XXX 单位

网络信息安全管理机制汇编 v2.0

（2022 年 10 月 20 日发布，2022 年 11 月 1 日起实施）

XXX 单位

2022 年 10 月 20 日

声　明

本文档归 XXX 单位所有。本文对网络安全与信息化建设过程中各项工作进行规定，旨在规范单位信息安全管理工作，请各部门自觉学习、遵守，管理制度由单位信息化建设领导小组负责解释。

文件名称	XXX单位网络信息安全管理机制汇编v2.0		
文件编号	20221020001	**控制级别**	内部资料（保密）
文件类别	管理制度	**文件页数**	
编制	信息中心	**日期**	2022年10月9日
审核	信息安全领导小组	**日期**	2022年10月16日
签发	信息安全领导小组	**日期**	2022年10月20日

目 录

第一章 安全策略总纲

1.1、信息安全策略总纲

1.1.1、 总则

第一条 为贯彻国家对信息安全的规定和要求，指导本单位信息系统的使用、维护和管理过程中，实现信息系统安全防护的基本目的，提高信息系统的安全性，防范和控制系统故障和风险，确保信息系统安全、可靠、稳定运行,维护社会秩序、公共利益和国家安全，特制定《本单位信息安全策略总纲》(以下简称《总纲》)。

第二条 《总纲》根据国家信息安全相关政策法规而制定。

第三条 本制度适用于本单位各类信息系统，适用于本单位拟建、在建以及运行的非涉密信息系统。

1.1.2、 信息安全工作总体方针

第一条 本单位信息系统的安全保护管理工作总体方针是“保持适度安全；管理与技术并重；全方位实施，全员参与；分权制衡，最小特权；尽量采用成熟的技术”。“预防为主”是本单位信息安全保护管理工作的基本方针。

第二条 《总纲》规定了本单位信息系统安全管理的体系、策略和具体制度，为信息化安全管理工作提供监督依据。

第三条 本单位信息系统安全管理体系是由信息安全策略总纲、安全管理制度、安全技术标准以及安全工作流程和操作规程组成

的。

(一) 《总纲》是信息安全各个方面所应遵守的原则方法和指导性策略文件。

(二) 《总纲》是制定本单位信息安全管理制度和规定的依据。

(三) 本单位信息安全管理制度和规定了信息安全管理活动中各项管理内容。

(四) 本单位信息安全技术标准和规范是根据《总纲》中对信息安全方面相关的规定所引出的，其规定了信息安全中的各项技术要求。

第四条 本单位信息安全工作流程和操作规程详细规定了主要应用和事件处理的流程、步骤以及相关注意事项，并且作为具体工作时的具体依照。

1.1.3、 信息安全总体策略

第一条 本单位信息系统总体安全保护策略是：系统资源的价值大小、用户访问权限的大小和系统重要程度的区别就是安全级别的客观体现。信息安全保护必须符合客观存在和发展规律，其分级、分区域、分类和分阶段是做好信息安全保护工作的前提。

第二条 本单位信息系统的安全保护策略由本单位信息安全领导小组负责制定与更新。

第三条 本单位信息安全领导小组根据信息系统的安全保护等级、安全保护需求和安全目标，结合本单位自身的实际情况，依

据国家信息安全法规和标准，制定信息系统的安全保护实施细则和具体管理办法，并根据实际情况，及时调整和制定新的实施细则和具体管理办法。

第四条 本单位信息系统的安全保护工作应从技术体系和管理体系两个方面进行，技术体系包括物理环境安全、通信安全、边界安全、安全计算环境和安全管理中心等五个部分，管理体系包括安全管理制度、安全管理机构、人员安全管理、系统建设管理和系统运维管理等五个部分，由技术体系和管理体系共十个部分构成信息系统安全等级保护体系。

（一）物理环境安全包括：周边环境安全，门禁检查，防盗窃、防破坏、防火、防水、防潮、防雷击、防电磁泄露和干扰，电源备份和管理，设备的标识、使用、存放和管理等；

（二）通信安全包括：网络的拓扑结构，网络的布线和防护，网络设备的管理和报警，网络攻击的监察和处理，网络安全审计和检查及边界完整性检查；

（三）计算环境安全包括：主机的身份鉴别、访问控制、安全审计、入侵防范、恶意代码防范、监控和终端接入控制等；

（四）边界安全包括：应用系统的身份鉴别、访问控制、安全审计、剩余信息保护、通信完整性和保密性、抗抵赖、软件容错和资源控制等；

（五）数据安全包括：数据传输的完整性和保密性、数据存储的完整性和保密性、数据的备份和恢复等；

（六）安全管理制度是信息系统安全策略、方针性文件，规定信息安全工作的总体目标、范围、原则和安全框架，是管理制度体系的灵魂和核心文件；

（七）通过构建和完善信息安全组织架构的措施，明确不同安全组织和不同安全角色的定位、职责以及相互关系，强化信息安全的专业化管理，实现对安全风险的有效控制；

（八）人员安全管理包括人员录用、人员管理、人员考核、保密协议、培训、离岗离职等多个方面；

（九）系统建设管理根据信息密级、系统重要性和安全策略将信息系统划分为不同的安全域，针对不同的安全域确定不同的信息安全保护等级，采取相应的保护。信息系统安全等级的定级决定了系统方案的设计、实施、安全措施、运行维护等信息系统建设的各个环节。信息系统定级遵循“谁建设、谁定级”的原则；

（十）系统运维管理对信息系统进行综合监控管理，对支撑重要信息系统的资源进行监控保护，确保密码防护、病毒防护、系统变更等事件按照规定的信息安全管理策略实行，建立安全管理监控中心，实现对人、事件、流程、资产等方面的综合管理。

1.1.4、 安全管理

第一条 本单位信息系统定级备案管理完全按照国家相关信息安全标准的相关政策要求进行。要求所有接入本单位的信息系统均按照等级保护定级备案要求进行定级，由各应用系统接入单位自主定级并填写

定级报告，本单位信息安全领导小组填写定级备案表，经本单位信息安全领导小组批准，由本单位信息安全领导小组统一负责向公安机关进行备案。所有本单位信息系统必须确定其信息安全保护等级，并在本单位信息安全领导小组进行登记和备案。

第二条 业务应用需求和设计单位，要充分考虑信息系统的安全需求分析，统一按照业务系统归属进行安全域划分，确定定级备案情况；具体参考《信息安全等级保护管理办法》、《信息系统安全等级保护基本要求》，参照《信息系统安全等级保护实施指南》、《信息系统通用安全技术要求》、《信息系统安全工程管理要求》、《信息系统等级保护安全设计技术要求》等标准规范要求，结合行业特点进行安全需求分析。

（一）信息安全需求分析，至少包括以下信息安全方面的内容：

1. 安全威胁分析；
2. 系统脆弱性分析；
3. 影响性分析；
4. 风险分析；
5. 系统安全需求。

（二）可行性分析中须包括以下信息安全方面的内容：

1.明确项目的总体信息安全目标，并依据信息安全需求分析的结论提出相应的安全对策，每个信息安全需求都至少对应一个信息安全对策，信息安全对策的强度根据相应资产/系统的重要性来选择；

2.描述如何从技术和管理两个方面来实现所有的信息安全对策，并形成信息安全方案；

3.增加项目建设中的信息安全管理模式、信息安全组织结构、人员的安全职责、建设实施中的安全操作程序和相应安全管理要求；

4.对安全方案进行成本-效益分析；

5.需求分析阶段必须明确地定义和商定新系统的需求和准则，并形成文件，便于后期验收。相关信息安全需求的要求和准则应包括：用户管理、权限管理、日志管理和数据管理等。

第三条 业务应用的安全设计应按照国家信息安全标准进行，并依照信息安全需求分析评估得出的结论，通过相关专家评审会后，综合多方意见，进行安全设计。

具体要求如下：

(一) 物理安全-设计中要充分考虑到物理访问控制、防盗窃和防破坏、防雷击、防火、防水、防潮、电力、物理位置、防静电和电磁防护，做到增强控制，对人员和设备的出入进行监控；

(二) 边界安全-设计中要充分考虑到结构安全、访问控制、设备防护、安全审计、边界完整性检查、入侵防范、恶意代码防范，确保重要主机的优先级，做到应用层过滤，对入网设备的接入进行非法外联的定位和阻断，对形成的记录进行分析、形成报表，对审计系统进行两种以上鉴别技术，保证特权用户分离；

(三) 安全计算环境-设计中充分考虑主机系统(操作系统)的身份

鉴别、访问控制、入侵防范、恶意代码防范、安全审计、资源控制、剩余信息保护，要求必须监控服务器相关服务，保证最小授权原则，对形成的记录进行分析并形成报表；

(四) 数据安全-设计中充分考虑数据完整性、数据备份和恢复、数据保密性；

(五) 应用安全-设计中充分考虑应用系统的身份鉴别、访问控制、通信完整性和保密性、软件容错、安全审计、资源控制、剩余信息保护、抵赖性。

在信息系统安全规划设计时，应该考虑系统的容量和资源的可用性，以减少系统过载的风险，并采取相应的保密措施，控制涉及核心数据软件设计的相关资料的使用，并应遵循以下原则：

(一) 充分考虑应用安全实现的可控性，以便尽可能地降低安全系统与应用系统结合过程中的风险；

(二) 保持安全系统与应用系统的相互独立性，避免功能实现上的交叉或跨越；

(三) 建立完善的信息安全控制机制，包括：用户标识与认证、逻辑访问控制、公共访问控制、审计与跟踪等。

第四条 信息系统安全建设管理需要按照国家信息安全标准的相关要求，并在安全管理组织的领导下，结合应用的实际情况，进行信息安全建设。

在建设中应充分考虑系统定级管理、安全方案设计管理、产品采购和使用管理、自行以及外包软件开发管理、工程实施管理、测试验

收管理、系统交付管理、安全服务商选择管理、系统备案管理、等级测评管理等因素对信息系统安全的影响程度。

信息系统安全建设管理要求将系统建设过程有效程序化，明确指定项目实施监理负责人，确保系统设计文档和相关代码的安全，对销毁过程要进行安全控制，自行开发时应当严格控制对程序资源库的访问。

第五条 信息系统安全验收管理按照国家相关信息安全标准的要求，结合本单位信息系统的实际情况进行安全验收管理规范化。项目验收需得到各业务部门、本单位信息安全领导小组共同确认签字验收。项目应达到项目任务书中制定的总体安全目标和安全指标，实现全部安全功能。验收报告中应包括项目总体安全目标及主要内容。验收报告中应包括项目采用的关键安全技术内容。系统验收并移交后，必须立即修改系统中的默认口令。应用系统项目验收应审查如下内容：

(一) 功能检查包括对软件功能完整性、正确性进行审查和评价；

(二) 项目管理审查包括对项目计划、采用标准、需求方案及其执行情况进行审查和评价；

(三) 测试结果审查包括对项目测试报告、监理单位出具的监理报告等进行审查；

(四) 技术文档检查包括对项目开发单位交付的文档资料（纸质文档和电子文档）进行审查。

(五) 系统交付时，应根据合同要求制定系统交付的清单；

(六) 系统运行所需要的全部设备；

(七) 系统运行所需要的全部软件；

(八) 系统文档，包括系统建设过程中的文档，详细的系统使用和维护文档；

(九) 系统应急方案；

(十) 系统使用培训教材。

系统建设项目有下列情况之一，不能通过安全验收：

(一) 验收文件、资料、数据不真实；

(二) 未达到安全设计要求；

(三) 设计不符合国家信息安全建设相关标准要求；

(四) 擅自修改设计目标和建设内容；

(五) 系统建设过程中出现重大问题，未能解决和做出说明，或存在纠纷。

项目验收完毕后，系统建设部门应对负责系统使用和维护的人员进行相应培训，并履行服务承诺。

第六条 安全测评管理是按照国家信息安全标准测评的相关要求，结合本单位的实际情况进行安全测评。项目验收时应按照信息安全法律法规和标准情况，进行自评估或委托具有国家相关技术资质和安全资质的第三方测评机构进行测评，并出具测评报告，测评报告将作为项目验收的参考依据。信息系统的安全性测试验收应独立进行，测试程序应包括以下内容：

(一) 测试验收前根据设计方案或合同要求等制订测试验收方案，测试验收方案应对参与测试部门、人员、现场操作过程等

进行要求，并确保测试和接收标准被清晰定义并文档化；

(二) 测试方案应通过本单位信息安全领导小组的论证和审定；

(三) 严格依据测试方案进行测试，测试验收过程中详细记录测试结果；

(四) 至少应审查主机端口开放情况是否符合系统说明、使用网络侦听工具查通讯数据包是否符合系统说明和使用恶意代码软件检测软件包中可能存在的恶意代码等。

(五) 拟定测试验收报告，并由相关负责人签字确认。

第七条 安全运维管理按照国家信息安全标准的要求，项目验收完毕后，结合本单位的实际情况进行运行维护管理工作。信息安全管理部门接管后，负责物理安全、边界安全、通信安全、安全计算环境等管理工作，并定期和不定期的进行信息安全检查，确保信息系统安全运行。各业务系统的维护人员负责维护和监控责任范围内的应用系统，不得越权进行访问。信息安全运行维护项目应包括但不限于以下内容：

(一) 对物理安全的机房环境、温湿度等检查；

(二) 对网络的连通性、时延、丢包率，检查网络的状况、故障及攻击事件等；

(三) 对设备运行状态检查；

(四) 对出口链路或关键链路流量进行检查，设备配置进行备份工作等。

(五) 对新购置的设备和软件在上线之前进行安全性检查、策略

合理性测试。

(六) 对设备和软件的日志进行定期和不定期的审计。

(七) 对设备和软件进行版本升级和相关库升级。

(八) 建立监控平台，对设备安全漏洞、安全事件、系统日志等信息进行监控，制定各项计划性的安全维护工作。

(九) 建立本单位作业计划应包括以下内容安全设备维护、安全监控、操作日志、日志审核、故障管理、测试等工作，明确执行期限，落实到人。安全维护作业计划在编制和确定后，各业务科室应根据其内容严格执行。定期对维护计划执行情况进行总结分析。

(十) 定期出具安全运行维护报告，报告涉及方面包括但不限于以下内容：安全设备维护内容、安全监控内容、操作日志、系统日志、故障处理内容等。

1.1.5、 制度的制定与发布

第一条 本单位负责制订信息系统安全管理制度，并以文档形式表述，经本单位信息安全领导小组讨论通过，由本单位信息安全领导小组负责人审批发布。

第二条 本单位负责组织制度编制、论证、监督检查和修订等工作。

第三条 本单位负责根据信息系统安全管理制度，结合系统的特点进行细化和制定实施细则，报本单位信息安全领导小组审批，

以正式形式发布。

第四条 本单位信息系统安全管理制度编写格式统一，并进行版本控制。

第五条 信息安全管理制度由本单位信息安全领导小组负责审核，以正式文件形式发布，同时注明发布范围并有收发文登记。

1.1.6、 制度的评审和修订

第一条 由本单位信息安全领导小组负责文档的评审,对安全策略和制度的有效性进行程序化、周期性评审，并保留必要的评审记录和依据。

第二条 本单位负责定期组织对安全管理制度的执行情况进行检查，并结合国家信息安全主管部门每年定期对信息安全进行检查中发现的问题，对安全管理制度进行有针对性的修订与完善。

第三条 当发生重大安全事故、出现新的安全漏洞以及技术基础结构发生变更时，本单位要对安全管理制度的细则进行修订，修订后报本单位信息安全领导小组进行审批。

第四条 每个策略和制度文档有相应的负责人或负责科室，负责对明确需要修订的文档进行维护，并制定信息安全管理制度对应负责人或负责科室的清单。

1.1.7、 附则

第一条 本规定的解释权归 XXX 单位。

第二条　本规定自发布之日起生效。

第二章 安全管理机构

2.1、 信息安全领导小组及岗位职责管理规定

2.1.1、 总则

第一条 为了加强本单位对信息安全工作的管理，全面提高信息安全管理能力，规范信息安全管理组织体系，建立健全信息安全机构职责，特制定本规定。

第二条 本规定依据《国家信息化领导小组关于加强信息安全保障工作的意见》、《信息安全技术信息系统安全管理要求》等政策标准制定。

第三条 本规定依照“信息安全管理的主要领导负责、全员参与、依法管理、分权和授权和体系化管理”原则编制，具体原则如下：

（一）主要领导负责原则：本单位应确保主要领导参与并确立组织统一的信息安全保障宗旨和政策，组织有效的安全保障队伍，调动并优化配置必要的资源，协调安全管理工作与各部门工作的关系，并确保其落实、有效；

（二）全员参与原则：信息系统所有相关人员普遍参与信息系统的安全管理，并与相关方面协同、协调，共同保障信息系统安全；

（三）依法管理原则：信息安全管理工作应保证管理主体合法、管理行为合法、管理内容合法、管理程序合法；

（四）分权和授权原则：对特定职能或责任领域的管理功能实施分离、独立审计等实行分权，避免权力过分集中所带来的隐患，以减

小未授权的修改或滥用系统资源的机会。任何实体（如用户、管理员、进程、应用或系统）仅享有该实体需要完成其任务所必须的权限，不应享有任何多余权限。

（五）体系化管理原则：本单位整体应符合信息系统等级保护三级的体系化管理目标和要求。

第四条　本规定适用于本单位。

2.1.2、　信息安全领导小组组织机构

第一条　本单位应建立由信息安全领导小组安全管理机构。

第二条　由本单位主管领导或主管领导授权的主管机构领导担任本单位信息安全领导小组组长，小组成员包括：

（一）本单位信息化主管领导；

（二）本单位各业务科室的主管领导；

第三条　本单位信息安全领导小组是信息安全工作的执行机构，负责执行本单位信息安全领导小组交办的各项工作，由本单位信息化主管领导担任负责人，成员为各业务科室的主管领导，信息安全执行层包括：

（一）本单位的网络管理员、系统管理员、安全管理员、安全审计员、安全策略/规划员、数据库管理员、应用管理员；

（二）本单位各业务科室的安全员。

第四条 应设立信息安全管理岗位，分别为安全管理员、安全审计员、网络管理员、系统管理员、数据库管理员、应用管理员，负

责执行网络、系统、数据库、应用和机房的安全管理和运维工作。

第五条 其他信息化相关科室应指派安全员，负责协调本科室信息安全工作的落实和具体执行情况。

2.1.3、 信息安全领导小组职责

第一条 本单位信息安全领导小组负责领导本单位的信息系统安全工作，组织职责如下：

（一）根据国家和行业有关信息安全的政策、法律和法规，确定信息安全工作的总体方向、总体原则和安全工作方法；

（二）根据国家和行业有关信息安全的政策、法律和法规，批准本单位信息系统的安全策略和发展规划；

（三）确定各有关科室在信息系统安全工作中的职责，领导安全工作的实施；

（四）监督安全措施的执行，并对重要安全事件的处理进行决策；

（五）指导和检查的各项工作；

（六）建设和完善信息系统安全组织体系和管理机制。

第二条 本单位信息安全领导小组负责贯彻、落实和执行本单位信息安全领导小组下达的各项工作，组织职责如下：

（一）贯彻、落实和解释国家和行业有关信息安全的政策、法律、法规和信息安全工作要求，起草本单位信息系统的安全策略和发展规划；

（二）落实和执行本单位信息安全工作的日常事务，对具体落实

情况进行总结和汇报；

（三）负责安全措施的实施或组织实施，组织并参加信息安全重要事件的处理；

（四）负责内、外部组织和机构的信息安全沟通、协调和合作工作；

（五）组织编制和落实信息安全规划、方案、实施、测试和验收等工作；

（六）指导和检查相关单位信息系统安全工作落实情况；

（七）监控信息系统安全总体状况，提出安全分析报告；

（八）指导和检查相关单位和下级单位信息系统安全人员及要害岗位人员的信息安全工作；

（九）协同有关部门共同组成应急处理小组，组织处理信息安全应急响应工作；

（十）负责组织信息系统安全知识的培训和宣传工作。

2.1.4、 信息安全岗位职责

第一条 本单位信息安全组织中应建立信息安全岗位，明确信息安全岗位职责。

第二条 信息安全工作主管(负责人)的岗位职责如下：

（一）组织、协调落实各项信息安全工作；

（二）组织评审信息安全总体策略、规划方案、管理制度和技术规范；

（三）组织评审信息安全产品技术规格和相关产品安全规格；

（四）组织监督、检查信息安全工作的落实情况。

第三条　安全管理员(专职)的岗位职责如下：

（一）起草和编制本单位信息安全方针、信息安全保障体系框架和信息安全策略、制度和技术规范；

（二）起草和编制本单位信息安全总体规划，收集信息系统安全需求；

（三）推动本单位信息安全方针、信息安全策略、信息安全管理制度及信息安全技术规范的实施落实。

（四）定期组织信息系统漏洞扫描和信息安全风险评估工作，形成信息系统和整体安全现状报告，并向本单位信息安全领导小组进行汇报；

（五）负责制定总体网络访问控制策略和规则，并对其进行监控和审计工作，定期发布策略执行情况；

（六）负责制定全员的安全培训计划，组织开展安全培训工作；

（七）对网络、系统、应用、数据库管理员进行安全指导；

（八）定期收集信息安全漏洞和公告信息，并告知相关部门的信息安全运维管理人员及安全员；

（九）协调信息安全应急响应组织和技术支撑单位。

第四条　安全审计员的岗位职责如下：

（一）定期审计信息安全策略执行情况，收集信息系统日志和审计记录，并提供审计报告；

（二）对安全、网络、系统、应用、数据库、机房管理员的操作行为进行监督，安全职责落实情况进行检查；

（三）组织检查相关单位和下级单位信息系统安全人员及要害岗位人员的信息安全工作。

第五条 系统管理员的安全职责如下：

（一）根据本单位安全策略定期对系统进行自评估；

（二）依照安全策略对系统进行安全配置和漏洞修补；

（三）对系统进行日常安全运维管理，定期更改系统账号，并定期提交安全运行维护记录或报告；

（四）在发生系统异常和安全事件时对系统进行应急处置。

第六条 网络管理员的安全职责如下：

（一）根据本单位安全策略定期对网络设备、网络架构进行自评估；

（二）依照安全策略对网络设备进行安全配置；

（三）对网络设备、安全设备进行日常安全运维管理，并定期提交安全运行维护记录或报告；

（四）在发生系统异常和安全事件时，对网络设备、安全设备进行应急处置。

第七条 数据库管理员的安全职责如下：

（一）根据本单位安全策略定期对数据库安全进行自评估；

（二）依照安全策略对数据库进行安全配置和漏洞修补；

（三）对数据库进行日常安全运维管理，定期检查数据库用户，

并提交安全运行维护记录或报告；

（四）在发生数据库异常和安全事件时，对数据库以及备份数据进行应急处置和恢复。

第八条　相关科室安全员的岗位职责如下：

（一）负责本科室信息安全工作的开展，并配合的信息安全工作；

（二）遵照本单位的信息安全策略协调本科室的信息安全技术落实；

（三）指导并参与信息安全相关项目的建设；

（四）协调本科室的信息安全工作，并接受数据定期和不定期的检查。

2.1.5、 信息安全岗位要求

第一条　本单位应设立专职的信息安全管理岗位，并由专人负责，根据信息安全管理的实际工作情况制定人员编制。

第二条　本单位设立专职的安全管理员。

第三条　关键岗位应配备多人共同管理，定期轮岗，关键岗位人员配备坚持“权限分散、不得交叉覆盖”的原则，安全管理员和安全审计员不能由一人身兼。

第四条　应根据岗位职责，确定岗位所需要的安全技能，并对所有信息安全岗位人员进行相应的安全技能培训。

第五条　本单位信息系统的安全技术岗位可由其他相关管理员兼任，其中网络安全管理、系统安全管理、数据库安全管理以及应

用安全管理工作可分别由网络管理员、系统管理员、数据库管理员以及应用管理员执行。

第六条 重要业务系统操作人员应在日常工作中认真执行本单位安全策略和技术安全规范中的各项要求。

第七条 各个业务科室的安全员应紧密配合部信息安全工作，协调本单位信息安全策略的落实和信息安全工作的具体执行。

第八条 管理员角色的权限分工具体如下图：

管理员角色的权限分工表

	安全主管	系统管理员	网络管理员	安全审计员
制定安全规划和策略	√	×	×	×
安全审计	√	×	×	√
系统日常审计和监控	×	×	×	√
审计设备安全管理	×	×	×	√
网络安全	√	×	√	×
网络安全管理制度的建立和实施	×	×	√	×
系统账号密码管理	×	×	√	×
计算机病毒防治	×	×	√	×
材料归档	×	×	√	×
系统维护	×	√	×	×
系统安全	×	√	×	×
涉密信息设备安全保密策略维护	×	√	×	×
平台信息更新和上传	×	√	×	×

2.1.6、 附则

第三条 本规定的解释权归 XXX 单位。

第四条 本规定自发布之日起生效。

2.2、审核和检查管理制度

2.2.1、 总则

第一条 为了加强本单位信息安全检查与审计工作管理，确保信息安全管理符合国家有关要求，特制订本制度。

第二条 本规定适用于本单位。

2.2.2、 安全检查

第一条 信息安全检查包括各业务科室自查和信息安全处定期执行的安全检查。

第二条 各业务科室的自查内容应包括业务系统日常运行、系统漏洞和数据备份等情况，自查工作应保留自查结果。自查应至少一个季度组织一次。

第三条 执行的安全检查内容应包括现有安全技术措施的有效性、安全配置与安全策略的一致性、安全管理制度的执行情况和业务处室自查结果抽查等。安全检查应至少半年组织一次。

