

武汉市数据局文件

武数据发〔2025〕4号

市数据局关于印发武汉市 电子政务外网管理办法（试行）的通知

各区人民政府，市直各部门和单位：

《武汉市电子政务外网管理办法（试行）》已经市人民政府同意，现印发给你们，请认真贯彻落实。



武汉市电子政务外网管理办法（试行）

第一章 总 则

第一条 为进一步加强全市电子政务外网（以下简称“政务外网”）管理，提升网络支撑能力，确保网络安全、可靠、高效和稳定运行，根据《中华人民共和国网络安全法》等相关法律法规、国家政务外网管理相关标准规范和湖北省有关规定，结合本市实际，制定本办法。

第二条 本办法适用于全市政务外网建设、接入、运行、安全管理等活动。

第三条 本办法所称的政务外网是指按照国家、湖北省有关要求和技术标准建设的，服务于各级政务部门及开展政务应用的其他单位，满足其政务服务、社会管理和公共服务等方面需要的非涉密政务公共网络，与互联网逻辑隔离，实现“国家-省-市-区-街道（乡镇）”五级互联，支撑跨部门、跨层级、跨地区的数据共享和业务协同。

第四条 本市政务外网管理遵循“统筹规划、统一标准、分级管理、协同管控、保障安全”的原则。

第二章 职责分工

第五条 市级数据行政管理部门是市级政务外网主管部门，负责指导监督和协调推进全市政务外网工作。承担市级政务外网

规划建设、接入管理、运行维护和安全管理等技术保障工作的单位（简称市级政务外网运行管理机构），按照政务外网相关标准规范，指导区级政务外网建设运行管理有关工作。

第六条 各区人民政府（含武汉东湖新技术开发区、武汉长江新区、武汉经济技术开发区、武汉市东湖生态旅游风景区管委会，下同）应明确本区政务外网主管部门和运行管理机构，按照国家、省、市统一规划和标准规范，健全制度规范，做好本级政务外网建设和运行管理工作。

第七条 接入单位负责本单位（含下属单位）接入政务外网的管理工作。

第三章 规划建设

第八条 市级政务外网由全市统一的光传输网（OTN）承载，具有大带宽、低时延、高可靠、可扩展等特点，能够满足全场景政务业务承载的网络需求。

第九条 各级政务部门不得新建非密业务专网，已建成的应按程序融合连通政务外网或由光传输网（OTN）承载，国家和湖北省另有规定除外。

第十条 政务外网采用的软件、硬件和技术路线按照国家法律、政策法规要求，强化安全可靠技术和产品应用，切实提高自主可控水平。

第十一条 政务外网应基于 IPv6 下一代互联网体系开展软硬件设施建设，确保对互联网协议第六版（IPv6）的全面支持。

原则上应直接使用 IPv6 地址，非必要不再使用 IPv4 地址。

第十二条 政务外网网络安全按照国家网络安全等级保护要求实施防护，政务外网应达到信息系统网络安全等级保护第三级要求。

第十三条 政务外网上使用的密码产品或密码部件要符合国家密码管理有关法律法规和标准规范。

第十四条 政务外网互联网出口实行统一出口、统一管理，各接入单位原则上不再单独建设或租用互联网出口，应通过本级政务外网统一出口接入互联网。政务外网涉及跨境数据交换的，按国家有关规定执行。

第四章 接入管理

第十五条 网络接入包括光传输网(OTN)接入和政务外网接入。

第十六条 本市政务外网实行分级接入。原则上，市级单位接入到市级政务外网，区级及以下单位接入到区级政务外网。

市级政务外网运行管理机构负责市级单位与国家、省级政务外网的网络对接工作；区级政务外网运行管理机构负责区级及以下单位与国家、省级政务外网的网络对接工作。

第十七条 光传输网(OTN)接入仅面向具有部门业务专网的市级单位，由业务主管部门向市级政务外网主管部门提出光传输网(OTN)使用申请和实施方案，经市级政务外网主管部门审核同意后实施接入。

第十八条 政务外网接入由接入单位向同级政务外网主管部门提出申请，经政务外网主管部门审核同意后实施接入。市直二

级单位、非政务部门因工作需要确需接入政务外网的，应由行政或业务主管部门提出网络接入申请。未经允许，任何单位和个人不得以任何方式接入政务外网。接入所需相关费用由接入单位自行承担。

