江苏省人民政府办公厅关于印发江苏省电子政务外网管理办法(试行)的通知

苏政办发〔2023〕32号

各市、县(市、区)人民政府,省各委办厅局,省各直属单位:

《江苏省电子政务外网管理办法(试行)》已经省人民政府同意,现印发给你们,请认真贯彻实施。

江苏省人民政府办公厅

2023年9月5日

江苏省电子政务外网管理办法(试行)

第一章 总 则

第一条 为进一步加强全省电子政务外网(以下简称政务外网)建设管理,提升网络支撑能力和安全保障能力,确保网络安全可靠、高效稳定运行,根据《中华人民共和国网络安全法》等相关法律法规和国家政务外网管理相关标准规范,结合我省实际,制定本办法。

第二条 本办法适用于全省政务外网建设、接入、运行、安全管理等活动。

第三条 本办法所称全省政务外网,是国家政务外网的组成部分,与互联网逻辑隔离,为非涉密网络。

省政务外网由省级政务外网和设区市及以下政务外网组成,服务全省各级党委、人大、政府、政协、纪委监委、法院、检察院和人民团体等,主要运行各级政务部门数字化履职的非涉密业务和不需在政务内网运行的业务,支撑跨

部门、跨层级、跨区域数据共享和业务协同，满足科学决策、社会治理、公共服务等工作需要。

第四条 省政务外网遵循统一规划、统一标准、统一管理、统筹建设、分级负责、保障安全的原则。

第五条 除国家另有规定外，各级部门和单位不得新建非涉密业务专网；已经建成的，应当按相关标准规范整合至政务外网。

第二章 职责分工

第六条 省政务服务管理办公室是省级政务外网主管部门，负责制定相关标准规范，组织、协调、指导、监督全省政务外网管理工作。省大数据管理中心是省级政务外网运行管理机构，按照政务外网相关标准规范，承担建设和运行管理相关工作。

第七条 各设区市政府应明确政务外网主管部门和运行管理机构，按照国家、省统一规划和标准规范，健全制度规范，层层压实责任，做好本地区政务外网建设和运行管理工作。涉及政务外网重大建设或调整事项，应及时报省政务服务管理办公室备案。

第八条 政务外网接入部门和单位（以下简称接入部门）负责本部门及其下属机构接入政务外网的管理工作。

第三章 接入管理

第九条 全省各级党政机关、事业单位、中央驻苏单位、法律法规授权的具有管理公共事务职能的单位和因履行工作职责需要接入政务外网的其他单位，按照属地管理原则，向当地政务外网主管部门申请接入政务外网。未经政务外网主管部门同意，任何部门和单位不得擅自扩大政务外网接入范围。

第十条 申请接入政务外网的部门和单位（以下简称申请部门）提出的申请，应当包括接入理由、接入范围、接入位置、预测流量、技术要求等内容。接入需求同时涉及省市两级政务外网的，由申请部门统一向省政务服务管理办公室提出申请。

第十一条 政务外网主管部门对接入申请进行审核确认，对符合要求的，应当在10个工作日内审核批准，由政务外网运行管理机构指导协助申请部门制定接入方案，在30个工作日内完成接入实施工作；条件不具备或审核未通过的，应当在10个工作日内告知原因。

第十二条 接入部门应健全相关管理制度，明确分管领导、责任部门和责任人，及时报同级政务外网主管部门备案。

第四章 运行管理

第十三条 政务外网运行管理机构应按照相关规范要求，构建运行支撑体系和安全监测体系，健全上下贯通、职责明确、运转高效的长效管理机制，提升网络质量分析、安全监测、态势预警和故障处置能力，确保政务外网安全稳定运行。

第十四条 政务外网运行管理机构应强化网络基础设施资产管控能力，健全网络资源动态调整机制，主动监测分析并合理优化配置网络资源。

第十五条 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部门。接入部门调试、升级本部门网络，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。

第十六条 政务外网上运行的信息系统实行备案制。接入部门部署在政务外网的信息系统，应在上线或发生变更前向同级政务外网运行管理机构备案。

接入部门网络资源需求发生变更的，应提前向政务外网运行管理机构申请。

第十七条 接入部门因机构变更等原因不再具有政务外网业务需求的，应及时向政务外网主管部门申请撤销政务外网接入节点。

第五章 IP地址与域名管理

第十八条 省大数据管理中心负责全省政务外网IPv4/IPv6地址规划与分配管理，设区市政务外网运行管理机构负责当地政务外网IPv4/IPv6地址细化

与分配管理。

第十九条 政务外网运行管理机构负责互联地址管理，接入部门负责业务及终端地址管理。

第二十条 省大数据管理中心负责全省政务外网域名规划、编制与分配管理，设区市政务外网运行管理机构负责当地政务外网域名细化编制与分配管理。接入部门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，并通过域名提供服务。

第六章 安全管理

第二十一条 政务外网运行管理机构和接入部门应落实国家网络安全等级保护、关键信息基础设施保护、密码应用安全性评估、信任体系建设以及工作秘密信息管理等相关要求。新建、改建、扩建政务外网，应同步规划、同步建设、同步运行网络安全保障体系。

第二十二条 政务外网主管部门、运行管理机构和接入部门应建立健全网络安全组织机构和管理制度，按照“谁主管谁负责、谁运行谁负责、谁使用谁负责”的原则落实网络安全管理责任和数字化建设外包网络安全管理要求。

第二十三条 接入政务外网的网络应做好边界管理和内部网络安全管理，与其他网络做好隔离。

第二十四条 接入政务外网的终端实行专机专用，不得联通互联网或其他网络。所有终端和设备在入网前，应采取符合要求的安全防护措施，有效防范计算机病毒和网络攻击、网络侵入等危害网络和数据安全行为。

第二十五条 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制度和关键信息基础设施安全保护、密码应用、工作秘密信息管理等相关要求，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。信息系统与互联网及其他网络进行业务交互应通过统一的安全交换区进行。

第二十六条 政务外网运行管理机构和接入部门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，切实提升应急处置能力，及时发现、定位、分析、处置安全事件。

接入部门出现网络安全问题，影响政务外网正常运行的，政务外网运行管理机构有权中断其政务外网连接。

第二十七条 任何部门、单位和个人不得将涉密的计算机、设备（含存储介质）或网络接入政务外网；不得利用政务外网存储、处理、传输涉密信息；不得利用政务外网从事危害国家安全、传播有害信息、非法侵入信息系统等法律法规禁止的活动。

第七章 监督与检查

第二十八条 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，对网络安全事件进行通报，责令存在问题的部门、单位限期整改。

第二十九条 接入部门有下列情形之一的，由政务外网主管部门予以通报；造成严重后果的，由相关主管部门依法依规追究相应责任。

（一）不履行网络安全保护义务的；

（二）拒绝或阻碍有关部门依法依规实施监督检查的。

第八章 附 则

第三十条 各设区市可参照本办法制定管理细则。

第三十一条 本办法由省政务服务管理办公室负责解释。

第三十二条 本办法自印发之日起施行。