第四条 自查和安全检查均应在检查之前形成检查表，自查检查表应经过业务科室领导审核通过，安全检查表应经过信息安全工作小组审核通过。

第五条 应严格按照检查表实施检查，检查完毕，记录下所有检查结果，检查记录需经各业务科室领导签字认可。

第六条 应对检查记录进行归档，只有授权人员可以访问阅读。

第七条 应对检查结果进行汇总分析，形成安全检查报告，检查报告应对问题进行分析，提出解决建议。

第八条 应制定措施防止安全检查结果的非授权散布，只对经过授权的人员通报安全检查结果。

第九条 各业务科室应阅读并理解安全检查报告，在信息安全工作小组的指导下对出现的问题进行整改。应对整改过程进行监督，并将整改结果报送信息安全工作小组。

2.2.3、 安全审计

第一条 安全审计作为整体审计工作的一个部份，依据审计工作相关管理办法开展安全审计工作。

第二条 安全审计人员的配备应根据实际情况，采用如下方法的一种，原则上应以审计科室培养自身独立的安全审计人员为主，其他手段为辅。

1、由审计科室独立完成，使用审计科室具备相应技能的人员完成审计工作；

2、由审计科室和业务科室共同完成，指派熟悉技术的人员配合审计科室完成审计工作，本情形需注意审计独立的原则，进行交叉审计；

3、聘请外部专业审计单位完成审计工作。

第三条 安全审计的内容主要包括：

1、 相关法律法规的符合情况；

2、 管理部门的相关管理要求的符合情况；

3、 现有安全技术措施的有效性；

4、 安全配置与安全策略的一致性；

5、 安全管理制度的执行情况；

6、 安全检查和自查的检查结果及检查报告；

7、 日志信息是否完整记录；

8、 各类重要记录是否免受损失、破坏或伪造篡改；

9、 检查系统是否存在漏洞；

10、 检查数据是否具备安全保障措施。

第四条 安全审计工作应具有独立性，避免有舞弊的情况发生。

第五条 安全审计的方式分为：

1、全面审计：即审计内容覆盖安全管理范围内的所有科室，以及所有信息安全控制措施要求的检查。

2、专项审计：即审计内容只涉及部分科室，或部分信息安全控制措施要求的检查。

第六条 无论是采用全面审计还是专项审计方式，安全审计应每一年对所有的科室，以及所有的信息安全控制措施要求至少进行过一次审计。

第七条 被审计方应积极配合信息安全审计工作，应对审计结果进行确认。

第八条 安全审计工作中发现的不符合事项应按照审计管理相关

制度要求进行改进。审计科室应将改进过程和结果通告给信息安全工作小组。

2.2.4、 附则

第一条 本制度的解释权归 XXX 单位。

第二条 本制度自发布之日起生效。

2.3、 授权审批与控制制度

2.3.1、 总　则

第一条 为进一步加强本单位信息系统及重要场所访问授权和审批的管理，依据信息安全方针精神，制定本管理制度。

第二条 本管理制度适用于对信息系统产生影响的各项重要活动。

第三条 网络安全和信息化领导小组负责制定授权和审批事项，并定期审查、更新授权和审批的项目、审批部门、批准人和审查周期等。

2.3.2、 授权和审批事项

第四条 授权和审批主要包括但不限于如下事项：

（1）外部人员访问机房

（2）外部人员网络接入

（3）外部人员访问重要信息系统

（4）信息系统变更

（5）应用系统访问授权

第五条 除以上必须设立的授权审批事项外，网络安全和信息化领导小组应根据信息安全需求对相关事项设立授权审批机制，制定授权审批申请单，并督促执行。

第六条 以上的事项的授权审批必须通过填写正式的审批单，经过

相关责任人和网络安全和信息化领导小组领导逐级审批，签字确认后方可生效。

第七条 信息安全工作小组应该归档保存所有的授权审批记录，并指定专人管理。

2.3.3、 外来人员访问中心机房

第八条 外部人员需要进入机房进行相关维护操作时，需填写外部人员机房物理访问申请表，注明进入机房的事由，涉及的信息系统对象，进入预计的时间范围等。

第九条 外部人员机房物理访问申请表填写完成后，需先由安全管理员进行确认，在安全管理员确认完成后，由信息安全工作小组领导进行审批。在审批完成后，外部人员方可进入机房进行维护操作。

第十条 外部人员进入机房时需要填写机房出入登记表，记录进入机房的事由和进出时间，机房管理中心应安排相关人员进行全程陪同，对外部人员进行全程监控。

2.3.4、 外部人员网络接入

第十一条 外部人员因为工作需要连接到内部网络中需要先填写外部人员网络接入申请表，注明接入网络需要访问的网络和系统范围，以及需要执行的相关操作等，如涉及到对信息系统进行变更，应同时执行系统变更的相关流程。

第十二条 外部人员网络接入申请表填写完成后，需先由安全管理员进行确认，在安全管理员确认完成后，由信息安全工作小组领导进行审批，在审批完成后，由网络管理员负责提供网络接入。

第十三条 在接入内部网络前，网络管理员应通过技术手段对接入内部网络的外部人员电脑进行安全检测，在安全检测通过后允许接入到内部网络。

第十四条 网络管理员应根据外部人员申请访问网络和信息系统的范围分配相应的网络访问权限，分配给外部人员指定的线路和 IP 地址。

第十五条 网络管理员应采取技术手段防止外部人员同时连接内网和互联网，并对外部人员的网络访问进行监控。

2.3.5、 外部人员访问重要信息系统

第十六条 外部人员是指与签订合作协议的单位做委派来进行项目实施相关工作人员。

第十七条 外部人员因工作关系需要访问内部任何信息系统前，应填写外部人员访问申请表，明确访问系统对象、访问原因、访问时间、访问方式等信息，必须经过相关项目责任人及信息安全工作小组领导确认签字后，在旁人陪同或监控下访问。

第十八条 信息系统工作人员在审批外部人员访问信息系统请求时，应该认真核对对方申请的真实性、必要性和其工作的正确性。若无需访问也可以解决问题，则工作人员应引导外部人员通过别

的方式获取信息系统必要信息，包括但不限于：提供信息内容讲解、导出必要的信息内容文件或截图等。

2.3.6、 信息系统变更

第十九条 当内部人员或外部人员需要对信息系统相关配置进行修改和调整时，需要填写信息系统变更申请表，注明信息系统变更内容，同时需要提交信息系统变更方案，包括变更的步骤，可能造成的影响以及回退措施。

第二十条 信息系统变更申请表填写完成后与变更方案同时提交，需先由安全管理员进行确认，在安全管理员确认完成后，由信息化分管领导进行审批，在审批完成后，方可进行信息系统变更。具体内容请参见《变更管理制度》。

2.3.7、 应用系统访问授权

第二十一条 当单位内部职工需要新申请业务账号或调整相应访问权限时需要填写信息系统账号授权申请表，注明使用人，科室以及需要授权的相关信息。

第二十二条 信息系统变更申请表填写完成后与变更方案同时提交，需先由申请人员科室领导签字确认后，再由应用管理员进行二次确认，在确认后由信息安全工作小组领导进行审批，在审批后由应用系统管理员进行相关账号授权操作。

2.3.8、附　则

第二十三条 本制度的解释权归 XXX 单位。

第二十四条 本制度自发布之日起生效。

2.4、沟通与合作制度

2.4.1、总　则

第一条 信息安全领导小组负责高层信息安全例会的发起，信息安全工作小组负责中层信息安全例会的发起。信息安全小组负责中高层信息安全例会记录工作、与外部相关单位的沟通与协作管理。

2.4.2、信息安全内部例会管理

第二条 信息安全例会由信息安全工作小组负责发起，至少每月需要组织一次常规的信息安全例会，例会参会人员至少要包括信息安全工作小组主要成员和执行层各角色的管理人员。在发生小范围内信息安全事件时如需要，信息安全工作小组可随时召集发起信息安全工作会议，通知相关人员参加，就信息安全管理各项制度和执行情况做出及时调整和部署。

第三条 常规的信息安全例会的主要内容是就各阶段的信息安全检查结果进行上会检查和审批，对信息安全检查中发现的各项问题提出解决办法和规避措施，对外包运维人员的工作内容进行确认和审核，就发现的各类信息安全问题及时提出解决方案并落实到相关责任人。

第四条 遇有工程或项目时，可根据工程和项目进度情况或者工程和项目的需要随时召开信息安全例会，且可不拘泥于信息安全工

作小组范围，可召集相关的合作单位、合作方、内部相关科室的相关人员一起参加信息安全例会，并由信息中心做好例会的记录工作。

2.4.3、 外部协作管理

第五条 由信息安全工作小组负责建立并保持与兄弟单位如教育局、公安机关、电信公司等对口单位的合作与沟通，就兄弟单位的成熟经验、政策法规、当前的信息热点事件展开交流与合作。如交流与合作内容比较正式，且有正式的会议形式，则需要由信息中心做好会议记录工作，会议记录的模板可用信息安全例会的模板代替，但会议主题需注明为“合作沟通”，必要时建立外联单位联系列表，包括外联单位名称、合作内容、联系人和联系方式等信息，以方便联系。

第六条 由信息安全工作小组负责建立并加强与供应商、业界专家、专业的安全公司、安全组织的合作与沟通，就最新信息安全技术、信息热点事件等进行交流和咨询。如交流与合作内容比较正式，且有正式的会议形式，则需要由信息中心做好会议记录工作，会议记录的模板可用信息安全例会的模板代替，但会议主题需注明为“合作沟通”。

第七条 由信息安全领导小组聘请信息安全专家作为常年的信息安全顾问，指导信息安全建设，参与安全规划和安全评审，由信息安全工作小组负责与信息安全专家的接口和合作。

2.4.4、附　　则

第八条　本制度的解释权归 XXX 单位。

第九条　本制度自发布之日起生效执行。

第三章 安全管理人员

3.1、内部人员信息安全管理规定

3.1.1、 总则

为保障本单位人员信息安全管理的规范性，制定本规定。

人员信息安全管理包括与信息化工作有关的人员录用、岗位人选、人员转岗和离岗、人员考核、人员惩戒、人员教育和培训等的信息安全管理。本规定适用于本单位。

3.1.2、 人员录用

第一条 本单位员工录用，应该遵守相关人事和劳动法律法规。

第二条 本单位本着量才适用、择优录取的原则，公开、公平、公正地进行人员录用程序，为本单位招录适用的人才。

第三条 人事科室负责人员录用工作的实施，用人科室协助执行。

第四条 人事科室组织应聘人员进行笔试和面试。

第五条 应严格考察该人员的学历证书、业务技术水平及相关资质认证（相关计算机认证证书等）。

第六条 人事科室组织应聘人员进行笔试和面试。

第七条 对人员背景进行审查，不考虑录用有犯罪前科、重大行政处分纪录和“黑客”经历的人员。如有特殊情况，需要经综合部同意后，方可考虑录用。

第八条 人员录用时，本单位与所有被录用人员签署《保密协议》，

协议的内容应包括保密范围、保密责任、违约责任、协议的有效期限和责任人的签字等内容。

第九条 对于本单位关键岗位的人员必须是本单位正式员工，并签署包含岗位安全责任、违约责任、协议的有限期和责任负责人签字等内容的《岗位安全协议书》。

3.1.3、 岗位人选

第一条 明确所有信息安全岗位人员在信息系统安全保护中的职责和权限，其工作、活动范围应当被限制在完成其任务的最小范围内。

第二条 安全管理员、安全审计员、网络管理员、系统管理员、数据库管理员、机房管理员等和信息安全有关的岗位人员，必须经过严格的审查并考核其业务能力。

3.1.4、 人员转岗和离岗

第一条 人员的转岗和离岗由所在科室及时通知人事科室，只有具备经过人事科室签字的保密承诺文档后才能办理转岗和离岗手续。

第二条 人员转岗和离岗时，需及时终止离岗人员的所有访问权限，及时变更转岗人员的访问权限。

第三条 对转岗和离岗人员，要对设备上保留的数据进行安全处理，包括备份需要留存的数据以及删除不必要的数据。

第四条 本单位的所有服务器，交换机，路由器的用户名和密码口令。

第五条 网络系统集成的文档，包括：路由器、交换机和服务器参数、网络拓扑图、网络布线图、虚网划分、IP 地址分配等网络机密资料。

第六条 随机赠送的服务器、网络通信设备携带的说明书、各种文字资料等网络系统的重要资料。

第七条 有关网络建设与信息化建设的各种合同。上级科室的各种批文，网络管理和配备的各种规则、条例等文字材料。

第八条 离岗离职人员因职务上的需要所持有或保管的一切记录着单位秘密信息的文件、资料、图表、笔记、报告、信件、传真、磁带、磁盘、仪器以及其他任何形式的载体，均归本单位所有。

第九条 离岗离职人员应在离岗离职时，或者向本单位提出请求时，返还全部属于本单位的财物，包括记载着本单位秘密信息的一切载体。若记录着秘密信息的载体是由离岗离职人员自备的，则视为离岗离职人员已同意将这些载体物的所有权转让给单位，本单位应当在离岗离职人员返还这些载体时，给予离岗离职人员相当于载体本身价值的经济补偿；但秘密信息可以从载体上消除或复制出来时，可以由本单位将秘密信息复制到单位享有所有权的其他载体上，并把原载体上的秘密信息消除，此种情况下离岗离职人员无须将载体返还，信息中心也无须给予离岗离职人员经济补偿。

第十条 离岗离职人员离岗离职时，应将工作时使用的电脑、U 盘等其他一切存储设备中与工作相关或与本单位相关的信息、文件等内容交接给本科室领导，不得在离岗离职后以任何形式带走相关信息。

第十一条 对关键岗位的转岗和离岗人员需重申调离后的保密义务，要求调离人员在保密承诺文档上签字，承诺相关保密义务后方可离开。

3.1.5、 人员考核

第一条 每年对所有岗位人员进行信息安全考察，内容如下：

（一）对所有人员进行信息安全意识考核；

（二）对涉及信息安全管理、检查和执行的岗位人员，将定期进行信息安全技能的考核，包括信息安全管理知识的掌握程度、所管理业务系统中安全产品的操作技能、所管理业务系统中使用的操作系统和应用软件的安全使用等；

（三）每年发生的信息安全事故、信息安全检查结果和信息安全审计结果将纳入考察内容。

第二条 信息安全考察结果将进行存档，以便查询，及与上次考核进行对比分析。

第三条 技术人员的技能考核每年进行两次考核，以理论考核、实操考核或其他方式进行考核，每次考核有两次机会；考核成绩合格分三个档次合格、良好、优秀；技术人员考核成绩不合格者要

进行补考，如不再不合格则调离响应岗位。

第四条 对于考核中发现有违反信息安全法规行为的人员或发现不适于承担信息安全关键岗位的人员要依据有关规定处理。

第五条 每年还将对信息安全三大员（系统管理员、安全管理员、安全审计员）的人员进行一次工作督察，督察的内容参照《安全组织人员岗位职责》中有关的要求执行。

3.1.6、 人员惩戒

第一条 人员违反信息安全策略和规定时，依照相关规定进行处理。

第二条 如该信息安全违规行为涉及法律层面，则将移交司法机关处理。

3.1.7、 人员教育和培训

第一条 由制定培训计划，实施信息安全教育和培训工作，培训计划分层次、分阶段，循序渐进地进行。分层次培训是指对不同层次和不同岗位的人员，如对管理层（包括决策层）、安全管理员、系统管理员和所有信息安全相关人员开展有针对性和不同侧重点的培训。分阶段培训是指在信息安全管理体系的建立、实施和保持的不同阶段，实施不同的培训内容。

第二条 新员工在正式上岗前，需进行信息安全方面的培训，明确岗位所要求遵守的信息安全管理制度、技术规范以及操作流程。

第三条 对信息系统的维护人员和管理人员需定期开展信息安全技术教育培训（每年至少一次），明确如何安全使用有关系统，包括各业务系统、主机操作系统、电子邮件系统以及计算机硬件设备等。

第四条 定期开展由供应商或厂家提供的专业安全技术培训，帮助相关信息安全管理人员和技术人员了解掌握正确、安全地安装、配置和维护系统。

第五条 在信息安全教育和培训后实行书面的考核，确认教育和培训的效果，对安全教育和培训的情况和结果记录并归档保存。

第六条 日常的信息安全教育和培训以内部培训为主，对于暂时没有条件实施内部培训的，可根据需要，邀请厂商、合作伙伴或者专业的培训机构实施培训。

3.1.8、 附则

第一条 本规定的解释权归 XXX 单位。

第二条 本规定自发布之日起生效。

3.2、外部人员访问管理规定

3.2.1、 总则

第一条 为有效防范外部人员访问带来的信息安全风险，加强和规范外来人员的信息安全管理，保证信息资源的安全，制定本规定。

第二条 本规定适用于本单位。

3.2.2、 定义

第一条 本规定所述的外部人员包括软件开发商、产品供应商、系统集成商、设备维护商、服务提供商以及外单位借调人员和挂职人员等外来人员，外部人员分为临时外部人员和非临时外部人员。

第二条 临时外部人员指因业务洽谈、技术交流、提供短期和不频繁的技术支持服务而临时来访的外部人员。

第三条 非临时外部人员指因从事合作开发、参与项目工程、提供技术支持、顾问服务及外单位借调人员和挂职人员等外来人员，是非必须在本单位长期办公的外部人员。

3.2.3、 外部人员访问信息安全管理

第一条 外部人员的访问方式包括现场访问和远程网络访问。

第二条 接待人是指本单位受访科室派出的，负责接待外部人员的接口人。

第三条 临时外部人员访问重要信息资源所在物理区域（如机房、重要服务器或设备等），需获准后方可进入。

第四条 接待人必须全程陪同临时外部人员，告知有关安全管理规定，不应透露与外部工作无关的信息，不得任其自行走动和未经允许使用本单位的计算机设备。

第五条 非临时外部人员，由接待科室提出申请，出具意见，向保卫科室提出申请，依照保卫科室审批结果办理工作手续。

第六条 原则上禁止外部人员携带的电脑接入本单位网络，如因工作需要（如软件开发测试）接入本单位网络，必须向信息中心申请，并使用的设备或经过检查认可的设备。

第七条 第三方人员如有需要访问信息时，需要依照如下几个阶段进行：

1、 访问申请阶段，接待人根据第三方人员实际需要提出某时间段内访问网络、主机等相关信息的申请；

2、 审批申请阶段，接待人所属科室管理者审批申请。审批后备案；

3、 注销访问阶段，第三方人员访问结束，接待人终止访问申请，并备案；

第八条 不允许外部人员进行远程网络访问。如确因维护需要远程访问，必须上报审批后方可进行。

第九条 外部人员开发测试环境只能连接开发网，且必需采用防火墙进行有效隔离，严禁接入业务网。确需在线测试的项目，应上报分管领导批准，采取必要的防护措施，选择适当的时间进行。

第十条 外部人员在机房内的所有操作，都必需说明该操作可能引起的安全风险，并由接待人确认后才能操作。接待人必须对外部人员的操作进行全程监控，记录外部人员的操作内容并存档备案。

第十一条 必须定期评估外部人员带来的安全风险，至少每年评估一次。必须防范外部人员带来的以下安全风险：

1、 外部人员的物理访问带来的设备、资料盗窃；

2、 外部人员的误操作导致各种软硬件故障；

3、 外部人员的资料、信息外传导致泄密；

4、 外部人员对计算机系统的滥用和越权访问；

5、 外部人员给计算机系统、软件留下后门；

6、 外部人员对计算机系统的恶意攻击。

3.2.4、 第三方安全要求

第一条 非临时外部人员必须签署安全保密协议后才能进场工作。禁止外部人员试图了解和查阅与工作无关的本单位资料以及访问与工作无关的信息系统，外部人员如因业务需要查阅本单位资料或访问本单位信息系统，必须获得相关负责人批准并详细登记，并确认已与签署有效的保密协议。

第二条 未经批准，禁止外部人员携带移动存储介质进入本单位，移动存储介质必须在接待人的监控下使用。

第三条 外部人员访问受控区域（如机房、办公场所、系统、设备、信息等）前先提出书面申请，对申请人、申请原因、申请访问的范围、申请时间等进行说明，将申请书提交有关科室负责人进行审批并在申请书上签字确认。

第四条 不应在有信息系统敏感信息的办公区域接待来访人员，应统一在接待区域接待来访人员。来访人员以及外部人员在访问控制区域（如机房等）前得到相关科室领导的授权和审批，批准后由专人全程陪同或监督，并登记备案。

第五条 外部人员调试所涉及的信息系统内的账号、权限、邮箱以及信息化设备等变化情况要及时记录，管理人员在外面人员调试完成后要及时对其使用的账号、权限等进行清理。

第六条 未经相关负责人特别许可，外部人员不得在办公区域和机房内摄影、拍照。

3.2.5、 附则

第一条 本规定的解释权归 XXX 单位。

第二条 本规定自发布之日起生效。

第四章 安全建设管理

4.1、定级和备案管理规定

4.1.1、 总则

第一条 为本单位信息系统定级备案管理，制定本规定。

第二条 本规定适用于本单位拟建、在建以及运行的非涉密重要信息系统。

4.1.2、 定义

第一条 信息系统的安全保护等级分为以下五级

第一级，信息系统受到破坏后，会对公民、法人和其他组织的合法权益造成损害，但不损害国家安全、社会秩序和公共利益。

第二级，信息系统受到破坏后，会对公民、法人和其他组织的合法权益产生严重损害，或者对社会秩序和公共利益造成损害，但不损害国家安全。

第三级，信息系统受到破坏后，会对社会秩序和公共利益造成严重损害，或者对国家安全造成损害。

第四级，信息系统受到破坏后，会对社会秩序和公共利益造成特别严重损害，或者对国家安全造成严重损害。

第五级，信息系统受到破坏后，会对国家安全造成特别严重损害。

第二条 名词定义

业务科室:信息系统的使用部门。

业务信息安全：从业务信息安全角度反映的信息系统安全。

系统服务安全: 从系统服务安全角度反映的信息系统安全。

受侵害客体：等级保护对象受到破坏时所侵害的客体包括以下三个方面：

a)公民、法人和其他组织的合法权益；

b)社会秩序、公共利益；

c)国家安全。

对客体的侵害程度：等级保护对象受到破坏后对客体造成侵害的程度有造成一般损害、造成严重损害和造成特别严重损害。

一般损害：工作职能受到局部影响，业务能力有所降低但不影响主要功能的执行，出现较轻的法律问题，较低的财产损失，有限的社会不良影响，对其他组织和个人造成较低损害。

严重损害：工作职能受到严重影响，业务能力显著下降且严重影响主要功能执行，出现较严重的法律问题，较高的财产损失，较大范围的社会不良影响，对其他组织和个人造成较严重损害。

特别严重损害：工作职能受到特别严重影响或丧失行使能力，业务能力严重下降且或功能无法执行，出现极其严重的法律问题，极高的财产损失，大范围的社会不良影响，对其他组织和个人造成非常严重损害。

第三条 角色定义

应用系统负责人：由业务科室为每个信息系统指定的定级备案工作负责人；

系统定级管理负责人：由指定的定级备案负责人。

4.1.3、 岗位及职责

第一条 业务科室：应对待定级系统指定应用系统负责人，对待建、在建和已建信息系统根据等级保护相关要求进行定级，并完成定级报告。

第二条 ：本单位信息安全领导小组指定系统定级管理负责人，完成定级备案表，并报本单位信息安全领导小组审核，审核通过后报公安机关备案。

4.1.4、 系统定级方法

第一条 信息系统定级方法如图所示：

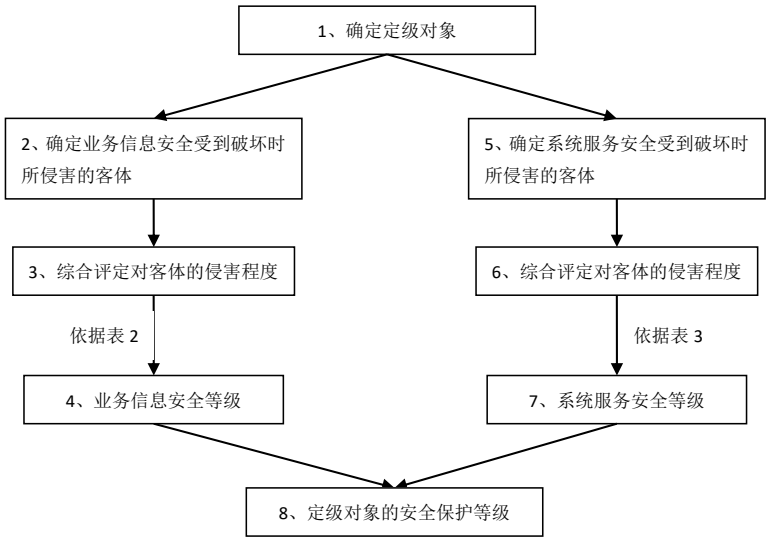

图 1 信息系统定级方法图

第二条 信息系统的安全保护等级由两个定级要素决定：等级保

护对象受到破坏时所侵害的客体和对客体造成侵害的程度，定级要素与信息系统安全保护等级的关系如表 1 所示：

表1 业务信息安全保护等级矩阵表

受侵害的客体	对客体的侵害程度		
	一般损害	严重损害	特别严重损害
公民、法人和其他组织的合法权益	第一级	第二级	第三级
社会秩序、公共利益	第二级	第三级	第四级
国家安全	第三级	第四级	第五级

第三条 信息系统安全包括业务信息安全和系统服务安全，与之相关的受侵害客体和对客体的侵害程度可能不同，因此，信息系统定级应由业务信息安全和系统服务安全两方面确定。

第四条 根据业务信息安全被破坏时所侵害的客体以及对相应客体的侵害程度，依据表 2 业务信息安全保护等级矩阵表，即可得到业务信息安全保护等级。

表2 业务信息安全保护等级矩阵表

业务信息安全被破坏时所受侵害的客体	对相应客体的侵害程度		
	一般损害	严重损害	特别严重损害
公民、法人和其他组织的合法权益	第一级	第二级	第三级
社会秩序、公共利益	第二级	第三级	第四级
国家安全	第三级	第四级	第五级

