共数据标准体系建设，制定省、设区的市、县（市、区）公共数据平台建设标准以及公共数据处理和安全管理等标准，推动公共数据国家标准、行业标准和地方标准有效实施。

第三章　公共数据收集与归集

第十五条　公共管理和服务机构收集数据应当遵循合法、正当、必要的原则

，按照法定权限、范围、程序和标准规范收集。

可以通过共享获取数据的，公共管理和服务机构不得重复收集；共享数据无法满足履行职责需求的，公共管理和服务机构可以向公共数据主管部门提交数据需求清单，由公共数据主管部门与相关公共管理和服务机构协商解决。

第十六条　公共管理和服务机构按照法定权限、范围、程序和标准规范收集单位、个人数据的，有关单位、个人应当予以配合。

收集公共数据应当遵守网络安全、数据安全、个人信息保护等法律、法规以及国家标准的强制性要求。

第十七条　收集公共数据应当分别以下列号码或者代码作为必要标识：

（一）公民身份号码或者个人其他有效身份证件号码；

（二）法人统一社会信用代码；

（三）非法人组织统一社会信用代码或者其他识别代码。

公共管理和服务机构收集数据时，不得强制要求个人采用多种方式重复验证或者特定方式验证。已经通过有效身份证件验明身份的，不得强制通过收集指纹、虹膜、人脸等生物识别信息重复验证。法律、行政法规另有规定的除外。

第十八条　省公共数据主管部门应当会同省有关部门在省公共数据平台建立和完善人口、法人、信用、电子证照、自然资源和空间地理等基础数据库，以及跨地域、跨部门专题数据库。省公共管理和服务机构应当根据公共数据目录，按照应用需求将公共数据统一归集到省公共数据平台基础数据库和专题数据库。

设区的市、县（市、区）公共数据主管部门应当在本级公共数据平台建立和完善跨地域、跨部门专题数据库。公共管理和服务机构应当根据公共数据目录，按照应用需求将公共数据统一归集到本级公共数据平台专题数据库。

第十九条　自然人、法人或者非法人组织对涉及自身的公共数据有异议或者发现公共数据不准确、不完整的，可以向公共管理和服务机构提出校核申请。公共管理和服务机构应当自收到校核申请之日起五个工作日内校核完毕；情况复杂的，经公共管理和服务机构负责人批准，可以延长至十个工作日。公共管理和服务机构应当将校核处理结果及时告知当事人。

自然人、法人或者非法人组织对涉及自身的公共数据有异议或者发现公共数据不准确、不完整的，也可以向公共数据主管部门提出校核申请。公共数据主管部门应当自收到校核申请之日起两个工作日内转交相应公共管理和服务机构，并督促公共管理和服务机构在前款规定的期限内校核完毕。

公共数据主管部门、公共管理和服务机构发现数据不准确、不完整或者不同

的公共管理和服务机构收集、提供的数据不一致的，由公共数据主管部门通知数据收集、提供单位限期校核。数据收集、提供单位应当在期限内校核完毕。

第二十条　公共数据主管部门、公共管理和服务机构应当建立健全数据全流程质量管控体系，加强数据质量事前、事中和事后的监督检查，及时更新已变更、失效数据，实现问题数据可追溯、可定责，保证数据的及时性、准确性、完整性。

第二十一条　为了应对突发事件，公共管理和服务机构按照应对突发事件有关法律、法规规定，可以要求自然人、法人或者非法人组织提供应对突发事件所必需的数据，并根据实际需要，依法、及时共享和开放相关公共数据，为应对突发事件提供支持；收集的数据不得用于与应对突发事件无关的事项；对在履行职责中知悉的个人信息、商业秘密、保密商务信息等应当依法予以保密。

突发事件应急处置工作结束后，公共管理和服务机构应当对获得的突发事件相关公共数据进行分类评估，将涉及个人信息、商业秘密、保密商务信息的公共数据采取封存等安全处理措施，并关停相关数据应用。

第四章　公共数据共享

第二十二条　本条例所称公共数据共享，是指公共管理和服务机构因履行法定职责或者提供公共服务需要，依法使用其他公共管理和服务机构的数据，或者向其他公共管理和服务机构提供数据的行为。

公共数据应当以共享为原则、不共享为例外。

第二十三条　公共数据按照共享属性分为无条件共享、受限共享和不共享数据。

公共管理和服务机构应当按照国家和省有关规定对其收集、产生的公共数据进行评估，科学合理确定共享属性，并定期更新。列入受限共享数据的，应当说明理由并明确共享条件；列入不共享数据的，应当提供明确的法律、法规、规章或者国家有关规定依据。

公共数据主管部门对同级公共管理和服务机构确定的公共数据共享属性有异议，经协商不能达成一致意见的，报本级人民政府决定。

第二十四条　公共管理和服务机构需要通过共享获取数据的，应当向数据提供单位的同级公共数据主管部门提出申请，明确应用场景，通过统一的公共数据共享通道以接口调用、批量数据使用等方式获取数据。

无法按照前款规定获取数据的，可以向公共数据主管部门提交数据需求清单，由公共数据主管部门与相关公共管理和服务机构协商解决。

第二十五条　公共管理和服务机构申请使用无条件共享数据的，公共数据主管部门应当在两个工作日内予以共享。

申请使用受限共享数据的，公共数据主管部门应当自收到申请之日起一个工作日内征求数据提供单位意见，数据提供单位应当在三个工作日内反馈意见。数据提供单位同意共享的，公共数据主管部门应当在两个工作日内予以共享。数据提供单位不同意共享的，应当说明理由，公共数据主管部门应当自收到反馈意见之日起两个工作日内完成审核，认为应当共享的，应当在两个工作日内予以共享，并告知数据提供单位；认为不应当共享的，应当立即告知提出申请的公共管理和服务机构。

