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）

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。

（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）破坏国家宗教政策，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）宣传淫秽、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）含有法律、行政法规禁止的其他内容的。

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。