第五条 根据系统服务安全被破坏时所侵害的客体以及对相应客体的侵害程度，依据表 3 系统服务安全保护等级矩阵表，即可得到系统服务安全保护等级。

表3 系统服务安全保护等级矩阵表

系统服务安全被破坏时所受侵害的客体	对相应客体的侵害程度		
	一般损害	严重损害	特别严重损害
公民、法人和其他组织的合法权益	第一级	第二级	第三级
社会秩序、公共利益	第二级	第三级	第四级
国家安全	第三级	第四级	第五级

4.1.5、 系统定级备案管理

第一条 本单位应按《信息安全等级保护管理办法》和《信息安全技术信息系统安全等级保护定级指南》的要求进行信息系统的定级、设计、建设、测评、备案和变更管理，具体的定级备案工作由和业务需求科室共同负责。

第二条 本单位信息系统定级遵循“自主定级”的原则，由业务科室进行自主定级，本单位信息系统安全保护等级一般为第三级，如因特殊情况需定级为第四级或以上，需由相关主管单位确认。

第三条 信息系统定级流程如下：

(一) 应用系统负责人应参照相关标准填写《信息系统安全等级保护定级报告》，完成自主定级，报告应中明确信息系统安全保护等级，详细说明定级的方法和理由，定级方法详见第 4.1.4 节内容。

(二) 业务科室完成自主定级后，将《信息系统安全等级保护定级报告》提交进行存档，并将定级结果报信息安全领导小组审核。

(三) 由协助业务科室组织相关科室和有关安全技术专家对信息系统定级结果的合理性和正确性进行论证和审定，并对专家论证文档

进行保存，记录专家对定级结果的论证意见。

(四) 如安全技术专家对信息系统定级结果的合理性和正确性存在异议，则由业务科室、和技术专家组共同讨论确认信息系统的安全保护等级，并由业务科室根据最终的论证意见重新填写《信息系统安全等级保护定级报告》。

(五) 如安全技术专家对信息系统定级结果的合理性和正确性无异议，则由本单位信息安全领导小组，指定的定级管理负责人根据《信息系统安全等级保护备案表》中填表说明填写《备案表》，并进行备案工作。

第四条 信息系统备案流程如下：

(一) 定级管理负责人进行信息系统备案时应当提交公安机关公共信息网络安全监察部门《备案表》（一式两份）及其电子文档。第三级及以上信息系统备案时需提交《备案表》中的表一、二、三；第三级及以上信息系统还应当在系统整改、测评完成后 30 日内提交《备案表》表四以及其相关材料；

(二) 备案资料经公安机关公共信息网络安全监察部门审核通过后，定级管理负责人会收到由公安机关公共信息网络安全监察部门出具的《信息系统安全等级保护备案材料接收回执》；

(三) 公安机关公共信息网络安全监察部门审核后认定备案资料不齐全的，会在当场或者在五日内一次性告知定级管理负责人其补正内容，定级管理负责人应根据公安机关公共信息网络安全监察部门告知的补正内容补齐相关资料，并提交公安机关公共信息网络安全监察

部门；

(四) 备案材料经公安机关公共信息网络安全监察部门审核通过后，定级管理负责人会在递交材料的十个工作日内收到加盖公安机关印章（或等级保护专用章）的《备案表》一份；

(五) 备案材料经公安机关公共信息网络安全监察部门审核未通过，认为其不符合等级保护要求的，公安机关公共信息网络安全监察部门会在十个工作日内通知定级管理负责人进行相应整改，并向定级管理负责人出具《信息系统安全等级保护备案审核结果通知》。

(六) 定级管理负责人收到公安机关公共信息网络安全监察部门出具的由公安部统一监制《信息系统安全等级保护备案证明》后，信息系统备案工作结束。

第五条 每个信息系统相应的应用系统负责人都应在进行登记，如应用系统负责人发生变更，业务科室应及时通知对人员信息进行变更。

第六条 应用系统负责人有义务配合以及公安部进行信息安全等级保护检查工作。

第七条 拟建以及在建的重要信息系统在投入使用前应按本规定进行信息系统定级，并且在信息系统投入使用后，应当按要求和程序进行该信息系统安全等级备案工作。

第八条 信息系统发生重大变更导致系统安全保护等级变化时，和业务科室应重新确定信息系统的安全保护等级，按相应程序报备，并按新的等级要求调整保护措施。

第九条 本制度的解释权归 XXX 单位。

第十条 本制度自发布之日起生效。

4.2、安全方案设计管理规定

4.2.1、 总则

第一条 为本单位信息系统安全方案的设计管理，制定本规定。

第二条 本单位信息系统安全方案应参考国家信息安全相关标准的要求进行设计。

第三条 本规定适用于本单位。

4.2.2、 安全建设总体规划责任部门

第一条 本单位信息安全领导小组负责对本单位信息系统的安全建设进行总体规划，制定近期和远期的安全建设工作计划。

4.2.3、 安全方案的设计和评审

第一条 本单位应根据信息系统的安全保护等级选择相应的基本安全措施，并依据风险分析的结果补充和调整安全措施。

第二条 信息系统的安全保护等级确定后，应选择具有相应资质的单位，依照国家信息安全等级保护管理规范和技术标准进行安全方案设计。

第三条 信息安全方案应包括安全保障体系的总体安全策略、安全技术框架、安全管理策略、总体建设规划和详细设计方案等相关配套文件。

第四条 信息安全方案设计完成后，应组织相关部门和有关安全技术专家对总体安全策略、安全技术框架、安全管理策略、总体建设规划、详细设计方案等相关配套文件的合理性和正确性进行论证和审定，记录专家论证意见。

第五条 信息安全方案经过信息本单位信息安全领导小组批准后，才能正式实施。

第六条 安全方案的调整和修订。

第七条 由根据等级测评、安全评估的结果定期调整和修订总体安全策略、安全技术框架、安全管理策略、总体建设规划、详细设计方案等相关配套文件。

第八条 应维护信息安全方案相关配套文件的历史版本和修订版本，并有维护记录。

第九条 附则

第十条 本规定的解释权归 XXX 单位。

第十一条 本规定自发布之日起生效。

4.3、产品采购和使用管理规定

4.3.1、 总则

第一条 为规范本单位在信息系统产品采购和使用中信息安全有关的事项，制定本规定。

第二条 本单位按国家信息安全相关政策法规和标准的规定进行信息系统产品的采购和使用。

第三条 本规定适用于本单位。

4.3.2、 产品采购和使用

第一条 本单位的信息技术产品的采购由信息中心统一负责。

第二条 本单位的信息化产品采购活动需要符合国家信息安全政策要求，特别是信息安全产品必须要有资质证明。

第三条 本单位应按照《中华人民共和国招标投标法》和《中华人民共和国政府采购法》的有关规定，优先选择国产自主可控的信息安全设备、核心网络设备、基础软件、系统软件和业务应用软件等关键产品，以确保信息系统的安全可控。因特殊原因必须选用国外信息技术产品的，应请国家有关部门进行安全审查，并报本单位信息安全领导小组批准。

第四条 采购信息安全产品时，本单位将要求产品研制、生产单位提供相关材料，包括：营业执照、产品的版权或专利证书、提

供的声明和通过国家认定的信息安全产品检测实验室的检测证明以及计算机信息系统安全专用产品销售许可证等材料。

第五条 信息系统安全等级为三级（以上）信息系统在选择信息安全产品时，除遵守以上规定外，还应当符合以下条件：

（一）产品研制、生产单位是由中国公民、法人投资或者国家投资或者控股的，在中华人民共和国境内具有独立的法人资格；

（二）产品的核心技术、关键部件具有我国自主知识产权；

（三）产品研制、生产单位及其主要业务、技术人员无犯罪记录；

（四）产品研制、生产单位声明其产品没有故意留有或者设置漏洞、后门、木马等程序；

（五）对已列入信息安全产品认证目录的，应当取得国家信息安全产品认证机构颁发的认证证书。

第六条 产品采购到货后，组织验收小组对供货方的货物进行技术方面的验收，验收时候需要查验产品的各种文档、证书、报告及证明文件，确认符合前述各条款规定。

4.3.3、 产品采购清单的维护

第一条 预先对产品进行选型测试，确定产品候选范围，并定期审定和更新候选产品名单。

第二条 根据产品的更新换代情况每年对产品采购候选清单进行审定和更新。

4.3.4、 附则

第一条 本规定的解释权归 XXX 单位。

第二条 本规定自发布之日起生效。

4.4、软件开发管理制度

4.4.1、 总则

第一条 为了规范自有软件研发以及外包软件的管理工作，特制定本制度。本制度适用于本单位（以下简称本单位）软件开发与管理。

第二条 本制度中软件开发指新系统开发和现有系统重大改造。

第三条 本制度中自行开发是指主要依赖中心自身的管理、业务和技术力量进行系统设计、软件开发、集成和相关的技术支持工作，一般仅向外购置有关的硬件设备和支撑软件平台；合作开发是本单位与专合作商共同协作完成技术应用的项目实施和技术支持工作，一般形式是本单位负责提供业务框架，合作商提供技术框架，双方组成开发团队进行项目实施，技术系统的日常支持由信息中心和合作商共同承担，信息中心支持，合作商负责外部支持；外包开发是指将应用项目的设计、开发、集成、培训等任务承包给外包单位负责应用项目的实施。

第四条 软件开发遵循项目管理和软件工程的基本原则。项目管理涉及立项管理、项目计划和监控、配置管理、合作开发管理和结项管理。软件工程涉及需求管理、系统设计、系统实现、系统测试、用户接受测试、试运行、系统验收、系统上线和数据迁移。

第五条 除特别指定，本制度中项目指软件开发项目。

4.4.2、 立项管理

第六条 提出开发需求的信息中心门参与本单位层面立项，进行

立项的技术可行性分析，编写《立项分析报告》开展前期筹备工作。《立项分析报告》应明确项目的范围和边界。

第七条 应用系统主要使用部门将《立项分析报告》上交本单位负责领导进行立项审批，以保证系统项目与单位整体策略相一致。

第八条 《立项分析报告》得到批准后，成立项目组（如果是外包开发，则成立外包商项目组；如果是合作开发，则与外包商共同成立合作开发项目组，以下统称“项目组”），项目组应包括信息中心。本单位委派一名员工负责监督项目的进度，进行项目管理工作，确保开发能及时完成并能满足业务需要。项目组人员的选择应满足项目对业务及技术要求，项目组人员应有足够的业务和技术方面的专业知识来胜任项目各方面的工作。

4.4.3、 需求分析

第九条 立项后业务组对用户需求进行汇总整理，出具《业务需求说明书》，并确保《业务需求说明书》中包含了所有的业务需求。经系统使用科室审批确认，作为业务需求基线。

第十条 信息中心在获得《业务需求说明书》后，提出技术需求和解决方案，并对系统进行定义，出具《系统需求规格说明书》。《系统需求规格说明书》需详细列出业务对系统的要求（界面、输入、输出、管理功能、安全需求、运作模式、关键指标(KPI)等）。《系统需求规格说明书》需要由信息中心提交给相关业务流程负责人确认。

第十一条 对于合作开发的项目，当业务需求发生变更时，信息中心应提交《需求变更申请》，开发组审批后交给合作开发商实施。

第十二条 项目组应对需求变更影响到的文档及时更新。

4.4.4、 项目计划和监控

第十三条 软件开发采用项目形式进行管理。项目经理负责整个项目的计划、组织、领导和控制。

第十四条 需求分析过程中，项目经理组织制定详细的《项目计划书》，包括具体任务描述和项目进度表等。

第十五条 在项目的各个阶段，信息中心需配合项目经理制定阶段性项目计划。信息中心需配合项目经理对项目计划执行情况进行监控，确保项目按计划完成。

第十六条 项目计划需要变更时，项目经理填写《项目计划变更说明》，并提交本单位主管领导审批，通过审批后，交给信息中心执行。

4.4.5、 系统设计

第十七条 系统设计应分为概要设计和详细设计，系统设计要遵循完备性、一致性、扩展性、可靠性、安全性、可维护性等原则。

第十八条 在系统设计阶段中，业务科室应充分参与，确保系统设计能满足系统需求。

第十九条 项目组进行详细设计，出具《设计说明书》和《单元测试用例》。《设计说明书》中需要定义系统输入输出说明和接口设计说明。本单位主管领导组织相关人员对概要设计进行评审，出具《设计评审报告》。信息中心应参加此评审并对评审意见签字确认。

第二十条 设计评审均以《业务需求说明书》和《系统需求规格说明书》为依据，确保系统设计满足全部需求。

第二十一条 对已确认通过的系统设计进行修改需获得管理科室

领导的审批后方可进行。

第二十二条 对系统设计的修改的文档须由文档管理人员进行归档管理。

4.4.6、 系统实现

第二十三条 项目组根据《设计说明书》制定系统实现计划，并提交项目经理对计划可行性进行审批。

第二十四条 系统实现包括程序代码、单元测试和集成测试。

第二十五条 项目组保证开发、测试和生产环境独立，为各环境建立访问权限控制机制，并明确项目成员的职责分工。对开发环境、测试环境与生产环境在物理或逻辑方面应该做到隔离；如果环境的分隔是通过逻辑形式实现的，应定期检查网络设置。项目组对已授权访问生产环境的人员进行详细记录，并对该记录进行定期检查，确保只有经授权的人员才能访问到生产环境。

第二十六条 软件开发要求：

1、开发环境与实际运行环境物理分开，开发人员和测试员各行其职，测试数据和测试结果受到控制；

2、开发人员需为单位内部专职人员，开发活动应按单位相关规定进行，并接受审查；

3、软件开发的代码要单位给定的规范来编写；

4、应软件开发时设计的相关文档和使用指由负责保管提供；

5、软件开发过程中任何变动都需负责审批和批准。

第二十七条 项目组进行单元测试、集成测试和安全测试，测试人员签字确认测试结果。

4.4.7、 系统测试和用户测试

第二十八条 项目组制定《系统/用户测试计划》，并提交项目经理对计划可行性进行审批。

第二十九条 《系统/用户测试计划》必须定义测试标准，并明确各种测试的测试步骤和需要的系统设置要求。

第三十条 项目组向数据拥有科室申请获取测试用业务数据的使用权，对获取的数据进行严格的访问控制，确保只有相关项目人员才能访问及使用。

第三十一条 项目组负责测试数据准备，测试用数据要足够模拟生产环境中的实际数据。对已评定为敏感信息的数据进行敏感性处理和保护。

第三十二条 信息中心或合作开发商建立测试环境进行系统测试。在系统测试中对新系统内部各模块之间的接口和与其他系统的接口进行充分测试；在系统安全性测试中，对系统进行主机漏洞扫描、主机安全基线检查、系统渗透测试等项目。出具《系统测试报告》和《系统上线安全检查报告》，测试人员签字确认测试结果。

第三十三条 系统测试通过后，信息中心配合业务组建立用户测试环境，根据用户测试用例进行用户测试，出具《用户测试报告》，信息中心应在用户测试报告中签字确认。

第三十四条 项目组完成系统帮助文档（其中包括《用户操作手册》和《安装维护手册》）。凡涉及应用系统的变更，应对系统帮助文档及时更新。

4.4.8、 试运行

第三十五条 系统主要使用科室根据项目规模及影响决定试运行策略。

第三十六条 项目组制定《试运行计划》，并制定试运行验收指标，上报本单位主管领导审批。《试运行计划》中应包含问题应对机制，明确问题沟通渠道和职责分工。

第三十七条 项目组联合试运行单位进行相关系统部署工作，准备培训资料，对相关用户和技术人员进行培训。用户培训的完成度应为实施后评估的指标之一。

第三十八条 项目组根据《试运行计划》进行系统转换和数据迁移。系统转换前，检查系统环境，确保运行环境能满足新应用系统的需要。系统转换时必须详细记录原系统中的重要参数、设置等系统信息，并填写试运行报告相关内容。系统参数、设置的转换工作作为系统上线的验收的评估指标之一。

第三十九条 数据迁移前，应制定详细的《数据迁移计划》，《数据迁移计划》中应包含迁移方案、测试方案、数据定义，新旧数据对照表、迁移时间、回退计划等信息。数据迁移计划需经项目经理和主管领导签字审批。

第四十条 数据迁移后，项目组对数据迁移的完整性和准确性作出检查，出具《数据迁移报告》，其中包括数据来源、转换前状态、转换后状态，数据迁移负责人、对完整性检查情况、对准确性检查情况等内容。各相关科室验收转换结果后在该报告上签字确认。

第四十一条 系统转换和数据迁移由试运行单位业务科室和单位主管领导共同监督并进行验收。

第四十二条 系统转换和数据迁移验收通过后，正式启动试运行。在试运行过程中，试运行单位把系统运行情况（系统资源使用，反应速度等）记录到试运行报告中。必要时，项目组应根据系统运行情况对应用系统进行优化。

第四十三条 试运行达到试运行计划规定的终止条件时，项目组编写《试运行报告》。此报告应由项目组和试运行单位签字确认，并提交本单位主管领导审阅。本单位主管领导审阅试运行结果，决定试运行结束或延期。

4.4.9、 系统验收

第四十四条 系统主要使用科室及信息中心联合组成独立系统验收小组，也可授权原项目组作为验收小组。验收小组从功能需求及技术需求层面对系统进行综合评估。验收小组负责制定系统交付清单，并对清单中的交接物件进行清点核验。交付清单中应包括设备列表、设计文档、部署方案、测试文档、验收文档、源程序等。

第四十五条 验收小组应根据验收情况整理形成《系统验收报告》提交系统主要使用科室和信息中心审阅。

第四十六条 系统主要使用科室和信息中心负责人根据系统测试、试运行情况签署验收意见。

4.4.10、 系统上线

第四十七条 系统上线应遵循稳妥、可控、安全的原则。

第四十八条 通常情况下，系统上线包含数据迁移工作。

第四十九条 项目组制定《系统上线计划》，上报本单位主管领

导审批。在上线计划得到批准后才能开始部署上线工作。

第五十条 《系统上线计划》内容应包括但不限于：

（一）部署方式和资源分配（包括人力资源及服务器资源）；

（二）上线工作时间表；

（三）上线操作步骤以及问题处理步骤；

（四）项目阶段性里程碑和成果汇报（项目执行状态的审阅、进度安排等）；

（五）数据迁移的需求和实施计划；

（六）完整可行的应急预案和“回退”计划；

（七）用户培训计划（包括：培训计划、培训手册、培训考核等）；

（八）本单位下发的系统标准参数配置。

第五十一条 上线本单位在上线初期需加强日常运行状态监控，出现问题时应及时处理，对重大问题应启动紧急预案。

第五十二条 在完成上线后要填写《系统验收评估报告》，上报本单位项目组汇总整理。《系统验收评估报告》内容包括：数据准确性、系统性能及稳定性、接口问题、权限问题、业务操作影响度、问题处理情况、备份、批处理等。

第五十三条 上线本单位管理层要对《系统验收评估报告》进行审批签字。

第五十四条 本单位主管领导批准结项后，开发组将整理的文档提交各自科室统一管理。

4.4.11、 合作开发管理

第五十五条 合作开发商的选择应遵循单位相关规定，合作商资

质认定参见第三方管理制度。

第五十六条 合作开发商必须遵循本单位《软件开发管理制度》。

第五十七条 项目经理同合作开发商明确规定项目变更的范围和处理方式，重点关注需求和设计变更。

第五十八条 项目经理负责监控合作开发商的项目管理及软件开发活动。合作开发商应按计划定期向项目经理报告进展状态，并提交阶段性成果文档。发生重大问题时，合作开发商需及时向项目经理汇报。

第五十九条 信息中心派专人监控合作开发商的质量保证过程。

第六十条 项目组同合作开发商商定验收的标准和方法。

第六十一条 以上各要求需要在开发合同中明确。

4.4.12、 外包开发管理

第六十二条 立项申请经本单位信息中心审批通过后，通过招标程序选定开发商，确保承包方有相应资质，签订外包开发合同。

第六十三条 与中标软件开发商签订保密协议，明确其保密责任。

第六十四条 要求选定开发商提供所有必要的软件配置项。

第六十五条 应确保所有软件配置项为最新，与实际运行环境配套。

第六十六条 应确保所有软件配置项安全，由专人负责管理。

第六十七条 应在软件安装之前根据开发要求检测软件质量，包括功能、性能和安全的各个方面，检测软件包中可能存在的恶意代码等。

第六十八条 应要求开发商提供需求分析说明书、软件设计说明

书、软件操作手册等软件开发文档和使用指南，并指定专人负责保管以上文档。

第六十九条 应要求开发商提供软件源代码，对软件中可能存在的后门进行审查，或者可以委托第三方检测机构进行,提供软件源代码审查记录，详细记录审查结果。

第七十条 若未能提供软件源代码，要求开发单位提供第三方机构出具的安全性测试报告。

第七十一条 要求开发商制定培训方案，对本单位使用人员和运维人员进行相应的技能培训。

4.4.13、 外包服务管理

第七十二条 外包服务的服务商必须具有相应的资质要求。

第七十三条 服务商及其法定代表人在征信系统中必须无不良信用记录。

第七十四条 与外包服务商签订正规的外包服务合同，明确其权利和责任。

第七十五条 与选定的外包服务商签订与安全相关的协议，明确约定相关责任，确保提供相应的技术培训和服务承诺。

第七十六条 应确保外包服务商的系统访问权限受到约束。

第七十七条 外包服务商进行现场技术支持服务时，应事先提交计划操作内容，经相关负责人批准后，由专人陪同服务外包人员，核对操作内容并准确记录实际操作内容。外包服务人员不得查看、复制或带离任何机构的敏感信息。

第七十八条 要求外包服务商严格履行服务外包合同（协议）中

的各项安全承诺，在提供技术服务期间，遵守本单位的安全管理规定与操作规程。

4.4.14、 附则

第七十九条 本制度的解释权归 XXX 单位。

第八十条 本制度自发布之日起开始执行。

4.5、工程实施安全管理制度

4.5.1、 总则

第一条 为本单位信息系统工程（以下本文件所涉及的“工程”均指本单位信息系统工程）实施管理，制定本制度。

第二条 本单位应按国家相关信息安全相关政策法规和标准的规定进行信息系统工程实施管理。

第三条 本制度适用于本单位。

4.5.2、 工程实施管理

第一条 由负责信息系统工程实施过程的管理工作。

第二条 工程实施单位应提供其能够安全实施信息系统建设的资质证明和能力保证。

第三条 在工程实施之前，由工程实施单位制定详细的工程实施方案，实施方案需要经信息安全领导小组批准认可后方可实施。

第四条 工程实施方案应包括工程时间限制、进度控制和质量控制等方面内容。

第五条 工程实施单位在实际工程实施中应按照工程实施方案内容对工程实施过程进行进度和质量控制，并定期向提交阶段性工程报告等文档。

第六条 由工程实施单位和监理单位共同制定工程实施方面的管

理制度，明确说明实施过程的控制方法和人员行为准则，管理制度需要得到的批准。

4.5.3、 实施过程控制方法

第一条 在工程实施过程中，使用主动控制的方法：

(一) 预测和估计潜在的风险，在问题发生之前采取有效的防范措施；

(二) 评价项目的现状和进展趋势，分析其影响并提出建设性意见；

(三) 对项目状态持续不断的跟踪、监测，有效而经济地预防意外事故。

第二条 在确定项目总目标和阶段目标并开始按计划实施后，进入项目控制期。项目经理要始终不断明确以下关键问题：

(一) 项目目前处于什么阶段；

(二) 项目的最终和本阶段目标是什么；

(三) 怎样做才能实现项目目标；

(四) 现在采取的措施是否都是正确的。

第三条 项目进度控制措施如下：

(一) 组织措施

1. 明确项目控制人员的具体职责；

2. 进行项目工作结构的分解，创建项目工作控制基线及项目控制时间；

3. 确定项目进度工作制度和工作计划，如项目每周例行会议。

(二) 经济措施：确保项目资金的提供；

(三) 信息管理：

1. 对影响项目进度的干扰和风险因素进行分析；

2. 进行计划进度和实际进度的比较；

3. 定期制作各种进度情况报告。

第四条 质量控制的关键：

(一) 加强质量意识：提高所有实施人员特别是负责人的质量意识，认识到质量是项目成功与否的关键。

(二) 明确质量责任：项目经理及有关科室负责人和项目组成员都要明确自己在保证项目质量工作中的责任。

(三) 提高人员素质：选择满足实施需求且高质量的人员组建项目组。

(四) 制定质量标准：建立一套完整的质量标准化体系，根据项目计划工作内容由责任人逐一制定。

第五条 项目质量的保证措施：

(一) 项目总体目标明确、清晰、量化。如果项目实施过程发生变化，要重新考虑项目目标。

(二) 将项目总体目标分解为阶段目标，并将工作任务分解为最小单位。

(三) 根据工作任务，在计划中设定检查控制点

(四) 对每项工作任务进行评价，并对各种问题进行总结。

(五) 评价整个项目。评价总结工作在项目结束后进行，目的是系统地分析项目工作成果是否达到了项目目标的要求。

第六条 项目风险控制和管理：

(一) 风险识别：确定各阶段工作的风险种类、对项目的影响；

(二) 风险量化：对风险及风险产生的影响进行评估；

(三) 应对计划：制定风险管理计划，采取措施增大制约风险的机会；

(四) 风险控制：不断对风险管理计划进行更新，并对风险因素采取预防和纠正措施。

第七条 项目执行过程中为了保障项目在预期的目标（进度、质量/范围、成本）范围内完成，必须严格执行项目计划，尽量避免项目需求变更和人员变更。如果出现不可预知的因素导致项目变更，必须及时调整项目目标、项目计划，并通知工程管理人员，由其签字确认。