第二十六条　公共管理和服务机构通过共享获取的公共数据，应当用于本机构依法履行职责的需要，不得用于或者变相用于其他目的。

第五章　公共数据开放与利用

第二十七条　本条例所称公共数据开放，是指向自然人、法人或者非法人组织依法提供公共数据的公共服务行为。

公共数据开放应当遵循依法、规范、公平、优质、便民的原则。公共数据按照开放属性分为无条件开放、受限开放和禁止开放数据。

第二十八条　省公共数据主管部门根据国家和省有关公共数据分类分级要求，组织编制全省公共数据开放目录。设区的市公共数据主管部门可以组织编制本行政区域公共数据开放子目录。公共数据开放目录按照实际需要实行动态调整。

公共数据开放目录应当标注数据名称、数据开放主体、数据开放属性、数据格式、数据类型、数据更新频率等内容。

第二十九条　省、设区的市公共数据主管部门应当根据当地经济社会发展需要，会同同级公共管理和服务机构制定年度公共数据开放重点清单，优先开放与民生紧密相关、社会迫切需要、行业增值潜力显著和产业战略意义重大的公共数据。

确定年度公共数据开放重点清单，应当听取相关行业组织、企业、专家和社会公众的意见。

第三十条　公共数据有下列情形之一的，禁止开放：

（一）开放后危及或者可能危及国家安全的；

（二）开放后可能损害公共利益的；

（三）涉及个人信息、商业秘密或者保密商务信息的；

（四）数据获取协议约定不得开放的；

（五）法律、法规规定不得开放的。

前款第三项规定的公共数据有下列情形之一的，可以列入受限开放或者无条件开放数据：

（一）涉及个人信息的公共数据经匿名化处理的；

（二）涉及商业秘密、保密商务信息的公共数据经脱敏、脱密处理的；

（三）涉及个人信息、商业秘密、保密商务信息的公共数据指向的特定自然人、法人或者非法人组织依法授权同意开放的。

省公共数据主管部门应当会同省网信、公安、经济和信息化等部门制定公共数据脱敏、脱密等技术规范。

第三十一条　公共管理和服务机构应当按照国家和省有关规定对其收集、产生的公共数据进行评估，科学合理确定开放属性，并定期更新。

公共数据主管部门对同级公共管理和服务机构确定的公共数据开放属性有异议，经协商不能达成一致意见的，报本级人民政府决定。

第三十二条　自然人、法人或者非法人组织需要获取无条件开放的公共数据的，可以通过统一的公共数据开放通道获取。

第三十三条　自然人、法人或者非法人组织需要获取受限开放的公共数据的，应当具备相应的数据存储、处理和安全保护能力，并符合申请时信用档案中无因违反本条例规定记入的不良信息等要求，具体条件由省、设区的市公共管理和服务机构通过本级公共数据平台公布。

自然人、法人或者非法人组织需要获取受限开放的公共数据的，应当通过统一的公共数据开放通道向公共数据主管部门提出申请。公共数据主管部门应当会同数据提供单位审核后确定是否同意开放。

经审核同意开放公共数据的，申请人应当签署安全承诺书，并与数据提供单位签订开放利用协议。申请开放的公共数据涉及两个以上数据提供单位的，开放利用协议由公共数据主管部门与申请人签订。开放利用协议应当明确数据开放方式、使用范围、安全保障措施等内容。

申请人应当按照开放利用协议约定的范围使用公共数据，并按照开放利用协议和安全承诺书采取安全保障措施。

第三十四条　县级以上人民政府应当将公共数据作为促进经济社会发展的重要生产要素，促进公共数据有序流动，推进数据要素市场化配置改革，推动公共数据与社会数据深度融合利用，提升公共数据资源配置效率。

自然人、法人或者非法人组织利用依法获取的公共数据加工形成的数据产品

和服务受法律保护，但不得危害国家安全和公共利益，不得损害他人的合法权益。

第三十五条　县级以上人民政府可以授权符合规定安全条件的法人或者非法人组织运营公共数据，并与授权运营单位签订授权运营协议。禁止开放的公共数据不得授权运营。

授权运营单位应当依托公共数据平台对授权运营的公共数据进行加工；对加工形成的数据产品和服务，可以向用户提供并获取合理收益。授权运营单位不得向第三方提供授权运营的原始公共数据。

授权运营协议应当明确授权运营范围、运营期限、合理收益的测算方法、数据安全要求、期限届满后资产处置等内容。

省公共数据主管部门应当会同省网信、公安、国家安全、财政等部门制定公共数据授权运营具体办法，明确授权方式、授权运营单位的安全条件和运营行为规范等内容，报省人民政府批准后实施。

第三十六条　县级以上人民政府及其有关部门应当通过产业政策引导、资金扶持、引入社会资本等方式，拓展公共数据开发利用场景。

县级以上人民政府及其有关部门可以通过政府购买服务、协议合作等方式，支持利用公共数据创新产品、技术和服务，提升公共数据产业化水平。

公共数据主管部门可以通过应用创新大赛、补助奖励、合作开发等方式，鼓励利用公共数据开展科学研究、产品开发、数据加工等活动。

第六章　公共数据安全

第三十七条　公共数据安全管理应当坚持统筹协调、分类分级、权责统一、预防为主、防治结合的原则，加强公共数据全生命周期安全和合法利用管理，防止数据被非法获取、篡改、泄露、损毁或者不当利用。

