青岛大学医学院附属医院HIS系统信息安全工程实施方案

姓名 学号

**[摘要]** 随着医疗信息化水平的不断提升，医院信息系统（HIS）在支持临床诊疗、资源配置与管理决策中发挥着核心作用。然而，系统中大量存储与传输的患者隐私、诊疗数据正面临日益复杂的网络安全威胁。

本方案以青岛大学医学院附属医院的 HIS 系统为研究对象，依据《网络安全等级保护制度 2.0》开展信息安全工程设计。首先明确系统运行环境与资产组成，识别七大模块下的核心安全需求；随后结合定级指南将系统整体确认为三级保护等级；采用风险矩阵法评估系统在边界防护、数据保护、账号管理等方面存在的中高风险；最后从网络通信、数据加密、身份认证、应用加固、安全监控、管理制度与应急恢复等方面提出覆盖“预防—检测—响应—恢复”的综合防护措施，构建具有医院场景针对性的信息安全保障体系。

**[关键词]** HIS系统、信息安全、等级保护、风险评估、安全保障方案

目录

[第一章 引言 3](#_Toc200371337)

[（一）研究目的 3](#_Toc200371338)

[（二）研究内容与结构 3](#_Toc200371339)

[第二章 需求分析 3](#_Toc200371340)

[（一）系统概况 3](#_Toc200371341)

[（二）业务模块信息安全需求分析 3](#_Toc200371342)

[（三）信息资产识别 4](#_Toc200371343)

[（四）运行环境 6](#_Toc200371344)

[第三章 安全定级 6](#_Toc200371345)

[（一）等级保护原则与标准依据 6](#_Toc200371346)

[（二）等级判定结果 6](#_Toc200371347)

[（三）安全模块细化定级与说明 7](#_Toc200371348)

[第四章 信息安全风险评估 8](#_Toc200371349)

[（一）风险评估方法说明 8](#_Toc200371350)

[（二）威胁与脆弱性识别 8](#_Toc200371351)

[（三）风险等级评定结果 10](#_Toc200371352)

[第五章 安全保障解决方案 12](#_Toc200371353)

[（一）网络通信安全防护 12](#_Toc200371354)

[（二）数据安全保护 13](#_Toc200371355)

[（三）身份认证与访问控制 13](#_Toc200371356)

[（四）应用系统安全加固 14](#_Toc200371357)

[（五）安全监控与态势感知 14](#_Toc200371358)

[（六）安全管理体系 15](#_Toc200371359)

[（七）应急响应与业务连续性 15](#_Toc200371360)

[参考文献 17](#_Toc200371361)

[附录 18](#_Toc200371362)

[风险矩阵 18](#_Toc200371363)

**[正文]**

# 引言

## （一）研究目的

随着“健康中国2030”战略推进，青岛大学医学院附属医院的 HIS 系统已成为支撑诊疗与管理的核心平台，广泛涉及挂号、住院、医嘱、药品与费用结算等关键环节。然而，随着业务复杂度提升，系统逐渐暴露出网络攻击、数据泄露与服务中断等多重风险。为保障患者隐私与系统连续性，青岛大学医学院附属医院（下文中简称“青医附院”）依据《网络安全等级保护2.0》要求，全面开展 HIS 系统的安全定级、风险评估与防护方案设计，构建可持续的多层次信息安全体系，旨在构建覆盖“预防、检测、响应、恢复”的全生命周期安全体系，切实保障医院业务连续性与患者信息安全。

## （二）研究内容与结构

本报告围绕“青医附院HIS系统信息安全工程实施方案”展开，共分为五章，内容安排如下：

第二章 需求分析：对青医附院HIS系统的业务模块、资产构成与运行环境进行安全需求识别；

第三章 安全定级：依据国家等级保护制度，对系统进行安全等级的定级判断；

第四章 风险评估：采用风险矩阵法识别潜在威胁、分析脆弱性并评定风险等级；

第五章 安全保障解决方案：从技术和管理两个维度提出综合性的安全对策；

# 需求分析

## （一）系统概况

青医附院 HIS 系统承担着全院门诊、住院、检验、药品、手术、收费等关键业务信息的处理与流转，覆盖医护人员工作站、科室终端与后勤服务系统等多类场景。系统由统一数据中心支撑，部署在高可用服务器集群之上，并通过核心交换网络连接院内各功能子系统。