第八条 项目经理应根据项目计划的关键路线图，在项目执行过程中关注关键路线的执行情况。针对项目中出现的变更采用补救、更新计划等方式进行处理。

4.5.4、 实施人员行为准则

第一条 工程开通和维护要严格按照工程规范的要求进行。

第二条 规范施工、文明施工，严禁马虎作业。

第三条 进入机房施工须征得机房管理员同意，按照外来人员访问

管理规定执行。

第四条 在机房和办公场所工作时，要严格遵守本单位的各项规章制度。

第五条 对设备进行维护操作时，须经部相关科室主管人员认可，并在相关人员陪同下进行。

第六条 对设备硬件进行操作注意要有防静电措施。

第七条 在科室内网计算机上不允许使用未经授权的存储介质（U盘、光盘、硬盘等）。

第八条 携带物品进入机房须征求机房值班人员和主管的同意，并放置在指定位置，不可随意乱放。

第九条 实施人员每天工作结束后,要清理工作现场,保持机房整洁。

第十条 严禁擅自使用办公电话，如确实需要，须经相应科室人员同意后方可使用。

第十一条 严禁在机房或办公场所内吸烟、玩游戏和乱动其它厂家设备。

4.5.5、 附则

第一条 本制度的解释权归 XXX 单位。

第二条 本制度自发布之日起生效。

4.6、测试验收安全管理规定

4.6.1、 总则

第一条 为本单位信息系统测试验收管理，制定本规定。

第二条 本单位应按国家信息安全相关政策法规和标准的规定进行信息系统测试验收管理工作。

第三条 本规定适用于本单位。

4.6.2、 测试验收管理

第一条 由组织验收小组负责信息系统测试验收，并按照本管理规定的要求完成系统测试验收工作。

第二条 由本单位委托具备国家相关技术资质和安全资质的第三方测试机构对系统进行安全性测试，并出具安全性测试报告。

第三条 在测试验收前由第三方测试机构根据设计方案或合同要求等制订测试验收方案，《测试验收方案》的内容包括：

(一) 测试策略：描述测试策略；

(二) 测试描述：包括测试环境、测试人员安排、测试方法和测试时间安排等；

(三) 测试规定：包括环境准备、数据准备、测试人员行为准则和测试用例准备等；

(四) 可交付件：测试完成后，提交测试日志、缺陷报告和测试

报告等。

第四条 本单位信息安全领导小组对第三方测试机构提交的《测试验收方案》进行审定，审定通过后按《测试验收方案》开展测试活动。在测试验收过程中应详细记录测试验收结果，并形成测试验收报告。

第五条 测试验收报告中需要给出测试是否通过的结论，如果报告中提出了存在的问题，则同时还需要提供针对这些问题的改进报告。测试报告和改进报告都需要有第三方测试机构的签字或盖章。

第六条 由组织验收小组对系统测试验收报告进行审定，并签字确认。

第七条 信息系统验收完成后，应明确负责信息系统的运行维护工作的责任人，明确岗位安全责任。

第八条 认真做好信息系统建设项目的档案建设工作，建设完成后及时移交相关部门。

4.6.3、 测试验收控制方法

第一条 由测试负责人组织测试人员准备测试环境，并进行系统测试。

第二条 由测试人员根据《测试验收方案》中的测试用例对系统进行测试。

第三条 测试人员在测试过程中填写《测试用例表》，并将发现的

问题及时交给实施单位，并令其在一定期限内修改完毕。

第四条 根据实际情况可以对系统进行初步测试验收【初验】和最终测试验收【终验】。测试验收全部完成后由测试人员根据测试情况编制《测试验收报告》，《测试验收报告》由验收小组负责审核批准。

第五条 软件产品需要通过单元测试、集成测试和系统测试。

4.6.4、 测试人员行为准则

第一条 测试人员严格按照《测试验收方案》中规定的时间进场开展测试。

第二条 测试人员严格按照测试规范执行各项测试活动。

4.6.5、 附则

第一条 本规定的解释权归 XXX 单位。

第二条 本规定自发布之日起生效。

4.7、系统交付安全管理规定

4.7.1、 总则

第一条 为本单位信息系统的交付管理，制定本规定。

第二条 本单位应按国家信息安全相关政策法规和标准的规定进行信息系统交付管理工作。

第三条 本规定适用于本单位。

4.7.2、 交付管理

第一条 由负责系统交付的管理工作，并按照本管理规定的要求完成系统交付工作。

第二条 工程验收完成后，由督促工程实施单位提供详细的系统交付清单，并根据交付清单对所交接的设备、软件和文档等进行清点，确保工程实施单位提供系统建设过程中的文档和指导用户进行系统运行维护的文档。

第三条 工程实施单位应对负责系统运行维护的技术人员进行相应的技能培训，并对培训情况进行记录，包括培训内容、培训时间和参与人员等。

4.7.3、 系统交付的控制方法

第一条 系统试运行完成后，工程实施单位项目经理参照项目合同及项目实施计划，判断项目现状是否达到需方要求以及项目是

否可进入验收阶段。

第二条 若验收条件满足，由工程实施单位项目经理出面与共同拟定《系统验收计划》，同时，工程实施单位项目经理填写《项目验收申请表》、《系统交付清单》，提交审批。

第三条 确认《系统验收计划》和《系统交付清单》后，工程实施单位派出代表和验收小组、监理单位一起进行项目验收工作。

第四条 项目验收过程中，工程实施单位项目经理应详细记录问题。对于验收过程中出现的问题，实施单位项目经理应安排实施人员对项目进行修改和完善，并取得验收小组认可。

第五条 项目验收完毕后，验收小组在《项目验收报告》上签字确认。

第六条 项目验收完毕，工程实施单位应组织项目组执行系统交付工作，按《系统交付清单》提交交付物，并为负责系统运行维护的技术人员提供相应的技能培训。

4.7.4、 参与人员行为准则

第一条 参与系统交付的工程实施单位人员应严格按照《系统交付清单》准备交接的设备、软件和文档等。

第二条 参与系统交付的人员根据《系统交付清单》对交付物进行逐项清点，发现问题及时与工程实施单位人员沟通。

4.7.5、 附则

第一条 本规定的解释权归 XXX 单位。

第二条 本规定自发布之日起生效。

4.8、信息系统等级测评管理规定

4.8.1、 总则

第一条 为本单位信息系统等级测评管理工作，特制定本规定。

第二条 本规定适用于本单位。

第三条 本单位按国家信息安全相关政策法规和标准的规定进行信息系统等级测评管理工作。

4.8.2、 等级测评管理

第一条 由本单位负责本单位信息系统等级测评管理工作。

第二条 选择具有国家相关技术资质和安全资质的测评单位进行等级测评。

第三条 安全等级为第三级（含）以上的信息系统应当选择符合下列条件的等级保护测评机构进行测评,按照第三级系统要求，自主选择测评机构。

(一) 在中华人民共和国境内注册成立（港澳台地区除外）；

(二) 由中国公民投资、中国法人投资或者国家投资的企事业单位（港澳台地区除外）；

(三) 从事相关检测评估工作两年以上，无违法记录；

(四) 工作人员仅限于中国公民；

(五) 法人及主要业务、技术人员无犯罪记录；

(六) 使用的技术装备、设施应当符合本办法对信息安全产品的要求；

(七) 具有完备的保密管理、项目管理、质量管理、人员管理和培训教育等安全管理制度。

第四条 在信息系统运行过程中，第三级信息系统应每年对系统进行一次等级测评，发现不符合相应等级保护标准要求的应及时整改。

第五条 在系统发生变更时及时对系统进行信息系统等级测评，发现级别发生变化的及时调整级别并进行安全改造，发现不符合相应等级保护标准要求的及时整改。

4.8.3、 附则

第一条 本规定的解释权归 XXX 单位。

第二条 本规定自发布之日起生效。

4.9、信息系统安全服务商选择管理办法

4.9.1、 总则

第一条 为本单位信息系统的安全服务商选择管理，特制定本办法。

第二条 本单位按国家信息安全相关政策法规和标准的规定进行信息系统安全服务商的选择工作。

第三条 本办法适用于本单位。

4.9.2、 安全服务商选择和评价

批注 [1]:

第一条 信息系统建设过程中，应选择具有相关服务资质并且信誉较好的厂商，要求其已获得国家主管部门的资质认证并取得许可证书，能有效实施安全工程过程，并且有成功的实施案例。

第二条 对重要的信息系统工程建设项目，需在主管部门指定或在特定范围内选择具有服务资质的信誉较好的厂商，并经实践证明是安全可靠的厂商。

第三条 在确定好安全服务商后，与安全服务商签订安全责任合同书或保密协议，规定保密范围、安全责任、违约责任、协议的有效期限等。

第四条 在确定好安全服务商后，与其签订服务合同，确保其提供技术培训和服务承诺。

第五条 服务供应商评价，对提供网络安全产品和安全服务的供应商，应由 XXX 部门对其进行调查，并将调查结果记录于《供应商评价表》，经 XXX 审核后，由最高管理层决定是否可列为合格的供应商；

服务供应商的评价应包括以下内容：

(1) 供应商的资信能力；

(2) 供应商的质量保证能力；

(3) 价格；

(4) 交货情况；

(5) 服务情况。

4.9.3、 附则

第一条 本办法的解释权归本单位。

第二条 本办法自发布之日起生效。

第五章 安全运维管理

5.1、环境安全管理规定

5.1.1、 总则

第一条 为保证本单位办公区和机房内设备处于最佳状态，使其运行服务质量能够满足业务使用的需求，并保证信息资产不被非法物理访问，特制订此规定。

第二条 本规定适用于本单位。

5.1.2、 机房安全管理

第三条 设备的维护必须有专人负责，他人不可随意操作。设备需要停机检查时，应经运维工作小组批准后，方可进行。关闭设备时，应经运维工作小组领导同意。

第四条 明确各设备的安全管理责任人。

第五条 机房内严禁从事与工作无关的各项工作。

第六条 机房内设备必须按照设计及相关规定布置，机房内预留位置不能随意占用。

第七条 设备安放合理，布线整齐，强电与通信电缆走线分离，避免交叉，禁止随意改动布线。

第八条 操作维护终端应具备 UPS 不间断电源或逆变器，应该有明确的防病毒措施，定期进行检查。维护终端设备严禁上网，严禁装载游戏软件等。

第九条 无人职守机房必须有配套的环境监控设备，如出现环境监控告警应及时解决。

第十条 机房空调应指定专人负责，使机房温、湿度应符合机房维护技术指标要求，机房正常温度应保持在 20℃－25℃，相对湿度保持在 40%－60%。

第十一条 机房应有良好的防静电措施，机房内配置防静电手环，地面铺设防静电地板。

第十二条 机房照明设备安全可靠，应配备应急灯，各种照明设备应有专人负责，定期检修。

第十三条 机房门窗要密闭，环境保持卫生清洁，机房内设备摆放整齐。

第十四条 交换机、路由器应建立防尘缓冲带，备有工作服和工作鞋。

第十五条 维护人员要切实遵守安全制度，认真执行用电、防火的规定，做好防火、防盗、防爆、防雷、防冻、防潮等工作，确保人身和设备的安全。

第十六条 机房配置灭火设备，各种灭火设备要定位摆放，定期对防火设备进行检查。一旦发生火情，值班人员应按机房灭火流程图及应急措施进行处理，并立即逐级上报。

第十七条 在维护、测试、装载、故障处理、日常操作及工程施工等工作中，应采取预防措施，防止造成工伤和通信事故。

第十八条 机房内非特殊需要，严禁使用明火。

第十九条 机房应配置电子门禁系统，外来人员不得擅自进入机房。因公原因进入机房，应经相关领导批准后，进行物理登记和电子记录双重备案，方可进入。

第二十条 定期对无人职守机房进行巡查，在洪水、冰凌、台风、雷雨、严寒等情况下，应加大巡视强度，以确保机房室内外环境的良好与安全，保证机房设备正常运行。

第二十一条 机房内严禁吸烟、饮食、睡觉、闲谈。各种与工作无关的书刊、报纸和其它物品不准带入机房。

第二十二条 值班不做与工作无关的事，严禁在终端设备上操作与工作无关的程序。值班人员不得撤离工作岗位。

第二十三条 按时、按质、按量完成各种维护测试，发现问题及时分析处理，认真完成各项质量指标。

第二十四条 按时、按质、按量完成各项作业计划，要符合作业计划的周期要求。

第二十五条 各项维护记录齐全、准确。

5.1.3、 办公区信息安全管理

第一条 任何员工进入办公区域时，必须佩带工卡，工卡必须戴在外部可见的地方。员工如果忘记或丢失工卡，由门卫登记并向员工提供临时出入卡。

第二条 员工在办公区发现没有在明显位置佩带工卡/临时卡的人员必须主动询问对方的身份并要求出示相关证件。

第三条　不允许转借自己的工卡或使用其他员工的工卡。

第四条　未经许可，员工不得企图进入严格限制的办公区域，如机要室、存储介质室等。

第五条　当携带计算机存储介质离开办公区时必须具备通行证，所有此类物品的出门都必须在门卫处记录。

第六条　在员工离职时，所有的访问权必须立即收回（工卡、钥匙等）。

第七条　对所有需要进入办公区域的供应商、顾问、拜访者等非内部人员，必须有员工陪同，在门卫处进行登记，并发放临时卡后方可进入。

第八条　接待人不得引领和允许供应商、合作商进入未经批准的机房、办公区或其它机要区域，员工有权拒绝或制止供应商、合作商进入未经批准的办公区域。、

第九条　接待科室原则上应为供应商、合作商安排专门的办公场所。业务洽谈应当在接待室或对外会议室内进行，重大项目的会谈应当在专门的会议室进行，不得在进行。

第十条　员工下班后桌面上不能有敏感信息的纸件文档，敏感信息的文档应放在抽屉或保密柜内，存放敏感信息文件的保密柜必须设置密码。

第十一条　员工离开座位超过 30 分钟，必须对计算机进行锁屏，桌面上不能有敏感信息的纸件文档。

第十二条　所有有单独房间的员工，在离开时必须锁门。当无人

时，离开必须锁门。

第十三条　妥善保管好个人的贵重物品和仪器，下班后必须把贵重物品和仪器存放在保密柜内。

第十四条　员工调离部门或更换时，必须立即交还原钥匙。

5.1.4、 附则

第一条　本规定的解释权归 XXX 单位。

第二条　本规定自发布之日起生效。

第一条

5.2、资产安全管理制度

5.2.1、 总则

第一条 为加强本单位信息系统系统资产（包括设备和介质等）的安全管理，对信息系统资产使用、传输、存储及维护等方面的管理做出规定，规范信息系统资产管理和使用的行为，特制定本制度。

第二条 本制度适用于本单位信息系统资产的管理和使用。

5.2.2、 资产相关活动

第三条 信息资产等级划分

根据信息资产的重要度和对本单位的影响度，将资产分为三级：

机密级：涉及本单位重要业务活动的资产。如财务数据和报表、重大决策、人事数据、合同、程序原代码等。

内部级：涉及本单位主要业务活动，有一定保密要求的资产。如体系文件，管理制度等。

非内部级：除秘密级和内部级以外的其他资产。

第四条 信息资产的分类

根据信息资产的特点和用途，将信息资产分类如下：

信息与数据资产：主要指在工作过程产生的电子数据为主，存储在相关介质中的数据和信息。

工作设备资产：主要指工作用的设备和其相关配件。

纸制文件和记录：以纸制形式存放的文件和相关记录。

客户资产：非单位资产，因各种原因暂时放在单位内的客户资产。

第五条 信息资产的标识

信息与数据资产：应在页眉或文件的首页左上角标注其重要等级。

工作设备资产：根据本单位的固定资产管理相关规定，须根据其类别，重要度，用途或功能在明显位置进行标记，设备上的所有标记或编号只能由云计算部人员进行标识和管理，其他人员不得随意涂改或是撕毁标记。

对服务器和个人 PC：在显示器和主机上都须有编号，服务器必须在明显位置进行标记（如，在服务器的机箱或是显示器上贴上‘服务器’字样），不得与其他个人 PC 混放在一起；

移动计算机：所有移动计算机须设置统一编号；

对于客户提供的设备资产应进行特别的标记并形成相应的记录。

纸制文件和记录：应在文件的首页或页眉上进行标记。

客户提供的应在其适当位置注明是客户资产。

5.2.3、 信息系统资产使用

第六条 信息系统资产采购后交付使用部门的资产管理员，资产管理员对资产按照规则命名和标识，使用人要在本部门《资产清单》上进行领用登记，然后由资产管理员交付资产给使用人。

第七条 信息系统资产的使用人、责任人是其资产的第一责任人，要按照产品手册、操作规程、管理制度等要求正确的使用设备或介质资产，防止其被盗、遗失、被未授权修改以及信息的非法泄

漏。

第八条 信息系统资产的传输、存储、维护或销毁参照介质管理中相关内容执行。

第九条 信息系统资产基本信息发生变化时，使用人/责任人需要到本部门资产管理员处进行相关的信息变更。

5.2.4、 信息系统资产传输

第十条 含有敏感工作信息的信息系统资产在传输过程中必须亲自交给接受方。

第十一条 通过外部运输人员传输的信息系统资产需要接受者签字等措施，以保证传送安全到达。

第十二条 需要有日志记录含有敏感工作信息的信息系统资产的传输过程（多少、在哪里、接收者姓名、地址等）。

第十三条 含有敏感工作信息的信息系统资产不能在旅游时携带，除非经过管理科室审批同意。

5.2.5、 信息系统资产存储

第十四条 信息资产领取使用后，按照信息资产明细账和信息资产登记卡片，明确信息资产的使用人员和存放地点，使用人员是信息资产保管的责任人，负责固定资产在使用过程中的安全和完整。

第十五条 贵重的、精密程度较高的信息系统资产应指定专人保管。

5.2.6、 信息系统资产维护

第十六条 信息系统资产日常维护包括巡检与监控、备份与恢复、停机检修。

第十七条 巡检与监控人员对应用系统、网络系统和机房的运行状况进行监控，定期检查系统日志，填写机房巡检日志，及时报告、处理发生的异常事件，并定期汇总上报。

第十八条 备份与恢复人员按方案进行系统备份，并在系统环境发生重大变化时对系统和数据及时进行恢复。

第十九条 资产维护人员制定详细停机检修方案，报审批后，在网上发布停机公告，电话通知重点用户，确认对用户无重大影响后，按方案停机检修，尽量安排在节假日期间。

第二十条 信息系统资产需外出维修的，必须由使用人员提出申请，科室负责人签字确认，经审核方可，如设备未出保修期，由资产管理科室向提供产品保修证书，所有产品保修证书统一由资产管理科室编号保管。

第二十一条 各科室人员均不得擅自拆装信息系统资产设备，如有故障，不得私自拆修，须及时通知，由技术人员进行检查维修。

第二十二条 所有信息系统资产使用人员应爱护资产设备，自觉进行日常清理保洁及相关简单的维护。

5.2.7、 信息系统资产报废

第二十三条 信息资产正常报废时，填报《信息系统资产报废申请

表》，办理相关手续。

（一）信息资产报废科室填写《信息系统资产报废申报表》一式三份，由本单位负责人批准。

（二）单位批准后，经办人员携带报废申请表及信息系统资产实物到进行核实鉴定。

（三）经核实后，信息资产管理科室将报废信息资产回收（自收自支事业单位除外），并在《信息系统资产报废申报表》上级资产管理科室意见处签字。

（四）签字后，报主管领导审批，办理报废审批。

（五）《信息系统资产报废申请表》经主管领导审批后，一份作为本单位固定资产管理科室核销固定资产台账依据，一份作为本单位财务科室核销固定资产账和固定资产卡片依据，一份作为回收依据。

第二十四条 本单位在信息系统资产损毁或丢失时，分清责任后进行处理，并办理相关手续。

（一）使用科室或个人发生信息系统资产损毁或丢失时，应及时报本科室信息系统资产专管人员，由专管人员确认后，查明原因，报本单位领导审批。

（二）经领导批准后，本单位填写《信息系统资产报废申请表》一式三份，按信息系统资产报废的手续办理。

（三）本单位查清责任原因后，责任人写出检查并按信息系统资产实际价值的 10%做出赔偿，另有规定的从其规定。

第二十五条 本单位报废信息系统资产由进行统一处置。

（一）各单位将报废的信息系统资产交回（自收自支单位除外），不得自行处置，及时办理交接手续，统一由进行处置。

（二）将处置的信息系统资产残值收回后，统一由挂账，集中安排使用。

第二十六条 为了确保信息资料安全，本单位在信息系统资产处置前，涉及到网络、软件系统及计算机类设备时，通知专管人员进行检查、清理计算机硬盘资料后，再行处置。

5.2.8、 信息资产的分级管理

第二十七条 信息资产的存放应立足于管理和安全的考虑，为了便于保管、提取、查询，信息资产应尽量以电子介质的形式存储，因此，对于存储在纸介质等其他非结构化的信息资产，如果技术上允许并且有必要的话，应及时进行适当的处理，转换为结构化的电子信息，并以电子介质的形式存储。

第二十八条 信息资产的存储介质存放的地点要求如下：

（一）对于对外公开信息，存放地点没有要求；

（二）对于对内公开信息，如果是结构化的电子信息，应存放在内部服务网络中的文件服务器等；如果是非结构化的其他信息，应存放在室内文件柜中，并有明显的分类标识；

（三）对于内部敏感信息，如果是结构化的电子信息，应存放在有严格管理制度、具有足够的安全防护措施的机房环境中的相关服务器和存储设备上；如果是非结构化的其他信息，应存放在室内具有较

强防盗窃能力的文件柜中，并造册登记，分项存放；

（四）对于内部重要敏感信息，如果是联机存储的结构化电子信息，应存放在有严格管理制度、具有高强度的安全防护措施的机房环境中的相关服务器和存储设备上； 如果是脱机存储的结构化电子信息，以及非结构化的其他信息，应存放在具有严格保安措施的、专门的保管环境中（如档案室等），并造册登记，分项存放。

第二十九 资产的存储介质使用控制要求如下：

（一）对于对外公开信息，介质使用没有限制要求，任何人在任何场合均可以使用；

（二）对于对内公开的信息和存储在电子介质上的信息，必须通过内部网络（如通过技术中心搭建的网盘和 OA 系统进行文件的传递），以注册的合法身份，登录访问和下载使用；对于非结构化的其他信息，经介质保存部门同意，可以提取存储信息的介质使用，使用完毕放回原处；

（三）对于内部敏感信息和存储在电子介质上的信息，原则上要求联机使用，信息只能通过办公 OA 系统专用界面使用，使用者必须具有足够的使用权限；内部敏感信息的脱机提取或抄录，必须有相关领导的书面批准意见，其提取或抄录的相关细节必须记录在案，使用者必须对其提取或抄录内部敏感信息的安全保密负责；对于非结构化信息的使用，必须符合秘要程度文件的相关使用规定，信息的提取或抄录必须有相关领导的书面批准意见，其相关细节必须记录在案，使用者必须对其提取或抄录内部敏感信息的安全保密负责；

（四）对于内部重要敏感信息和存储在电子介质上的信息，必须联机使用，信息只能通过应用系统专用界面使用，使用者必须具有足够的使用权限；内部重要敏感信息绝对禁止的脱机提取，特殊信息的抄录，必须有相关领导及保密人员的书面批准意见，抄录的过程及内容必须有保密人员现场监督检查，抄录的相关细节必须记录在案，使用者必须对其抄录的内部重要敏感信息的安全保密负责；对于非结构化信息的使用，必须符合机要程度文件的相关使用规定，特殊信息的抄录必须有相关领导及保密人员的书面批准意见，其相关细节必须记录在案，使用者必须对其提取或抄录内部敏感信息的安全保密负责。

5.2.9、 附则

第三十条 本制度的解释权归 XXX 单位。

第三十一条 本制度自发布之日起生效。

5.3、介质安全管理制度

5.3.1、 总则

第一条 为加强本单位介质安全管理，即对存储介质的使用、存储、携带、记录、清单等活动提供明确的安全管理标准，特制订此制度。

第二条 本制度适用于本单位。

5.3.2、 介质管理标准

第一条 保管人控制下的存储介质和用来备份或是用做灾难恢复的，需存放在一定安全级别的区域，当无人看管时，要将这些介质存放在或保密柜中。

第二条 用做一般系统备份的存储介质可以与用户控制下的存储介质分开放置，必须被慎重管理以保证在需要恢复的情况下能够得到，同时必须记录在管理员的目录清单里。

第三条 必须建立存储介质的原始存储目录清单，并定期对备用目录清单进行盘点，以备将来使用，当所有权发生变化时，必须进行存储库盘点。

第四条 存储介质库中介质的转移和支配应该是可记录的。

第五条 必须对所有存储介质的出库和入库及其保持记录进行控制。

第六条 存储介质被运离或送出时，要被放在一个被锁住的箱子里，用防篡改的封条封住。

第七条 安装和使用存储介质时必须防止非授权的访问。

第八条 任何的存储介质盘点与检查出现差异必须报告给运维工作小组，并且介质库中的所有介质，包括打开过的空白带和格式化过的、擦除过的、媒体操作装置中的介质都必须有清单列表。责任人必须对所有的清单文档签字。

第九条 含有敏感工作信息的存储介质在邮递或内部传输时候必须被放在标记的密封套子或是包装盒中，被邮递或传输到外部时，内盒需要明确标记为敏感信息，外盒或封套不要标记敏感信息字样，重要敏感数据需经过加密处理，安装防拷贝系统防止非法访问。