第三十八条　公共数据、网信、公安、国家安全、密码等部门应当按照各自职责，对下级公共数据主管部门、本级公共管理和服务机构的公共数据安全承担监督管理责任。

公共管理和服务机构在公共数据、网信、公安、国家安全、密码等部门指导下，开展本系统、本领域公共数据安全保护工作。

第三十九条　公共数据安全实行谁收集谁负责、谁使用谁负责、谁运行谁负责的责任制。公共数据主管部门、公共管理和服务机构的主要负责人是本单位数据安全工作的第一责任人。

公共数据主管部门、公共管理和服务机构应当强化和落实数据安全主体责任

，建立数据安全常态化运行管理机制，具体履行下列职责：

（一）落实网络安全等级保护制度，建立健全本单位数据安全管理制度、技术规范和操作规程；

（二）设置数据安全管理岗位，实行管理岗位责任制，配备安全管理人员和专业技术人员；

（三）定期组织相关人员进行数据安全教育、技术培训；

（四）加强数据安全日常管理和检查，对复制、导出、脱敏、销毁数据等可能影响数据安全的行为，以及可能影响个人信息保护的行为进行监督；

（五）加强平台（系统）压力测试和风险监测，发现数据安全缺陷、漏洞等风险时立即采取补救措施；

（六）制定数据安全事件应急预案，并定期进行演练；

（七）法律、法规、规章规定的其他职责。

第四十条　公共数据主管部门应当会同网信、公安、国家安全、密码等部门建立健全公共数据分类分级、安全审查、风险评估、监测预警、应急演练、安全审计、封存销毁等制度，并督促指导公共管理和服务机构实施。

第四十一条　公共数据主管部门、公共管理和服务机构应当结合公共数据具体应用场景，按照分类分级保护要求，建立健全公共数据安全防护技术标准和规范，采取身份认证、访问控制、数据加密、数据脱敏、数据溯源、数据备份、隐私计算等技术措施，提高数据安全保障能力。

第四十二条　公共数据主管部门、公共管理和服务机构在处理公共数据过程中，因数据汇聚、关联分析等原因，可能产生涉密、敏感数据的，应当进行安全评估，并根据评估意见采取相应的安全措施。

第四十三条　公共数据主管部门、公共管理和服务机构依法委托第三方服务机构开展平台（系统）建设以及运行维护的，应当按照国家和省有关规定对服务提供方进行安全审查；经安全审查符合条件的，签订服务外包协议时应当同时签订服务安全保护及保密协议，约定违约责任，并监督服务提供方履行数据安全保护义务。

服务外包协议不生效、无效、被撤销或者终止的，公共数据主管部门、公共管理和服务机构应当撤销账号或者重置密码，并监督服务提供方以数据覆写、物理销毁等不可逆方式删除相关数据。

第四十四条　自然人、法人或者非法人组织认为开放的公共数据侵犯其合法权益的，有权向公共管理和服务机构提出撤回数据的要求。

公共管理和服务机构收到撤回数据要求后，应当立即进行核实，必要时立即中止开放；经核实存在前款规定问题的，应当根据不同情形采取撤回数据或者处理后再开放等措施，并将有关处理结果及时告知当事人。当事人对处理结果有异议的，可以向公共数据主管部门申请复核。

公共管理和服务机构在日常监督管理过程中发现开放的公共数据存在安全风险的，应当立即中止开放，并在消除安全风险后开放。

第四十五条　公共数据主管部门、公共管理和服务机构可以组织有关单位、专家或者委托第三方专业机构，对公共数据共享、开放和安全保障等工作开展评估，提升公共数据管理水平。

第七章　法律责任

第四十六条　违反本条例规定的行为，法律、行政法规已有法律责任规定的，从其规定。

第四十七条　公共管理和服务机构有下列情形之一的，由公共数据主管部门按照管理权限责令限期整改：

（一）未按照规定编制或者更新公共数据子目录的；

（二）违反规定新建业务专网或者新建、扩建、改建独立数据平台的；

（三）违反规定在公共数据平台外开发、升级改造应用系统的；

（四）违反规定重复收集数据的；

（五）未及时向公共数据平台归集数据或者归集的数据不符合标准要求的；

（六）未按照规定校核、封存、撤回公共数据或者关停数据应用的；

（七）未按照规定共享或者开放公共数据的；

（八）违反规定将共享获取的公共数据用于其他目的的；

（九）未依法履行公共数据安全管理职责的；

（十）违反本条例规定的其他情形。

公共管理和服务机构应当在规定期限内完成整改，并反馈整改情况；未按照要求整改的，由公共数据主管部门提请本级人民政府予以通报批评；情节严重的，由有权机关对负有责任的领导人员和直接责任人员依法给予处理。

第四十八条　公共数据主管部门及其工作人员在公共数据发展和管理工作中，不履行或者不正确履行本条例规定的职责，造成危害后果或者不良影响的，或者存在其他玩忽职守、滥用职权、徇私舞弊行为的，由有权机关对负有责任的领导人员和直接责任人员依法给予处理。

第四十九条　自然人、法人或者非法人组织有下列情形之一的，公共管理和

服务机构、公共数据主管部门应当按照职责责令改正，并暂时关闭其获取相关公共数据的权限；未按照要求改正的，对其终止开放相关公共数据：

（一）未经同意超出公共数据开放利用协议约定的范围使用数据的；

（二）未按照公共数据开放利用协议和安全承诺书采取安全保障措施的；

（三）严重违反公共数据平台安全管理规范的；

（四）其他严重违反公共数据开放利用协议的情形。

第五十条　自然人、法人或者非法人组织违反公共数据开放利用协议，第三方服务机构违反服务安全保护协议或者保密协议，授权运营单位违反授权运营协议，属于违反网络安全、数据安全、个人信息保护有关法律、法规规定的，由网信、公安等部门按照职责依法予以查处，相关不良信息依法记入其信用档案。

