西藏自治区气象局网络安全管理实施细则

（试行）

# 第一章 总则

1. 为贯彻落实《中华人民共和国网络安全法》、《中国气象局网络安全管理办法（试行）》，规范西藏气象部门网络安全管理，提高信息网络安全保护能力，保障全区气象部门网络安全，结合实际，制定本实施细则。
2. 本细则适用于西藏气象部门非涉密系统的网络安全管理。

# 第二章 组织管理

1. 西藏气象部门网络安全遵循国家网络安全法律法规、技术标准和中国气象局相关文件规定，坚持依法依规管理，按照“明确责任、提高能力、加强监控、主动防御、确保安全”方针，构建西藏气象部门网络安全防线。
2. 西藏自治区气象局观测与网络处（以下简称观测处）负责西藏自治区气象局网络安全管理，统筹协调、部署全区气象部门网络安全工作，监督检查全区气象部门网络安全工作执行情况。

**第五条** 西藏自治区气象局有关职能处室按照归口管理原则，负责气象新闻、气象服务产品等通过网站、电视、广播、微信、短信、抖音等信息化手段发布的信息安全监督。

**第六条** 西藏自治区气象信息网络中心（以下简称信息中心）是全区气象部门网络安全运行与技术监管单位，负责全区网络安全防御体系技术设计；负责新建项目规划设计的网络安全审查；负责通用性、基础性网络安全防护系统运行；负责全区气象部门网络安全态势监测和网络安全预警信息发布；牵头重大网络安全事件应急处置；为其它单位提供网络安全技术指导和咨询建议。

**第七条** 区局各直属事业单位和各地（市）、县级气象部门（以下简称运行管理单位）负责本单位（部门）网络安全工作的组织落实、制度建设、能力建设、监督检查、问题整改和应急处置。运行管理单位领导班子主要负责人是本单位网络安全第一责任人，主管网络安全的领导班子成员是直接责任人。

**第八条** 按照“谁主管谁负责，谁建设谁负责，谁运行谁负责，谁使用谁负责”的原则，运行管理单位落实网络安全责任，建立健全覆盖各系统的网络安全责任制，指定部门或专人负责网络安全，确定每个系统的网络安全责任人。

**第九条** 按照网络安全等级保护（以下简称等级保护）制度规定和国家标准，建立健全基础信息网络、云计算平台/系统、大数据应用/平台/资源、物联网（IoT）、工业控制系统和采用移动互联技术的系统等（以下简称等级保护对象）及场地环境和运维人员等网络安全管理制度。重点加强信息基础设施资源池、大数据云平台和气象观测、预报、服务、政务、培训等系统的网络安全管理制度。

# 第三章 规划建设管理

**第十条** 全区气象部门所有等级保护对象均应按照《中华人民共和国网络安全法》，遵循“同步规划、同步建设、同步运行”原则，遵照国家等级保护标准进行设计、定级、建设、备案、测评和运维管理。其中，气象观测系统应根据组成部分性质，按国家等级保护标准中的信息系统、物联网或工业控制系统等相关要求开展等级保护工作。

**第十一条** 等级保护对象建设单位负责在建设阶段同步落实等级保护制度。在项目设计阶段按照国家等级保护标准，合理确定所建等级保护对象的等级保护级别，确定与等级保护级别对应的网络安全方案，落实相关建设经费，按对应等级保护标准开展建设。

新建项目规划设计方案应通过网络安全审查，信息中心组织网络安全技术、管理专家，组成专家组开展审查并出具网络安全审查意见。

新建等级保护对象未确定等级保护级别的，或未取得网络安全审查意见的，或网络安全审查意见认为网络安全保护方案不完善的，不予立项。等级保护对象建设单位应落实相关网络安全建设经费，新建信息系统项目网络安全预算低于项目总预算5%的，原则上不予立项。

