

实验报告

课程名称： 信息安全工程

实验项目：实验一：基于ISSE过程的网络安全需求分析

学 生 姓 名：

学 号：

二级学院名称： 媒体工程学院

专 业： 网络工程

指 导 教 师：

**1实验目的和要求**

1）熟练掌握基于ISSE过程的信息安全需求分析的内容和过程。

**2实验设备及材料**

1）Windows系统

2）Microsoft Word

**3实验内容**

假定本校现教中心为保密单位，以该保密单位的运作为基础，实现基于ISSE过程的信息安全需求分析，并完成需求分析报告。

**4实验总结**

本次实验以实现现教中心的保密为目的，设计并完成了需求分析报告。

**更新历史**

|  |  |  |  |
| --- | --- | --- | --- |
| **修改人员** | **日期** | **变更原因** | **版本号** |
| **Xxx** | **2025/4/21** |  | **V0.1草稿** |
| **xxx** | **2025/4/23** | **完善系统边界描述、增加安保岗位条件说明** | **V0.2草稿** |
| **xxx** | **2025/4/27** | **新增应急响应计划模块** | **V0.3草稿** |

目录

[1 引言 6](#_Toc196751198)

[1.1 编制目的 6](#_Toc196751199)

[1.2 项目范围 6](#_Toc196751200)

[1.3 参考资料 7](#_Toc196751201)

[2 系统总体描述 7](#_Toc196751202)

[2.1 项目前景与背景 7](#_Toc196751203)

[2.2 系统边界与组成 8](#_Toc196751204)

[2.2.1 系统边界 8](#_Toc196751205)

[2.2.2 系统组成 8](#_Toc196751206)

[2.2.3 信息中心各部门及其职责 9](#_Toc196751207)

[2.3 安全功能 10](#_Toc196751208)

[3 安全需求分析 10](#_Toc196751209)

[3.1 物理安保要求 10](#_Toc196751210)

[3.1.1 安保设施与环境 10](#_Toc196751211)

[3.1.2 人员管理 11](#_Toc196751212)

[3.2 系统安全要求 11](#_Toc196751213)

[3.2.1 功能安全设计 11](#_Toc196751214)

[3.2.2 内网通信与数据传输 12](#_Toc196751215)

[3.2.3 日志审计与异常监测 12](#_Toc196751216)

[3.3 安全管理与人员职责 13](#_Toc196751217)

[3.3.1 安全组织结构与岗位要求 13](#_Toc196751218)

[3.3.2 安全培训与意识建设 13](#_Toc196751219)

[3.4 应急响应计划 13](#_Toc196751220)

[3.4.1 应急响应团队 13](#_Toc196751221)

[3.4.2 应急响应流程 14](#_Toc196751222)

[3.4.3 应急演练 15](#_Toc196751223)

[4 附录 15](#_Toc196751224)

# 引言

## 编制目的

本报告基于 ISSE过程模型，对本校现代教育中心（以下简称“现教中心”）作为涉密单位的网络安全需求进行系统性分析。内容涵盖人员管理、身份认证机制、软硬件资产分类保护等多个关键领域，旨在为后续信息系统的安全架构设计、风险评估与防护策略制定提供规范化的需求依据。