第八章　附则

第五十一条　本条例自2022年3月1日起施行。浙江省人民政府发布的《浙江省公共数据和电子政务管理办法》同时废止。

浙江省数字经济促进条例

（2020年12月24日浙江省第十三届人民代表大会
常务委员会第二十六次会议通过）

目录

第一章　总则

第一条 为了促进数字经济发展，加快建设现代化经济体系，提升核心竞争力，推动高质量发展，推进省域治理现代化，根据有关法律、行政法规，结合本省实际，制定本条例。

第二条 本省行政区域内促进数字经济发展，以及相关的数字政府、数字社会建设，适用本条例。

本条例所称数字经济，是指以数据资源为关键生产要素，以现代信息网络为主要载体，以信息通信技术融合应用、全要素数字化转型为重要推动力，促进效率提升和经济结构优化的新经济形态。

第三条 发展数字经济是本省经济社会发展的重要战略，应当遵循优先发展、应用先导、数据驱动、创新引领、人才支撑、包容审慎以及保障数据安全、保护个人信息的原则。

第四条 县级以上人民政府应当加强对数字经济发展工作的领导，将数字经济发展纳入国民经济和社会发展规划，建立健全数字经济发展工作协调机制，统筹政策制定，督促检查政策落实，协调数字经济发展中的重大问题，并将数字经济发展相关指标纳入高质量发展绩效评价体系。

县级以上人民政府应当采取措施，鼓励和支持开展数字技术研发和推广应用，培育和发展数字经济新产业、新业态和新模式，加快建设与数字经济发展相适应的技术创新体系、产业生态体系、公共服务体系和现代治理体系，营造有利于数字经济发展的最优环境。

第五条 省经济和信息化主管部门负责推进、协调、督促全省数字经济发展工作。

设区的市、县（市、区）人民政府经济和信息化主管部门或者设区的市、县（市、区）人民政府确定的其他部门（以下统称数字经济主管部门），负责推进、协调、督促本行政区域内的数字经济发展工作。

县级以上人民政府数据发展主管部门或者设区的市、县（市、区）人民政府确定的其他部门（以下统称公共数据主管部门），负责组织、指导、协调公共数据管理和推进政府数字化转型工作。

县级以上人民政府其他有关部门按照各自职责做好促进数字经济发展工作。

第六条 省经济和信息化主管部门会同省有关部门编制省数字经济发展规划，报省人民政府批准后组织实施。

设区的市、县（市、区）数字经济主管部门会同同级有关部门根据省数字经济发展规划的要求和实际需要，编制本地区数字经济发展规划，报本级人民政府批准后组织实施。

第七条 省标准化主管部门应当会同省经济和信息化等有关部门推进本省数字经济标准体系建设，建立和完善基础通用标准、关键技术标准、融合应用标准和安全评估标准等各类数字经济标准，指导和支持有关单位采用先进的数字经济标准。

县级以上人民政府应当组织和支持行业协会、产业联盟、龙头企业等参与制定数字经济国际标准、国家标准、行业标准和地方标准。鼓励行业协会、产业联盟、龙头企业等自主制定数字经济团体标准或者企业标准。

县级以上人民政府标准化主管部门、有关行政主管部门应当对标准的实施情况开展监督检查。

第八条 省经济和信息化主管部门应当会同统计等有关部门建立健全数字经济统计监测指标体系和发展综合评价体系，制定和完善数字经济核心产业统计分类目录，依法实施日常统计和运行监测，开展数字经济年度发展评价，定期向社会公布主要统计指标、监测结果和发展综合评价指数。

第九条 县级以上人民政府应当加强数字经济领域国际交流合作，参与“一带一路”建设，增强数字经济的资源集聚和发展辐射能力。

县级以上人民政府应当按照长三角区域一体化发展等国家战略要求，加强数字经济发展跨省域合作，推动重大数字基础设施共建共享、公共数据标准统一、

公共数据资源共享开放、智能制造协同发展，以及区域一体化协同治理和治理数字化应用。

县级以上人民政府应当加强省内数字经济跨区域合作，创新体制机制，加强政策协调，共同促进数字经济发展。

第二章 数字基础设施

第十条 本条例所称数字基础设施，是指以信息技术为支撑、以信息网络为基础，为经济、社会发展及居民生活提供感知、传输、存储、计算及融合应用等基础性信息服务的公共设施体系，主要包括信息网络基础设施、算力基础设施、新技术基础设施、融合基础设施、信息安全基础设施等。

第十一条 省经济和信息化主管部门应当会同有关部门，根据省数字经济发展规划的要求编制全省数字基础设施发展规划，按照省人民政府规定的权限报经批准后组织实施。

设区的市、县（市）人民政府数字经济主管部门应当会同有关部门，根据全省数字基础设施发展规划编制相关数字基础设施建设专项规划，报本级人民政府批准后组织实施。数字基础设施建设专项规划应当符合国土空间总体规划，并与市政、交通、电力、公共安全等相关基础设施专项规划相互协调和衔接。

编制、实施数字基础设施发展规划和建设专项规划应当遵循技术先进、适度超前、安全可靠、共建共享、避免重复、覆盖城乡、服务便捷的原则，重点推进新一代移动通信网、大数据中心、工业互联网、物联网、车联网、人工智能、区块链、卫星通信等新型数字基础设施建设，加快市政、交通、能源、电力、水利等传统基础设施的数字化改造。

县级以上人民政府应当探索建立跨行业基础设施“多规合一”体制机制，推动数字基础设施共建共享。

第十二条 县级以上人民政府及其有关部门、省通信管理机构，应当推进新一代移动通信网建设、光纤网络优化布局和互联网络演进升级，加强骨干网、城域网和接入网建设，提高网络容量、通信质量和传输速率。

县级以上人民政府及其有关部门、省通信管理机构，应当按照乡村振兴战略等要求，加强山区、海岛等地区网络基础设施建设，提升乡村光纤网络、移动网络建设水平和覆盖质量，实现农村电信普遍服务。