**第十二条** 新建等级保护对象在试运行阶段，其建设单位负责向属地公安部门完成等级保护备案，并按照备案要求开展等级保护测评和网络安全风险评估，定级备案结果报观测处。

等级保护测评达不到定级标准要求的系统，必须通过整改达到相应要求，否则不能通过业务验收和竣工验收。

**第十三条** 安全保护等级第三级及以上级别的保护对象，其定级或级别调整的，由运行管理单位根据《信息安全技术网络安全等级保护定级指南》（GA/T 1389-2017）进行初步定级，经区局批准报中国气象局预报司进行专家评审、审批确定，最后由运行管理单位向公安部门提交相关材料以完成备案（备案调整）审查。

安全保护等级第二级的保护对象，其定级或级别调整（调低）的，由运行管理单位根据《信息安全技术网络安全等级保护定级指南》（GA/T 1389-2017）进行初步定级，然后组织专家对初步定级结果的合理性进行评审，最后将初步定级结果和专家评审意见报观测处审批；观测处出具的审批文件作为运行管理单位向公安部门提交备案（备案调整）审查的依据。

安全保护等级第一级的保护对象，其定级由运行管理单位根据《信息安全技术网络安全等级保护定级指南》（GA/T 1389-2017）进行自主定级，并对定级结果的合理性进行评审，最后将定级结果和专家评审意见报观测处备案。

在全区范围安装部署的等级保护对象由牵头建设的运行管理单位统一定级并向公安部门备案，各分系统由运行管理单位按统一定级级别向当地公安部门备案，备案时不得自行更改分系统的等级保护级别和定级对象内容。

**第十四条** 等级保护对象拟确定为区级关键信息基础设施，或区级关键信息基础设施拟调整、变更的，所属运行管理单位需报观测处，观测处按照地方要求组织运行管理单位进行确定，并报中国气象局预报司备案。

# 第四章 运行管理

**第十五条** 各运行管理单位应贯彻落实网络安全法律法规，落实网络安全保护责任，按等级保护制度要求做好等级保护对象的运行管理，保障等级保护对象的网络安全。

**第十六条** 各运行管理单位所负责的网络软、硬件系统，或购置、使用的网络关键设备和网络安全专用产品应当符合相关国家标准的强制性要求，并应得到持续的安全维护。

**第十七条** 各运行管理单位应加强所辖机房场地网络安全管理，为等级保护对象提供安全的运行场所，包括但不限于：

（一）机房场地应达到所承载等级保护最高级别等级保护对象的网络安全要求，其不间断电源、油机发电机等系统在需要时应能够正常工作。

（二）建立外部人员进入机房审批制度。机房应配置电子门禁系统和监控系统，控制外部人员进入，记录其行为，电子门禁系统和视频监控系统的记录留存不得少于180天。

**第十八条** 建立健全网络管控制度。对全区气象网络系统实行分区分域管理，严格控制跨区跨域通信，加强应用内容控制，包括但不限于：

（一）加强局域网与气象广域网、行业专线、电子政务外网和互联网的网络边界安全管控。关闭网络上的威胁端口。严格禁止非气象部门的单位、组织或个人直接连接到局域网络中访问气象应用及数据资源。特殊部门用户气象数据访问接口必须由信息中心统一提供，严格禁止其他事业单位和地（市）、县级气象部门对外提供网络接口。

（二）严格管控互联网出口，互联网出口由信息中心统一集约建设、运行和管理。互联网与局域网之间必须安装防火墙、入侵防御、网络审计等网络安全控制设备，控制设备由信息中心统一管理。

地（市）和县级气象部门不得自建互联网出口，但可在确保与业务内网物理隔离的前提下，做好相应的网络安全防护措施后，建设小规模网络用于互联网访问。

（三）运行管理单位提供对外服务的应用系统必须严格部署在DMZ区（隔离区），DMZ区由信息中心建设、运行和管理。DMZ区与局域网络之间必须安装网络安全控制设备，控制设备由信息中心统一管理，采用白名单方式实施严格访问控制。所有对外服务区的互联网流量需要通过探针搜集全部流量，接入信息中心的网络安全态势感知平台。

（四）远程访问局域网络资源的虚拟专用网（VPN）仅供气象部门员工使用，必须且仅能由控制局域网与互联网连接的网络安全设备提供。虚拟专用网系统应采用包括密码技术的至少两种鉴别技术对用户每次登录进行身份标识和鉴别，身份鉴别信息具有复杂度要求并定期更换，应具备登录连接超时自动退出等措施。用户按国家法律法规使用。VPN账户申请由观测处审批，离职、退休人员账户必须及时注销。