除非另有明确说明，本文所列需求均为优先级最高的关键性安全需求，应在系统设计与实施阶段优先考虑与落实，确保现教中心整体信息安全水平满足涉密单位运行标准。

## 项目范围

包含现教中心相关的全部物理空间、网络设备、信息系统及其工作人员。具体包括：

1. 物理范围：

现代教学中心所占场所的建筑空间、办公室、机房、多媒体教室、实验室等实体场所；

1. 网络与硬件资产：

所有归属于现现教中心管理范围的服务器、交换机、路由器、防火墙、监控系统、终端主机、多媒体设备等网络与计算设施；

1. 软件与数字化资产：

包含教学素材管理平台、视频资源平台、教学控制系统、操作系统与数据库软件、配置脚本与文档模板等；

1. 人员与身份对象：

涉及日常教学管理、系统运维、网络维护、安全审计、资源调度等岗位的教职工与授权访问人员。

## 参考资料

1. 《浙江传媒学院教职工行为手册 》
2. 《浙江传媒学院全体师生守则 》
3. 《互联网信息安全管理条例 》
4. 《浙江传媒学院信息资产管理条例 》
5. 《浙江传媒学院校规 》
6. 《浙江传媒学院运行管理办法》
7. 《GB/T 22239-2019 网络安全等级保护基本要求》
8. 《保密要害部门部位确定标准（试行）》
9. 《ISSE 信息系统安全工程模型》

# 系统总体描述

## 项目前景与背景

随着《国家网络安全法》《保密法》及相关技术规范的不断更新，我国对信息系统安全性、保密性的要求日益提高。现教中心作为本校涉密单位之一，承载着教学资源管理、课件生产、多媒体平台运行等关键任务，其信息系统面临越来越严峻的安全挑战。

当前现教中心部分系统仍依赖传统身份认证方式、网络边界模糊、审计追踪机制不完善，难以有效防范日趋复杂的网络攻击和数据泄露事件。尤其在日常教学运行、科研交流等过程中，存在较多潜在的涉密信息泄露风险，亟需构建与国家保密要求相匹配的防护体系。

本项目旨在对现有安全体系进行全面的检查与重构，通过引入身份认证机制、构建完整的物理与逻辑边界控制体系、加强信息资产动态监控及审计，实现保密环境下的现代教学信息系统安全能力升级。

## 系统边界与组成

### 2.2.1 系统边界

1. 物理边界：

现代教育中心所有实体建筑空间，包括办公室（如现教楼304, 306等）、机房、多媒体教室、视频编辑室、会议室等。由综合科协调日常管理和安全检查工作。

1. 网络边界：

内部有线网络、无线接入点、核心交换设备、防火墙、外部VPN网关及与校园网或互联网的连接节点。由网络技术与安全部门负责设计、部署和维护。

1. 信息边界：

中心管理的所有教学资源、视频素材、教学管理系统数据库、脚本模板、配置文件等信息资产。数据应用部负责制定信息化建设规划与标准，推进大数据治理。

### 2.2.2 系统组成

1. 身份认证与访问控制模块：

由网络技术与安全部门负责实施和维护，对教职员工、授权外部人员进行权限识别与控制，确保符合《互联网信息安全管理条例》等相关法律法规要求。

1. 安防监控与告警系统：实现物理空间的 7×24 小时安防监控；

由综合科协调，网络技术与安全部提供技术支持。实现物理空间的7×24小时安防监控。安保人员需按照规定执行日常检查，并通过监控系统记录所有进出人员的信息。

1. 资源管理平台：包含课件上传、视频制作、资源分发系统；

教育技术部负责平台的技术支持和内容管理。包含课件上传、视频制作、资源分发系统。该平台应具备严格的访问控制机制，并定期备份重要资料。日志与审计子系统：记录所有关键操作并追踪用户行为；