系统整体架构包括三大层次：

1. 基础网络层：包括 VPN 网关、核心交换、无线接入等设施，连接院区各终端；
2. 应用支撑层：包括数据库、中间件、API 服务网关等，提供统一数据交互能力；
3. 业务应用层：包括医生工作站、住院管理、病案系统、PACS 等核心业务模块。

## （二）业务模块信息安全需求分析

结合系统实际使用功能，对关键业务模块进行信息安全需求分析：

**（1）门诊挂号与缴费系统**

该模块负责患者挂号预约与费用缴纳，涉及患者基本信息、挂号科室、缴费项目及医保账户等敏感数据。系统需实现数据传输加密、敏感字段存储保护和接口防护，防止信息泄露与伪造挂号行为。同时应保障挂号记录完整可审计，防止越权操作和非法调用医保接口。

**（2）医生工作站与医嘱开立系统**

医生工作站用于病历查看、开具处方、提交医嘱等操作，涉及大量诊疗信息与核心医疗决策。系统应确保仅授权医生可访问患者病历，防止越权访问与非法篡改，并启用日志记录、自动锁屏和权限校验机制，提升操作可追溯性与身份可信性。

**（3）护士工作站与护理系统**

护理系统支持执行医嘱、记录生命体征与护理措施。涉及数据包括体温单、用药执行记录等，需防止操作越权与伪造。应配置角色权限边界、日志留存与终端环境管控措施，确保护理数据真实、完整、可溯源，保障患者安全。

**（4）住院管理系统**

住院管理模块涵盖患者入院、转科、出院与床位调配流程，涉及完整的住院病程与费用信息。系统应限制访问权限，防止非授权用户操作住院信息，并确保住院流程记录完整留痕，支持事后审计与灾难恢复。

**（5）医学检验与影像系统（LIS/PACS）**

该模块管理检验报告与医学图像数据，包含 CT/MRI 图像、检验结果与分析结论。系统应启用传输加密与访问控制，防止图像被非法截取或重构；同时对报告浏览、下载、打印行为进行日志审计，确保合规使用。

**（6）药品管理系统**

药品管理涉及药品入库、出库、盘点与处方发药，数据包括药品库存与使用记录。需防范药品盗用与处方滥用风险，系统应支持对接处方系统、配置操作审批流程，并记录所有出入库操作及用户身份信息。

**（7）病案与数据统计系统**

该模块存储出院病案全文与医疗质控数据，支撑医院报表统计。系统需确保病案数据分类保护、权限分级访问，出院病历禁止任意修改，并限制病案查询、导出、打印等敏感操作，保障数据安全与合法使用。