（五）除由信息中心正式设置的虚拟专用网外，禁止任何形式的由互联网以及互联网对外服务区主动进入局域网络的网络访问，禁止通过互联网以及互联网对外服务区对局域网络计算机进行远程控制、桌面共享、数据传输等的应用。

（六）严格禁止在局域网络内设立访问局域网络或互联网络的无线网络访问设备。访问互联网的无线访问设备应与局域网络物理隔离，并按国家法律法规采取网络安全管控措施。区局大院互联网无线网络访问系统由信息中心统一集约建设和管控。各单位不得自建无线网络访问系统。

**第十九条** 西藏气象网络与外部的互联互通，包括区局业务网络外部门接入、区局互联网IP资源使用等，应同时符合其他管理规定要求。

**第二十条** 加强用户终端管理，保障用户终端安全，包括但不限于：

（一）关闭主机上不必要的端口、共享访问及远程桌面连接。

（二）信息中心统一部署上网行为监控管理系统和计算机防病毒系统，实现所有用户计算机、服务器和信息基础设施资源池中虚拟机的全覆盖，未部署防病毒系统的计算机或服务器禁止接入业务内网。

（三）严格执行气象内网、专网系统的补丁升级和漏洞修复措施。定期对重要数据进行备份。

（四）积极使用自主可控的国产正版操作系统、办公软件和防病毒软件。

（五）及时更新或升级用户终端的操作系统等系统软件，确保得到安全补丁支持。

（六）禁止通过一机双卡、使用网络切换器、内外网网线换插等方式实现内网计算机访问互联网或互联网计算机访问内网。

（七）禁止使用非本单位的移动存储介质，本单位内部在使用移动存储介质时，应采取有效的技术措施先检测其安全情况，确认安全后方可使用。

**第二十一条** 加强联网标识、感应、控制设备及摄像头等物联网设备管理，强化运行状态监测，及时修复安全漏洞，防止设备被利用实施分布式拒绝服务攻击。

**第二十二条** 加强用户管理。具备用户身份识别、访问授权、权限控制和行为记录能力。加强离职人员使用的业务及应用系统账户管理，及时更改密码或注销账户。各应用系统账户采用实名制。尽量减少公用账户开设，必须开设的公用账户应确定其责任人。

**第二十三条** 加强信息系统的口令管理，强制使用强安全口令并定期更换，采取技术手段杜绝默认口令、弱口令、通用口令和长期不变口令，加强对暴力破解口令的技术防范措施。使用国家密码管理主管部门认证核准的密码技术和产品，落实国家密码应用政策要求，加强国产商用密码技术和产品应用。

**第二十四条** 采取有效措施加强气象数据和公民个人信息安全管理，包括但不限于：

（一）梳理内部网络与互联网上各信息系统中采集、存储（含缓存）、传输、使用、提供、销毁等环节的气象数据和公民个人信息等数据，形成数据资产清单并及时更新。数据资产清单每年按要求报观测处备案。

（二）严格数据访问授权，建立覆盖数据生命周期的用户实名制数据访问管控机制和数据追踪技术手段。加强对数据环境中数据访问和气象业务应用系统中数据使用的日志记录与日常审计，排查、解决数据泄露安全隐患。

（三）采取数据分类、备份、加密等措施，保障数据安全。加强互联网出口监控，及时发现并阻断数据异常流出。存储气象数据和大量公民个人信息的数据库接入互联网应采取严格安全防范措施。

（四）关键信息基础设施运行中收集和产生的重要数据应在境内存储，因业务需要确需向境外提供的，应按照国家有关规定进行安全评估后根据评估结果提供。

（五）依法收集公民个人信息，不得收集与气象业务、服务无关的公民个人信息。采取技术手段和其他必要措施，保障收集的公民个人信息安全。不得泄露、篡改、毁损收集的公民个人信息。未经被收集者同意，不得向他人提供公民个人信息。

