**XXX单位**

**信息安全工作总体方针**

V1.0

目录

[1 总则 1](#_Toc479441312)

[1.1 目标 1](#_Toc479441313)

[1.2 适用范围 1](#_Toc479441314)

[1.3 建设思路 1](#_Toc479441315)

[1.4 建设原则 3](#_Toc479441316)

[1.5 建设目标 5](#_Toc479441317)

[2 体系框架 5](#_Toc479441318)

[2.1 安全模型 6](#_Toc479441319)

[2.2 体系框架 7](#_Toc479441320)

[3 建设内容 13](#_Toc479441321)

[3.1 组织机构 13](#_Toc479441322)

[3.2 人员管理 13](#_Toc479441323)

[3.3 物理管理 14](#_Toc479441324)

[3.4 网络管理 14](#_Toc479441325)

[3.5 系统管理 14](#_Toc479441326)

[3.6 应用管理 14](#_Toc479441327)

[3.7 数据管理 15](#_Toc479441328)

[3.8 运维管理 15](#_Toc479441329)

[4 总体安全策略 15](#_Toc479441330)

[4.1 物理安全策略 16](#_Toc479441331)

[4.2 网络安全策略 16](#_Toc479441332)

[4.3 主机安全策略 17](#_Toc479441333)

[4.4 应用安全策略 18](#_Toc479441334)

[4.5 数据安全策略 18](#_Toc479441335)

[4.6 病毒管理策略 19](#_Toc479441336)

[5 附则 20](#_Toc479441337)

# 总则

为加强和规范XXX单位信息系统安全工作，提高信息系统整体安全防护水平，实现信息安全的可控、能控、在控，依据国家有关法律、法规的要求，制定本文档。

## 目标

本文档的目的是为XXX单位信息系统安全管理提供一个总体安全架构文件，该文件将指导信息系统的安全管理体系的建立。安全管理体系的建立是为信息系统的安全管理工作提供参照，以实现统一的安全策略管理，提高整体的网络与信息安全水平，确保安全控制措施落实到位，保障网络通信畅通和业务系统的正常运营。

## 适用范围

本文档适用于信息系统安全方案规划、安全建设实施和安全策略的制定。

## 建设思路

XXX单位信息安全建设工作的总体思路如下图所示：



信息化建设是基于当前通用的网络与信息系统基础技术，针对安全性问题和支撑安全技术，通过安全评估，对信息化建设和信息安全建设进行分析和总结，其中包括对建设现状和发展趋势的完整分析，归纳出系统中当前存在和今后可能存在的安全问题，明确网络和信息系统运营所面临的安全风险级别。

从支撑性安全技术展开，对现有网络和信息技术的固有缺陷出发，总结了普遍存在的安全威胁，并根据其它系统中的信息安全建设实践中的经验，从信息安全领域的完整框架、思路、技术和理念出发，提供完整的安全建设思路和方法。

在此基础之上，对信息安全领域的理论、框架和技术基础与XXX单位的安全问题有机地进行结合，有针对性地提出XXX单位安全保障总体策略。安全保障总体策略包括了整体建设目标，安全技术策略，以及相应的管理策略。

以安全保障总体策略为核心，分三个方面进行整体信息安全体系框架的制定，包括安全技术体系，安全管理体系和运营保障体系。在现实的运营过程中，安全保障不能够纯粹依靠安全技术来解决，更需要适当的安全管理，相互结合来提高整体安全性效果。

在信息安全体系框架的指导下，依据相应的建设标准和管理规范，规划和制定详细的信息安全系统实施方案和运营维护计划。

信息安全体系建设的思路体现了以下的特点：

* 统筹规划和设计在建设过程中占有非常重要的地位；
* 充分结合建设现状与信息安全通用技术和理念；
* 充分考虑了当前的建设现状以及未来业务发展的需要；
* 注重安全管理体系的建设，以及管理、技术和保障的相互结合。

## 建设原则

信息系统安全坚持“安全第一、预防为主，管理和技术并重，综合防范”的总体方针，实现信息系统安全可控、能控、在控。依照“分区、分级、分域”总体安全防护策略，执行信息系统安全等级保护制度。