第十条 制定硬盘加密，硬盘口令等具体措施。

第十一条 含有敏感工作信息的存储介质不再使用时，应与安全管理工作人员联系，销毁这些敏感信息存储介质。

第十二条 存储介质要全面考虑数据分类标签的需求，如磁带、磁盘及其它存储介质等有不同的分类标签。

第十三条 含有敏感信息的存储介质的复制要有跟踪、出处、输送记录，对拷贝的人需要了解具体情况。

第十四条 在复制或输出敏感信息到存储介质时，需要有人监控（不能让敏感信息自行输出到远程存储介质，特别是远程可移动存储介质）。

第十五条 存储介质的存放，需要用不同的标签或介质类型来表示是原件还是拷贝件。

第十六条 含有敏感信息的存储介质在传递过程中必须亲自交给接受方。

第十七条 通过外部运输人员传递的存储介质需要接受者签字等措施，以保证安全到达。

第十八条 需要有日志来记录含有敏感信息的存储介质的传递过程（多少、在哪里、接收者姓名、地址等）。

第十九条 除非经过管理部门特别同意，旅游时不能携带含有敏感信息的存储介质。

第二十条 除非存储介质内的敏感信息已经被加密，否则存储介质不许在无人看管的可移动设备上使用。

第二十一条 可移动存储介质必须放在随身携带的手提箱中，而不能放在其他的货物托管地方。

第二十二条 所有含有内部信息的存储介质对外部人员都是保密的，严禁员工、顾问和合作方带走。

第二十三条 任何计算机存储介质不再用于存储保密信息之前，必须要进行格式化。

第二十四条 不允许将含有敏感信息的存储介质和非敏感信息的存储介质混放在一起。

第二十五条 存储介质删除敏感信息后，必须执行重复写操作防止数据恢复。

第二十六条 含有硬拷贝形式的敏感信息存储介质的报废处理方式是切碎或者烧毁。

第二十七条 如果将存储介质给第三方使用，需要确认敏感信息已经删除。

第二十八条 当携带存储介质离开时必须出示通行证，所有此类物品必须在门卫处记录。

第二十九条 访问磁带、磁盘和文档库需要提出申请，并且要对磁带、磁盘、和文档库进行数据加密，加密方式有用户加密码或其他加密方式进行加密，由审批同意放可进行，并登记备案。

5.3.3、 附则

第一条 本制度的解释权归 XXX 单位。

第二条 本制度自发布之日起生效。

5.4、设备安全管理制度

5.4.1、 总则

第一条 为加强本单位设备安全管理，明确维护人员责任，保障系统的安全稳定运行，特制订本制度。

第二条 本制度适用于本单位。

5.4.2、 设备安全管理

第一条 负责对本单位信息系统相关的各种设备（包括备份和冗余设备）、线路等定期进行维护管理。

第二条 信息系统的各种软硬件设备的选型、采购、发放和领用参照《系统建设管理-信息系统产品采购和使用管理规定》执行。

第三条 信息处理设备的带离需由带离人员填写设备出门条，经由设备所属科室领导签字后方可带离单位。

第四条 设备出现故障、须开机箱维修的，应由派工程师到现场进行维修或送维修，严禁各部门私自开机箱维修。现场维修时，应由相关人员全程陪同。

第五条 在处理设备故障、进行维修过程中，故障维修申请人应及时提供该机相关资料、文档，确保维修工作得以顺利进行。

第六条 计算机维修人员在维修过程中，对于需要更换的零部件，在价格和型号等方面要及时与申请人沟通，取得认同后再更换。

第七条 维修人员应当认真填写《设备维修记录表》。

第八条 在接到用户提出需外单位维修人员对计算机、数字复印机等设备进行现场维修申请时，计算机维修人员需全程陪同，严禁外单位维修人员擅自读取和拷贝计算机、数字复印机中存储的信息。

第九条 禁止在系统外对设备进行远程维护和远程监控，并严格控制系统内的设备远程维护和远程监控。

第十条 设备的维修流程如下：

（一）由设备管理人员填写《设备维修记录表》；

（二）由派工程师到现场进行维修或送维修；

（三）维修人员填写《设备维修记录表》。

第十一条 设备超过使用年限或发生故障无法维修且无相应配件更换时，可予以报废，必须办理相应报废手续。设备报废参照《系统运维管理-资产安全管理制度》中关于信息系统资产报废的规定执行。

5.4.3、 配套设施、软硬件维护管理

第一条 由负责信息系统配套设施、软硬件的维护管理工作，制定相应的巡检表格和操作规程，规范运行维护活动。

第二条 运行维护工作由系统运维负责人指定相关资产责任人按照操作规程进行，资产责任人承担某一资产的维护和管理。

第三条 对配套设施、软硬件设备和线路的常规运行维护操作按

照操作规程进行，操作规程由资产责任人负责更新和维护。

第四条 对供电和通信设施进行巡检，发现问题及时处理。

第五条 重要线路线缆埋放地点应有明显警示装置，防止因施工等原导致意外破坏，并将系统内所有线路线缆的布置图进行整理汇编，以备查看。

第六条 每半年对软硬件系统（包括备份和冗余设备）进行巡检，发现问题及时处理。系统信息中心按照实际需要制定巡检要求，并按照规定巡检。

第七条 巡检对照巡检表格逐项巡检，巡检表保存一年。

第八条 巡检工作由运维单位组织，具体检查工作每天进行、每周回顾、每月总结。

第九条 巡检包括网络巡检、主机以及数据库巡检、应用系统巡检、机房相关设备巡检。

第十条 网络巡检主要内容：

网络设备外观、接电情况、指示灯、cpu 利用率、内存负载（byte）、广域网接口状态、局域网接口状态、模块状态等。

第十一条 主机巡检主要内容：

CPU 使用率、内存使用率/pagingspace、文件 系统空间、磁盘、IO、网络状况、系统错误日志/mail、硬件报警灯、增减用户、应用纪录、TOP5 应用进程、参数调整纪录、故障/异常纪录、维护总结等。

第十二条 数据库巡检主要内容：

数据库 CPU 使用率、内存使用率/pagingspace、文件系统空间、

磁盘 IO、网络状况、系统错误日志、oracle 进程数、alert.log 纪录信息、表空间使用率、TOP5 数据库进程、用户表空间权限变更、故障/异常纪录、维护总结等。

第十三条 应用服务状况巡检主要内容：

应用服务器 CPU 使用率、内存使用率、文件系统空间、磁盘 IO、网络状况、系统错误日志、oracle 进程数、alert.log 纪录信息、表空间使用率、TOP5 数据库进程、用户表空间权限变更、故障/异常纪录、维护总结等。

第十四条 机房相关设备巡检主要内容：

门禁系统、机房温度、机房湿度、门窗状况、机房清洁状况、UPS 状况、UPS 电池状态、空调机器状况等。

第十五条 巡检工作的开展

（一）网络巡检由运维单位指定的网络设备维护人员进行巡查和操作；主机巡检由运维单位指定的主机设备维护人员进行巡查和操作系统巡检，必须按规定的时间和项目巡视检查管辖下的设备；应用服务巡检由应用开发商指定、认可的应用系统维护人员进行巡查和操作，每个工作日巡视检查管辖下的设备和系统；数据库巡检由运维单位指定的数据库维护人员进行巡查；

（二）巡检人员应根据当班设备的具体运行情况，对运行的设备进行巡检和监控；

（三）巡检人员发现设备有缺陷，发现设备运行状态指示灯有损坏，发现安全保护有变化，均应即时通知系统管理员调整或更换，保

证设备的监控元件在完好状态下运行；

（四）巡检人员发现设备和系统有不正常的噪音、压力、内存泄露等又不能迅速排除的，必须立即报告，并采取适当的防护措施，防止事故的发生或扩大；

（五）每次巡检均须在相应的巡检记录上依顺序做好巡查情况和结果记录；

（六）系统管理员每周一次对巡查情况和结果进行抽查，发现问题追查原因，如属人为应追究当事人责任。

第十六条 及相关的系统管理员、网络管理员、应用系统开发商等应给予巡检人员配合，提交相关的管理记录文档、系统资源信息，信息提供人对信息的真实性承担负责。

5.4.4、 设备使用管理

第一条 服务器安全操作规程

（一）服务器只能由系统管理员或授权的人员操作；

（二）服务器应使用独立的 UPS 后备电源并不得随意断电、重启，一旦发生故障，应当及时通知系统管理员处理；

（三）系统管理员应妥善设置系统密码，不得泄漏，并定期更改；

（四）系统管理员应当定期升级程序补丁，在升级补丁之前应做好相应测试，并备有应急恢复机制；

（五）每天上班首先检查服务器是否正常工作，发现问题及时处理。

（六）服务器开关机要求如下：

- ✓ 一般情况下，服务器不得随意关机，在以下情况下，可以关机，但尽量安排在晚上：安装必要的服务、安装必要的软件、正常的维护需要。
- ✓ 服务器在出现严重故障非重起不能解决时，通过邮件或电话方式通知用户；
- ✓ 服务器在得到 UPS 停电通知时，必须在 1 个小时内关闭。此项设置必须在 APC 的监控软件中设置；
- ✓ 服务器出现严重的硬件故障时，应立即通知网络用户并立即关机，同时通知硬件供应商处理；
- ✓ 服务器在开机时必须确认 UPS 供电是否正常。

第二条 计算机终端使用安全要求

（一）用户终端必须按照要求统一部署防病毒软件及终端安全管理及补丁分发系统，并确保其能够接受来自服务器的自动更新，对接入系统的存储设备要经过计算机病毒与恶意代码的检查处理；

（二）对于本人在系统中的身份标识符，采用英文字母、数字和特殊字符中两者以上组合的 8 位长度口令。要对使用本人身份标识符产生的操作行为负责；

（三）用户在退出系统时，要注销帐号；

（四）用户在暂时离开显示器时，要锁屏；

（五）所有用户均有责任报告所发现的安全弱点和可疑事件，但任何情况下用户均不应尝试验证弱点。用户发现安全弱点和可疑事件

时，应立即向运维单位报告。

第三条 网络设备安全使用要求

（一）网络设备必须放置并固定在专用机柜中。放置机柜的房间要求通风良好、消防设施齐备，并由专人管理；

（二）网络设备必须提供不间断电源以防止突然断电对设备造成损害及数据丢失；

（三）核心网络设备必须提供冗余供电，提高整体运行可靠性；

（四）网络设备需要定期更换管理口令；

（五）网络管理员定期检查各网络设备运行情况；

（六）法定节假日指定专人对网络设备的运行状态进行监控；

（七）只允许经过专业培训，并授权的信息安全保护关键岗位人员才能对网络设备进行调整或对硬件设施进行维护；

（八）对网络设备的配置进行操作变更时应做好记录，保存与备份更新后的配置。

5.4.5、 附则

第一条 本制度的解释权归 XXX 单位。

第二条 本制度自发布之日起生效。

5.5、运行维护和监控管理规定

5.5.1、 总则

第一条 为保障本单位网络与信息系统安全、稳定运行，加强网络与信息系统运行维护和监控管理，特制订此规定。

第二条 本规定适用于本单位。

5.5.2、 运行维护和监控工作

第一条 由负责本单位信息系统的安全运行维护和监控工作，保证各项业务的正常运行。

第二条 建立安全管理中心，对通信线路、主机、网络设备和应用软件的运行状况，对设备状态、恶意代码、网络流量、补丁升级、安全审计等安全相关事项进行集中管理；并形成监测记录文档，指定专人对监测记录进行整理并保管。

第三条 监测记录应包括监测对象、监控内容、监控的异常现象处理等方面。

第四条 组织人员定期对监测记录进行分析、评审，发现可疑行为时采取必要的措施；形成分析报告，分析报告应包括监测到的异常现象和处理措施等。

第五条 维护项目应包括但不限于以下内容：

(一) 机房环境、温湿度检查；

(二) 网络链路的实时监控；

(三) 网络的连通性（内网、外网）、时延、丢包率检查；

(四) 设备运行状态检查：CPU 负荷、连通性等；

(五) 出口链路或关键链路流量检查；

(六) 设备备份工作等。

第六条 定期和不定期对安全设备的策略进行检查，确保安全策略符合系统现状的要求。

第七条 对新购置的设备和软件在上线之前进行安全性检查、策略合理性测试。

第八条 对设备和软件的日志定期和不定期进行审计，了解整个网络的状况、设备的运行状况和网络故障及攻击事件。

第九条 设备和软件分为版本升级和相关库（如病毒库、IDS 策略库）两部分。在业务不能满足或者出现一个很严重的漏洞的情况下，要进行相关升级和逐级上报。

第十条 各系统运维人员负责维护和监控责任范围内的设备，不得越权进行访问。

第十一条 安全运行维护和监控作业计划

第十二条 系统运维人员根据维护和监控工作内容制定各项计划性的安全维护工作。

第十三条 作业计划应包括以下内容：安全设备维护、安全监控、操作日志、日志审核、故障管理、测试等工作。

第十四条 编制安全维护作业计划时，应充分考虑可能发生的各

种情况，明确执行期限，落实到人。

第十五条 编制安全维护作业计划时，应明确各项作业的执行完成标志，提供可操作的核查手段。

第十六条 系统运维人员应定期提交下年安全维护作业计划，由核准后实施。

第十七条 安全维护作业计划核准下达后，要保质、保量、按时完成，不得任意更改，如系统环境变化或遇特殊情况需要临时变动时，须经核准后及时更新。

第十八条 安全维护作业计划在编制和确定后，应根据其内容严格执行。

第十九条 系统运维人员应及时填写维护报告并和相应的维护作业计划归档。

第二十条 系统运维人员应定期对维护计划执行情况进行总结分析。

第二十一条 对于未及时完成或完成情况欠佳的安全维护作业计划，应及时认真地作好总结工作，分析原因，避免下次出现同样的问题。

第二十二条 安全维护作业计划确定严格执行，并由进行定期检查。

第二十三条 安全运行维护报告是安全维护工作小组工作的重要成果之一，对以后的安全运行维护工作有着指导性的意义，是以后运行维护计划制定的可行性依据之一。

第二十四条 安全运行维护报告的内容，应根据作业计划执行情况的对应信息作为参考，结合实际情况来编写。

第二十五条 安全运行维护报告涉及方面包括但不限于以下内容：安全设备维护、安全监控、操作日志、日志审核、故障管理和测试等工作。

第二十六条 远程维护人员通过互联网对内部网络资源的远程运维访问均应得到授权和批准并通过 VPN 接入方式，以达到对传输的数据加密保护。禁止非授权的便携式或移动式设备私自通过远程接入内部网络。因工作需要需将便携式或移动式设备通过远程接入内部网络进行远程运维时，由远程运维人员填写远程运维权限申请单，经过网络管理者及信息中心领导同意后，由网络管理员操作执行。接入操作前，网络管理人员应对即将接入的便携式或移动式设备进行安全检测评估，必要时进行恶意代码查杀。确认安全后方可接入网络。

5.5.3、 附则

第一条 本规定的解释权归 XXX 单位。

第二条 本规定自发布之日起生效。

5.6、网络安全管理制度

5.6.1、 总则

第一条 为了进一步规范本单位（以下简称“本单位”）网络的管理，确保单位网络资源高效、安全运行，加强对网络资源安全性保护，特制定本制度。

批注 [2]：两个“本单位”

5.6.2、 范围

第二条 本制度适用于本单位范围内网络系统的安全和信息安全的管理。

5.6.3、 立项管理

第三条 本制度所称的网络安全：是指本单位所使用的网络，在网上提供各种应用和服务的所有硬件和软件等信息资产的安全。

第四条 本制度所称的信息安全：是指包括由服务器、客户机及其附属设备上的，根据开发设计、技术文档、财务报表、培训资料、人事管理等要求建立的信息系统、报表文档、数据库、图片以及其它包含单位商业机密的相关文档、文件和资料的保密和安全。

第五条 本单位网络与信息的安全管理，应当保障计算机网络设备和配套设施的安全、信息的安全、运行环境的安全。保障本单位网络系统的正常运行，保障信息系统的安全运行。

第六条 由信息中心负责全本单位的网络安全和信息安全工作，不定期对网络内所有人员进行网络安全和信息安全方面的教育，并对

网络中的信息进行有效的监督和审查。

第七条 本单位网络内的所有部门和人员必须接受并配合信息中心依法进行的监督检查，必须接受信息中心进行的网络系统及信息系统的安全检查。

第八条 信息中心对网络安全配置、日志保存时间、安全策略、升级与打补丁、口令更新周期等方面进行管理和规定。

第九条 本单位网络内的所有科室和人员有义务向信息中心报告违反本管理办法的科室和个人或对本单位网络正常安全运行有害的行为。

5.6.4、 网络安全管理规定

第十条 本单位网络由信息中心统一规划、建设并负责运行、监督、管理和维护，包括设置路由器、交换机、防火墙、台式电脑、笔记本电脑及与网络安全相关的软硬件。

第十一条 本单位网络的 IP 地址、子网规划以及涉及网络安全的各种系统登录帐户和默认密码的软硬件设备等均由信息中心集中部署管理，登记后分配至个人，并不定期进行监督和检查。任何人必须严格使用由信息中心分配的“IP 地址”、“机器名”、“系统登录帐户”以及个人电脑等软硬件配置，严禁私自更改或盗用他人的软硬件配置。

第十二条 严禁利用本单位信息类资产包括电脑，打印机、传真机或 RTX、QQ、MSN 等软硬件以及网络资源进行与工作无关或无益的私人活动，不得私自安装与工作无关的软件程序。

第十三条 严禁以空密码登录本单位内部各种涉及网络安全的信息系统或软硬件设备。个人在获得由信息中心分配的各种系统登录默

认密码后，应及时更改密码。各类密码的设置，均应遵循不易被破译的原则，密码的位数应在七位以上。不得把自己的密码告诉他人，也不得把密码写在纸上。密码应经常更换，尤其是重要涉密岗位，同一密码最长使用时间不应超过二个月。

第十四条 严禁以任何手段窃取或试图窃取未授权使用的各种涉及网络安全的软硬件设备的系统登录密码，也不得以他人帐号、IP地址等任何形式登录或试图登录未授权使用的包括电脑在内的各种涉及网络安全的软硬件设备。严禁以任何手段、任何形式查询、访问、修改和删除或试图查询、访问、修改和删除未授权的网络资源。

第十五条 严禁在本单位网络内制作、散播计算机病毒或木马程序。所有接入本单位网络的电脑均须保证安装有防病毒软件，任何人在发现陌生或可疑邮件、计算机非正常运行或是电脑未安装防病毒软件等情况时应及时向信息中心相关人员报告。

第十六条 严禁以任何方式、任何理由对影响本单位网络系统正常运行的服务和软硬件设备实施攻击、干扰和破坏。

第十七条严禁在本单位范围内使用属于个人的或未授权的各类存储介质或可移动的信息设备，如软盘、光盘、移动硬盘、U盘、笔记本电脑等。未经允许不得私自将上述设备带入本单位使用，如确因工作需要须使用，应报本科室经理和行政科室审批。

第十八条 根据厂家提供的软件升级版本对网络设备进行更新，并在更新前对现有的重要文件进行备份。

第十九条 定期对网络系统进行漏洞扫描，对发现的网络系统安全漏洞进行及时修补。

第二十条 具备设备的最小服务配置，并对配置文件进行定期离

线备份，每月进行一次备份。

第二十一条 对变更性的运维割接，应填写割接方案审批单，经信息中心主管领导审批后方可实施；运维割接应按规范统一使用日常操作的运维工具、降低因工具不熟练导致的安全风险；运维割接如需开通远程运维通道，须经领导审批，保证所有与外部系统的连接都必须得到授权和批准。运维割接过程中的操作应保留完整的审计日志，操作完成后应及时更新变更信息、删除临时操作的敏感数据、关闭临时开通的运维通道。

第二十二条 根据安全策略允许、拒绝便携式和移动式设备的网络接入。

第二十三条 定期检查违反规定拨号上网或其他违反网络安全策略的行为。

5.6.5、 信息安全管理规定

第二十四条 各科室的计算机信息安全保密管理由各科室主管或直接领导负责，并指定有关人员具体承办，信息中心负责检查、监督。

第二十五条 对于本单位允许开通互联网的使用人员必须对自己在互联网发布的信息负责，不得进入非法的网站或利用本单位网络资源进行与工作无关，危害单位、国家安全利益的犯罪活动。

第二十六条 严禁利用本单位网络对内或对外制作、查阅、复制和传播反动、封建迷信、淫秽色情等言论、图片以及其它有碍社会治安的信息，更不得在网上公开发布、宣传、谈论涉及单位商业秘密或与工作无关和无益的言论。由于工作原因需向单位内部及外部网站上发布信息或文件资料的，须由科室主管审查批准方可发布或上传。

第二十七条 在本单位网络内任何人因工作需对外联络沟通时，如需使用电子邮件，只允许使用本单位企业邮箱进行信息发送。

第二十八条 原则上不允许在个人电脑上共享本单位有商业价值的重要文件或在科室公共盘上存放有商业价值的重要文件。确因特殊情况需要共享的，应报本科室主管审批通过后，由信息中心进行信息安全方面的处理后，方可共享使用。

第二十九条 涉密信息的传输、查询、修改、删除等处理只限在与之相关或被授权的人员内进行，授权可以采用文字或口头的方式，也可以通过网络应用软件授权。上网用户只能根据自己的权限查询涉密信息，不得越权查询或下载。涉密信息查询或处理人员离开计算机所在房间时，必须退出查询或处理模块。如长时间离开，需锁定或关闭计算机，否则须对因此造成的泄密事件负责。

第三十条 未经科室主管允许，任何人严禁将保存有本单位保密信息的信息存储设备、笔记本电脑或打印资料带离单位；对科室内含有涉密信息的各类存储介质或可移动的信息设备，如软盘、光盘、移动硬盘、U 盘、笔记本电脑等均须列入保密管理范畴，经科室主管允许后方可使用。各类数据备份介质，需由各科室主管指派专人保管，并做好记录，如数据丢失或泄密，科室主管须承担连带管理责任。

第三十一条 本单位员工应积级主动地按照信息中心指定的服务器备份目录定期做好涉及本单位重要信息数据的备份，应达到自己本地电脑和服务器的重要数据的同步和双备份的要求。

第三十二条 本单位信息系统商业数据及商业资料是本单位经营决策的重要商业秘密，各科室员工须树立严格的保密观念，遵守保密规定。涉密的本单位信息系统存储介质及信息系统资料，由各科室指

定专人管理，在其本人离职时必须交回直接领导。

第三十三条 当本科室员工出现工作岗位异动或离职等情况时，科室主管或直接领导应根据情况提前或立即以相应方式通知信息中心相关工作人员取消其相应的权限、密码。

第三十四条 各科室负责人或直接领导应认真、严格地对待和审批下属员工提交的涉及互联网权限的申请，须对其进行有效的监督和管理，并对其上网后的行为和发布的信息严格审查和把关。如因下属员工开通互联网权限后触犯本管理办法的，科室主管须承担连带的监督、管理责任。

第三十五条 本单位所有员工必须自觉遵守本制度，提高信息安全防范意识，防止泄密事件的发生。各科室及个人如发现有单位或个人违反上述规定、或计算机信息系统正在泄密或已经泄密的情况，均有权利与义务及时采取补救措施并向信息中心举报，本单位将视情况对举报行为给予奖励。

第三十六条 认真执行各项管理制度和技术规范，监控、封堵、清除网上有害信息。为有效地防范网上非法活动、各子网站要加强出口管理和用户管理。重要网络设备必须保存日志记录，时间不少于180天，且应保证无一天以上的中断。

5.6.6、 处罚办法

第三十七条 对于违反本管理规定的，信息中心将酌情予以通报批评和断网处理，由此造成的一切后果由该使用人以及部门经理或直接领导负责。

第三十八条 对盗用IP地址、用户账号等对网络及信息系统造成

严重危害且对单位造成经济损失的行为，一经查实，将对当事人直接予以辞退，并处以一定的行政处罚。

第三十九条 凡发生网络安全和信息泄密事件或因员工上网行为违反国家相关法律的，如情形严重、造成国家、本单位或他人财产损失的，无论员工是否有意，均须依法承担民事责任，本单位将按照国家有关法规移交司法机关处理，并追究当事人责任。

5.6.7、 网络设备的管理

第四十条 应定期通过远程监控系统的网络设备的运行状态及各种性能指标实时监控，监控内容包括但不限于：CPU 及内存利用率，端口状态及数据流量信息等。

第四十一条 应定期对网络设备配置信息进行安全检查，对发现的网络设备配置文件中存在的安全脆弱性进行及时的分析与修补，至少半年进行一次。

第四十二条 应定期对网络设备 IOS 版本信息进行检查，对低版本或存在安全漏洞的系统 IOS 版本进行安全分析和相应的更新，至少半年进行一次。

5.6.8、 网络接入管理

第四十三条 核心交换网络区域及关键网络区域应实现网络设备和链路冗余备份，并且定期进行冗余恢复测试，至少每年进行一次。

第四十四条 与其他有业务关联的科室有网络互联时应采取专用网络通道方式进行部署（专用物理通道或虚拟逻辑通道）。

第四十五条 远程用户通过互联网对内部网络资源的访问均应得

到授权和批准并通过 VPN 接入方式，以达到对传输的数据加密保护。

第四十六条 禁止非授权的便携式或移动式设备私自接入网络。

第四十七条 因工作需要需将便携式或移动式设备接入网络时，由接入申请者填写网络接入申请单，经过网络管理者及信息中心领导同意后，由网络管理员操作执行。接入操作前，网络管理人员应对即将接入的便携式或移动式设备进行安全检测评估，必要时进行恶意代码查杀。确认安全后方可接入网络。

5.6.9、 安全隔离与访问控制

第四十八条 内部网络与 Internet 互联网连接须通过防火墙等安全防护设备进行隔离与控制。

第四十九条 应在高安全网络区域边界部署安全防护设施（如防火墙），并根据业务访问需求进行访问控制，以实现网络访问服务最小化，（以严格控制其他区域对高安全网络区域数据的访问行为），防止非授权访问行为的发生。