## （三）信息资产识别

| **安全模块类别** | **资产名称** | **资产类型** | **所属位置** | **简要说明** |
| --- | --- | --- | --- | --- |
| 网络通信安全防护 | 防火墙、防毒墙、VPN网关 | 网络设备 | 网络边界 | 边界隔离与访问控制核心设施 |
| 核心交换机 | 网络设备 | 数据中心 | 构成内网骨干，承载HIS数据流量 |
| 数据安全保护 | HIS数据库 | 数据资产 | 数据库服务器 | 存储患者个人信息与病历数据 |
| 病历图像归档系统（PACS） | 数据资产 | 文件服务器 | 包含医学影像数据（如CT/MRI） |
| 数据备份服务器 | 应用资产 | 异地灾备机房 | 用于业务恢复与灾难应对 |
| 身份认证与访问控制 | 医护账号、运维账号 | 身份凭据 | 统一认证系统 | 用户身份识别与权限配置基础 |
| 域控制器、LDAP服务器 | 应用系统 | 认证服务平台 | 提供集中式账户认证与管理 |
| 应用系统安全加固 | 门诊收费系统 | 应用系统 | 应用服务器集群 | 涉及医疗收费与医保结算 |
| 医生/护士工作站软件 | 应用程序 | 终端设备 | 医嘱录入、护理执行等关键操作 |
| 安全监控与态势感知 | 安全日志平台 | 安全系统 | 安全运维平台 | 实现全院操作审计与事件分析 |
| 入侵检测系统（IDS） | 安全系统 | 网络出口 | 用于实时发现异常入侵行为 |
| 安全管理体系 | 信息安全制度文档 | 管理文档 | 信息办/内审科室 | 包括权限分配、安全策略等管理规定 |
| 安全运维岗位人员 | 人员角色 | 信息中心 | 负责系统维护与安全管理 |
| 应急响应与业务连续性 | 灾备服务器、UPS电源 | 物理设备 | 机房/分中心 | 确保系统在突发事件中的运行保障 |
| 应急预案与演练记录 | 文档资料 | 安全管理档案 | 响应突发安全事件的重要依据 |

## （四）运行环境

青大附院HIS系统采用集中式部署结构，主要技术运行环境包括：

（1）网络架构：核心交换 + 业务接入层组成三级结构，内部设置VLAN隔离；

（2）服务器环境：Windows Server/Linux，虚拟化平台（如VMware）；

（3）数据库系统：Oracle、SQL Server、MySQL等关系型数据库；

（4）中间件/平台软件：Tomcat、WebLogic、Apache等；

（5）终端设备：医生/护士工作站、护士移动PDA、信息查询终端等；

（6）外部系统接口：医保系统、HIS接口引擎、实验室信息系统（LIS）、影像归档系统（PACS）等。

# 安全定级

## （一）等级保护原则与标准依据

评估维度如下表所示：

|  |  |  |
| --- | --- | --- |
| **评估维度** | **评估结论** | **分析说明** |
| **业务影响** | 高 | HIS系统直接支持门诊、住院、药房收费等核心诊疗流程，系统失效将导致医疗服务大规模中断。 |
| **数据敏感度** | 高 | 存储患者个人隐私数据、病历、检验报告，属《个人信息保护法》所定义的“敏感个人信息”类别。 |
| **服务对象范围** | 中 | 服务群体主要为院内医护人员与患者，面向特定区域公众，不属于全国性公众服务平台。 |
| **社会影响与可损性** | 高 | 数据泄露或系统瘫痪将引发舆论风险与法律责任，危及医疗安全，危害社会公共利益。 |

综合评估结果显示：HIS系统一旦遭受破坏，将对青医附院核心业务与患者权益造成重大影响，具有较高社会危害性。

## （二）等级判定结果

依据 GB/T 22239-2019 等保标准，青医附院 HIS 系统安全保护等级定为第三级（★★★），即“系统受到攻击或损害后，将对社会秩序和公共利益造成严重危害，但对国家安全影响有限”。

## （三）安全模块细化定级与说明

为明确系统中各子模块的安全管控深度，进一步划分各模块的控制等级：

1. **网络通信安全防护模块**

安全等级：高级

网络通信安全防护是信息系统安全的第一道技术防线，负责阻止外部攻击、非法访问和恶意扫描等行为。考虑到近年来针对青医附院行业的勒索病毒、APT 攻击频率显著增加，且一旦成功入侵将导致系统瘫痪、数据泄露等重大损失，因此将该模块定为高级安全等级。

1. **数据安全保护模块**

安全等级：高级

HIS 系统中存储着大量患者个人信息、诊疗记录、医学影像数据等敏感数据，数据安全模块通过数据库加密、字段脱敏、传输加密、备份恢复与数据泄露防护（DLP）等机制，确保数据在存储与传输过程中的完整性与保密性。这些数据一旦泄露将引发严重的法律、伦理及社会舆情风险，故该模块的安全等级定为高级。