信息安全体系的建设，涉及面广、工作量大，必须坚持以下的原则，保证建设和运营的效果。

* **统一规划**

要对的信息安全体系建设进行统一的规划，制定信息安全体系框架，明确保障体系中所包含的内容。同时，还要制定统一的信息安全建设标准和管理规范，使得信息安全体系建设能够遵循一致的标准，管理能够遵循一致的规范。

* **分步有序实施**

信息安全体系的建设，内容庞杂，必须坚持分步骤的有序实施原则，循序渐进地进行。

* **基于安全需求**

依据信息系统担负的使命，积累的信息资产的重要性以及可能受到的威胁及面临的风险分析安全需求，按照信息系统等级保护要求确定相应的信息系统安全保护等级，遵从相应等级的规范要求，从全局上恰当地平衡安全投入与效果。

* **技术管理并重**

仅有全面的安全技术和机制是远远不够的，安全管理也具有同样的重要性，XXX单位信息安全体系的建设，必须遵循安全技术和安全管理并重的原则。制定统一的安全建设管理规范，指导的安全管理工作。

* **突出安全保障**

信息安全体系建设要突出安全保障的重要性，通过数据备份、冗余设计、应急响应、安全审计、灾难恢复等安全保障机制，保障业务的持续性和数据的安全性。

* **持续改进**

信息系统安全管理是一种动态反馈过程，贯穿整个安全管理的生存周期，随着安全需求和系统脆弱性的时空分布变化，威胁程度的提高，系统环境的变化以及对系统安全认识的深化等，应及时地将现有的安全策略、风险接受程度和保护措施进行复查、修改、调整以至提升安全管理等级，维护和持续改进信息安全管理体系的有效性。

* **依法管理**

信息安全管理工作主要体现为管理行为，应保证信息系统安全管理主体合法、管理行为合法、管理内容合法、管理程序合法。对安全事件的处理，应由授权者适时发布准确一致的有关信息，避免带来不良的社会影响。

* **自保护和国家监管结合**

对信息系统安全实行自保护和国家保护相结合。组织机构要对自己的信息系统安全保护负责，政府相关部门有责任对信息系统的安全进行指导、监督和检查，形成自管、自查、自评和国家监管相结合的管理模式，提高信息系统的安全保护能力和水平，保障国家信息安全。

## 建设目标

根据XXX单位信息安全体系建设需求和原则，XXX单位信息安全的建设目标，可以用“一个目标、两种手段、三个体系”进行概括。

* **一个目标**

XXX单位信息安全的建设目标是：基于安全基础设施、以安全策略为指导，提供全面的安全服务内容，覆盖从物理、网络、系统、直至数据和应用平台各个层面，以及保护、检测、响应、恢复等各个环节，构建全面、完整、高效的信息安全体系，从而提高XXX单位信息系统的整体安全等级，为XXX单位的业务发展提供坚实的信息安全保障。

* **两种手段**

信息安全体系的建设应该包括安全技术与安全管理两种手段，其中安全技术手段是安全保障的基础，安全管理手段是安全技术手段真正发挥效益的关键，管理措施的正确实施同时需要有技术手段来监管和验证，两者相辅相成，缺一不可。

* **三个体系**

XXX单位信息安全体系的建设最终形成3个主要体系，具体包括安全技术体系、安全管理体系、以及运行保障体系。

# 体系框架

XXX单位进行信息安全建设的目标是建立起一个全面、有效的信息安全体系，在这个体系中，包括了安全技术、安全管理、人员组织、教育培训、资金投入等关键因素，信息安全建设的内容多，规模大，必须进行全面的统筹规划，明确信息安全建设的工作内容、技术标准、组织机构、管理规范、人员岗位配备、实施步骤、资金投入，才能够保证信息安全建设有序可控地进行，才能够使得信息安全体系发挥最优的保障效果。