1. 日志与审计子系统：

网络技术与安全部负责系统的运行和维护。记录所有关键操作并追踪用户行为。确保日志数据的安全存储和定期审查，以便及时发现潜在的安全威胁。

### 2.2.3 信息中心各部门及其职责

为了更全面地理解各部门在信息安全管理体系中的角色，以下是信息中心各主要部门的具体职责概述：

（1）综合科

主要职责：负责办公室日常管理，科室协调，计划总结，制度建设，资产管理等；承担学校信息化工作的整体战略规划以及各类材料撰写。

安全相关职责：确保文档管理和数据上报过程中的信息安全，防止未经授权的访问和数据泄露。

（2）数据应用部

主要职责：负责学校数据应用领域的信息化建设规划与标准制定；推进大数据治理，建立数据化管理体系；促进全校信息系统集成与共享。

安全相关职责：实施严格的数据访问控制策略，保护敏感数据不被非法获取或篡改。

（3）网络技术与安全部

主要职责：负责校园基础网络及各类专网的规划、建设和运行；保障网络信息安全稳定；执行网络安全培训。

安全相关职责：部署防火墙、入侵检测系统等网络安全措施；定期进行网络安全评估和漏洞扫描。

（4）教育技术部

主要职责：负责公共智慧教室、多媒体教室等的教学环境建设和维护；提供在线学习平台的技术支持；推广教育技术创新应用。

安全相关职责：保证教学环境中使用的软硬件的安全性，尤其是在线平台的安全防护，避免学生个人信息泄露。

## 安全功能

SF1 身份认证机制强化  
所有教职员工登录系统须通过多因子认证（含动态口令、物理证件），访客与外部接入用户需提前登记并审批授权。

SF2 物理空间全时监控  
所有教学中心重要区域配备高清视频监控设备，支持远程访问与回放功能。管理员操作全程审计，不可修改或删除。

SF3 核心设备检测与数据留存  
每日对中心关键硬件设备进行巡检，检测结果须于 23:00 前上传。系统自动比对数据上报时间，触发超时预警。

SF4 出入登记与安全检查机制  
所有出入中心的人员（含员工与访客）需经过物理安全检查，访客实行实名登记制，并录入安全访问系统。

SF5 内网通信行为监控  
实时分析终端与服务器之间的内网通信流量，识别异常访问行为并触发告警，防止横向渗透与数据转移。

SF6 外部信息传输监控与终端屏幕抓取  
每 30 秒定时对操作终端屏幕进行截取存档，结合网络数据流量分析，监控用户通过互联网传输的涉密信息。

# 安全需求分析

## 物理安保要求

### 安保设施与环境

1. 门禁控制系统

所有重点区域（如机房、监控室、多媒体资源区）需部署门禁系统，支持 IC 卡识别、人脸识别等方式，并实现记录查询功能。

1. 视频监控与录像保存

关键场所需部署 7×24 小时监控系统，录像数据保存时间不少于 90 天，并具有远程访问与导出功能。

1. 环境与防护设施

安装防火报警系统、防雷接地装置、防盗窗与电子围栏等设施；还应具备断电后的备用电源保障。

### 人员管理

1. 访问授权机制

实施岗位分类授权，仅允许经审批的人员进入涉密场所；进入机房等核心区域需经二级审批。

1. 访客管理制度

所有访客须提前预约登记，核验身份后方可进入，入出信息须完整记录并保存不少于 6 个月。

1. 保密协议与岗前签署

所有正式工作人员及实习人员入职前必须签署保密承诺书，明确涉密职责与违规后果。

1. 安保岗位人员要求

身体素质要求：健康、稳定、无传染性疾病，无心理疾病史，具备应急处理能力；

外观形象与行为规范：性格稳重、举止得体，能够胜任日常安检与突发事件响应任务；

政治立场：拥护中国共产党纲领，政治立场坚定。

## 系统安全要求

### 功能安全设计

1. 内外网逻辑隔离

系统设计应确保内外网物理隔离或 VLAN 分区，禁止通过无线共享、个人热点等方式跨网通信。

1. 行为日志与信息追踪

系统需对所有用户的访问行为、操作记录、数据上传下载等活动进行详尽日志记录，支持回溯查询。

1. 随机口令机制与动态预警