省发展改革、经济和信息化、自然资源等有关部门，应当按照陆海统筹、空天一体要求推动信息网络基础设施建设。

第十三条 县级以上人民政府及其有关部门、省通信管理机构，应当按照空间集聚、规模发展、技术先进、节能降耗的要求，加强高等级绿色数据中心建设和传统数据中心整合改造，推动云计算、边缘计算等多元计算协同发展，构建高效协同的数据处理体系。

第十四条 县级以上人民政府及其有关部门应当推动物联网技术发展，推进城乡基础设施、城乡治理、物流仓储、生产制造、生活服务等领域建设和应用感知系统，实现感知系统互联互通和数据共享。

第十五条 国土空间总体规划应当体现数字基础设施建设的相关要求，国土空间详细规划应当对数字基础设施建设专项规划确定的设施位置、空间布局等内容作出安排。

基础电信业务经营者应当按照数字基础设施建设专项规划的要求，科学合理做好基站、室内分布系统、多功能智能杆塔、汇聚机房布局。

第十六条 新建、扩建建设工程，根据国土空间详细规划需要配套建设数字基础设施的，国有建设用地使用权出让前，自然资源主管部门应当将配套建设数字基础设施的要求纳入规划条件。

新建、扩建建设工程，根据国土空间详细规划需要配套建设数字基础设施的，建设单位应当按照国家和省有关标准预留基站站址，配套建设机房、管道、电力线路、电器装置、防雷、接地等通信基础设施，并与主体工程同步设计、同步施工、同步验收。老旧小区改造应当配套建设前述通信基础设施。

建设工程移动通信基础设施建设标准，由省住房城乡建设主管部门会同省通信管理机构及有关单位制定。

第十七条 公共机构以及公共场所、公共设施的所有者、管理者或者使用者应当支持通信设施建设，按照国家和省有关规定开放建筑物、绿地、杆塔等资源，推进智慧杆塔建设和一杆多用。禁止收取进场费、分摊费等不合理费用。

第三章 数据资源

第十八条 数据资源管理应当遵循依法规范、促进流通、合理使用、保障安全的原则，加强数据资源全生命周期管理，提升数据要素质量，培育发展数据要素市场，促进大数据开发利用和产业发展，推进治理工作数字化。

本条例所称数据资源，是指以电子化形式记录和保存的具备原始性、可机器读取、可供社会化再利用的数据集合，包括公共数据和非公共数据。

本条例所称公共数据，是指国家机关、法律法规规章授权的具有管理公共事务职能的组织（以下统称公共管理和服务机构）在依法履行职责和提供公共服务过程中获取的数据资源，以及法律、法规规定纳入公共数据管理的其他数据资源。

第十九条 任何单位和个人收集、存储、使用、加工、传输、提供、公开数据资源，应当遵循合法、正当、必要的原则，遵守网络安全、数据安全、电子商务、个人信息保护等有关法律、法规以及国家标准的强制性要求，不得损害国家利益、社会公共利益或者他人合法权益。

第二十条 公共数据应当按照规定在公共管理和服务机构之间实现共享或者协同应用。通过共享获得的公共数据，应当用于履行本机构职责，不得用于其他目的。

公共管理和服务机构应当按照需求导向、分类分级、统一标准、安全可控、便捷高效的原则向社会开放公共数据。鼓励使用公共数据从事科学技术研究、咨询服务、产品开发、数据加工等活动。

公共数据采集单位对所采集数据的真实性、准确性、完整性负责。公共数据主管部门发现公共数据不准确、不完整或者不同采集单位提供的数据不一致的，可以要求采集单位限期核实、更正。采集单位应当在要求的期限内核实、更正。

公共数据共享和开放的具体办法，按照国家和省有关规定执行。

第二十一条 县级以上人民政府及其有关部门应当通过产业政策引导、社会资本引入、应用模式创新、强化合作交流等方式，引导企业、社会组织等单位和个人开放自有数据资源。

鼓励企业、社会组织等单位和个人通过省、设区的市公共数据平台，对外提供各类数据服务或者数据产品。

第二十二条 县级以上人民政府及其有关部门应当坚持保障安全与发展数字经济并重的原则，建立健全网络安全、数据安全保障体系，完善协调机制以及安全预警、安全处置机制。

县级以上人民政府有关部门应当加强对个人信息数据收集、存储、使用、加工、传输、提供、公开等活动的监督管理，依法查处个人信息数据泄露、窃取、篡改、非法使用等危害个人信息数据安全的违法活动。

网络运营者等有关单位和个人，应当依法建立健全数据安全管理制度，采取相应技术措施和其他必要措施，保障数据安全。

第四章　数字产业化

第二十三条 本条例所称数字产业化，是指现代信息技术通过市场化应用，形成电子信息制造业、软件和信息技术服务业、电信广播卫星传输服务业和互联网服务业等数字产业。

第二十四条 省人民政府应当根据全球数字经济的技术、产业发展趋势，结合本省数字产业发展水平和各地区经济禀赋差异，统筹规划全省数字产业发展，通过提升产业链、保障供应链安全、培育产业集群等方式，促进产业协同创新和供应保障，提高数字产业整体竞争力。

第二十五条 县级以上人民政府及其有关部门应当按照全省数字产业发展要求，结合本地区实际，通过规划引导、政策支持、市场主体培育等方式，重点推动集成电路、高端软件、数字安防、网络通信、智能计算、新型显示、新型元器件及材料、网络安全等产业发展，促进云计算、大数据、物联网、人工智能等技术与各产业深度融合，培育区块链、量子信息、柔性电子、虚拟现实等产业发展。