## 安全模型

根据XXX单位信息安全体系建设目标和总体安全策略，建立了与之对应的目标模型，称为WP2DRR安全模型，该模型是基于时间的，由预警（Warning）、策略（Policy）、保护（Protection）、检测（Detection）、响应（Response）、恢复（Recovery）六个要素环节构成了一个完整的、动态的信息安全体系。预警、保护、检测、响应、恢复等环节都由技术内容和管理内容所构成。



* Policy(安全策略)：根据风险分析和评估产生的安全策略描述了系统中哪些资源要得到保护，以及如何实现对它们的保护等。在WP2DRR安全模型中，策略处于核心地位，所有的防护、检测、响应、恢复都依据安全策略展开实施，安全策略为安全管理提供管理方向和支持手段。
* Warining（预警）：根据以前所掌握的系统的弱点和当前了解的犯罪趋势预测未来可能受到的攻击和及危害。包括风险分析、病毒预报、黑客入侵趋势预报和情况通报、系统弱点报告和补丁到位。
* Protection（防护）：通过修复系统漏洞、正确设计开发和安装安全系统来预防安全事件的发生；通过定期检查来发现可能存在的系统弱点；通过教育等手段，使用户和操作员正确使用系统，防止意外威胁；通过访问控制、监控等手段来防止恶意威胁。
* Detection（检测）：检测是非常重要的一个环节，检测是动态响应和加强防护的依据，它也是强制落实安全策略的有力工具，通过检测和监控网络和信息系统，发现新的威胁和弱点，通过循环反馈来及时做出有效的响应。
* Response（响应）：响应是对安全事件做出反应，包括对检测到的系统异常或者攻击行为做出响应动作，以及处理突发的安全事件。恰当的响应动作和响应流程可以降低安全事件的不良影响，加强对重要资源的保护。
* Recovery（恢复）：灾难恢复能力直接决定了业务应用的持续可用性，任何意外的突发事件都可能造成服务中断和数据受损，优秀的灾难恢复计划能够针对灾难事件做到未雨绸缪，即使系统和数据遭受破坏，也能够在最短的时间内，完成恢复操作。

WP2DRR安全模型的特点就是动态性和基于时间的特性。它阐述了这样一个结论：安全的目标实际上就是尽可能地增大保护时间，尽量减少检测时间和响应时间。

WP2DRR模型是在传统的P2DR模型的基础上新增加了预警Warning和恢复Recover，增强了安全保障体系的事前预防和事后恢复能力，一旦系统安全事故发生了，也能恢复系统功能和数据，恢复系统的正常运行。

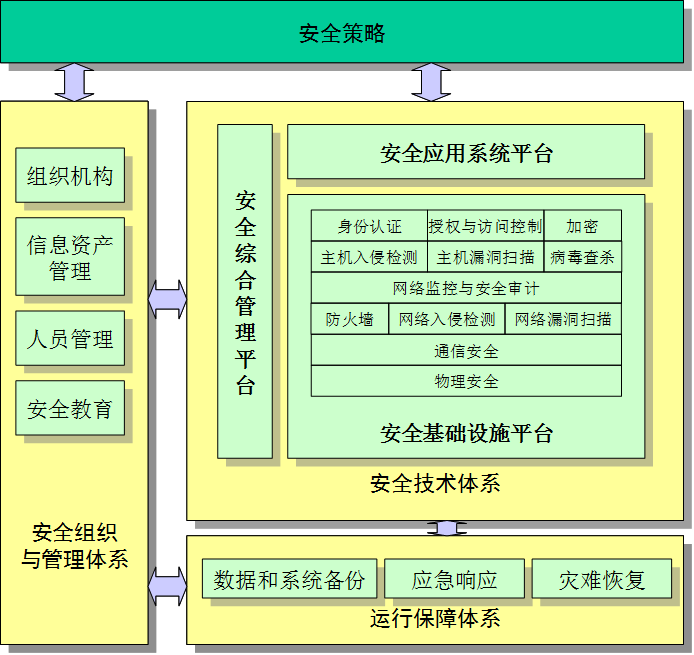
安全目标模型是信息安全体系框架的基础，XXX单位的信息安全体系框架紧密围绕这个安全模型的6个要素环节进行设计，每个要素环节的功能都在安全技术体系、安全组织和管理体系以及运行保障体系中体现出来。