**第二十五条** 全区气象部门只能采购通过了国家云计算服务安全评估的云计算服务。使用互联网云计算服务的信息系统，由负责该系统运行的单位按网络安全管理要求加强管理并承担其网络安全管理责任。

**第二十六条** 加强电子邮件系统管理。自建或租用电子邮件系统应具备安全防护和安全威胁清洗措施，用户密码符合管理要求。关闭邮件自动转发功能。及时清理非在职人员邮箱。

**第二十七条** 严格管控系统建设、开发和运维等文档。不得在公共云中存储相关文档。确保文档中包含的IP地址、网络连接、系统配置、用户口令、程序源码等技术细节不对外泄露。

**第二十八条** 严格控制网络安全态势感知等系统获取、存储的数据，确保其仅在气象部门网络范围内存储和使用。

**第二十九条** 运行管理单位应对已上线运行但三个月内未使用的等级保护对象采取断网、停机等下线措施，再次上线使用前应当开展漏洞修补、病毒库更新等工作。对停机下线不再使用的，应按等级保护规定做好剩余信息保护，并妥善处理其存储的数据。

**第三十条** 运行管理单位要与系统开发、运维等单位和个人按照等级保护等规定签订网络安全服务协议，明确外部人员的安全责任与义务，规定所获取内部数据等资源的使用与扩散范围。建立健全外部人员承担的系统开发及系统维护管理制度，加强人员背景审核，加强外部人员使用气象信息系统和数据等资源的权限管理与日志存留。

**第三十一条** 外部运维人员现场接入局域网络，应对其计算机进行安全检查，确保其满足网络安全要求后方能接入，接入过程中需派人全程陪同监督使用。

# 第五章 网站和气象服务手段管理

**第三十二条** 落实网站安全责任制，确定每个网站的网络安全责任人。切实增强网站的网络安全防护能力。运行管理单位要将网站的运行情况、内容变更和网络安全情况纳入实时业务监控。移动应用软件服务端按网站管理。

**第三十三条** 网站要获得网站公安备案号、电信与信息服务业务经营许可证（ICP）号、等级保护备案号等，事业单位网站要加挂“事业单位网站”标识。不具有行政管理职能的事业单位网站禁止使用“gov.cn”域名。

**第三十四条** 网站因网络安全隐患被要求整改并实施整改后，或网站新栏目、新功能上线之前，必须进行安全测评。安全测评由建设单位或委托第三方网络安全服务机构开展。根据测评结果完成问题整改，并达到相应网络安全要求后方可上线。

**第三十五条** 建立覆盖气象服务产品制作、审核、发布等全工作流程的网络安全管理制度。建立健全电话、手机短信、广播、影视、对外网站、移动应用软件、大喇叭和显示屏等对外服务手段信息发布和内容审核制度，明确审核的程序和责任，确保发布内容的合法性、真实性、准确性和安全性。

**第三十六条** 通过电话、手机短信、广播电台、电视台、网站、移动终端等开展气象服务的，应明确与电信运营商、广播电台、电视台、内容分发及网络服务提供商等的网络安全责任，做到节目（内容）提供与安全发布（播出）界限清晰，责任明确。

**第三十七条** 为公共广播电台、电视台制作提供广播和影视气象节目的，应建立节目移交审核登记制度，确保播出内容安全。

**第三十八条** 广播、影视直播节目需具备必要的延时手段和应急措施，强化对节目的监控，监督参与直播的人员遵守直播管理制度和技术设备操作规范。

**第三十九条** 大喇叭和显示屏等必须采用密码技术，具备身份认证等技术手段，避免使用远程和无线方式管理，坚决屏蔽非法内容，确保播出或显示内容正确。对公共区域的LED屏幕和大喇叭，要明确专人负责，承担安全责任。

**第四十条** 利用电话、手机短信、广播、影视、对外网站、移动应用软件、大喇叭、显示屏等开展非汉语类气象服务时，需配备具备该语言能力、能够胜任相应语言节目制作、审核等工作的专业人员。

# 第六章 监控、预警、通报和应急

**第四十一条** 信息中心开展全区气象部门网络安全态势监测，建立常态化网络安全信息汇集与分析研判机制，综合网络安全运行情况及接收的网络安全信息通报，及时研判、发布、报送网络安全监测预警信息。在安全可控的前提下，鼓励利用社会力量提升全区气象部门网络安全监测预警能力。