第二十六条 省人民政府及其有关部门应当推动国家和省实验室、重点实验室、技术创新中心、制造业创新中心、企业技术中心等科技创新平台和大型科技基础设施建设，支持科研机构、高等院校、企业参与建设有关平台和设施。

利用财政性资金或者国有资本购置、建设大型科学仪器设施的，应当在保障安全规范的前提下，为科研机构、高等院校、企业等开展创新活动提供共享服务。省科技主管部门应当建立大型科学仪器开放共享平台，为仪器设施共享提供信息发布、使用预约等服务。

鼓励、支持企业加强信息技术和产品研发，加大资金投入，加强人才引进和储备，培育研发机构，提升研发能力。

县级以上人民政府及其科技等部门应当培育和发展数字产业技术交易市场，促进技术转让、创新成果转化和产业化。

市场监督管理部门、司法机关等应当完善知识产权领域的区域和部门协作机制，建立健全知识产权快速维权体系，提供境内外知识产权维权援助。

第二十七条 县级以上人民政府及其有关部门应当采取措施，培育多层次、递进式的数字产业企业梯队，形成大中小微企业协同共生的数字经济产业生态。

鼓励和支持企业、科研机构、高等院校及其他单位或者个人创建数字经济领域科技企业孵化器、大学科技园和众创空间等线上线下创新创业平台。

鼓励提供数字产业化服务的第三方机构，为数字产业相关企业引进落地、融资增资、股改上市、平台化转型、跨境并购和合作等提供服务，推动数字产业发展。

第五章　产业数字化

第二十八条 本条例所称产业数字化，是指利用现代信息技术对工业、农业、服务业等产业进行全方位、全角度、全链条改造，提高全要素生产率，实现工业、农业、服务业等产业的数字化、网络化、智能化。

第二十九条 县级以上人民政府经济和信息化主管部门应当推动企业实施制造装备、生产线、车间、工厂的智能化改造和产品智能化升级，推进网络化协同、个性化定制、柔性化生产、共享制造等智能制造和服务型制造。

县级以上人民政府应当通过服务指导、试点示范、政策支持等方式，加大对工业互联网发展的支持力度，推进行业级、产业链级、区域级、企业级等工业互

联网平台建设及应用，推动工业技术软件化，促进大型企业开展研发设计、生产加工、经营管理、销售服务等集成创新，降低中小企业使用工业互联网成本，推动中小企业普及应用工业互联网。

鼓励和支持企业主动上云、深度用云，提升生产和管理效能。

第三十条 县级以上人民政府及其有关部门应当推进旅游、健康、家庭、养老、教育等生活性服务业数字化，推动数字技术和生活性服务业深度融合，丰富服务产品供给，促进生活消费方式升级。

县级以上人民政府及其有关部门应当通过培育服务业数字化转型试点等方式，推进研发设计、现代物流、检验检测服务、法律服务、商务咨询、人力资源服务等生产性服务业数字化，提升生产性服务业智能化、网络化、专业化水平。

县级以上人民政府及其有关部门应当通过建设数字文化创意产业试验区等方式，推进网络视听、数字影视、数字动漫、网络游戏、数字广告、互动新媒体等数字文化创意产业发展。

第三十一条 县级以上人民政府及其有关部门应当通过示范带动、技术指导、政策支持等方式，推广农业物联网应用，加快农业生产、农产品加工、农产品流通领域大数据基础和应用平台建设，加大农村仓储、物流、冷链设施建设支持力度，提升农业农村数字化、网络化、智能化改造和应用水平。

第三十二条 县级以上人民政府及其有关部门应当推进移动支付在全省域范围内的普及应用，有关国家机关、企事业单位、社会组织履行公共管理和公共服务职能时，应当推广应用移动支付，并鼓励市场主体应用移动支付。

省地方金融监督管理部门应当会同人民银行、银行保险监管、证券监管等有关机构制定相关政策，引导和支持现代信息技术在支付结算、信贷融资、保险业务、征信服务等金融领域融合应用，推动金融业数字化发展。

第三十三条 县级以上人民政府及其有关部门应当制定相关政策，引导和支持电子商务发展，促进跨境电商综合试验区建设，提升跨境电商普及应用水平，推广新零售，发展电子商务新业态新模式，推进数字生活新服务。

第三十四条 县级以上人民政府及其有关部门应当通过政策支持、市场主体培育等方式，促进互联网平台经济发展，推动建设产业互联网平台，完善工业、农业、服务业等互联网平台经济支撑体系，促进产业优化升级。

鼓励和支持工业信息工程企业、科研机构、高等院校及其他主体提供产业数字化转型第三方服务，加强对产业数字化转型的技术支撑保障，推动产业数字化转型。

鼓励互联网平台、提供产业数字化转型服务机构与中小微企业建立对接机制，针对不同行业的中小微企业需求场景提供数字化解决方案。

第三十五条 县级以上人民政府及其有关部门应当完善开发区（高新区）、小微企业园、农业产业园等各类园区的数字基础设施，提升园区数字化管理服务功能，加强现代信息技术在园区的融合应用，支撑园区内企业数字化转型和数字产业集聚发展。

第六章 治理数字化

第三十六条 本条例所称治理数字化，是指在政治、经济、文化、社会、生态文明等领域，运用现代信息技术，实现治理机制、方式和手段的数字化、网络化、智能化，推进治理体系和治理能力现代化。