## 体系框架

通过对XXX单位的网络和应用现状、安全现状、面临的安全风险的分析，根据安全保障目标模型，制定了XXX单位信息安全体系框架，制定该框架的目的在于从宏观上指导和管理信息安全体系的建设和运营。

该框架由一组相互关联、相互作用、相互弥补、相互推动、相互依赖、不可分割的信息安全保障要素组成。在此框架中，以安全策略为指导，融会了安全技术、安全管理和运行保障三个层次的安全体系，达到系统可用性、可控性、抗攻击性、完整性、保密性的安全目标。

XXX单位信息安全体系框架的总体结构如下图所示：



* **安全策略**

在这个框架中，安全策略是指导。安全策略与安全技术体系、安全组织和管理体系以及运行保障体系这三大体系之间的关系也是相互作用的。一方面，三大体系是在安全策略的指导下构建的，主要是要将安全策略中制定的各个要素转化成为可行的技术实现方法和管理、运行保障手段，全面实现安全策略中所制定的目标；另一方面，安全策略本身也有包括草案设计、评审、实施、培训、部署、监控、强化、重新评估、修订等步骤在内的生命周期，需要采用一些技术方法和管理手段进行管理，保证安全策略的及时性和有效性。

* **安全技术体系**

安全技术体系是整个信息安全体系框架的基础，包括了安全基础设施平台、安全应用系统平台和安全综合管理平台这三个部分，以统一的信息安全基础设施平台为支撑，以统一的安全系统应用平台为辅助，在统一的综合安全管理平台管理下的技术保障体系框架。

安全基础设施平台是以安全策略为指导，从物理和通信安全防护，网络安全防护，主机系统安全防护，应用安全防护等多个层次出发，立足于现有的成熟安全技术和安全机制，建立起的一个各个部分相互协同的完整的安全技术防护体系。

安全应用系统平台处理安全基础设施与应用信息系统之间的关联和集成问题，应用信息系统通过使用安全基础设施平台所提供的各类安全服务，提升自身的安全等级，以更加安全的方式，提供业务服务和内部信息管理服务。

安全综合管理平台的管理范围尽可能地涵盖安全技术体系中涉及的各种安全机制与安全设备，对这些安全机制和安全设备进行统一的管理和控制，负责管理和维护安全策略，配置管理相应的安全机制，确保这些安全技术与设施能够按照设计的要求协同运作，可靠运行。它在传统的信息系统应用体系与各类安全技术、安全产品、安全防御措施等安全手段之间搭起桥梁，使得各类安全手段能与现有的信息系统应用体系紧密的结合实现无缝连接，促成信息系统安全与信息系统应用的真正的一体化，使得传统的信息系统应用体系逐步过渡向安全的信息系统应用体系。

统一的安全管理平台有助于各种安全管理技术手段的相互补充和有效发挥，也便于从系统整体的角度来进行安全的监控和管理，从而提高安全管理工作的效率，使人为的安全管理活动参与量大幅下降。

* **安全管理体系**

安全组织和管理体系是安全技术体系真正有效发挥保护作用的重要保障，安全管理体系的设计立足于总体安全策略，并与安全技术体系相互配合，增强技术防护体系的效率和效果，同时也弥补当前技术无法完全解决的安全缺陷。

技术和管理是相互结合的，一方面，安全防护技术措施需要安全管理措施来加强，另一方面技术也是对管理措施贯彻执行的监督手段。在XXX单位信息安全体系框架中，安全管理体系的设计充分参考和借鉴了国际信息安全管理标准《BS7799（ISO17799）》的建议要求。

XXX单位信息安全管理体系由若干信息安全管理类组成，每项信息安全管理类可分解为多个安全目标和安全控制。每个安全目标都有若干安全控制与其相对应，这些安全控制是为了达成相应安全目标的管理工作和要求。信息安全管理体系一共包括了12项管理类：