**第四十二条** 区局建立全区气象网络安全信息通报机制。各运行管理单位确定通报机制负责人和通报联络员，明确职责任务、信息报送流程，建立内部通报机制，及时报送、传达网络安全风险和监测预警信息，有针对性地及时组织开展检查、整改工作。国家重大活动、重要会议等敏感时期，应向观测处报告每日网络安全保障情况。

**第四十三条** 各运行管理单位应制定完善本单位网络安全事件应急预案和各等级保护对象的应急预案，建立应急技术队伍，明确网络安全应急流程，切实提高应急预案的可行性和可操作性。

**第四十四条** 信息中心负责制定完善网络安全应急演练方案，观测处每年至少组织开展一次网络安全应急演练。

**第四十五条** 各运行管理单位按照等级保护工作要求，做好重要数据备份，建立重要信息系统应急备份机制，推动应急备份系统建设。

# 第七章 经费保障和宣传培训

**第四十六条** 各运行管理单位要加大网络安全相关人力、财力、物力的支持和保障力度，将网络安全经费纳入年度预算，统筹安排专项经费开展网络安全建设和保障工作。

**第四十七条** 加强网络安全宣传与人才培养。各运行管理单位要积极参与国家网络安全宣传周活动，要采取多种方式加强网络安全培训，实现网络安全培训全员化、常态化。新入职员工培训和领导干部培训需安排网络安全内容。同时，各运行管理单位要强化网络安全人才培养，提高网络安全人才专业技能。

# 第八章 监督考核和表彰

**第四十八条** 观测处组织开展全区气象部门的年度网络安全检查，一般采用现场检查、在线扫描和攻防演练等形式。各运行管理单位定期对等级保护对象进行网络安全自查，发现问题及时整改。

**第四十九条** 区局将网络安全工作纳入各运行管理单位重点工作任务开展年度目标考核，重点对网络安全责任落实、等级保护制度落实、关键信息基础设施保护、网络安全攻防演练结果、网络安全事故等情况开展考核，考核结果作为领导班子和有关领导干部综合考核评价的重要内容。

**第五十条** 在网络安全建设、技术应用、运维保障、应急处置和信息通报等方面做出突出贡献或工作业绩优秀的技术人员，优先推荐为西藏自治区气象局年度气象信息网络工作优秀个人。对工作特别突出或业绩特别优秀的技术人员，直接推荐为年度全国优秀气象信息技术人员。

# 第九章 责任追究

**第五十一条** 对违反或未能正确履行本细则第十至第十二条和第四至第六章的相关规定，视情节和产生的后果，依据有关规定追究当事人、网络安全负责人直至主要负责人责任；协调监管不力的，还应追究网络安全管理职能部门负责人责任。

**第五十二条** 有下列情形之一的，对责任单位、责任人进行提醒，责令整改：

（一）未按“同步规划、同步建设、同步运行”原则，未遵照国家等级保护标准，对等级保护对象进行设计、定级、建设、备案、测评和运维管理的。

（二）未落实网络管控、分区分域管理要求，或允许非气象部门的单位、组织或个人连接到气象局域网络，或私自接入互联网，或在局域网络内设立访问局域网络的无线网络访问设备的。

（三）允许外单位移动存储介质在本单位计算机上使用的。

（四）未按本细则要求对用户进行实名制管理，或存在默认口令、弱口令、通用口令和长期不变口令的。

（五）未按本细则要求加强重要数据和公民个人信息安全管理的。

（六）未按本细则要求加强网站和气象服务手段管理的。

（七）未按本细则要求与系统开发、运维等单位和个人签订网络安全服务协议，或外部人员安全管理制度不健全的。

（八）等级保护对象存在安全隐患和漏洞，未按期整改，可能导致门户网站或其它对外网站及对外服务手段等页面或信息被篡改、重要数据或公民个人信息被窃取或泄露、对关键信息基础设施运行安全造成威胁等，未造成实质性损失、危害或不良影响的。