县级以上人民政府应当推动建立政府监管、平台自治、行业自律、公众参与的多元共治体系，通过治理数字化促进数字经济发展。

第三十七条 县级以上人民政府及其有关部门应当深化“最多跑一次”改革，按照整体智治的要求，推动数字技术与政府履职全面深度融合，推进政务服务

、政府办公全流程网上办理、掌上办理，实现数据共享和业务协同，推进政府数字化转型。

前款规定以外的公共管理和服务机构，应当按照高水平推进省域治理现代化的要求，加强数字化建设和应用，提升治理效能。

第三十八条 省人民政府及其有关部门应当完善并规范使用全省统一的行政处罚办案系统，推进简易处罚的掌上办理，完善行政执法监管系统功能，推动行政执法与刑事司法衔接。

行政机关按照行政执法证据的要求进行采集、固定并经审核确认的电子监测记录，可以作为行政执法的证据。

鼓励有关部门依托物联网、区块链等技术，在教育、医疗、交通、邮政、生态环境保护、药品监管、工程建设、公共安全等重点领域推行监管智能化应用。

第三十九条 省、设区的市人民政府应当统筹规划和推进公共数据平台建设，实现基础设施、数据资源和公共应用支撑体系共建共享。

县级以上人民政府应当推进经济调节、市场监管、社会治理、生态环境保护、政府自身运行等领域的数字化应用体系建设，逐步实现政府履职全业务、全流程数字化，提高政府科学决策、高效监管、精准治理水平。

第四十条 县级以上人民政府及其有关部门应当按照省有关规定加强智慧城市建设，依托省、设区的市公共数据平台，推动“城市大脑”应用推广，促进现代信息技术在城市交通、平安建设、医疗健康、生态环境保护、文化旅游等领域的综合应用，通过数据资源整合共享，实现城市运行态势监测、公共资源配置、宏观决策、统一指挥调度和事件分拨处置数字化，提升城市治理水平。

县级以上人民政府应当加强乡村数字基础设施建设，促进现代信息技术在乡村产业发展、公共服务、农村集体资产管理等领域的综合应用，提升乡村治理水平。

第四十一条 县级以上人民政府及其教育主管部门应当加强教育领域数字基础设施和数字校园建设，加快数字技术与教育管理、教育教学的深度融合，采取措施支持符合条件的各类主体规范发展在线教育，培育优质数字教育资源。

县级以上人民政府及其卫生健康、医疗保障等有关部门应当加强智慧医疗健康体系建设，推广电子凭证、电子病历、电子处方、电子票据的应用，实行医疗检验、检查信息共享，拓展医疗保障数字化平台便民应用。

省人民政府及其民政部门应当加强智慧养老体系建设，建立全省统一的智慧养老服务平台。民政部门应当通过智慧养老服务平台，为各类用户提供简便快捷的养老政务服务、公共服务和链接市场服务。

第四十二条 县级以上人民政府及其有关部门应当按照省有关规定统筹规划和推进社会治理数字化转型，强化综合治理工作平台、市场监管平台、综合执法平台、便民服务平台等基层治理平台建设和运营管理，提高社会治理社会化、智能化和专业化水平。

县级以上人民政府及其有关部门应当按照省有关规定，开展未来社区示范建设，以数字技术提升精细化、网络化管理能力，构建未来邻里、教育、健康、创业等数字化创新应用场景。

第四十三条 县级以上人民政府及其有关部门应当创新监管理念和方式，对数字经济领域的新技术、新产业、新业态和新模式实行包容审慎监管。

省公安机关、市场监督管理等部门应当会同有关部门建立数字经济领域跨区域异地执法协调机制，实现违法线索互联、监管标准互通。

市场监督管理部门应当按照国家和省有关规定和要求，加强数字市场竞争监管，发挥行业协会、产业联盟和其他组织作用，维护公平竞争秩序。从事数字经济活动的单位和个人不得有滥用市场支配地位、实施垄断协议等行为以及从事不正当竞争活动。

第四十四条 互联网平台经营者应当依法依约履行产品和服务质量保障、消费者权益保护、生态环境保护、知识产权保护、网络安全与个人信息保护、劳动者权益保护等方面的义务，建立健全平台规则和用户账号信用管理、投诉举报等制度。鼓励互联网平台经营者建立争议在线解决机制，制定并公示争议解决规则。

省人民政府及其有关部门应当组织建设网络交易监测平台。有关部门应当通过网络交易监测平台，对互联网平台经营者以及网络交易违法行为实施在线监测，实现网络交易的风险预警、协同监管、电子存证。

第四十五条 鼓励和支持行业协会、产业联盟和其他组织在数字经济发展中发挥技术指导和服务作用。县级以上人民政府及其有关部门可以通过向行业协会等组织购买服务等方式，开展技术推广、职业技能培训和咨询服务。

数字经济行业协会、产业联盟和其他组织应当依法依规开展活动，加强自律管理，开展纠纷处理和信用评价，反映合理诉求，依法维护企业合法权益。

鼓励和支持企业、第三方机构和社会公众参与数字经济治理。

第四十六条 县级以上人民政府及其有关部门应当按照优化传统服务与创新数字服务并行的原则，制定和完善老年人等运用智能技术困难群体在出行、就医、消费、文娱、办事等方面的服务保障措施，保障和改善运用智能技术困难群体的基本服务需求和服务体验。

第七章 激励和保障措施

第四十七条 省人民政府设立数字经济产业投资基金，用于数字经济领域重大项目建设。

县级以上人民政府应当完善产业投资基金投资融资机制，引导社会资本投资数字经济领域重大项目，拓宽数字经济企业融资渠道。

第四十八条 省人民政府及其有关部门应当将数字经济重大科技攻关项目的自主创新研究、应用示范和产业化发展列入国家或者省科技发展规划、高新技术产业发展规划，并安排财政性资金予以支持。

县级以上人民政府及其有关部门应当根据省有关规定并结合实际，安排财政性资金支持数字产业化发展、产业数字化转型以及数字经济企业培育等，引导和支持社会资本参与数字经济发展。