1. **身份认证与访问控制模块**

安全等级：中级

身份认证与访问控制模块承担对青医附院内部医护、管理和运维人员的账号身份鉴别与权限边界控制任务，主要通过账号体系、多因素认证（MFA）、统一身份管理（如LDAP/AD）实现授权访问。该模块能有效防止非法登录与权限滥用，是内部安全控制的关键环节。尽管重要性不容忽视，但其暴露面相对有限，且技术机制较成熟，故安全等级定为中级。

1. **应用系统安全加固模块**

安全等级：中级

该模块聚焦于青医附院业务应用的运行环境安全，包括门诊收费系统、医生工作站、护士终端等系统的接口加固、漏洞扫描、代码审计等。应用系统虽然是信息系统的直接使用平台，但其主要面临的攻击多源于输入验证失效、漏洞滥用等开发或配置失误，相较于网络或数据层面的破坏性略低，故本模块的安全等级评定为中级。

1. **安全监控与态势感知模块**

安全等级：高级

该模块涵盖安全日志管理、安全事件集中监控、安全态势分析等内容，是青医附院信息安全体系的“感知中枢”。通过接入日志平台、入侵检测系统、安全信息与事件管理（SIEM）平台等，实现对系统运行状况和异常行为的实时掌控。由于该模块能对攻击行为实现提前预警与快速响应，其失效将导致整个安全防御体系“失明”，故定为高级。

1. **安全管理体系模块**

安全等级：中级

该模块涵盖安全制度建设、人员角色划分、安全岗位责任、培训考核等“软”安全措施，是支撑整个技术系统的管理基础。尽管该模块对于保障制度执行、预防人为失误至关重要，但其失效多表现为间接风险，通常不会立即导致系统瘫痪，故本模块的安全等级设定为中级。

1. **应急响应与业务连续性模块**

安全等级：高级

应急响应模块覆盖容灾备份、UPS 电力保障、主备切换机制及应急预案管理，是保障青医附院业务 7×24 小时连续运行的核心保障。在面对勒索病毒、电力故障、机房火灾等突发事件时，该模块是唯一能够确保快速恢复、减少损失的机制。故其安全等级应设定为高级，以确保关键业务系统具备足够的抗灾恢复能力。

# 信息安全风险评估

## （一）风险评估方法说明

本章采用矩阵风险评估方法。其核心思路是分别量化“威胁发生频率 (F)”“脆弱性严重程度 (S)”与“资产价值 (V)”，通过三层矩阵逐步推导出最终风险等级。具体说明如下：

1. **威胁发生频率（F）**：代表该类型威胁的可能出现概率，划分为五个等级：很低 (1)、低 (2)、中 (3)、高 (4)、很高 (5)。
2. **脆弱性严重程度（S）**：代表系统在此类威胁下可能遭受的破坏程度，亦划分为五个等级：无风险 (1)、低危 (2)、中危 (3)、高危 (4)、危急 (5)。
3. **资产价值（V）**：代表资产本身的重要程度，同样划分为五个等级：很低 (1)、低 (2)、中 (3)、高 (4)、很高 (5)。

基于上述三项指标，风险评估按照以下三步实施：

1. **事件发生可能性评定**：由脆弱性 S 与威胁频率 F 构建评分，得出安全事件的发生可能性等级。
2. **事件影响程度评定**：由资产价值 V 与脆弱性 S 组合，衡量安全事件发生后对系统的实际损害。
3. **风险等级综合判定**：最后以“发生可能性 (P)”与“影响程度 (I)”构建风险矩阵，得到该事件的综合风险等级，并据此确定处置优先级。

