湖南省电子政务外网安全管理暂行办法

第一章 总则

第一条 为保障湖南省电子政务外网(以下简称省政务外网)的运行安全，落实政务外网相关部门的安全责任，根据《[中华人民共和国网络安全法](https://baike.baidu.com/item/%E4%B8%AD%E5%8D%8E%E4%BA%BA%E6%B0%91%E5%85%B1%E5%92%8C%E5%9B%BD%E7%BD%91%E7%BB%9C%E5%AE%89%E5%85%A8%E6%B3%95/16843044?fromModule=lemma_inlink" \t "https://baike.baidu.com/item/%E6%B9%96%E5%8D%97%E7%9C%81%E7%94%B5%E5%AD%90%E6%94%BF%E5%8A%A1%E5%A4%96%E7%BD%91%E5%AE%89%E5%85%A8%E7%AE%A1%E7%90%86%E6%9A%82%E8%A1%8C%E5%8A%9E%E6%B3%95/_blank)》等有关[法律](https://baike.baidu.com/item/%E6%B3%95%E5%BE%8B/84813?fromModule=lemma_inlink" \t "https://baike.baidu.com/item/%E6%B9%96%E5%8D%97%E7%9C%81%E7%94%B5%E5%AD%90%E6%94%BF%E5%8A%A1%E5%A4%96%E7%BD%91%E5%AE%89%E5%85%A8%E7%AE%A1%E7%90%86%E6%9A%82%E8%A1%8C%E5%8A%9E%E6%B3%95/_blank)、[法规](https://baike.baidu.com/item/%E6%B3%95%E8%A7%84/3040487?fromModule=lemma_inlink" \t "https://baike.baidu.com/item/%E6%B9%96%E5%8D%97%E7%9C%81%E7%94%B5%E5%AD%90%E6%94%BF%E5%8A%A1%E5%A4%96%E7%BD%91%E5%AE%89%E5%85%A8%E7%AE%A1%E7%90%86%E6%9A%82%E8%A1%8C%E5%8A%9E%E6%B3%95/_blank)，以及国家电子政务外网的各项标准规范，结合我省实际，制定本办法。

第二条 省政务外网是国家电子政务外网的组成部分，由省、市州、县市区、乡镇(街道)、行政村(社区)五级政务外网组成，上联国家，横向连接各级党委、人大、政府、政协、法院、检察院及其所直属各部门(单位)，纵向覆盖省、市州、县市区、乡镇(街道)、行政村(社区)。政务外网是我省电子政务的公共基础设施，承载全省政务部门非涉密信息化系统，实现基础信息资源开放共享。

第三条 本办法适用于本省政务外网各级建设运维安全管理单位，依托政务外网开展信息化系统建设的各级政务部门，以及接入政务外网的各单位。

第二章 总体要求

第四条 各级政务外网建设运维安全管理单位(以下简称政务外网管理单位)要严格落实网络安全工作责任制，履行关键信息基础设施的相关安全保护义务，做好采购产品和服务的安全评估工作，采取措施保护政务外网安全。

第五条 省级和市级政务外网应达到等级保护2.0三级标准，县级政务外网应达到等级保护2.0二级标准。

接入政务外网的信息化系统正式对外提供服务前，应当按照国家网络安全等级保护制度要求，落实网络安全主体责任和安全技术措施，完成等级保护测评备案、整改加固，通过验收后方可正式上线提供服务。

第六条 接入政务外网的信息化系统，应当使用由具备资格的机构检测认证合格的商用密码产品，进行加密保护和安全认证。

第三章 职责分工

第七条 政务外网按照“谁管理谁负责、谁建设谁负责、谁使用谁负责、谁发布谁负责”的原则，分级建设、分级管理、各负其责。

省政府发展研究中心(省政府政务服务中心)负责全省政务外网建设的整体规划，制定本省政务外网的标准规范，负责省级政务外网的建设、运维及安全管理工作，指导全省政务外网的建设、运维及安全管理工作，制定电子政务外网统一接入标准，定期组织市州及县市区开展相关业务培训，并向国家政务外网管理部门报告。