* 安全策略与制度，确保XXX单位拥有明确的信息安全方针以及配套的策略和制度，以实现对信息安全工作的支持和承诺，保证信息安全的资金投入。
* 安全风险管理，信息安全建设不是避免风险的过程，而是管理风险的过程。没有绝对的安全，风险总是存在的。信息安全体系建设的目标就是要把风险控制在可以接受的范围之内。风险管理同时也是一个动态持续的过程。
* 人员和组织安全管理，建立组织机构，明确人员岗位职责，提供安全教育和培训，对第三方人员进行管理、协调信息安全监管部门与行内其它部门之间的关系，保证信息安全工作的人力资源要求，避免由于人员和组织上的错误产生的信息安全风险。
* 环境和设备安全管理，控制由于物理环境和硬件设施的不当所产生的风险。管理内容包括物理环境安全、设备安全、介质安全等。
* 网络和通信安全管理，控制和保护网络和通信系统，防止其受到破坏和滥用，避免和降低由于网络和通信系统的问题对XXX单位业务系统的损害。
* 主机和系统安全管理，控制和保护XXX单位的计算机主机及其系统，防止其受到破坏和滥用，避免和降低由此对业务系统的损害。
* 应用和业务安全管理，对各类应用和业务系统进行安全管理，防止其收到破坏和滥用。
* 数据安全和加密管理，采用数据加密和完整性保护机制，防止数据被窃取和篡改，保护业务数据的安全。
* 项目工程安全管理，保护信息系统项目工程过程的安全，确保项目的成果是可靠的安全系统。
* 运行和维护安全管理，保护信息系统在运行期间的安全，并确保系统维护工作的安全。
* 业务连续性管理管理，通过设计和执行业务连续性计划，确保信息系统在任何灾难和攻击下，都能够保证业务的连续性。
* 合规性（符合性）管理，确保XXX单位的信息安全保障工作符合国家法律、法规的要求；且XXX单位的信息安全方针、规定和标准得到了遵循。

12项信息安全管理类之间的关系，如下图所示。



12项信息安全管理类的作用关系为：

* 方针和策略：是XXX单位整个信息安全管理工作的基础和整体指导，对于其它所有的信息安全管理类都有指导和约束关系。
* 人员和组织管理：是要依据方针和策略来执行信息安全管理工作。
* 合规性：指导如何检验信息安全管理工作的效果。特别是对于国家法律法规、方针政策和标准符合程度的检验。
* 根据“方针和策略”，由“人员和组织”实施信息安全管理工作。在实施中主要从两个角度来考虑问题，即风险管理和业务连续性管理。
* 根据信息系统的生命周期，可以将信息系统划分为两个阶段，即项目工程开发阶段和运行维护阶段。这两个信息安全管理类体现了信息系统和信息安全工作的生命周期特性。
* 最终所有的信息安全管理工作都作用在信息系统之上。信息系统可以划分成5个层次，从底层到上层依次为环境与设备管理、网络与通信管理、主机与系统管理、应用与业务管理、数据/文档/介质管理。这5个信息安全管理类体现了信息系统和信息安全工作的层次性。
* **运行保障体系**

运行与保障体系由安全技术和安全管理紧密结合的内容所组成，包括了系统可靠性设计、系统数据的备份计划、安全事件的应急响应计划、安全审计、灾难恢复计划等，运行和保障体系对于XXX单位网络和信息系统的可持续性运营提供了重要的保障手段。

* **建设实施规划**

建设实施规划是在安全管理体系、安全技术体系、运行保障体系设计的基础上进一步制定的建设步骤和实施方案。在建设实施规划中突出体现了分步有序实施的原则。

任何信息安全建设都需要人员负责管理和实施，因此，首先应该建立信息安全工作监管组织机构，明确各级管理机构的人员配备，职能和责任。其中信息安全管理机构负责信息安全策略的审核与颁布、统一技术标准和管理规范的制定、指导和监督信息安全建设工作、对信息安全系统进行监控与审计管理。然后，对所有员工进行基本安全教育，为信息安全系统相关技术人员提供专门的安全理论和安全技能培训，提高全员的安全意识，打造一支高素质的专业技术和管理队伍。