（说明：以上评分区间为1–5，完整评分矩阵详见附录。）

## （二）威胁与脆弱性识别

| **安全模块类别** | **资产名称** | **风险描述** | **资产价值（V）** | **脆弱性严重程度（S）** | **威胁发生频率（F）** |
| --- | --- | --- | --- | --- | --- |
| 网络通信安全防护 | 防火墙/防毒墙/VPN 网关 | VPN用户身份认证机制薄弱，易被爆破 | 高（4） | 中危（3） | 高（4） |
| 防火墙策略配置错误，外网暴露过多端口 | 高（4） | 中危（3） | 高（4） |
| 核心交换机 | 存在默认账号，管理接口未加密 | 高（4） | 低危（2） | 中（3） |
| 缺乏链路备份，设备故障将导致网络瘫痪 | 高（4） | 中危（3） | 中（3） |
| 数据安全保护 | HIS数据库 | 关键字段未加密，访问日志缺失 | 很高（5） | 危急（4） | 高（4） |
| 权限配置过宽，存在越权访问可能 | 很高（5） | 中危（3） | 高（4） |
| PACS 系统 | 图像传输未加密，可能被截获重构 | 高（4） | 中危（3） | 中（3） |
| 图像访问缺少权限细分，可能被非授权浏览 | 高（4） | 低危（2） | 中（3） |
| 数据备份服务器 | 备份数据未隔离部署，勒索病毒可能加密备份 | 高（4） | 中危（3） | 中（3） |
| 缺乏备份校验机制，可能出现不可用镜像 | 高（4） | 低危（2） | 中（3） |
| 身份认证与访问控制 | 医护/运维账号 | 密码复杂度不足，未启用MFA | 很高（5） | 中危（3） | 高（4） |
| 账号回收不及时，离职员工仍可登录 | 高（4） | 低危（2） | 中（3） |
| LDAP认证平台 | 单点部署，系统压力高时可能宕机 | 高（4） | 低危（2） | 中（3） |
| 无访问日志，无法审计非法登录行为 | 高（4） | 中危（3） | 中（3） |
| 应用系统安全加固 | 门诊收费系统 | Web接口参数未校验，存在SQL注入风险 | 很高（5） | 中危（3） | 高（4） |
| Session未失效，登录状态可被劫持 | 高（4） | 低危（2） | 高（4） |
| 医生/护士工作站软件 | 支持U盘运行，易被插入恶意程序 | 高（4） | 中危（3） | 高（4） |
| 软件未更新补丁，存在高危漏洞 | 高（4） | 中危（3） | 中（3） |
| 安全监控与态势感知 | 安全日志平台 | 日志未集中，留存时间不足 | 中（3） | 低危（2） | 中（3） |
| 日志文件可被本地删除，未防篡改 | 中（3） | 中危（3） | 中（3） |
| IDS系统 | 特征库未及时更新，无法识别最新攻击手法 | 中（3） | 中危（3） | 中（3） |
| 未部署与防火墙联动，无法实时阻断攻击 | 中（3） | 低危（2） | 中（3） |
| 安全管理体系 | 安全制度文档 | 制度不完善，未细化岗位职责 | 中（3） | 低危（2） | 低（2） |
| 制度未定期更新，已与技术变更脱节 | 中（3） | 低危（2） | 低（2） |
| 安全运维人员 | 运维无最小权限原则，越权操作未审计 | 高（4） | 中危（3） | 中（3） |
| 无岗责划分，部分运维操作口头下达无记录 | 高（4） | 低危（2） | 中（3） |
| 应急响应与业务连续性 | 灾备服务器、UPS电源 | 灾备方案未演练，UPS缺少故障告警机制 | 高（4） | 低危（2） | 中（3） |
| 主备切换流程无人掌握，缺乏应急分工 | 高（4） | 中危（3） | 中（3） |
| 应急预案与演练记录 | 预案未修订、未演练，信息过时 | 中（3） | 低危（2） | 低（2） |
| 未明确响应角色与时限，造成响应混乱 | 中（3） | 中危（3） | 中（3） |