省公安厅负责政务外网网络安全的监督、检查、指导和违法犯罪案件的查处。

省互联网信息办公室负责统筹协调政务外网网络安全工作和相关监督管理工作。

各市州人民政府应明确一个本级政务外网管理单位，负责本级政务外网的统一建设、运维及安全管理工作。各县市区人民政府应明确一个本级政务外网管理单位，负责本级以及下辖乡镇(街道)、行政村(社区)的政务外网统一建设、运维及安全管理工作。

接入政务外网的单位负责本单位局域网和接入政务外网的信息系统安全，负责本单位发布内容安全。

各级政务外网使用单位应当确定至少两名本单位工作人员作为政务外网安全联系人，并且将联系人名单提交给本级政务外网管理单位。

第八条 各级政务外网管理单位是本级政务外网的安全责任主体，各政务外网接入单位是本单位政务外网的安全责任主体。

政务外网安全工作实行领导责任制。各级政务外网管理单位主要领导是本级政务外网安全第一责任人，分管政务外网的领导是直接责任人;各接入单位的主要领导是本单位政务外网安全的第一责任人。

各运营商、承建商、运维公司、外包服务公司等按合同规定承担相应的安全责任。

第九条 各级政务外网管理单位参照本办法制定本级政务外网安全管理制度，报上一级政务外网管理单位备案。各政务外网接入单位应制定本单位的信息安全管理制度，报本级政务外网管理单位备案。

第四章 运维管理

第十条 各级政务外网管理单位应做好安全保障系统的规划、设计和建设工作，落实运行维护管理中的安全检查、等级保护测评和风险评估等工作责任。各级财政应保障本级政务外网的建设、运维和安全管理经费。

第十一条 各级政务外网管理单位要开展网络安全监控工作，及时发现、定位、分析、处置安全事件，每6个月向上一级政务外网管理单位汇报网络安全状况。发生重大网络安全事件的，应立即报告公安、网信、国安等信息安全主管职能部门。

第十二条 各级政务外网管理单位都应组织制定本级政务外网网络与信息安全应急预案，并定期开展应急演练。

第十三条 各级政务外网管理单位都要加强安全审计工作，审计记录的保存时间不少于6个月。

第十四条 各级政务外网管理单位应当按照国家政务外网安全检查和风险评估统一要求，定期组织开展网络与信息安全自查和风险评估，并按照信息安全主管职能部门和上级政务外网管理单位的要求做好本级政务外网信息安全检查和风险评估工作。

各级政务外网管理单位应将本级政务外网自查结果及时报上一级政务外网管理单位。在自查中发现接入单位存在问题的，应责成存在问题的单位进行整改。对问题较严重的单位，原则上应立即断开其政务外网连接，待整改完成后再重新接入。

第十五条 各级政务外网管理单位要建立信息安全定期报告制度，每3个月向上一级政务外网管理单位报告本级政务外网出现的信息安全事件。

第十六条 各级政务外网管理单位要加强信息安全教育，每年至少对本级从事信息安全工作的人员开展一次专业技术培训。

第十七条 各级政务外网管理单位及接入部门应对从事政务外网信息安全工作的人员按照“分工负责、职责明确、最小授权和任期有限”的原则进行管理。

第十八条 各级政务外网管理单位应设置系统管理、安全管理和安全审计岗位，分别负责网络运行、安全和审计工作。系统管理员、安全管理员和安全审计员的权限设置应相互独立、相互制约。

第十九条 管理、使用政务外网的各级单位，应当同运维机构签订保密协议，并且约定运维机构同运维人员个人签订保密协议。运维机构签署的所有的保密协议都应当提交到政务外网的管理、使用单位备案。