第四十九条 省人民政府及其有关部门应当加强产业链协同创新统筹协调，引导和支持科研机构、高等院校、企业加强协同攻关，共同开展数字经济基础前沿研究和关键共性技术研究。

县级以上人民政府科技主管部门可以通过向企业和创业者发放科技创新券的方式，支持数字经济产业科技创新和科技成果转化。科技创新券可以用于购买科技成果、检验检测、研究开发设计、中间试验、科技评估、技术查新、知识产权服务、技术培训等服务。科技创新券在全省范围内使用。推动科技创新券在长三角地区通用通兑。

第五十条 省人民政府或者其授权的单位可以根据需要，将云计算、大数据、人工智能等数字技术产品和服务列入全省集中采购目录。

政府采购的采购人经依法批准，可以通过非公开招标方式，采购达到公开招标限额标准的首台（套）装备、首批次产品、首版次软件，支持数字技术产品和服务的应用推广。

第五十一条 县级以上人民政府及其有关部门应当落实国家和省对高新技术企业研发、信息技术产品制造、软件开发、信息服务以及科技企业孵化器、大学科技园和众创空间等线上线下创新创业平台的税费优惠，并为相关单位和个人办理税费优惠提供便利。

第五十二条 本省实行有利于数字经济发展的金融政策，对符合国家和省数字经济产业政策的项目、企业、园区、平台和创新人才，金融机构、地方金融组织应当在贷款、政策性融资担保以及其他金融服务等方面给予支持。

鼓励银行业金融机构适应产业数字化和数字产业化需求，创新金融服务，开发融资产品，提高信用贷款、中长期贷款等产品的比重，提供无还本续贷、循环贷款或者其他创新型续贷产品。

支持保险业金融机构为符合国家和省数字经济产业政策的项目、企业贷款提供保证保险和信用保险。县级以上人民政府可以安排资金用于保证保险和信用保险的风险补偿等。

鼓励数字经济企业通过股权投资、股票债券发行等方式融资，提高直接融资比例，改善融资结构。

第五十三条 县级以上人民政府及其有关部门应当完善政策措施，强化创新服务，在土地供应、电力接引、能耗指标、频谱资源等方面优先保障数字经济发展。

第五十四条 县级以上人民政府及其有关部门应当支持举办数字经济领域的国内国际展览、赛事、论坛等活动，搭建数字经济展示、交易、交流、合作平台，帮助建立供需对接渠道，提高企业市场开拓能力。

县级以上人民政府及其有关部门应当支持数字经济领域企业参加境内外展览展销等活动。

第五十五条 县级以上人民政府及其有关部门应当制定扶持政策，加强数字经济领域关键核心技术人才培养，将数字经济领域引进高层次、高学历、高技能以及紧缺人才纳入政府人才支持政策体系，为其在职称评定、住房、落户、医疗保健，以及配偶就业、子女入学等方面提供支持。

教育、人力资源社会保障等部门应当指导和督促高等院校、职业学校开设数字经济专业、课程，培养数字经济研究和应用型人才。

高等院校、科研机构、职业学校等应当通过与企业产学研合作、共建实习实训基地等方式，培养符合数字经济发展需求的相关人才。

第五十六条 县级以上人民政府及其有关部门应当加强数字经济法律、法规、规章以及技术、知识的宣传、教育、培训，提升全民数字素养和数字技能。

教育、人力资源社会保障等部门应当指导和督促学校及其他教育机构将数字经济知识纳入教育教学内容，公务员主管部门应当将数字经济知识纳入公务员教育培训内容。

广播、电视、报刊、互联网等新闻媒体应当开展数字经济公益性宣传。鼓励社会团体、企事业单位加强员工数字经济知识培训，提升应用、管理和服务水平。

第五十七条 县级以上人民政府人力资源社会保障主管部门应当按照省有关规定，加强对数字经济新业态用工服务的指导，积极探索灵活多样的用工方式，

制定和完善数字经济新业态从业人员在工作时间、报酬支付、保险保障等方面规定，保障数字经济新业态从业人员的合法权益。

数字经济新业态从业人员通过互联网平台注册并接单，提供网约车、外卖或者快递等劳务的，平台经营者可以通过单险种参加工伤保险的形式为从业人员提供工伤保险待遇。平台经营者单险种参加工伤保险的，社会保险经办机构应当予以办理。法律、行政法规另有规定的，从其规定。

第五十八条 促进数字经济发展工作中出现失误，但同时符合下列条件的，对有关单位和个人不作负面评价：

（一）符合国家和省确定的改革方向；

（二）未违反法律、法规禁止性、义务性规定；

（三）决策程序符合法律、法规规定；

（四）勤勉尽责、未牟取私利；

（五）主动挽回损失、消除不良影响或者有效阻止危害结果发生。

第八章 法律责任

第五十九条 违反本条例规定的行为，法律、行政法规已有法律责任规定的，从其规定。

第六十条 建设单位违反本条例第十六条第二款规定，新建、扩建建设工程未按国家和省有关标准预留基站站址或者配套建设机房、管道、电力线路、电器装置、防雷、接地等通信基础设施的，由县级以上人民政府住房城乡建设主管部门责令限期改正；逾期不改正的，处五万元以上二十万元以下罚款。

第六十一条 县级以上人民政府有关部门、单位及其工作人员在促进数字经济发展中有下列行为之一的，由有权机关按照法定职责责令改正；情节严重的，对直接负责的主管人员和其他直接责任人员依法给予处分：

（一）篡改、伪造或者指使篡改、伪造数字经济主要统计指标的；

（二）未按规定履行公共数据共享和开放职责的；

（三）未按规定核实、更正公共数据的；

（四）其他玩忽职守、滥用职权、徇私舞弊的行为。

第九章 附则

第六十二条 本条例自2021年3月1日起施行。《浙江省信息化促进条例》同时废止。