信息安全体系建设，应该首先从物理环境安全建设入手，确保机房建设按照的统一标准进行建设，并且按照统一的管理规范进行管理。

接下来应该进行网络安全建设，应该对计算机网络的安全域进行划分，对网络结构进行调整，确保内部网络与外部网络、业务网络与办公网络边界清晰；在各安全域的边界处部署防火墙、网络入侵检测等安全产品，形成立体的区域边界保护机制，对各安全域进行逻辑安全隔离，禁止未授权的网络访问；在内部网络中部署网络脆弱性分析工具，定期对内部网络进行检查，并采取措施及时弥补新发现的安全漏洞。

在进行网络安全建设的同时，可以进行系统安全建设，在内部网络中全面部署网络病毒查杀系统，有效抑制计算机病毒在内部网络中传播，避免对系统和数据造成损害；另外，主机系统管理员还应该按照主机系统管理规范的要求，借助主机脆弱性分析和安全加固工具，定期对主机系统进行检查，更新安全漏洞补丁的级别，修正不当的系统和服务配置，查看和分析系统审计日志，控制和保证主机系统的良好安全状态。

应用安全建设包括建立身份认证系统、应用授权和访问控制系统、数据安全传输系统等，对业务应用系统和内部信息管理系统提供各种安全服务。

按照的统一标准，建立安全审计与分析系统、系统和数据备份计划、安全事件应急响应计划、灾难恢复计划等安全保障机制，重在保护业务数据等信息资产，保证内外应用服务的持续可用性。

# 建设内容

XXX单位的信息安全建设所涉及的工作内容包括以下部分。

## 组织机构

建立专职的信息安全监管机构，明确各级管理机构的人员岗位配置和职能权限，全面负责信息安全建设工作和维护信息安全系统的运营。

## 人员管理

依据信息系统安全等级保护要求，对人员录用、考核、培训、离岗等一系列管理进行规范性要求。

制定统一的人员安全管理和教育培训规范，定期对信息系统的用户进行安全教育和培训，对普通用户进行基本的安全教育，对安全技术岗位的用户进行岗位技能培训，提高全员的安全意识，培养高素质的安全技术和管理队伍。

## 物理管理

按照国家对于计算机机房的相关建设标准，制定统一的计算机机房建设标准和管理规范，对于计算机机房建设中的环境参数、保障机制，以及运行过程中的人员访问控制、监控措施等进行统一约定，颁布统一的计算机机房管理制度，对设备安全管理、介质安全管理、人员安全管理等作出详细的规定。

## 网络管理

网络安全是信息安全保障的重点，制定统一的网络结构技术标准，对如何划分内部信息系统的安全区域，安全区域的边界采取的隔离措施，进行约定，保证内部网络与外部网络、办公网与业务生产网之间的安全隔离。

制定统一的互联网接入点、外联网接入点的技术标准和管理规范，统一约定网络边界接入点的网络结构、安全产品的部署模式，保证内部网络与外部网络之间的安全隔离。

制定统一的网络安全系统建设标准和管理规范，包括防火墙、网络入侵检测、网络脆弱性分析、网络层加密等。

## 系统管理

系统安全的工作内容包括制定统一的系统安全管理规范，包括主机入侵检测、系统安全漏洞分析和加固， 提升服务器主机系统的安全级别。

制定统一的网络病毒查杀系统的建设标准和管理规范，有效抑制计算机病毒在内部网络和信息系统中的传播和蔓延。

## 应用管理

应用安全机制在应用层为业务系统提供直接的安全保护，能够满足身份认证、用户授权与访问控制、数据安全传输等安全需求。

制定统一的身份认证、授权与访问控制、应用层通信加密等应用层安全系统的建设标准和管理规范，改善业务应用系统的整体安全性。

## 数据管理

系统数据备份是重要的安全保障机制，为了保障业务数据的安全性，降低突发意外事件所带来的安全风险，制定统一的系统和数据备份标准与规范，采取先进的数据备份技术，保证业务数据和系统软件的安全性。