**第五十三条** 有下列情形之一的，对责任单位领导班子主要负责人或主管网络安全的领导班子成员进行警示约谈：

（一）等级保护第三级及以上级别等级保护对象存在安全隐患和漏洞，未造成实质性损失、危害或不良影响的。

（二）其它级别等级保护对象存在安全隐患和漏洞，造成一般性损失、危害或不良影响的。

（三）门户网站受到攻击未及时处置，导致网站瘫痪或违法有害信息扩散，且未按要求上报的。

（四）其它对外网站、对外服务手段等存在安全隐患和漏洞，导致被攻击篡改，未造成实质性损失、危害或不良影响的。

（五）等级保护第三级及以上级别等级保护对象存在安全隐患和漏洞，导致重要数据或公民个人信息被窃取、泄露、篡改或损毁，造成一般性损失、危害或不良影响的。

（六）关键信息基础设施存在安全隐患和漏洞，对关键信息基础设施运行安全造成严重威胁的。

（七）发生其它网络安全事件未及时处置或未按要求上报的。

（八）责令整改事项未按期整改，或年内责令整改事项反复发生的。

**第五十四条** 有下列情形之一的，对责任单位和相关责任人进行通报批评：

（一）等级保护第三级及以上级别等级保护对象存在安全隐患和漏洞，造成一般性损失、危害或不良影响的。

（二）其它级别等级保护对象存在安全隐患和漏洞，造成严重损失、危害或不良影响的。

（三）门户网站受到攻击未及时处置和上报，瘫痪时间小于6小时的。

（四）其它对外网站、对外服务手段等被攻击篡改，且未及时组织处置和上报，造成一般性损失、危害或不良影响的。

（五）等级保护第三级及以上级别等级保护对象存在安全隐患和漏洞，导致重要数据或公民个人信息被窃取、泄露、篡改或损毁，造成严重损失、危害或不良影响的。

（六）关键信息基础设施遭受网络安全攻击，未及时处置导致无法正常运行的，造成一般性损失、危害或不良影响的。

（七）发生其它网络安全事件未及时处置或未按要求上报的，造成一般性损失、危害或不良影响的。

（八）警示约谈事项未按期整改，或年内警示约谈事项反复发生的。

**第五十五条** 有下列情形之一的，除对责任单位和相关责任人进行通报批评外，视情节，由相关部门按照干部管理权限和有关规定，给予相关责任人组织处理或纪律处分：

（一）等级保护第三级及以上级别等级保护对象存在安全隐患和漏洞，造成严重损失、危害或不良影响的。

（二）门户网站受到攻击瘫痪6小时以上，或其它对外网站、对外服务手段等被攻击篡改，且未及时组织处置和上报，导致反动言论或谣言等违法有害信息大面积扩散的。

（三）等级保护第三级及以上级别等级保护对象存在安全隐患和漏洞，导致大量重要数据或大面积公民个人信息被泄露、篡改或损毁，造成严重损失、危害或不良影响的。

（四）关键信息基础设施遭受网络安全攻击，未及时处置导致大面积影响人民群众工作、生活，或者造成重大经济损失，或者造成严重不良社会影响的。

（五）封锁、瞒报网络安全事件情况，拒不配合有关部门依法开展调查、处置工作，或者对有关部门通报的问题和风险隐患不及时整改并造成严重后果的。

（六）阻碍国家有关机关依法维护国家安全、侦察犯罪以及防范、调查恐怖活动，或者拒不提供支持和保障的。

（七）发生其它网络安全事件未及时处置或未按要求上报的，造成严重损失、危害或不良影响的。

（八）通报批评事项未按期整改，或年内通报批评事项反复发生的。

**第五十六条** 实施责任追究应实事求是，分清集体责任和个人责任。追究集体责任时，领导班子主要负责人和主管网络安全的领导班子成员承担主要领导责任，参与相关工作决策的领导班子其他成员承担重要领导责任。

**第五十七条** 违反《中华人民共和国网络安全法》的，依法追究责任。

# 第十章 附则

**第五十八条** 本细则由观测处负责解释。

**第五十九条** 本细则自印发之日起施行。