第二十条 政务外网管理单位应当对运维机构、人员进行安全审查，对人员准入进行规范。

第五章 接入管理

第二十一条 接入政务外网的单位，应统一使用政务外网的互联网出口。如果单位确实需要独立的互联网出口，应报本级政务外网管理单位备案。

第二十二条 各级政务外网管理单位部署在各接入单位的设备，由政务外网管理单位管理运维，各接入单位无权登录，不得擅自关闭设备、修改配置。

未经政务外网管理单位许可，各接入单位不得改变政务外网接口的网络设备、结构或配置，不得在政务外网上搭接无线网络设备。

第二十三条 通过专线方式接入政务外网的单位局域网或业务系统，接入单位要保障本单位网络、系统的安全，应参照所接入政务外网的等级保护级别标准(二级或三级)，按照国家等级保护工作要求，开展测评整改，明确接入网络安全责任人。达到所接入政务外网的安全标准后，方能接入政务外网。

专线接入政务外网的单位应防止本单位局域网内的设备对政务外网进行攻击。如果出现这类情况，应根据攻击情况和系统影响范围报本级政务外网管理单位后断开政务外网连接，进行溯源、查杀等安全处置。

第二十四条 单机接入政务外网的，应明确安全责任人，保证接入政务外网的单机安全，避免中病毒或木马，避免成为攻击政务外网的跳板。当发现接入政务外网的单机有异常情况时，应先断开与政务外网的连接，立即对事故进行处置，并将异常情况及处置结果及时报本级政务外网管理单位。

第二十五条 通过拨号或VPN方式接入政务外网的单位，应明确安全责任人，要保障接入账号及接入终端的安全，避免非授权用户获取账号密码信息接入政务外网，避免含有恶意软件的终端接入政务外网。接入政务外网后不得有危害政务外网安全的行为。当发现接入政务外网的终端有异常情况时，应先断开与政务外网的连接，立即对事故进行处置，并将异常情况及处置结果及时报本级政务外网管理单位。

第二十六条 所有依托于政务外网运行的应用系统，所开放的端口应由使用单位提出要求并对每个端口的用途做出说明，经本级政务外网管理单位核准后开放。

第二十七条 各单位如果有独立的业务专网，并且业务专网需要与政务外网进行数据交换，使用单位应当自行在业务专网和政务外网之间部署隔离设备，并由各单位自行负责数据摆渡。

将现有业务专网迁入政务外网内运行的单位，迁移方案须经过省政府发展研究中心同意。

第二十八条 各单位依托于省政务外网新建业务专网，应首先与本级政务外网管理单位进行沟通，建设方案须经过本级政务外网管理单位同意，并报省政府发展研究中心备案。

第二十九条 依托于省政务外网运行的业务专网，应当与政务外网内的其他专网互相隔离。

第六章 安全管理边界

第三十条 各级政务外网管理单位应防止本级政务外网内的设备攻击本级以外政务外网。如果出现这种情况，由故障设备所属政务外网管理单位负责开展溯源、查杀等安全处置。

第三十一条 所有接入政务外网的单位需保障本单位内部的服务器、虚拟机和终端的安全，避免引入病毒或木马，需保障本单位所辖账户的安全，避免账户信息泄漏，对所辖账户的所有操作负责。接入政务外网的单位应防止本单位局域网设备攻击政务外网。如果出现这种情况，由接入单位负责开展溯源、查杀等安全处置。

第三十二条 使用省级政务外网网络、云平台、大数据平台及其他基础设施的单位，应严格控制所申请资源的使用范围，不得利用省级政务外网的网络、算力、存储、数据、基础设施等资源开展批准范围之外的应用。

第三十三条 使用省级政务外网统一云平台部署应用系统的省直单位，负责虚拟主机的操作系统、中间件及应用系统的安全和数据安全，并对该系统的访问控制进行优化，提出最小化开放策略。

第三十四条 设备托管在政务外网机房的单位，要保障托管设备及其系统层、应用层的安全和数据安全。

第三十五条 利用政务外网的机房、设备搭建业务专网的单位，要保障该专网的安全。

第三十六条 利用省级政务外网短信网关、网站集约化平台、邮件系统等基础设施平台发布信息的单位，对本单位发布的信息内容负责。

第七章 附则

第三十七条 本办法自发布之日起施行。 [2]