5.6.10、 认证加密管理

第五十条 网络系统中应部署统一集中的用户身份认证策略，负责管理和维护整个网络系统的用户认证管理。

第五十一条 网络中，严格限制明文传输敏感信息（用户账号口令信息等），需要采用加密或其他手段进行有效控制，如：采取 SSH 安全登录方式代替明文的 telnet 登录方式，或者对 telnet 的登录方式进行严格控制。

5.6.11、 网络变更管理

第五十二条 网络变更包括：网络设备更换、网络线路调整、网络配置修改、网络系统升级等的所有网络变更行为。

第五十三条 网络变更都须经过申请，禁止在没有通过审批流程的情况下私自进行网络变更或网络结构调整。

第五十四条 针对网络设备的任何配置变更，都应在变更前和变更后做好配置文件的备份工作，并且制定详细可行的回退方案，以应对变更失败时的变更回退操作。

第五十五条 所有的网络变更操作都应记录，并且做好网络变更的记录保存工作。

5.6.12、 用户管理

第五十六条 网络设备系统的账户管理，包括用户账号的申请、注销及变更，必须按照相关流程执行。

5.6.13、 监控管理

第五十七条 网络中应部署网络监控系统，对整体网络设备运行实时有效的监控。

5.6.14、 备份与恢复管理

第五十八条 应对网络设备的重要数据（网络设备的配置文件和安全设备的安全策略配置文件等）定期进行备份，至少半年进行一次。

第五十九条 网络设备的备份策略要满足以下策略：

第六十条 配置文件的变更前变更后进行完全备份；

第六十一条 备份数据应进行独立安全存储；

第六十二条 备份数据存储时间至少两年以上。

第六十三条 应对网络设备配置文件进行定期的检查核对，保证备份文件数据的完整性和可用性。

5.6.15、 安全事件管理

第六十四条 网络系统应部署安全运维监控系统，对网络系统中所发生的网络安全事件进行监控和预警，定期对网络系统进行漏洞扫描，对发现的网络系统安全漏洞进行及时的修补。

第六十五条 对于日常发生的网络安全事件，应按照事件处理流程处理。

5.6.16、 无线网络安全管理

第六十六条 人员使用的无线 SSID 名称应设定为至少 8 位。

第六十七条 人员使用的无线网络禁止开启无线网络的 SSID 广播。

第六十八条 无线网络应采用 WPA 的加密级别或更高级别。

5.6.17、 网络安全风险评估

第六十九条 网络安全风险评估至少每年进行一次。

5.6.18、 网络设备安全配置管理

第一节 账户

第七十条 应按照用户分配账号。避免不同用户间共享账号。避

免用户账号和设备间通信使用的账号共享。

第七十一条 应删除与设备运行、维护等工作无关的账号。

第二节 口令

第七十二条 静态口令必须使用不可逆加密算法加密，以密文形式存放。设置满足密码复杂度要求的口令。口令策略的设置一般要求：

口令长度至少 8 位；

包含数字、小写字母、大写字母和特殊符号中的三类；

账户口令的生存期不长于 180 天；

不能重复使用最近 5 次（含 5 次）内已使用的口令。

第三节 认证

第七十三条 设备通过相关参数配置，与认证系统联动，满足账户、口令和授权的强制要求。

第四节 日志

第七十四条 网络管理员每天通过监控软件查看网络及网络安全设备日志中产生的错误或可疑项。如无法分析判断错误或可疑项，应提交至网络安全和信息化领导小组，以便安排进行分析处理，处理结果应补充记录到日志检查记录中。各类设备本地日志保留时间根据磁盘空间状况确定，清理重要本地日志前需进行备份。

第七十五条 网络设备及网络安全设备的日志应每个月进行一次全面的检查，参与日志检查的人员需签字确认。应至少每个月一次对网络设备和安全设备的日志进行分析，并形成分析报告，日志分析发现异常问题时应及时安排人员进行排查，并采取相应的管控措施。

第七十六条 在有技术手段支持的情况下，应定期进行日志的备份，要求如下：

（一）每天至少一次将网络设备及网络安全设备生成的日志，进行集中备份。可单独备份到光盘介质。

（二）日志备份需保留至少 6 个月不能被改变，日志的备份介质应存放在安全区域，防止非授权人员查看、拷贝日志资料，避免因为各种原因的损坏导致收集到的相关日志不可用。

（三）除审计人员外，由于工作的需要查看日志备份时，需要进行申请审批后才能查看。

（四）日志的失效:日志在通常情况下，保存 6 个月之后，可以由网络管理员进行失效处理。如果有设备对日志的保留要求超过 6 个月，则在超过日志保留有效期后再作失效处理。对于日志保存在介质中，需清空介质中数据后再做处理。

第五节 软件版本和补丁

第七十七条 设备的软件版本必须处于厂家维护期，如果厂家已不再进行补丁维护，需要及时更新设备版本或者撤换。

第七十八条 网络管理员应根据厂商发布的最新补丁公告进行安全分析，在测试环境中测试后，确定在不影响网络系统正常运行的情况下，对存在安全漏洞的设备进行补丁升级，且在安装补丁升级前后应做好设备配置的备份。

第七十九条 网络管理员应在厂商的指导下进行设备补丁升级。

第六节 IP 协议安全

第八十条 基本协议安全

（一）配置路由器，防止地址欺骗。

（二）路由器以 UDP/TCP 协议对外提供服务，供外部主机进行访问，如作为 NTP 服务器、TELNET 服务器、TFTP 服务器、FTP 服

务器、SSH 服务器等，应配置路由器，只允许特定主机访问。

（三）过滤已知攻击：在网络边界，设置安全访问控制，过滤掉已知安全攻击数据包，例如 udp 1434 端口（防止 SQL slammer 蠕虫）、tcp445，5800，5900（防止 Della 蠕虫）。

（四）功能禁用：

1）禁用 IP 源路由功能，除非特别需要。

2）禁用 PROXY ARP 功能，除非路由器端口工作在桥接模式。

3）禁用直播（IP DIRECTED BROADCAST）功能。

4）在非可信网段内禁用 IP 重定向功能。

5）在非可信网段内禁用 IP 掩码响应功能。

（五）在条件允许的情况下，启用协议的认证加密功能，保证通信安全。

第八十一条 路由协议安全

（一）在条件允许的情况下，启用动态 IGP（RIPV2、OSPF、ISIS 等）或 EGP 协议时，启用路由协议认证功能，如 MD5 加密，确保与可信方进行路由协议交互。

（二）在网络边界运行 IGP 或 EGP 动态路由协议时，配置路由更新策略，只接受合法的路由更新，防止非法路由注入。只发布所需的路由更新，防止路由信息泄漏。

第八十二条 SNMP 协议安全

（一）修改 SNMP 的 Community 默认通行字，通行字符串应符合口令强度要求。

（二）只与特定主机进行 SNMP 协议交互。

（三）应根据需要确定是否启用 SNMP 的写（WRITE）功能，

无特殊需要时禁用 SNMP 的写（WRITE）功能。

第七节 其他安全配置

第八十三条 关闭未使用的接口，如路由器的 AUX 口。

第八十四条 要修改路由缺省器缺省 BANNER，BANNER 最好不要有系统平台或地址等有碍安全的信息。

第八十五条 配置定时账户自动登出。如 TELNET、SSH、HTTP 等管理连接和 CONSOLE 口登录连接等。

第八十六条 配置 CONSOLE 口密码保护功能。

第八十七条 关闭不必要的网络服务或功能：

（一）禁用 TCP SMALL SERVERS；

（二）禁用 UDP SMALL SERVERS；

（三）禁用 Finger ；

（四）禁用 HTTP SERVER；

（五）禁用 BOOTP SERVER；

（六）关闭 DNS 查询功能，如要使用该功能，则显式配置 DNS SERVER。

第八节 配置备份和恢复

第八十八条 针对网络设备的配置备份由网络管理员负责，一般在配置完成后或者配置变更前后需要进行备份和记录。

第八十九条 备份所需介质的管理遵循相关安全要求。

第九十条 如需进行配置恢复，应由网络管理员审批后完成恢复并记录。

第九十一条 网络管理员每季度应进行备份记录、备份介质使用情况和恢复记录的整理统计。

第九节 安全配置维护和定期检查

第九十二条 配置变更前，需要进行审批、测试以及备份。

第九十三条 管理员每月至少一次进行网络设备安全配置的符合性检查，针对检查发现的问题进行处理。

第九十四条 在有技术手段支持的情况下，可使用漏洞扫描工具辅助进行符合性检查。

5.6.19、 防火墙安全配置管理

第一节 安全策略配置

第九十五条 防火墙在配置访问规则列表时，最后一条必须是拒绝一切流量。

第九十六条 在配置访问规则时，源地址，目的地址，服务或端口的范围必须以实际访问需求为前提，尽可能的缩小范围。

第九十七条 隐藏防火墙字符管理界面的 BANNER 信息。

第九十八条 防火墙设备必须关闭非必要服务。

第二节 攻击防护配置

第九十九条 配置访问控制规则，拒绝对防火墙保护的系统中常见漏洞所对应端口或者服务的访问。

第一百条 对于防火墙各逻辑接口配置开启防源地址欺骗功能。

第三节 软件版本和补丁

第一百零一条 设备的软件版本必须处于厂家维护期，如果厂家已不再进行补丁维护，需要及时更新设备版本或者撤换。

第一百零二条 网络管理员应根据厂商发布的补丁公告进行安全分析，确定在必要且不影响网络系统正常运行的情况下，对存在安全

漏洞的设备进行补丁升级。

第一百零三条 网络管理员应在厂商的指导下进行设备补丁升级。

第四节 告警配置

第一百零四条 配置告警功能：报告防火墙的软硬件故障报警，包括系统内部错误。

第五节 其他安全配置

第一百零五条 对于外网口地址，关闭对 ping 包的回应。建议通过 VPN 隧道获得内网地址，从内网口进行远程管理。（若网管系统需要开放，可不考虑）

第一百零六条 鉴于目前情况，使用 SNMP V2 版本对防火墙做远程管理。(在今后条件具备的情况下，建议升级到 SNMP V3 版本)，去除 SNMP 默认的共同体名称(Community Name)和用户名。并且不同的用户名和共同体名称对应不同的权限（只读或者读写）。

第一百零七条 对防火墙的管理地址做源地址限制。可以使用防火墙自身的限定功能，也可以在防火墙管理口的接入设备上设置 ACL。

第六节 配置备份和恢复

第一百零八条 针对防火墙的配置备份由网络管理员负责，应确保重要的防火墙配置变更前以及完成后进行备份和记录，每半年至少进行一次配置备份和记录。

第一百零九条 如需进行配置恢复，应由网络管理员审批后完成恢复并记录。

第七节 日志

第一百一十条 防火墙应配置日志功能：

（一）配置记录流量日志，记录通过防火墙的重要的网络连接的信息。

（二）配置防火墙规则，记录重要的防火墙拒绝和丢弃报文的日志。

（三）配置记录防火墙管理员操作日志，如管理员登录，修改管理员组操作，账户解锁等信息。

第一百一十一条 网络管理员通过监控软件接收网络及网络安全设备日志中产生的错误或可疑项的报警。接到报警后，如果无法分析判断错误或可疑项，应提交至网络与信息安全领导小组处，以便安排进行分析处理，处理结果应补充记录到日志检查记录中。各类设备本地日志保留时间根据磁盘空间状况确定，清理重要本地日志前需进行备份。

第一百一十二条 网络设备及网络安全设备的日志应每三个月进行一次全面的检查，参与日志检查的人员需签字确认。

第一百一十三条 在有技术手段支持的情况下，应定期进行日志的备份，要求如下：

（一）每月至少一次将网络设备及网络安全设备生成的日志，进行集中备份。可单独备份到光盘介质。

（二）日志备份需保留至少 6 个月不能被改变，日志的备份介质应存放在安全区域，防止非授权人员查看、拷贝日志资料，避免因为各种原因的损坏导致收集到的相关日志不可用。

（三）除审计人员外，由于工作的需要查看日志备份时，需要进行申请审批后才能查看。

（四）日志的失效:日志在通常情况下，保存 6 个月之后，可以由网络管理员进行失效处理。如果有设备对日志的保留要求超过 6 个月，则在超过日志保留有效期后再作失效处理。对于日志保存在介质中，需清空介质中数据后再做处理。

5.6.20、 VPN 安全配置管理

第一节 VPN 账户

第一百一十四条 在访问控制规则中设置不同级别的访问权限。

第一百一十五条 设置一个用户一次至多可以建立两个连接。

第一百一十六条 实现同一终端通过 VPN 连接后不能同时连接互联网。

第二节 访问控制策略

第一百一十七条 在配置访问规则时，必须以实际访问需求为前提，尽可能的缩小范围。可参考防火墙安全策略配置中的内容。

第三节 软件版本和补丁

第一百一十八条 设备的软件版本必须处于厂家维护期，如果厂家已不再进行补丁维护，需要及时更新设备版本或者撤换。

第一百一十九条 网络管理员应根据厂商发布的最新补丁公告进行安全分析，确定在不影响网络系统正常运行的情况下，对存在安全漏洞的设备进行补丁升级。

第一百二十条 网络管理员应在厂商的指导下进行设备补丁升级。

第四节 配置备份与恢复

第一百二十一条 针对 VPN 的配置备份由网络管理员负责，一般

在配置完成后或者配置变更前后需要进行备份和记录。

第一百二十二条 备份所需介质的管理遵循相关安全要求。

第一百二十三条 如需进行配置恢复，应由网络管理员审批后完成恢复并记录。

第一百二十四条 网络管理员每年应进行备份记录、备份介质使用情况和恢复记录的整理统计。

第五节 日志

第一百二十五条 应开启 VPN 连接日志记录功能，记录 VPN 访问登录、退出等信息。

第一百二十六条 网络管理员每天通过监控软件查看网络及网络安全设备日志中产生的错误或可疑项。如无法分析判断错误或可疑项，应提交至信息安全主管处，以便安排进行分析处理，处理结果应补充记录到日志检查记录中。各类设备本地日志保留时间根据磁盘空间状况确定，清理重要本地日志前需进行备份。

第一百二十七条 网络设备及网络安全设备的日志应每个月进行一次全面的检查，并形成记录。

第一百二十八条 在有技术手段支持的情况下应定期进行日志的备份，要求如下：

（一）每月至少一次将网络设备及网络安全设备生成的日志，进行集中备份。可单独备份到光盘介质。

（二）日志备份需保留至少 6 个月不能被改变，日志的备份介质应存放在安全区域，防止非授权人员查看、拷贝日志资料，避免因为各种原因的损坏导致收集到的相关日志不可用。

（三）除审计人员外，由于工作的需要查看日志备份时，需要进

行申请审批后才能查看。

（四）日志的失效:日志在通常情况下，保存 6 个月之后，可以由网络管理员进行失效处理。如果有设备对日志的保留要求超过 6 个月，则在超过日志保留有效期后再作失效处理。对于日志保存在介质中，需清空介质中数据后再做处理。

5.6.21、 附则

第一百二十九条 本制度的解释权归 XXX 单位。

第一百三十条 本制度自发布之日起开始执行

5.7、系统安全管理制度

5.7.1、 总则

第一条 为加强本单位信息系统安全管理，明确岗位职责，规范操作流程，维护系统正常运行，确保计算机信息系统的安全，特制订本制度。

第二条 本制度适用于本单位。

5.7.2、 系统安全策略

第一条 由系统管理员根据业务需求和系统安全分析制定系统的访问控制策略，控制分配信息系统、文件及服务的访问权限。

第二条 对系统管理员用户进行分类，明确各个角色的权限、责任和风险，权限设定遵循最小授权原则。

第三条 由系统管理员定期对系统安装安全补丁程序，在安装系统补丁前，首先在测试环境中测试通过，并采取磁盘或磁带对重要文件进行备份后，方可实施系统补丁程序的安装。

第四条 由安全管理员每月对系统进行一次漏洞扫描，对发现的系统安全漏洞及时进行修补；形成漏洞扫描报告，内容包含系统存在的漏洞、严重级别和结果处理等方面。

第五条 各终端工作计算机未进行安全配置、未装防火墙或杀毒软件的，不得入网。各计算机终端用户应定期对计算机系统、杀

毒软件等进行升级和更新，并定期进行病毒清查，不允许下载和使用未经测试和来历不明的软件、不要打开来历不明的电子邮件、以及不要随意使用带毒 U 盘等介质。

第六条　禁止未授权用户接入本单位网络及访问网络中的资源，禁止未授权用户使用 BT、电驴等占用大量带宽的下载工具。

第七条　任何员工不得制造或者故意输入、传播计算机病毒和其他有害数据，不得利用非法手段复制、截收、篡改计算机信息系统中的数据。

第八条　禁止利用扫描、监听、伪装等工具对网络和服务器进行恶意攻击，禁止非法侵入他人网络和服务器系统，禁止利用计算机和网络干扰他人正常工作的行为。

第九条　计算机各终端用户应保管好自己的用户帐号和密码。严禁随意向他人泄露、借用自己的帐号和密码；严禁不以真实身份登录系统。计算机使用者更应定期更改密码、使用复杂密码。

第十条　IP 地址为计算机网络的重要资源，计算机各终端用户应在系统管理员的规划下使用这些资源，不得擅自更改。另外，某些系统服务对网络产生影响，计算机各终端用户应在系统管理员的指导下使用，禁止随意开启计算机中的系统服务，保证计算机网络畅通运行。

第十一条　网络参数配置文档、重要计算机信息系统详细开发资料及其源程序等核心技术文档，由严格管理。

第十二条　系统核心技术文档资料的外借应有审批手续和记录，

借阅人不得转借给他人，不得复制、泄露和引用具体技术内容。

第十三条 安全配置

第十四条 系统安全配置由系统管理员、安全管理员负责，其余任何人不得随意更改配置。

第十五条 安全配置的更改应有记录，由安全审计员负责审计。

5.7.3、 日志管理

第一条 由系统运维人员依据操作手册对系统进行维护，详细记录操作日志，包括重要的日常操作、运行维护记录、参数的设置和修改等内容，严禁进行未经授权的操作。

第二条 由安全审计员定期对运行日志和审计结果进行分析，形成分析报告，报告内容包括帐户的连续多次登录失败、非工作时间的登录、访问受限系统或文件的失败尝试、系统错误等非正常事件。

5.7.4、 日常操作流程

第一条 各应用系统的操作流程由各应用系统开发厂商提供，经业务科室进行确认，各业务科室工作人员在日常工作中按照操作流程执行。

5.7.5、 附则

第一条 本制度的解释权归 XXX 单位。

第二条 本制度自发布之日起生效。

5.8、 恶意代码防范管理规定

5.8.1、 总则

第一条 为加强本单位网络与信息系统安全保护，避免遭受恶意代码攻击和病毒感染，特制订此规定。

第二条 本规定适用于本单位。

5.8.2、 恶意代码防范工作原则

第一条 禁止任何业务科室或员工以任何名义制造、传播、复制、收集恶意代码。

第二条 员工在使用计算机的任何时间内必须运行防病毒软件，进行定期得病毒检测和清除。未经许可，不得随意下载标准规定之外的防病毒软件或病毒监控程序。

第三条 在发布最新版本杀毒软件后，必须在规定期限内，将个人计算机的杀毒软件升级。

第四条 新购置的、借入的或维修返回的计算机，在使用前应当对硬盘认真进行恶意代码检查，确保无恶意代码之后才能投入正式使用。

第五条 软盘、光盘以及其它移动存储介质在使用前应进行病毒检测，严禁使用任何未经防病毒软件检测过的存储介质。

第六条 计算机软件以及从其它渠道获得的电脑文件，在安装或使用前应进行病毒检测，禁止安装或使用未经检测过的软件或带

毒软件。

5.8.3、 职责

第一条 运维工作小组应制定防恶意代码和病毒管理办法并对执行情况进行检查。

第二条 各业务科室安全管理员的职责：

（一）对于已经实施安全域管理的系统，要定期进行从相关技术支撑单位获得相关升级支持，根据策略强制所有用户进行病毒代码更新；

（二）对于尚未进行安全域管理的系统，要定期进行从相关技术支撑单位获得相关升级支持。要在第一时间以邮件方式、书面、短信等方式通知所有负责用户进行升级，收到通知的用户在登陆局域网的当天要按照要求进行病毒代码升级，完成后以邮件方式、书面、短信方式回复安全管理员。安全管理员根据实际情况进行抽查；

（三）及时跟踪解决对用户反映的病毒问题；

（四）及时跟踪防病毒软件的升级情况，并及时将升级的版本及相关措施公布；

（五）对用户上报的病毒追踪其根源，查找病毒传播者；

（六）对于不能立即解决得病毒问题，应及时组织协同相关的技术和业务人员进行跟踪解决，在问题解决前尽快采取相应措施阻止事件进一步扩大；

（七）对病毒的发作时间、发作现象、清除等信息进行维护、备

案、并制作案例；

（八）日常病毒信息的公告和发布；

（九）对本科室员工进行病毒防治的教育和培训；

（十）相关工作日志（发送和接受）的保存和归档。

5.8.4、 工作要求

第一条 各业务科室向外发布文件或软件时，应该用规定的防病毒软件检查这些该文件或软件，有病毒应及时清除，之后才能向外发布。

第二条 对邮件中的附件在使用之前应该进行病毒检测，收到来历不明的邮件不要打开并及时通知安全管理员处理。

第三条 如果发现本机感染了病毒，不管病毒从何处传播而来，都应该向安全管理员进行汇报，如果确认从别的机器传播而来的，还应该及时通知该机器的使用者，以便采取相应的防治措施。

第四条 任何个人不得私自发布计算机病毒疫情。如果发现防病毒软件不能清除的病毒，在问题处理之前，还应禁止使用感染该病毒的文件，同时断开网络连接。

第五条 应指定专人对网络和主机进行恶意代码检测并保存检测记录。

第六条 用户有义务接受有关部门组织的恶意代码防范、防治的教育和培训。

5.8.5、 附则

第一条 本规定的解释权归 XXX 单位。

第二条 本规定自发布之日起生效。

5.9、密码使用管理制度

5.9.1、 总则

第一条 为本单位信息系统帐号、口令管理，保障各系统安全运行，特制订此制度。

第二条 本制度适用于本单位。

5.9.2、 密码使用管理

第一条 员工应了解进行有效访问控制的责任，特别是密码使用和员工设备安全的责任。

第二条 员工应保证密码安全，不得向其他任何人泄漏。对于泄漏密码向造成的损失，由员工本人负责。

第三条 不要共享个人密码。

第四条 应避免在纸上记录密码，或以明文方式记录计算机内。

第五条 不要在任何自动登录程序中使用密码，如在宏或功能键中存储。

第六条 用户忘记密码时，管理员必须在对该用户进行适当的身份识别后才能向其提供临时密码。

第七条 常规情况下，用户至少每个季度更改一次密码，避免再次使用旧密码或循环使用旧密码。

第八条 允许用户选择和变更他们自己的密码，并且包括确认程

序，以便考虑到输入出错的情况；。

第九条 当正在录入时，在屏幕上不显示密码。

5.9.3、 密码使用要求

第一条 密码应由不少于 8 位的大小写字母、数字以及标点符号等字符组成。帐号口令必须是在必要时间或次数内不循环使用。

第二条 密码应在 90 天内至少更换一次，对重要设备和系统可采用一次性口令方式进行认证。

第三条 密码设置不得使用最近 5 次以内重复的口令；密码重复尝试 5 次以后应暂停该帐号登录。

第四条 各级密码保管落实到人，密码所有人须妥善保存，各级密码不得以任何形式明文存放于可公共访问的设备中。

第五条 采取有效措施，保证用户密码在传输和存储时的安全，例如对密码进行加密传输和保存。

第六条 以下情况时相关密码必须立即更改并做好记录：

（一）掌握密码的网络管理人员离开岗位；

（二）工程施工、厂商维护完成；

（三）因工作需要，由相关厂家或第三方单位使用了登陆帐号及密码后；

（四）一旦有迹象表明密码可能被泄露。

第七条 当发生以下情况时，系统或帐号管理人员应立即取消帐号或更改密码，并做好记录：

（一）帐号使用者已经离开；

（二）帐号使用者由于工作的变动不再需要访问权限；

（三）帐号使用者违背了有关密码管理规定；

（四）发生其他情况，由上级主管人员认为不应再具有访问权限的。

第八条　系统管理员修改帐号密码时，应提前（或同时）通知帐号使用人，以免影响其正常使用。

第九条　系统的超级管理员帐号的密码属于系统最高机密，应该严格限定使用范围；其他人员确因工作需要而使用超级管理员帐号和密码的，应遵守“帐号管理”中，有关超级管理员帐号的管理规定。

第十条　用户应对系统中的帐户密码进行定期检查核实，对不符合要求账户密码及时进行整改。

第十一条　第三方人员使用系统账号权限时，同样需要遵守“最小权限原则”。

5.9.4、 附则

第一条　本制度的解释权归 XXX 单位。

第二条　本制度自发布之日起生效。

5.10、 变更管理制度

5.10.1、 总则

第一条 为本单位信息系统变更管理流程，控制变更产生的影响，减少变更发生的问题，保障信息系统安全运行和使用，特制订此制度。

第二条 本制度适用于本单位。

5.10.2、 变更定义

第一条 员工应了解进行有效访问控制的责任，特别是密码使用和员工设备安全的责任。

第二条 变更是指对系统/平台需求的增补或修改，所做增补或修改可能会影响生产环境的稳定性。变更区域包括但不限于硬件、系统软件(OS)、应用软件、网络、环境(冷却、供热等等)以及服务文件(如服务等级协议)。变更又分为计划型变更和应急变更。