## 运维管理

运维管理是在网络的基础设施建设完成之后，对运行环境（包括物理网络，软硬件环境等）、业务系统等进行维护管理。结合工作及信息化建设实际，建立运维管理标准及应用制度，采用标准的运维管理流程，完善系统运维管理体系，保证信息系统安全稳定的运行。

灾难是指对网络和信息系统造成任何破坏作用的意外事件，要制定详细的灾难恢复计划，考虑到数据大集中的安全需求，采用异地容灾备份等技术，确保数据的安全性和业务的持续性，在灾难发生后，尽快完成恢复。

制定统一的应急响应计划标准，建立应急响应计划，包括安全事件的检测、报告、分析、追查、和系统恢复等内容。在发生安全事件后，尽快作出适当的响应，将安全事件的负面影响降至最低，保障业务正常运转。

# 总体安全策略

信息安全策略是信息安全建设的核心，它描述了在信息安全建设过程中，需要对哪些重要的信息资产进行保护，以及如何进行保护。

总体策略的设计坚持管理与技术并重的原则，以确保网络和信息系统的安全性为主，采用多重保护、最小授权、和严格管理等措施，从宏观整体的角度进行阐述，是信息安全建设总的指导原则。

## 物理安全策略

（1）计算机机房的建设必须遵循国家在计算机机房场地选择、环境安全、布线施工方面的标准，保证物理环境安全。

（2）关键应用系统的服务器主机和前置机服务器、主要的网络设备必须放置于计算机机房内部的适当位置，通过物理访问控制机制，保证这些设备自身的安全性。

（3）应当建立人员出入访问控制机制，严格控制人员出入计算机机房和其它重要安全区域，访问控制机制还需要能够提供审计功能，便于检查和分析。

（4）进入机房的工作人员必须由安全管理员或机房管理员全程陪同。

（5）机房内部必须部署基础防护系统和设备，如电子门禁系统、监控报警系统、防雷设备、消防灭火系统、防水监控系统、温湿度控制系统、UPS供电系统和电磁屏蔽设备。

（6）建立计算机机房管理制度，对设备安全管理、介质安全管理、人员出入访问控制管理等做出详细的规定。

（7）管理机构应当定期对计算机机房各项安全措施和安全管理制度的有效性和实施状况进行检查，发现问题，进行改进。

## 网络安全策略

（1）必须对网络和信息系统进行安全域划分，建立隔离保护机制，并且在各安全域之间建立访问控制机制，杜绝发生未授权的非法访问现象，特别的，必须对生产网和办公网进行划分和隔离。