第十九条 接入单位应当在符合国家网络安全等级保护要求的前提下接入政务外网。接入单位应健全相关管理制度，明确分管领导、责任部门 and 责任人，及时报同级政务外网主管部门备案。

第二十条 政务外网接入可以采用专线直连、互联网 VPN 安全加密等多种方式。

位于同一办公地址的接入单位原则上采用共用政务外网链路的方式实施接入，接入单位有义务配合政务外网运行管理机构调整链路和设备的使用范围。

第二十一条 接入单位在政务外网网络开通后三个月内未开展联网应用的，政务外网运行管理机构应通知接入单位说明原因，接入单位未说明原因或主动要求关闭的，政务外网运行管理机构视情况关闭其接入链路。接入单位申请重新开通的，应重新申请并说明理由。

第五章 运行维护

第二十二条 政务外网运行管理机构应按照相关规范要求，构建网络运行支撑体系，健全上下贯通、职责明确、运转高效的政务外网长效运行管理机制，提升网络调优、故障处置和协同联动能力，确保政务外网稳定运行。

第二十三条 政务外网运行管理机构应当建立网络运行保障

制度、组建运维团队，负责网络运行监控、故障处理等运行维护工作，为接入单位提供技术支持和服务，及时响应事故报修和故障处理，提升政务外网服务能力。

第二十四条 政务外网运行管理机构进行网络调试升级，应提前两个工作日通知涉及的接入单位。接入单位调试、升级本单位网络，可能对政务外网运行造成影响的，应提前向政务外网运行管理机构申请，经批准后方可实施。

第二十五条 市级政务外网运行管理机构负责全市政务外网 IPv4/IPv6 地址规划和分配管理，区级政务外网运行管理机构负责本区政务外网 IPv4/IPv6 地址细化和分配管理。接入单位负责业务与终端地址管理。

第二十六条 市级政务外网运行管理机构按照国家政务外网相关标准规范要求提供域名申请、域名解析等域名管理服务，建立域名系统相关运维管理制度，接入单位发布信息系统应向同级政务外网运行管理机构申请政务外网域名。

第二十七条 政务外网上运行的信息系统实行备案制。接入单位部署在政务外网的信息系统，应在上线、变更、停用前向同级政务外网主管部门备案。

第六章 安全管理

第二十八条 政务外网主管部门、运行管理机构和接入单位应建立健全网络安全管理机制，按照“谁建设谁负责、谁管理谁负责、谁使用谁负责”的原则落实网络安全管理责任。

第二十九条 政务外网主管部门和接入单位应建立健全政务

外网安全防御体系，在网络侧、互联网接入侧、用户接入侧部署合规有效的安全防护措施，全方位保障政务外网网络安全。

第三十条 政务外网运行管理机构和接入单位应强化日常监测、通报预警和应急处置，不断拓展网络安全态势感知监测范围，加强大规模网络安全事件预警、发现和处置能力。

第三十一条 接入单位要对接入政务外网的设备和终端建立台账，并采取符合要求的安全防护措施，有效防范计算机病毒、网络攻击和网络入侵等行为。接入政务外网的终端实行专机专用，不得联通其他网络。

第三十二条 接入政务外网的信息系统和政务云平台，应按国家网络安全等级保护、关键信息基础设施安全保护、商用密码应用等相关要求，落实网络安全措施。信息系统上线前应做好相关安全检测工作，确保安全后方可上线运行。

第三十三条 政务外网运行管理机构和接入单位应建立健全网络安全应急预案和应急响应联动机制，定期开展网络安全风险评估和应急演练，提升应急处置能力。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，防止危害扩大。

第三十四条 接入单位不得随意变更政务外网的连接线路和网络接入设备，不得安装、接入无线设备；不得将涉密计算机、设备（含存储介质）和网络接入政务外网；不得利用政务外网存储、处理、传输涉密信息；严禁通过政务外网从事非法活动。

第三十五条 接入单位出现网络安全问题，经政务外网运行管理机构确认会影响政务外网中其它设备正常运行的，政务外网运行管理机构有权中断其网络连接。

第三十六条 政务外网主管部门及运行管理机构应定期对政务外网运行、使用和安全管理等情况进行检查，及时向本级信息安全主管部门报告发现的重大网络安全事件，并责成存在问题的单位进行整改。

第七章 附 则

第三十七条 各区可根据本办法制定本级政务外网建设管理实施细则。

第三十八条 本办法由武汉市数据局负责解释。

第三十九条 本办法自 2025 年 6 月 16 日起实施。