每日生成特定访问口令，结合用户身份校验；对未通过验证尝试的操作应触发预警机制。

1. 终端间通信控制

内部用户可在授权范围内进行终端文件互传、即时消息交流，但需经过审计代理服务器中转。

### 3.2.2 内网通信与数据传输

1. 安全通信协议

内网远程管理必须使用加密协议（如 SSH、SFTP、HTTPS 等）；禁用明文传输。

1. 云端数据备份机制

所有业务资料需定时同步至云端加密存储系统，确保关键数据不因本地故障而丢失。

1. 无线访问控制

禁止内部网段连接未授权无线网络；自动阻断检测到的无线热点分享行为。

### 3.2.3 日志审计与异常监测

1. 设备身份验证与行为控制

所有终端设备在使用前需通过身份认证与每日更新的动态口令校验，确保使用者合法性。

1. 屏幕监控与截屏机制

系统应每 30 秒自动抓取一次屏幕快照，保存为审计记录，用于事后可视化回溯。

1. 入侵检测系统（IDS）与日志分析系统

部署 IDS 监测网络异常访问行为，结合行为分析系统识别潜在攻击；日志应至少保留 180 天，具备可追踪性。

1. 异常行为响应机制

系统应具备基于策略的自动封锁、预警、锁定账号等应急响应机制，用于处理非法访问或敏感信息泄露风险。

## 安全管理与人员职责

### 安全组织结构与岗位要求

（1） 设立核心岗位角色

安全管理员：负责权限管理、策略配置、安全策略执行；

系统管理员：负责服务器与平台的部署、维护与更新；

信息审计员：对系统日志、屏幕截图、用户行为进行分析、留存和上报；

（2） 岗位要求与资质认证

安全岗位人员应熟悉局域网配置、常用网络协议，持有华为 HCIA/HCIP 或思科 CCNA/CCNP 等认证证书，具备数据库管理与办公自动化能力。

### 3.3.2 安全培训与意识建设

（1）定期培训与考核制度

每季度组织至少一次全员信息安全培训，内容涵盖保密法律法规、应急响应流程、常见威胁类型等。

（2）应急预案与实战演练

每年至少开展一次实战化应急演练，覆盖信息泄露、系统被控、突发攻击等情形。

（3）奖惩机制

对在安全事件中表现突出或主动发现问题者给予奖励；对违规操作人员进行公开通报与处罚，严重者追责。

## 应急响应计划

### 3.4.1 应急响应团队

（1）安全管理员：负责总体协调应急响应活动。

（2）系统管理员：负责技术层面的操作，如隔离受攻击的系统、恢复数据等。

（3）信息审计员：记录事件详情，包括时间线、受影响的系统和服务、采取的措施等。

（4）外部专家/顾问：提供专业建议和技术支持。

### 3.4.2 应急响应流程

（1）预防阶段

1. 定期进行风险评估，识别潜在威胁并制定相应的防护措施。
2. 实施持续监控机制，及时发现异常行为或入侵尝试。
3. 对所有员工进行定期的安全培训，提高他们的意识和应对能力。

（2）检测阶段

1. 使用入侵检测系统（IDS）、日志分析工具等手段实时监控网络流量和用户行为。
2. 设定自动报警规则，一旦检测到可疑活动立即通知相关人员。
3. 收集相关证据，包括但不限于日志文件、截图、网络流量记录等。

（3）响应阶段

初步评估：确定事件的性质和严重程度。如果必要，启动紧急会议讨论对策。

遏制措施：

1. 隔离受攻击的系统，防止问题扩散。
2. 关闭不必要的服务端口，限制访问权限。
3. 更新防火墙规则或其他网络安全设置。

根除威胁：彻底清除恶意软件或修复漏洞，恢复被篡改的数据。

恢复操作：将受影响的服务恢复正常运行状态，并验证系统的完整性和安全性。

（4）后续处理

对整个事件进行全面回顾，总结经验教训，改进现有的安全策略。如果涉及法律问题，配合执法机关调查取证。同时更新应急预案，确保未来类似事件能够得到更快更有效的处理。

### 3.4.3 应急演练

至少每年组织一次实战化应急演练，模拟不同类型的突发事件（如DDoS攻击、勒索软件感染等）。并详细记录演练过程中的每一个步骤及其效果，用于后续分析和改进。

# 附录