（2）应当部署网络管理体系，管理网络资源和设备，实施监控网络系统的运行状态，降低网络故障带来的安全风险。

（3）应当对关键的通信线路、网络设备提供冗余设计，防止关键线路和设备的单点故障造成通信服务中断。

（4）应当在各安全域的边界，综合部署网络安全访问措施，包括防火墙、入侵检测、VPN，建立多层次的，立体的网络安全防护体系。

（5）应当建立网络弱点分析机制，发现和弥补网络中存在的安全漏洞，及时进行自我完善。

（6）应当建立远程访问机制，实现安全的远程办公和移动办公。

（7）应当指定专门的部门和人员，负责网络安全系统的规划、建设、管理维护。

（8）应当建立网络安全系统的建设标准和相关的运营维护管理规范，在范围内指导实际的系统建设和维护管理。

（9）管理机构应当定期对网络安全措施和安全管理制度的有效性和实施状况进行检查，发现问题，进行改进。

## 主机安全策略

（1）应当对关键服务器主机设备提供冗余设计，防止单点故障造成网络服务中断。

（2）应当建立主机弱点分析机制，发现和弥补系统软件中存在的不当配置和安全漏洞，及时进行自我完善。

（3）应当建立主机系统软件版本维护机制，及时升级系统版本和补丁程序版本，保持系统软件的最新状态。

（4）应当建立主机系统软件备份和恢复机制，在灾难事件发生之后，能够快速实现系统恢复。

（5）可以建立主机入侵检测机制，发现主机系统中的异常操作行为，以及对主机发起的攻击行为，并及时向管理员报警。

（6）应当指定专门的部门和人员，负责主机系统的管理维护。

（7）应当建立主机系统管理规范，包括系统软件版本管理、主机弱点分析、主机审计日志检查和分析、以及系统软件的备份和恢复等内容。

（8）应当建立桌面系统使用管理规范，约束和指导用户使用桌面系统，并对其进行正确有效的配置和管理。

（9）管理机构应当定期对各项系统安全管理制度的有效性和实施状况进行检查，发现问题，进行改进。

## 应用安全策略

（1）应用系统必须在登录时要求输入用户名和口令。

（2）登录应用系统必须进行两种或两种以上的复合身份验证（如用户名口令+Ukey或用户名口令+IP与MAC地址绑定方式）。

（3）应用系统中设置的用户都必须是唯一用户，不能名称相同，且不能出现多人使用同一账户的情况。

（4）应用系统必须开启登录失败处理功能。

（5）应用系统必须开启登录连接超时自动退出等措施。

（6）应用系统必须开启身份鉴别、用户身份标识唯一性检查、用户身份鉴别信息复杂度检查以及登录失败处理功能，并根据安全策略配置相关参数。

（7）应用系统必须开启日志审计功能。

（8）应用系统存储用户信息的设备在销毁、修理或转其他用途时，必须清楚内部存储的信息。

## 数据安全策略

（1）在业务系统主要应用服务器中采用硬件冗余技术，避免硬件的单点故障导致服务中断。

（2）综合考虑性能和管理等因素，采用先进的系统和数据备份技术，在范围内建立统一的系统和数据备份机制，防止数据出现逻辑损坏。

（3）业务应用数据和设备配置文档都必须进行备份，以便发生问题时进行恢复。

（4）数据备份至其他设备上时，必须使用专门的备份通道，保证数据传输的完整性。

（5）数据本机备份时应检测其完整性。

（6）数据备份时必须使用专业的备份设备和工具，在数据传输和数据存储时，都必须是加密传输和存储。

（7）建立灾难恢复计划，提供灾难恢复手段，在灾难事件发生之后，快速对被破坏的信息系统进行恢复。

（8）应当建立专门岗位，负责用户权限管理，以及授权和访问控制系统的建设、运行、维护。

（9）建立日常数据备份管理制度，对备份周期和介质保管进行统一规定。

（10）建立灾难恢复计划，对人员进行灾难恢复培训，定期进行灾难恢复的模拟演练。

## 病毒管理策略

（1）应当建立全面网络病毒查杀机制，实现教育局全网范围内的病毒防治，抑止病毒的传播。

（2）所有内部网络上的计算机在联入内部网络之前，都应当安装和配置杀毒软件，并且通过管理中心进行更新，任何用户不能禁用病毒扫描和查杀功能。

（3）所有内部网络上的计算机系统都应当定期进行完整的系统扫描。

（4）从外部介质安装数据和程序之前，或安装下载的数据和程序之前，必须对其进行病毒扫描，以防止存在病毒感染操作系统和应用程序。

（5）第三方数据和程序在安装到内部网络的系统之前，必须在隔离受控的模拟系统上进行病毒扫描测试。

（6）任何内部用户不能故意制造、执行、传播、或引入任何可以自我复制、破坏或者影响计算机内存、存储介质、操作系统、应用程序的计算机代码

（7）应当指定专门的部门和人员，负责网络病毒防治系统的管理维护。

（8）应当建立网络病毒防治系统的管理规范，有效发挥病毒防治系统的安全效能。

（9）应当建立桌面系统病毒防治管理规范，约束和指导用户在桌面系统上的操作行为，以及对杀毒软件的配置和管理，达到保护桌面系统、抑止病毒传播的目的。

（10）应当定期对与病毒查杀有关安全管理制度的有效性和实施状况进行检查，发现问题，进行改进。

# 附则

本文件由XXX单位信息中心负责解释与修订。

本文件自颁布之日起发布执行。