郎溪县数据资源管理局关于印发《郎溪县电子政务外网管理办法》的通知

县直各单位、镇（街道）、有关企业:

为进一步加强全县电子政务外网管理，根据《安徽省电子政务外网管理办法(试行)》(皖数资〔2021〕9号)及《宣城市电子政务外网管理实施细则(试行)》，制定《郎溪县电子政务外网管理办法》，现印发给你们，请认真贯彻落实。

2024年10月14日

郎溪县电子政务外网管理办法

第一章　总　则

第一条　为进一步加强全县电子政务外网管理，提升网络支撑能力，保障安全、可靠、稳定、高效运行，根据国家、省、市有关规定，结合我县实际，制定本管理办法。

第二条　电子政务外网是全县电子政务重要基础设施，与互联网逻辑隔离，主要包括横向城域网，覆盖县域政务部门，并向乡镇（街道）、村（社区）延伸。

电子政务外网主要运行政务部门面向社会的专业性服务业务和不需在内网上运行的业务，满足县域政务部门社会管理、公共服务等需要。

第三条　电子政务外网的建设和管理应遵循统一规划、集约保障、应用共享的原则。

第四条　本管理办法适用于因工作需要需接入县电子政务外网或通过县电子政务外网连接国家和省市电子政务外网的部门和单位。

第五条　除国家、省、市另有规定外，行政机关不得新建非涉密专网；已经建成的，原则上应当分类实现与电子政务外网迁移整合或融合互联。

第二章　职责分工

第六条 县数据资源管理局是县级政务外网主管部门，负责以下工作:

（一）负责全县电子政务外网城域网的规划、建设、运维和安全管理工作;

（二）依据国家、省、市标准规范及本管理办法，负责县域电子政务外网网络地址接入申请审核和监督管理工作;

（三）指导乡镇（街道）、村（社区）电子政务外网建设与运维安全管理;

（四）负责与市级主管部门对接，并接受业务和技术指导;

（五）配合市级主管部门完成电子政务外网纵向信息系统在郎溪县落地实施。

第七条 电子政务外网接入单位负责以下工作:

（一）按照电子政务外网技术规范要求，负责本单位局域网的运维和安全监测管理工作;

（二）保障本单位内部的服务器、虚拟机和终端的安全，做好电子政务外网和互联网的隔离措施，防止引入病毒;

（三）加强本单位账号安全管理，避免账号信息泄露，对账号的所有操作负责;

（四）负责协调完成本单位局域网与电子政务外网的对接工作。

第三章　业务管理

第八条　属于下列情形之一的单位，可以接入电子政务外网：

（一）各类党政机关、群团组织和事业单位；

（二）上级部门要求接入电子政务外网的驻郎单位；

（三）为保障业务主管部门履行工作职责，确有需要接入电子政务外网的其他单位。

第九条　申请或变更电子政务外网相关业务执行以下流程：

（一）申请。接入单位向主管部门提出网络接入或变更申请，包括申请依据、接入地址等具体业务需求；

（二）审核。主管部门在5个工作日内对申请、变更依据等进行合规性、合理性审核。审核通过的，主管部门应当及时落实网络接入开通或变更；审核未通过的，应当将理由及时告知相关单位；

（三）制定方案。接入单位和主管部门联合制定业务实施技术方案；

（四）实施。具备实施条件的，主管部门应在10个工作日内连同拟接入运营商配合接入单位组织完成。涉及跨地区、跨部门的业务，由接入单位会同主管部门联合组织实施；

（五）业务测试。接入单位测试业务运行状况，向主管部门反馈测试结果。

第十条 接入单位在电子政务外网开通后3个月内未开展联网应用的，主管部门有权关闭其接入链路，并书面通知接入单位。接入单位申请重新开通的，须重新申请并说明理由。

接入单位需要调试电子政务外网接入设备的，须提前3个工作日向主管部门报备。

第四章 安全保障

第十一条 主管部门在网信部门指导下，会同公安部门加强电子政务外网安全管理，建立安全管理制度，落实安全管理责任，采取安全监测、预警等措施，保障电子政务外网网络安全。接入单位应当建立本单位安全管理制度，采取安全措施，保障本单位网络安全。

第十二条 县级电子政务外网应达到网络安全等级保护第三级的要求。主管部门按相关规定，主动做好网络安全等级保护备案、测评等工作。

第十三条 主管部门要加强电子政务外网安全防护，主要负责包括但不限于以下工作:

（一）做好全县电子政务外网安全保障工作;

（二）在进行电子政务外网规划、设计和建设时，应同步规划、同步建设、同步使用安全技术措施;

（三）利用市级电子政务外网安全监测平台，组织开展

网络安全监测、大数据分析、态势感知、预警通报等网络安全管理工作，及时发现、定位、分析、控制安全事件，责成存在问题的单位进行整改，形成可视、可管、可控、可调度、可持续扩展的安全防护体系；

（四）联合运营商制定网络安全事件应急预案，并定期开展应急演练。发现重大故障、安全事件要及时处理，并向上级主管部门及时报告，对较大及以上网络安全事件需同步向本级网信、公安部门报告；接入单位出现网络安全问题，影响或可能影响电子政务外网正常运行的，主管部门有权中断其与电子政务外网的连接，责令整改；

（五）指导运营商加强安全日志审计工作，日志审计记录的保存时间不少于半年。

第十四条 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做好电子政务外网接入工作；落实安全技术措施，开展安全检查等，保障本单位内部的服务器、虚拟机和终端的安全，做好电子政务外网和互联网的隔离措施，避免引入病毒；加强本单位账号安全管理，避免账号信息泄露，对账号的所有操作负责。接入单位应做好边界安全防护，防止本单位局域网设备攻击电子政务外网，如若出现此类情况，由接入单位开展溯源、查杀等安全处置。

第十五条 接入单位不得随意变更电子政务外网的连接线路和网络接入设备；不得将涉密计算机、设备（含存储

介质）和网络接入电子政务外网，不得利用电子政务外网存储、处理、传输涉密信息；严禁通过电子政务外网从事非法活动。

第十六条 未经主管部门授权审批，运营商不得私自开通电子政务外网专线，一经发现，主管部门将视情节严重给予全县通报、封停接入单位外网 IP、取消运营商电子政务外网接入资格等处罚。

第五章 评估管理

第十七条 主管部门每年组织对电子政务外网运行质量开展综合评估，主要评估接入单位的管理配合度、安全保护等情况。对发生危害电子政务外网正常运行或利用电子政务外网从事非法活动等情形的，由主管部门或网信、公安等其他有权机关给予通报批评，情节严重或造成严重后果的，依法依规进行责任追究。

第六章 附 则

第十八条 本办法由县数据资源管理局负责解释。

第十九条 本办法自印发之日起施行。