



11TH

2024年陕西省 第十一届全国网络安全宣传周

THE ELEVENTH NATIONAL CYBER SECURITY PUBLICITY
WEEK OF SHAANXI PROVINCE

· 网络安全为人民 网络安全靠人民 ·



前言

2024年国家网络安全宣传周将于2024年9月9日-15日举行，主题是“网络安全为人民、网络安全靠人民”，全国各省（直辖市、自治区）同步开展。陕西省第十一届国家网络安全宣传周由省委宣传部、省委网信办、省教育厅、省公安厅、省通信管理局、省总工会、共青团陕西省委、省妇女联合会和中国人民银行陕西省分行等九部门联合举办。将深入宣传《网络安全法》《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》等法律法规，《未成年人网络保护条例》《网络暴力信息治理规定》《促进和规范数据跨境流动规定》《互联网政务应用安全管理规定》等政策文件。开展相关宣传活动，编写发放宣传资料，推动媒体、社会团体广泛开展宣传普及、推进关键信息基础设施保护、大数据安全、个人信息保护等工作，通过展览、论坛、知识竞赛等多种形式，以及报刊、电台、电视台、网站等传播渠道，普及网络安全知识，提升全社会网络安全意识和防护技能，全面加强网络安全保障体系和能力建设，不断打造网络安全工作新格局。

“没有网络安全就没有国家安全，没有信息化就没有现代化”。网络安全和信息化已经成为事关国家安全、经济社会安全和国家发展的重大战略问题，要求我们必须贯彻以人民为中心的发展思想，本着对社会负责、对人民负责、对国家负责的态度，发展好网信事业、治理好网络空间、守护好这个亿万民众共同的精神家园，让互联网更好地造福人民。



2024年陕西省
第十一届国家网络安全宣传周
THE ELEVENTH NATIONAL CYBER SECURITY PUBLICITY
WEEK 2024 - SHANXI PROVINCE

中共陕西省委网信办
陕西省互联网信息办公室



9

活动时间

2024年9月9日 - 15日

主题日活动



网络安全为人民 网络安全靠人民

9月10日，校园日

9月11日，电信日

9月12日，法治日

9月13日，金融日

9月14日，青少年日

9月15日，个人信息保护日

活动介绍



举办单位

省委宣传部、省委网信办、省教育厅、省公安厅、
省通信管理局、省总工会、共青团陕西省委、省妇女联合会、
中国人民银行陕西省分行

重要活动



网络安全宣传周开幕式、网络安全博览会、
网络安全技术应用论坛、网络安全主题日活动、
网络安全进基层

法律

《中华人民共和国网络安全法》（节选）

06 — 09

行政法规

《未成年人网络保护条例》

10 — 23

部门规章

《网络暴力信息治理规定》

24 — 31

《促进和规范数据跨境流动规定》

32 — 35

《互联网政务应用安全管理规定》

36 — 44

《中华人民共和国网络安全法》

(节选)

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。

法律部分





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。



《未成年人网络保护条例》

《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。

行政
法规



目录

第一章	总则
第二章	网络素养促进
第三章	网络信息内容规范
第四章	个人信息网络保护
第五章	网络沉迷防治
第六章	法律责任
第七章	附则



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不信息的具体种类、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思。

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思。

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日户、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。

《网络暴力信息治理规定》

《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。



目录

- 第一章 总则
- 第二章 一般规定
- 第三章 预防预警
- 第四章 信息和账号处置
- 第五章 保护机制
- 第六章 监督管理和法律责任
- 第七章 附则

部门
规章





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,依法依规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,应当依法依规采取限制发言、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规采取警示、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。



《促进和规范数据跨境流动规定》

《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。



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,免于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,免于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,免于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器向境外提供负面清单外的数据,可以免于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 数据处理器向境外提供数据,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器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。

《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。



目录

- 第一章 总则
- 第二章 开办和建设
- 第三章 信息安全
- 第四章 网络和数据安全
- 第五章 电子邮件安全
- 第六章 监测预警和应急处置
- 第七章 监督管理
- 第八章 附则

部门规章





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 and 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。