第三条 影响系统安全状态的变更如：

（一）新的版本或修订；

（二）作业系统执行状态的变化；

（三）作业系统调度变更；

（四）网络设备软件安装补丁、更新。

（五）增/减软件或补丁；

（六）软件修改或增强；

（七）操作系统升级；

（八）增加/移动/变更相关业务处室硬件配置，包括磁盘、磁带、CPU 等；

（九）硬件和网络设备变更。

第四条 对于有计划的变更申请需要进行审批，变更前应预留一定的时间通知变更有关各方，通知时限取决于变更的严重程度。

第五条 应急变更是为了改正生产环境下的某一个重要问题而必须立即实施的变更，应急变更也需要进行审批，但在紧急情况下可免去通知时间和正常的变更程序要求。

5.10.3、 变更过程

第一条 变更申请人填写变更申请表提交各业务科室领导审批，变更申请应在计划变更实施日期之前预留必要的准备时间。

第二条 变更申请表中需要描述以下内容：

（一）变更内容、变更原由、实施时间和期限、执行人以及联络方式；

（二）对相关业务科室/用户/系统/平台的影响；

（三）特殊的变更指示；

（四）变更前的准备工作；

（五）变更执行步骤；

（六）保证变更成功的测试方法；

（七）变更失败时应采取的倒回程序。

第三条 变更申请人将审批的变更申请表提交信息中心。

第四条 信息中心在变更计划执行日期前 2 天对提交的变更申请进行批复，通知申请科室，对于批准的变更申请予以存档。

第五条 变更实施前，执行人应通知相关业务科室的运行操作人员，以便变更进行时监控变更期内系统和服务的正常运。

第六条 如发现对服务有影响，维护人员应通知实施者，如果是因变更导致的影响，变更执行人应立即对问题进行调查，如问题严重，变更执行人应采取紧急恢复措施或倒回程序，和维护人员配合，务求恢复服务。

第七条 运行操作日志中应记录变更事件以备后查。

第八条 变更执行人在执行后要测试变更结果并验证执行的成功与否。如果结果表明不成功，变更执行人应采取回退措施将变更倒回到变更执行前的状态并进行测试，保证倒回成功。

第九条 变更程序开发完成后由实施方或协同各业务处室制订测试文档（包含测试用例）进行测试，并填写测试结果及签字确认。如未通过规定的测试，变更程序不得被移植入生产环境。变更程序的测试必须在独立于生产环境的测试环境中进行。

第十条 完成变更步骤后，变更执行人在离开现场前要通知各业务处室维护管理人员，进行验收程序。负责程序移植的人员需要进行移植情况的检查，留下书面的检查报告并签字确认。

第十一条 变更执行人需待运行维护人员确定一切检查妥当方可

以离开，确定变更成功。

第十二条 如果变更实施成功，申请人通知信息中心关闭变更申请并提供实际实施时间和结果。

第十三条 信息中心要确保相关业务科室的运行操作已更新所有的相关文件和记录。

第十四条 应急变更属于特殊的变更申请，可以因问题紧迫取得特别批准，一般需要在变更申请批准后 24 小时内实施完成。申请人应随后创建一份变更申请，并补充相应的测试及审批文档。

5.10.4、 失败变更的预防措施与回退流程

第一条 回退预防

防止变更失败带来不可挽救的危害，变更实施人员应做好变更前的预防工作，包括：

1)备份变更所涉及的存储过程、函数等其他数据对象；

2)备份配置数据；

3)备份在线生产平台接口、应用、工作流等版本；

4)充分考虑可能存在的失败变更，并针对性的编制各种失败变更回退方案。

第二条 回退准备

发生变更不可控问题时，需启动回退机制。在启动回退机制前，做好以下工作：

1)变更失败后分析失败原因，寻找解决措施，填写《系统变更失

败恢复程序确认单》，并提交给信息中心领导签字审批；

2)通知用户准备回退；

3)确定需要回退的关联系统和回退时间点；

4)准备存储过程等数据对象回退版本；

5)准备配置数据回退版本；

6)准备应用程序、接口程序、工作流等回退版本。

第三条 回退步骤

1)通知用户，系统开始回退；

2)通知各关联系统进行版本回退；

3)回退存储过程等数据对象；

4)应用程序、接口程序、工作流等版本回退；

5)回退完成通知各周边关联系统；

6)回退测试；

7)通知用户回退完成。

第四条 回退总结

对引起回退的原因做深入分析、总结经验，避免下次回退发生。

5.10.5、 变更过程职责

第一条 对信息系统和应用程序的变更都需根据信息中心下发的软件版本更新公文或填写规定格式的变更申请表单，由信息中心审批签字。表单应包含变更时间、申请人、变更原由、变更名称、实施时间和期限、影响分析、变更方案、审批意见、归档日期等

内容。

第二条 信息中心是变更管理的职能部门，主要职责为：

（一）审核变更申请的准确性；

（二）确认变更申请的记录信息的完整性；

（三）确保执行计划和变更失败倒回程序的质量；

（四）对变更申请予以批复；

（五）监督变更申请的执行情况；

（六）确保相关业务处室根据变化情况修订有关文件和记录。

第一条 各信息系统维护人员职责：

（一）监督变更期间生产系统/平台的正常服务情况；

（二）在变更申请超出限制或影响服务时，警告执行者采取恢复/倒回措施；

（三）确保倒回程序的实施足以恢复正常服务；

（四）根据情况的变化修订有关的文件和记录；

（五）监督变更期间的出错报告并在报告有意外服务影响时，通知执行人和相关业务处室。

第三条 变更执行人员职责：

（一）执行已获批准的变更申请；

（二）变更失败时执行倒回程序。

第四条 变更申请人职责：

（一）确保变更可执行；

（二）列出变更范围；

（三）提出变更申请；

（四）指出变更影响的区域和相关各方；

（五）编制变更执行计划；

（六）编制倒回程序；

（七）确保必要时变更影响的用户都能得到通知、授权及批准。

5.10.6、 附则

第一条 本制度的解释权归 XXX 单位。

第二条 本制度自发布之日起生效。

5.11、 信息安全授权和审批管理制度

第一条 为加强本单位对各授权和审批可以保证安全有关工作得到认可和控制，排除盲目性和不一致性，使安全工作更加权威和科学，保障应用系统的正常运行，特制订本制度。

第二条 如果授权和审批工作做得不够完善，可能会带来执行难等问题，安全工作得不到控制，因安全带来的问题长期得不到解决，安全问题日积月累，最终导致严重安全事件的发生。

第三条 应按照以下规范进行授权和审批流程建设： 明确审批授权事项、审批授权科室；建立系统变更、重要操作、物理访问和系统接入等事项的审批程序，重要活动实施逐级审批；按照审批程序执行审批过程，记入文档并进行审计； 定期审查审批事项，及时更新需授权和审批的项目、审批科室和审批人等信息。

第四条 其中涉及到信息系统方面的工作统一由负责。

第五条 信息系统管理授权的方式，其中信息系统的授权以职位说明书和授权书为基准，逐级授权，其他授权方式或越级授权视为无效。

第六条 信息系统管理授权程序，全面负责本单位信息系统的安装、运维、管理等工作。

第七条 各科室对信息系统只有根据其职级的使用权与建议权，而无修改权，否则造成的全部后果由当事人承担。

第八条 申请审批流程有申请人发起申请提交相关负责人审批同意后方可进行操作。

第九条 本制度的解释权归 XXX 单位。

第十条 本制度自发布之日起生效。

5.12、 信息系统数据备份与恢复管理制度

5.12.1、 总则

为规范本单位信息系统备份管理工作，合理存储历史信息及保证信息的安全性，防止因硬件故障、意外断电、病毒等因素造成数据的丢失，保障中心技术资料的储备，特制订本管理制度。

5.12.2、 备份方式

异地备份、主备、移动硬盘、光盘、U 盘等。

5.12.3、 制度内容

第一条 针对本单位信息系统确定需要定期备份的重要业务信息、系统数据及软件系统信息等。

第二条 为了确保系统信息系统的数据安全，使得在信息系统失效或数据丢失时，能依靠备份尽快地恢复系统和数据，保护关键应用数据的安全，保证数据不丢失，制定备份与恢复管理相关的安全管理制度，对备份信息的备份方式、备份频度、存储介质和保存期等进行规范；并制定信息数据恢复程序，定期检查恢复数据是否正常执行，确保信息数据能在规定时间内恢复。

第三条 拥有重要系统或重要数据的科室应该及时对数据进行备

份，防止系统数据的丢失；涉及数据备份和恢复的科室要由专人负责数据备份工作，并认真填写数据备份记录表；根据数据的重要性和数据对系统运行的影响，制定数据的备份策略和恢复策略，并对备份数据进行统一命名等规范管理。

第四条 信息系统数据备份的基本原则是“谁使用、谁备份”，即由信息使用者按要求及时备份相关信息数据。

第五条 信息系统数据的备份分为定期备份和临时备份。定期备份是指按照规定的时间定期对信息数据进行备份；临时备份是指在特殊情况下（如电脑中毒、软件升级、更换设备等）进行的应急备份。各科室可依据自身的工作特点选择不同的备份模式。

第六条 所有信息系统数据备份工作由各科室指定管理员进行详实记录，包括信息数据的备份和恢复流程所形成的文件和记录建立记录档案。备份的数据应该严格管理，妥善保存；备份数据资料保管地点应有防火、防热、防潮、防尘、防磁、防盗设施。

第七条 信息数据的备份、恢复、转出、转入的权限都应严格控制。严禁未经授权将数据备份出系统，转给无关的人员或单位；严禁未经授权进行数据恢复或转入操作。

第八条 一旦发生数据丢失或数据破坏等情况，要由系统管理员进行备份数据恢复，以免造成不必要的麻烦或更大的损失。

第九条 参照制造商使用说明书正确使用数据存储介质，避免暴露于强电磁场内、过热或过冷的环境。

第十条 数据存储介质的存放需根据存载信息数据的类型，采取不同的保管方式。

第十一条 加强移动存储介质管理，其中对内网移动存储介质的管理要按照业务特点进行严格的防护。

第十二条 所有的移动存储介质都必须进行登记造册和编号管理，可以随时确认移动存储介质的存放位置和责任人等信息。

第十三条 所有的移动存储介质必须进行清晰的标识，其维修或销毁必须按相关规定执行。

5.12.4、 备份

第十四条 应用、数据库系统备份管理

（一）所有业务平台的应用系统及数据库系统均应在本地机房保存备份，并且备份频率为每月一次。保留四个月的备份系统。

（二）所有业务平台的应用系统及数据库系统均应在光盘介质保存备份，存放在本单位电脑。备份频率为每季度一次，保留三年的备份系统。

（三）配置文件应在每次更改前后均保存备份。

第十五条 数据、配置文件备份管理

（一）所有业务及系统数据、配置文件必须存放于专业的存储阵列中，并在本地机房保存备份。备份频率为每月一次全量备份，每天

一次增量备份。保留四个月的备份数据。

（二）所有业务及系统数据、配置文件均应在移动介质中保存备份，存放在本单位保险柜。备份频率为每月一次。

（三）配置文件应在每次更改前后均保存备份。

第十六条 备份恢复管理

备份管理员应制定相应的备份恢复计划，包括由于业务需求发起的备份恢复以及测试性的恢复计划。计划中应遵循数据重要性等级分类，保证按照优先级对备份数据进行恢复。

需要恢复备份数据时，需求科室应填写《数据恢复申请表》，内容包括数据内容、恢复原因、恢复数据来源、计划恢复时间、恢复方案等，由需求科室以及信息中心相关负责人审批。

备份管理员需按照备份恢复计划制定详细的备份恢复操作手册，手册应包含备份恢复的操作步骤、恢复前的准备工作、恢复失败的处理方法和跟进步骤、验收标准等。

备份管理员应每个月对备份数据进行恢复测试工作，确保备份恢复工作能够按照备份恢复操作手册顺利进行，备份恢复测试应作明细的纪录，填写《备份恢复测试表》根据测试结果更新备份恢复操作步骤。

本单位应指派专人对《数据恢复申请表》、《备份恢复测试表》以及备份恢复的系统日志记录进行保存和归档，单位相关负责人应每半

年对上述文档进行审阅，确保备份恢复工作的合规性。

5.12.5、 附则

第十七条 本制度的解释权归 XXX 单位。

第十八条 本制度自发布之日起开始执行。

5.13、 安全事件报告和处置管理制度

5.13.1、 总则

第一条 为规范和加强本单位安全事件报告和处置管理，明确安全事件的现场处理、事件报告和后期恢复的管理职责，保障系统的安全稳定运行，特制订本制度。

第二条 本制度适用于本单位。

5.13.2、 安全事件定级

第一条 安全事件定义：信息安全事件是由于自然或者人为以及软硬件本身缺陷或故障的原因，对信息系统造成危害，或对社会造成负面影响的事件。

第二条 安全事件分类：本单位网络中的安全事件分为有害程序事件、网络攻击事件、信息破坏事件、信息内容安全事件、设备设施故障、灾害性事件及其他事件等。

（一）有害程序事件：包括计算机病毒事件、蠕虫事件、特洛伊木马事件、僵尸网络事件、混合程序攻击事件、网页内嵌恶意代码事件和其他有害程序事件；

（二）网络攻击事件：包括拒绝服务攻击事件、后门攻击事件、漏洞攻击事件、网络扫描窃听事件、网络钓鱼事件、干扰事件和其他网络攻击事件；

（三）信息破坏事件：包括信息篡改事件、信息假冒事件、信息

泄露事件、信息窃取事件、信息丢失事件和其他信息破坏事件；

（四）信息内容安全事件：包括通过网络传播法律法规禁止信息，组织非法串联、煽动集会游行或炒作敏感问题并危害国家安全、社会稳定和公众利益的事件；

（五）设备设施故障：包括软硬件自身故障、外围保障设施故障、人为破坏事故和其他设备设施故障；

（六）灾害性事件：包括由自然灾害等其他突发事件导致的网络与信息安全事件；

（七）其他事件：包括不能归为以上 6 个基本分类的信息安全事件。

第三条　安全事件分级

安全事件分级原则：根据信息系统中断的时间长短、影响范围，以及信息系统中的数据丢失或被窃取、篡改、假冒时对国家安全和社会稳定构成威胁的严重程度或者造成的经济损失来对安全事件进行等级划分。

根据以上原则，同时参照《信息安全技术信息安全事件分类分级指南》，将本单位网络中的安全事件分为四级：特别重大(I 级)、重大(II 级)、较大(III 级)、一般(IV 级)。

（一）特别重大安全事件 (I 级)

是指能够导致特别严重影响或破坏的信息安全事件，包括以下情况：使特别重要的信息系统遭受特别严重的系统损失（比如全国联网的业务应用系统中断服务 2 小时以上等）；产生特别重大社会影响。

（二）重大安全事件 (II 级)

是指能够导致严重影响或破坏的信息安全事件，包括以下情况：使特别重要的信息系统遭受严重的系统损失，或使重要的信息系统遭受特别严重的系统损失；产生重大的社会影响。

（三）较大安全事件 (III 级)

是指能够导致较严重影响或破坏的信息安全事件，包括以下情况：使特别重要的信息系统遭受较大的系统损失，或使重要的信息系统遭受严重的系统损失、一般信息系统遭受特别严重系统损失；产生较大的社会影响。

（四）一般安全事件（(IV 级)：

是指不满足以上条件的信息安全事件，包括以下情况：使特别重要的信息系统遭受较小的系统损失，或使重要的信息系统遭受较大的系统损失，一般信息系统遭受严重或严重以下级别的系统损失；产生一般的社会影响。

5.13.3、 安全事件报告和处置管理

第一条 网络与信息系统重大信息安全事件的报告和处置管理工作坚持“统一领导、归口负责”的原则。

第二条 发生信息安全事件的单位首先以口头方式立即向报告。同时应当立即对发生的事件进行调查核实、保存相关证据，并在事件被发现或应当被发现时起 5 小时内将有关材料报至网安部门。

第三条 对于重大的信息安全事件，接到报告后，应当立即上报本单位信息安全领导小组，并负责组织协调相关成员单位对事件进行调查和处理。

第四条 发生重大信息安全事件的单位应当在事件处理完毕后 5 个工作日内将处理结果报网安部门备案。

第五条 发生重大信息安全事件的单位应当按照规定及时如实地报告事件的有关信息，不得瞒报、缓报或者授意他人瞒报、缓报。

第六条 任何单位或个人发现有瞒报、缓报、谎报重大信息安全事件情况时，有权直接向本单位信息安全领导小组举报。

第七条 发生重大信息安全事件，有关责任单位、责任人有瞒报、缓报和漏报等失职情况，本单位信息安全领导小组将予以通报批评；对造成严重不良后果的，将视情节由有关主管部门追究责任领导和责任人的行政责任；构成犯罪的，由有关部门依法追究其法律责任。

第八条 恢复重建工作按照“谁主管谁负责，谁运行谁负责”的原则，由事发单位负责组织制定恢复、整改或重建方案，报相关主管部门审核实施。

5.13.4、 安全事件报告和处理程序

第一条 信息安全事件发生后，事发单位应立即启动相关安全事件报告和处理程序，实施处置并及时报送信息。

（一）事发单位先期处置，采取各种技术措施，及时控制事态发

展，最大限度地防止事件蔓延。

（二）快速判断事件性质和危害程度。尽快分析事件发生原因，根据网络与信息系统运行和承载业务情况，初步判断事件的影响、危害和可能波及的范围，提出应对措施建议。

（三）事发单位在先期处置的同时要按照预案要求，及时向上级主管部门报告事件信息。

（四）做好事件发生、发展、处置的记录和证据留存。

第二条　事件信息一般包括以下要素：事件发生时间、发生事故网络信息系统名称及运营使用管理单位、地点、原因、信息来源、事件类型及性质、危害和损失程度、影响单位及业务、事件发展趋势、采取的处置措施等。

第三条　I、II 级响应：本单位信息安全领导小组启动 I、II 级响应，统一指挥、协调、组织应急处置工作。

（一）启动指挥体系。本单位信息安全领导小组组织专家顾问组专家、人才库专家及专业技术人员研究对策，提出处置方案建议，为领导决策提供支撑。

（二）掌握事件动态。事件影响单位及时将事态发展变化情况和处置进展情况及时上报，本单位信息安全领导小组组织全面了解网络与信息系统运行情况，及时汇总有关情况并上报。

（三）处置实施。控制事态防止蔓延。现场处理组全力组织事发单位及应急队伍，采取各种技术措施、管理手段，最大限度地阻止和控制事态发展。

（四）做好处置消除隐患。现场指挥部组织专家、应急技术力量、事发单位尽快分析事件发生原因、特点、发展趋势，快速制定具体的解决方案，组织实施处置，对业务连续性要求高的受破坏网络与信息系统要及时组织恢复。

第四条 III 级响应：事件发生单位主管部门启动 III 级响应，按照相关预案进行事件处置，根据需要指导、检查、协助应急处置工作。

（一）启动指挥体系。组织相关专家指导现场处置。

（二）掌握事件动态。现场处理组及时了解事发单位主管范围内的信息系统是否受到事件的波及或影响，并将有关情况及时报本单位信息安全领导小组。

（三）处置实施。控制事态防止蔓延。现场处理组及时采取技术措施阻止事件蔓延；本单位信息安全领导小组向下（同）级单位发布预警信息，督促、指导相关运行单位有针对性地加强防范。

（四）尽快分析事件发生原因，并根据原因有针对性地采取措施，恢复受破坏信息系统正常运行。

第五条 IV 级响应：事件发生单位启动 IV 级响应，按照相关预案进行事件处置。

（一）启动指挥体系。事件发生单位负责同志及时赶赴现场，组织协调、指挥所属技术力量进行事件处置工作，必要时请求支援处置。

（二）掌握事件动态。事发单位负责将事件信息、处置进展情况及时向本单位信息安全领导小组报告。

（三）处置实施。根据需要，本单位信息安全领导小组有关人员及时赶赴现场，指导、检查事发单位开展事件处置工作，协调相关专家、技术队伍参加事件处置。

（四）尽快分析事件发生原因，并根据原因有针对性地采取措施，恢复受破坏信息系统正常运行。

5.13.5、 重要事件处理程序和报告程序

第一条 关键服务器受到黑客攻击时的处理程序和报告程序

(一) 当通过各类安全设备提示发现有黑客正在对关键服务器进行攻击并危及服务器系统的安全时，或发现网站页面、信息系统出现异常变动等被攻击的现象时，应立即向运行科技信息管理科负责人报告情况。并断开系统与外网的物理连接。

(二) 应急处理工作小组技术人员应立即赶到机房，首先要判断入侵的来源，定位入侵的 IP 地址、上网帐号等信息，及时关闭入侵的端口，限制入侵地 IP 地址的访问，如入侵来自于内网，应断开攻击来源区域的链路，并将情况上报给网络安全和信息化领导小组，由领导小组负责人根据事件严重程度上报上级单位相关部门。

(三) 现场处理人员负责检查检查网站、信息系统的程序与数据库系统被入侵的情况，查询安全设备审计记录，分析入侵手段，检测漏洞并针对入侵途径进行修补，如系统遭受破

坏须进行系统软件恢复。

(四) 应急处理工作小组妥善保存有关记录、日志或审计记录，以供上级网络安全相关部门审计分析。

(五) 网络安全工作组彻查入侵来源，分析事故成因，研究并采取杜绝类似事件的措施，以书面形式报告网络安全和信息化领导小组。

第二条 数据泄露事件应急处理流程。

数据泄露事件系统由于受到外部攻击或者内部人员故意泄密等原因，造成的数据泄露事件

(一) 当发现有数据泄露时，应报告信息安全应急指挥组，由信息安全应急指挥组组织协调人员进行检查，及时防止数据泄露范围扩大影响。

(二) 由应急响应日常运行部门组织协调人员排查系统及数据库、应用系统等相关日志，及时下线或切断相关业务系统外联网络，并保留证据，记录一切信息，必要时公安机关介入。

(三) 现场处理人员负责检查检查信息系统的程序与数据库系统等相关日志，查询安全设备审计记录，查看监控设备，分析数据泄露原因，及时下线或切断相关业务系统外联网络，如是外部入侵，应检测漏洞并针对入侵途径进行修补；如是内部人员故意泄露，应加强完善人员管理、信息安全意识管理、账户权限管理；保留证据，记录一切信息，必要时公安机关介入。

(四) 应急处理工作小组妥善保存有关记录、日志或审计记录，以供上级网络安全相关部门审计分析。

(五) 网络安全工作组彻查数据泄露原因，分析事故成因，研究并采取杜绝类似事件的措施，以书面形式报告网络安全和信息化领导小组。

第三条 信息系统遭破坏性攻击时的处理程序和报告程序

(一) 发现信息系统遭到破坏性攻击，应立即向科技信息管理科相关负责人报告，并在科技信息管理科相关人员的指导下断开相应服务器的网络连接，信息系统停止运行。

(二) 科技信息管理科技术人员在接到通知后，应立即赶到现场，并负责更换相应服务器的登录密码，并查看系统受破坏程度。

(三) 科技信息管理科相关人员负责使用相应设备软件对受破坏的虚拟机、程序或数据库进行恢复，并更换相应系统的访问密码。

(四) 网络安工作组通过审计安全设备日志追查攻击来源，研究并采取杜绝类似事件的措施，以书面形式报告网络安全和信息化领导小组。

第四条 服务器发生故障时的处理程序和报告程序

(一) 一旦服务器发生故障，应急处理工作小组人员应立即检查故障原因，并向应急响应先遣小组报告。

(二) 如果故障原因属于接触不良或参数丢失，按照相应操作规程进行处理。

(三) 若故障服务器为物理服务器，且自动切换失败，则应急处理工作小组在确认备份服务器工作正常的情况下，手动将业务切换至备份服务器，并切断故障服务器网络连接。切换完成后，需对故障服务器进行分析、处理，测试正常后再重新上线；若切换失败，分析切换失败原因的同时，立即尝试从原服务器恢复业务。

(四) 若故障服务器为虚拟化服务器，应立即将服务器回退至前一快照节点。

(五) 如果故障原因属于硬件损坏，在向备机切换完成后，立即与厂商联系，要求尽快提供。在备用服务器运行期间，应急处理工作小组应对损坏的部件尽快进行维修。

(六) 应急响应先遣小组分析故障原因，研究并采取防止类似故障的措施，以书面形式报告枢纽台协调小组。

第五条 外电中断后的处理程序和报告程序

(一) 外电中断后，应立即通知应急响应小组，若油机正常启动，应立即观察油机的运行情况，并执行步骤三。

(二) 若油机不能正常启动，应立即观察 UPS 的运行情况，并立即向应急响应先遣小组负责人报告。

(三) 应急响应小组应立即查明原因，如因内部线路故障，请物

业服务部门迅速恢复。

（四） 如果是供电局的原因，应立即与供电局联系，请供电局迅速恢复供电。

（五） 如果需长时间停电，应做如下安排：

1）预计停电 4 小时以内，由 UPS 供电；

2）预计停电 4－24 小时，关掉非关键设备，确保各主机、路由器、交换机等关键设备供电；

3）预计停电超过 24 小时，白天工作时间关键设备运行，晚上所有设备停机；

4）机房值班人员应密切关注电池能量消耗情况，应在电池能量消耗完之前联系小型发电机自行发电或关闭机房内所有设备。

5.13.6、 信息安全泄密事件应急处置预案

一、指导思想

结合本单位保密工作实际情况，建立和健全单位失泄密应急处置机制，提高对失泄密突发事件的应急处置能力，最大程度地预防和减少失泄密突发事件造成的损害，保障国家秘密的安全。

二、工作原则

1.预防为主、依法监管。坚持预防为主的方针，加强单位涉密文

件资料收发登记管理，规范生产、技术、等过程保密管理，防止失泄密突发事件的发生，确保信息安全保密、万无一失。

2.统一领导、分级负责。网络安全领导小组统一领导和组织全单位失泄密突发事件的应对工作。单位各部门负责本部门保密日常管理和突发失泄密事件的报告和控制扩散范围工作，认真执行网络安全领导小组有关应急处置的各项指示和应急事件的处理工作。

3.快速反应、及时报告。一旦发生失泄密突发事件，做到快速反应，早发现、早报告、早处置，积极采取有效措施，防止失泄密范围的扩大，将失泄密事件造成的影响控制在最小范围内。

三、适应范围

单位在涉密文件、涉密技术档案资料、涉密载体借阅、存放，及涉密计算机使用管理等方面出现的突发失密、泄密事件。

四、指挥及工作系统

网络安全领导小组，负责对单位发生的失泄密事件采取有效措施，将失泄密事件影响控制在最小范围。

五、应急处置措施

1、如发生涉密文件、涉密技术档案资料失密、泄密事件，立即上报本市保密局，并组织专门人员对保密室、资料室、个人办公桌等进行查找。严格控制人员出单位，责成门卫对进出单位大门人员的物品进行严格检查，防止涉密资料文件被偷运出单位。

2、如发生涉密 U 盘、移动硬盘及涉密光盘等涉密载体丢失事件，立即上报本市保密局，并组织专门人员对涉密载体使用、保管人员的

办公场所进行检查。同时，对出入本单位大门的物品进行严格检查，防止涉密载体被偷运出单位。

3、如发生涉密计算机因违规上互联网造成失泄密事件，立即上报本市保密局，并组织专人及时切断该机与互联网的连接，防止涉密信息的进一步扩散。将涉嫌发生失泄密的计算机保存在安全地方，派专人值守，防止涉密计算机硬盘被盗走或破坏，影响失泄密事件的取证、侦办、查处管理工作。

4、及时报告公安派出所，将查出的涉嫌失泄密事件的相关人员进行管控，防止其潜逃。

5、及时将失泄密事件的自查、协助调查和侦办情况报告当地保密局，积极配合相关部门的各项调查取证工作。

5.13.7、 附则

第一条 本制度的解释权归 XXX 单位。

第二条 本制度自发布之日起生效。

5.14、 应急预案管理制度

5.14.1、 总则

第一条 为科学应对本单位信息安全突发事件、建立健全信息安全应急响应机制，有效预防、及时控制和最大限度地消除信息安全各类突发事件的危害和影响，特制定本应急预案。

第二条 本制度适用于本单位。

5.14.2、 组织机构与职责

第一条 设立信息安全应急指挥（简称“应急指挥”），应急指挥主要成员由技术人员组成，主要职责是：

（一）承担值守应急工作；

（二）收集、分析工作信息，及时上报重要信息；

（三）负责本单位网络与信息安全的监测预警和风险评估控制、隐患排查整改工作；

（四）组织制订、修订网络与信息安全突发事件相关的应急预案；

（五）负责组织协调网络与信息安全突发事件应急演练；

（六）负责对本单位网络与信息安全突发事件的宣传教育与培训。

第二条 借助外部力量成立网络与信息安全专家顾问组，专家顾问组的职责：

（一）在网络与信息安全突发事件预防与应急处置时，提供咨询与建议，必要时参与值班；

（二）在制定网络与信息安全应急有关规定、预案、制度和项目建设的过程中提供参考意见；

（三）及时反映网络与信息安全应急工作中存在的问题与不足，并提出改进建议；

（四）对本单位网络与信息安全突发事件发生和发展趋势、处置措施、恢复方案等进行研究、评估，并提出相关建议；

（五）参与网络与信息安全突发事件应急培训及相关教材编审等工作。

5.14.3、 安全事件应急预案框架

第一条 应急指挥根据需要，应编制信息安全事件应急预案，以指导安全事件的处理机制和流程。

第二条 安全事件应急预案框架的内容：

（一）启动应急预案的条件。描述启动每个计划前应遵循的过程；

（二）应急处理流程。描述危及业务操作的事故发生之后所要采取行动的应急程序；

（三）描述将基本业务活动或支持服务移到替代的临时地方，并在要求的时段内使业务过程回到运行状态的动作的回退程序；

（四）恢复和复原未完成时应遵循的临时操作程序；

（五）描述恢复正常业务操作的动作的恢复程序；

（六）规定如何及何时要检验该计划的维护时间表，以及维护该计划的过程；

（七）教育和培训活动，用来创建理解业务连续性过程，确保过程持续有效；

（八）各个人的职责，描述谁负责执行计划的哪个部分。若需要，应指定可替换的人；

（九）实行紧急的、回退和恢复程序所需的关键资产和资源。

5.14.4、 信息系统应急预案故障分类

第一条 根据网络与信息安全突发事件可控性、严重程度和影响范围的不同，分为以下四级：

I 级（特别重大）：本单位网络与信息系统发生服务器不能正常工作、光纤损坏、主服务器数据丢失、备份硬盘损坏、服务器工作不稳定、核心数据库被人删除或修改等造成的网络或应用性瘫痪，对内部专网或对外业务正常工作造成特别严重损害，且事态发展超出本单位信息安全领导小组控制能力的安全事件；

II 级（重大）：本单位网络与信息系统发生大规模瘫痪，对内部专网或对外业务正常工作造成严重损害，事态发展超出本单位单一部门自身控制能力，需本单位各科室协同处置的安全事件；

III 级（较大）：本单位某一区域的网络与信息系统瘫痪，对内部专网或对外业务正常工作造成一定损害，但信息中心可自行处理的安全事件；

IV 级（一般）：某一局部网络或信息系统受到一定程度损坏，对内部专网或对外业务某些工作有一定影响，但不危及本单位整体工作的安全事件。

5.14.5、 应急响应程序与故障处置方法

第一条 系统故障应急预案

（一）当发生系统故障事件时，发现人应及时通知，同时根据情况及时上报本单位信息安全领导小组；

（二）领导组织安全管理员、系统管理员及网络管理员等相关单位和人员及时分析事件发生源头，切断事件源头，控制事件范围，必要时停止系统运行；

（三）安全管理员应及时查看安全审计日志对异常事件发生源头、发生原因、影响范围做出判断，并提出补救措施；

（四）系统管理员立即停止发生问题的应用系统，对异常事件内容和范围予以确认；

（五）针对事件原因查找系统漏洞，提出系统安全策略调整方案，并报审批，填写《应急处置审批表》；

（六）审批通过后根据系统安全策略调整方案，对安全设备、应用系统等的安全控制策略做出相应调整，确认无误后恢复系统运行；

（七）安全管理员详细填写《系统异常事件处理记录》，并上报。

第二条 故障处置方法

针对 I 级故障，由信息中心主管上报本单位领导，由本单位组织

协调恢复工作。

针对 II 级故障，由网络管理人员上报信息中心主管，由信息中心集中解决。

针对 III、IV 级故障，由网络管理员单独解决，并详细登记维护情况。这两类故障的处置要根据网络与信息安全事件分类采取不同应急处置方式。

网络攻击事件处置：

判断攻击的来源与性质，关闭影响安全与稳定的网络设 备和服务器设备，断开信息系统与攻击来源的网络物理连接， 跟踪并锁定攻击来源的 IP 地址或其它网络用户信息，修复被破坏的信息，恢复信息系统。根据具体情况选择以下处置方式：

病毒传播：及时寻找并断开传播源，判断病毒的类型、性质、可能的危害范围；为避免产生更大的损失，保护健康的计算机，必要时可关闭相应的端口，甚至相应楼层的网络，及时请有关技术人员协助，寻找并公布病毒攻击信息，以及杀毒、防御方法。

外部入侵：判断入侵的来源，区分外网与内网，评价入侵可能或已经造成的危害。对入侵未遂、未造成损害的，且评价威胁很小的外网入侵，定位入侵的 IP 地址，及时关闭入侵的端口，限制入侵的 IP 地址的访问。对于已经造成危害的，应立即采用断开网络连接的方法，避免造成更大损失和影响。

内部入侵：查清入侵来源，如 IP 地址、所在等信息，同时断开对应的交换机端口，针对入侵方法调整或更新入侵检测设备。对于无

法制止的多点入侵和造成损害的，应及时关闭被入侵的服务器或相应设备。

设备故障事件处置：

判断故障发生点和故障原因，迅速联系服务厂商尽快抢修故障设备，优先保证主干网络和主要应用系统的运转。

供电系统断电处置：

在通知供电系统进行检修的同时，随时观察注意 UPS 不间断电源的运行情况，停电时间接近 4 小时，必须停止服务器的运行。待电源恢复后，再按正常操作步骤恢复系统运行。

灾害性事件处置：

根据实际情况，在保障人身安全的前提下，保障数据安全和设备安全。具体方法包括：硬盘的拔出与保存，设备的断电与拆卸、搬迁等。

信息内容安全事件处置：

接到网站出现不良信息的报案后，应迅速屏蔽该网站的网络端口或拔掉网络连接线，阻止有害信息的传播，根据网站相关日志记录查找信息发布人并做好善后处理；对公安机关要求协查的外网不良信息事件，根据上网相关记录查找信息发布人。

其它不确定安全事件处置：

可根据总的安全原则，结合具体情况，做出相应处理。不能处理的及时咨询信息安全公司或顾问。

5.14.6、 信息系统应急预案的撤消与恢复

信息中心确认故障信息系统恢复正常。

确认网络流量和系统响应秩序恢复正常。

信息系统正常运行 10 分钟以上，信息通信管理处上报，由主管领导批准撤消“信息系统应急预案”。

在“信息系统应急预案” 撤消后 24 小时内，信息中心整理有关故障经过，填报《信息系统应急响应报告》，上报信息安全领导小组和领导，必要时上报。

5.14.7、 信息系统应急预案的善后

信息系统恢复正常，信息系统应急预案撤销后，信息系统预案应急小组还需要开展以下善后工作：

查找事件发生原因，总结经验教训；

如事件由人为引起，追究相关人员责任，如触犯法律，可直接报告公安机关处理；

如事件因为管理疏忽引起，除追究当事人责任之外，还需要追究相关主管领导责任；

根据事件危害程度，在部门范围内或本单位范围内就信息安全事件处理情况进行通报；

如有必要，在相关部门或本单位范围内开展教育培训，提高人员安全意识，杜绝类似事件发生。

5.14.8、 应急预案审查管理

第一条 应急指挥定期对应急预案进行审查，根据实际情况，如演练过程中出现的问题等对内容进行更新，以便更贴合本单位实际情况。

5.14.9、 应急预案培训

第一条 为确保应急预案有效运行，应急指挥应定期或不定期地举办不同层次、不同类型的培训班或研讨会，以便不同岗位的应急人员都能全面熟悉并掌握信息安全应急处理的知识和技能。

5.14.10、 应急预案演练

第一条 为提高信息安全突发事件应急响应水平，应急指挥应每年至少组织一次预案演练；检验应急预案各环节之间的通信、协调、指挥等是否符合快速、高效的要求。通过演练，进一步明确应急响应各岗位责任，对预案中存在的问题和不足及时补充和完善。

5.14.11、 应急预案定期评审制度

第一条 本单位负责预案评审活动。

第二条 安全员负责组织准备预案评审所需的资料，负责整改措施跟踪检查的组织和报告工作。

第三条 各科室负责组织、准备并提供于本科室有关的评审所需资

料，并负责落实评审提出的整改措施。

第四条 预案评审活动以召开“评审会议”的形式进行，参与会议的范围可包括本单位全体人员。

第五条 评审会议至少每半年召开一次；当本单位内部机构发生重大变化或者重大事故时，网络安全领导小组可决定临时召开预案评审会议。

第六条 预案评审的范围可涉及到本单位的所有网络安全作业活动或者其中部分活动。

第七条 预案评审的内容可包括：

1、应急救援预案的贯彻实施情况及其适宜性；

2、危险目标的数量及其分布情况；

3、指挥机构的设置和职责；

4、应急装备及通讯网络和联络方式；

5、应急网络安全队伍的任务和训练；

6、 预防事故的措施；

第八条 根据需要可以对其中的单项内容进行评审。

1、安全员负责收集预案评审资料，提出预案评审会议中需要解决的问题，报安全主管负责人审核。

2、根据议题需要，确定预案评审会议的议程、时间。

3、安全负责人主持预案评审会议，对评审内容作出评价，提出整

改措施或建议。

4、安全员负责预案评审会议的记录及评审报告的编制。

5、各科室接到评审报告后，实施与本科室有关的整改措施，视需要按规定修改有关文件。

6、安全员对整改措施实施情况进行检查验证。

7、由安全管理保存预案评审的有关记录。

5.14.12、 应急保障措施

第一条 技术支撑保障。建立预警与应急处理的技术平台，提高安全事件的发现和分析能力；从技术上逐步实现发现、预警、处置、通报等多个环节和不同的网络、系统、科室之间应急处理的联动机制。加强信息安全人才培养，强化信息安全宣传教育，提高信息安全防御意识。

第二条 应急队伍保障。加强人才培养，强化宣传教育，提高安全防御意识，努力建设一支高素质、高技术的网络与信息安全核心技术人才和管理队伍。

第三条 物质条件保障。安排一定的资金用于预防或应对网络与信息安全突发事件，提供必要的硬件设备与软件工具，为应急处理工作提供可靠的物资保障。将本年度信息安全应急响应经费纳入年度财政计划和预算，建立专项资金用于信息安全事件的处置，购买相应的应急设施，避免时间拖延造成不必要的损失，保证应

急响应队伍技术装备的及时更新，以确保应急响应工作的顺利进行。

第四条 技术储备保障。要经常性组织相关技术人员进行培训，在允许的条件下，还可以邀请专家和科研力量，开展应急运作机制、应急处理技术等研究。建立预警与应急处理的技术平台，进一步提高信息安全事件的发现和分析能力。从技术上逐步实现发现、预警、处置、通报等多个环节和不同的网络、系统、科室之间应急处理的联动机制。

5.14.13、 附则

第九条 本制度的解释权归 XXX 单位。

第十条 本制度自发布之日起生效。

第六章 其他管理制度

6.1、安全设备运行维护规范

6.1.1、 总则

第一条 为统一本单位管理人员对本单位信息系统中安全设备的运行维护规范, 特制定本规范。

第二条 本规范适用于本单位。

6.1.2、 适用产品范围

第一条 本单位信息系统中的所有相关安全设备实施必须执行本规定，包括：

（一）安全防护类产品，如 UTM、防火墙等；

（二）恶意代码防护类产品，如防病毒软件；

（三）监测审计类产品，如 IDS、网络通讯协议分析系统等；

6.1.3、 安全策略配置规范

第一条 安全设备部署规范

（一）安全防护类产品：本单位所有局域网内的出网连接必须通过安全防护类产品进行防护。安全防护类产品至少部署在以下几个方面：

1. 互联网接入区；

2. 广域网接入区；

3. 内部各个区域边界与核心交换机之间。

（二）恶意代码防护类产品:对本单位的整体网络建立有效的、多层次的恶意代码防护体系，恶意代码防护类产品应分别部署到网关、邮件服务器、应用服务器以及客户端，并采用集中管理的方式。

（三）监测审计类产品：本单位信息系统中的重点服务器网段都应部署监测审计类产品。

第二条 安全设备策略配置规范

（一） 安全防护类产品策略配置规范如下：

1. 默认状态下拒绝通信：对于未明确允许的连接路径和互联网服务，必须通过安全防护类产品锁死，所有可允许通过的服务必须得到的批准并备案；

2. 所有访问本单位网络的入站通信（除普通互联网用户外）必须通过统一部署的 VPN 网关进行加密；

3. 对所有的重要网段进行子网的划分；

4. 互联网出口安全防护产品必须使用网络地址转换功能，各区域间的安全防护产品采用网桥的方式透明接入网络中，并启用访问控制功能；

5. 除普通的互联网用户外，对外服务系统应当使用动态口令或数字证书对用户进行认证；

6. 对所配策略应做出相应的注释，标明该策略的作用范围；对于临时的配置变更策略，应在《安全设备配置变更申请表》中注明

该策略生效时间，系统管理员配置临时策略时应对其添加时间限制策略。

（二）恶意代码防护类产品策略配置规范如下：

1. 设定每日进行预约更新；

2. 每日自动检测客户端的恶意代码定义文件是否都已经更新到最新版本；

3. 透过管理主控台，每周对各产品是否都已正常更新到新版的病毒定义状态进行检查；

4. 每周检查防病毒控制端软件的扫描记录文件；

5. 每两周对 PC 进行一次扫描；

6. 每月对服务器执行全面扫描，应当生成月报表记录。

（三）监测审计类产品策略配置规范如下：

1. 监测审计类产品监控范围应当包括重要应用服务器、各级网络设备等；

2. 监控策略配置为全策略，并不断优化。

6.1.4、 安全运维规范

第一条 报告及日志管理规范

（一）安全防护类产品报告及日志管理规范：

1. 对于安全防护类产品的配置参数、已启用服务和允许的连接等任何变化以及意外情况的处理，必须予以记录。另外，所有违背安全策略的可疑行为也必须予以记录；

2. 至少保留六个月日志，并保证日志的完整性；

3. 每月生成一次安全防护类产品运行状况的报告。

（二）恶意代码防护类产品报告及日志管理规范：

1. 基于不同应用层次和操作系统上的恶意代码防护类产品必须进行实时监控，建立系统内部完整的层次化更新体系，收集和汇总网络范围内的病毒事件，并可以通过单一节点进行恶意代码防护类产品的日常管理。对于防病毒软件配置参数、部署情况的任何变化以及意外情况的处理，应当予以记录。

2. 至少保留六个月日志，并保证日志的完整性；

3. 当恶意代码防护类产品运行发生问题时，系统管理员应进行记录，并向安全管理员提交报告。

（三）监测审计类产品报告及日志管理规范：

1. 对于配置参数、部署情况的任何变化以及意外情况的处理，必须予以记录。另外，所有违背安全策略的可疑行为也必须予以记录；

2. 至少保留六个月日志，并保证日志的完整性；

3. 每月生成一次监测审计类产品运行状况的报告。

第二条 安全产品备份管理规范

（一）应当每日对安全产品日志进行自动增量备份；

（二）至少每个月对安全产品日志、配置文件、报告等进行全备份；

（三）当配置发生变化或遇紧急事件的前后必须对这些数据进行全备份。

第三条　定期审查规范

（一）安全防护类产品定期审查规范：

1. 必须每个月对安全防护类产品进行审查。审查内容至少必须包括对配置参数、启用的服务、允许的连接、日志以及安全措施是否充分等问题的考虑；

2. 必须每月使用漏洞扫描软件对安全防护类产品进行一次安全评估；

3. 审查必须由系统管理员或熟练的专业技术人员进行。

（二）恶意代码防护类产品定期审查规范

1. 必须每周对恶意代码防护类产品的更新、病毒爆发事件、病毒清除等情况进行审查；

2. 必须每个月对恶意代码防护类产品的部署、策略管理、日志以及安全措施是否充分等进行审查；

3. 审查必须由系统管理员或熟练的专业技术人员进行。

（三）监测审计类产品定期审查规范

1. 必须每个月对监测审计类产品进行审查。审查内容至少必须包括对配置参数、日志以及安全措施是否充分等问题的考虑；

2. 审查必须由系统管理员或熟练的专业技术人员进行。

第四条　日常维护规范

（一）必须每周监控安全产品的运行状态；

（二）安全产品的升级必须得到的书面批准，升级前必须对系统的变更进行测试。

第五条 配置变更管理规范

（一） 当应用系统、网络系统出现变更需对安全设备的配置进行变更时，变更申请人应填写《安全设备配置变更申请表》，说明变更原因，系统管理员负责实施安全设备的配置变更操作，配置变更后应进行至少 3 小时的监控，若变更未达到预期效果，应向安全管理员反馈，并进行相关处理。

（二） 系统管理员应填写《安全设备配置变更记录表》，及时备份安全设备的最新配置信息，并妥善保存。

6.1.5、 附则

第一条 本规定的解释权归 XXX 单位。

第二条 本规定自发布之日起生效。

6.2、运维外包安全管理规范

6.2.1、 总则

第一条 为规范本单位运维工作，降低因运维外包管理不善造成的系统服务中断、信息泄露等安全风险，保障公司业务数据安全、系统稳定运行，特制定本规范。

第二条 本规范适用于本单位网络设备、业务平台、运维平台等的运维外包工作。

6.2.2、 组织与资质要求

第三条 信息中心、业务科室负责提出对基础网络、信息系统的运维服务需求，信息中心负责相关运维外包工作的组织和实施，包括：运维体系建设、运维资产管理、运维经费预算编报、运维外包项目招标、运维合同管理及绩效评估。

第四条 在选择承担运维安全服务工作的外包服务单位时，应选择获得网络安全服务能力或信息安全服务能力评估证书的单位。

6.2.3、 运维外包安全管理

第五条 运维外包需求科室应加强信息系统建设转运维阶段的安全风险管理，应按《软件开发管理制度》、《信息系统建设管理制度》等有关规定执行项目验收，未经验收通过的重要系统不得投入正式运行。

第六条 运维外包团队在实行运维过程中，对重大信息安全事件

的处置应按本单位《信息系统安全事件报告和处置管理制度》等文件执行。

第七条 信息中心应督促运维外包团队建立运行监控管理机制，动态掌握网络及信息系统的运行状况，针对可能出现的重大故障和灾难，制定相关应急预案，定期组织各相关方进行应急演练，并对各种异常情况做出快速响应。

第八条 引入运维安全管理类设备（如堡垒机），加强对运维外包人员运维过程的管理，对运维工程师运维操作情况进行有效规范、记录，确保对运维工程师的操作“有迹可寻”。

第九条 运维外包人员在进行重要操作、敏感信息访问（如数据库参数配置等）时必须出具书面告知书，经双方签字确认后方可进行操作，告知书中应包括操作内容、涉及信息系统、预计完成时间、可能出现的风险及风险等级预估，针对预估等级较高的风险应充分预估发生机率、影响范围等内容，拟定应急措施，确保及时解决。

第十条 认真执行安全事件惩罚机制，签订信息安全保密协议，加大对运维商运维过程中发生事故的处罚力度，提高运维商在出现事故后的处理成本，能够促使运维商主动加强对其人员的管理，减少信息系统运维安全事故的发生机率。

第十一条 运维外包人员对信息系统进行升级后，及时聘请拥有安全评估资质的第三方进行应用系统安全评估，评估后出具有效的评估报告，依据评估结果要求运维商进行整改，直至所有问题被解决。

第十二条 定期对网络设备、服务器操作系统等进行漏洞扫描，有效防止系统被植入病毒或预留后门，针对新发现的漏洞及时联系运维商进行处理，确保信息系统安全运行。

6.2.4、 运维外包人员管理

第十三条 对采用运维外包的工作，应要求外包服务企业加强对服务人员的甄选和培训，并对外包服务人员进行履历备案、身份验证、职业技能鉴定、背景调查等，关键岗位服务人员应进行政审并签署保密协议，实行权限管理，防止其擅自对本单位提供的任何文件进行修改、复制或带离现场。

第十四条 加强外包人员变更的管理。要求外包服务企业在合同期内保持主要负责人员的稳定。确需更换的，应由外包企业提供说明材料，提前一个月以书面形式向甲方单位提出人员变更申请，说明人员的离职原因、离职人员的安全保密措施、变更人员资质及身份证明材料等。离职人员应做好外包项目未尽任务和工作移交，经甲方单位同意后方可离开服务现场。

第十五条 加强外包人员现场管理，规范外包服务人员的在岗、离岗行为。外包人员需要离开服务岗位的，应事先征得甲方单位同意，重大项目主要负责人员离开岗位，应由其所在企业提供包含原因、返回现场时间、离岗期间工作安排等内容的书面材料，在取得甲方单位和有关部门同意后方可离开服务现场，未经允许不得擅自离岗。

6.2.5、 运维外包与合同管理

第十六条 在制定运维外包计划时，应：

(一) 明确外包范围，做好资产核查，对基础设施、信息系统、管理服务等进行整合，形成集约化运维项目。

(二) 针对外包的运维项目，分解并定义运维工作内容和质量要求，作为外包企业服务质量考核的依据。

第十七条 在选择运维外包企业时，应综合评估运维服务企业的商业信誉、相应的服务安全等级资质、技术能力、管理能力、相关运维项目经验、财务状况和责任承担能力等。涉密系统外包应遵守相关法规和政策，并报行业主管部门备案。

第十八条 本单位应同外包企业签订运维服务合同。合同内容应包括委托运维的资产、甲乙双方职责、服务内容和服务质量考核标准、安全保密要求、违约责任、知识产权归属、绩效考核要求和费用支付等条款。其中：

(一) 重要运维服务内容以及需要第三方服务的事项应在合同中明确约定。

(二) 运维服务价格和服务质量根据项目情况和行业特点，在合同中具体细化和量化。

(三) 运维合同周期根据运维工作实际需求确定，并逐年落实到年度运维预算中。

第十九条 与外包企业建立有效的信息交流机制，及时发现外包服务中可能出现的重大缺失，尤其需要考虑外包企业的重大资源损失、重大财务损失和重要人员变动，以及外包协议的意外终止，保证外包服务不间断。

第二十条 应建立服务质量管理流程，定期审核和修订服务水平协议，对运维外包企业的服务质量进行评估。

第二十一条 应分别对本单位和运维外包企业的运维工作进行绩效评估，其中，针对运维外包企业的绩效评估，应依据运维外包合同及相关服务质量评估标准设计运维绩效评估指标，绩效评估工作在年度中期和末期分别进行，绩效评估工作应有业务科室参与。

6.2.6、 附则

第二十二条 本规定的解释权归 XXX 单位。

第二十三条 本制度自发布之日起执行

XXX 单位

（信息安全领导小组）

2022 年 10 月 20 日