## （三）风险等级评定结果

最后得到的风险等级：低风险. （R1）、中低风险（R2）、中风险（R3）、中高风险（R4）、高风险（R5），以表格形式呈现如下：

| **安全模块类别** | **资产名称** | **风险描述** | **风险评估等级** |
| --- | --- | --- | --- |
| 网络通信安全防护 | 防火墙/防毒墙/VPN 网关 | VPN用户身份认证机制薄弱，易被爆破 | 中风险 |
| 防火墙策略配置错误，外网暴露过多端口 | 中风险 |
| 核心交换机 | 存在默认账号，管理接口未加密 | 中风险 |
| 缺乏链路备份，设备故障将导致网络瘫痪 | 中风险 |
| 数据安全保护 | HIS数据库 | 关键字段未加密，访问日志缺失 | 中高风险 |
| 权限配置过宽，存在越权访问可能 | 中高风险 |
| PACS 系统 | 图像传输未加密，可能被截获重构 | 中风险 |
| 图像访问缺少权限细分，可能被非授权浏览 | 中风险 |
| 数据备份服务器 | 备份数据未隔离部署，勒索病毒可能加密备份 | 中风险 |
| 缺乏备份校验机制，可能出现不可用镜像 | 中风险 |
| 身份认证与访问控制 | 医护/运维账号 | 密码复杂度不足，未启用MFA | 中高风险 |
| 账号回收不及时，离职员工仍可登录 | 中风险 |
| LDAP认证平台 | 单点部署，系统压力高时可能宕机 | 中风险 |
| 无访问日志，无法审计非法登录行为 | 中风险 |
| 应用系统安全加固 | 门诊收费系统 | Web接口参数未校验，存在SQL注入风险 | 中高风险 |
| Session未失效，登录状态可被劫持 | 中风险 |
| 医生/护士工作站软件 | 支持U盘运行，易被插入恶意程序 | 中风险 |
| 软件未更新补丁，存在高危漏洞 | 中风险 |
| 安全监控与态势感知 | 安全日志平台 | 日志未集中，留存时间不足 | 中风险 |
| 日志文件可被本地删除，未防篡改 | 中风险 |
| IDS系统 | 特征库未及时更新，无法识别最新攻击手法 | 中风险 |
| 未部署与防火墙联动，无法实时阻断攻击 | 中风险 |
| 安全管理体系 | 安全制度文档 | 制度不完善，未细化岗位职责 | 中低风险 |
| 制度未定期更新，已与技术变更脱节 | 中低风险 |
| 安全运维人员 | 运维无最小权限原则，越权操作未审计 | 中风险 |
| 无岗责划分，部分运维操作口头下达无记录 | 中风险 |
| 应急响应与业务连续性 | 灾备服务器、UPS电源 | 灾备方案未演练，UPS缺少故障告警机制 | 中风险 |
| 主备切换流程无人掌握，缺乏应急分工 | 中风险 |
| 应急预案与演练记录 | 预案未修订、未演练，信息过时 | 中低风险 |
| 未明确响应角色与时限，造成响应混乱 | 中风险 |

# 安全保障解决方案

## （一）网络通信安全防护

**技术措施：**

1. 加强VPN接入安全：

启用多因素认证（MFA）和VPN客户端设备准入控制。设置密码尝试次数限制与锁定策略。

1. 优化边界防火墙配置

梳理访问策略，关闭不必要端口，严格最小暴露原则，并引入IPS模块，与防火墙联动阻断异常行为。

1. 部署网络冗余链路

对核心交换机设置主备热备，部署双链路互通。网络拓扑中采用环网/双星结构，避免单点故障。

1. 启用网络设备日志审计

所有路由器、交换机、防火墙配置日志上传到集中SIEM平台，并开启变更告警机制。

**管理措施：**

1. 制定网络安全设备变更审批流程，配置文件变更需归档存证；
2. 安排季度策略审查与安全巡检计划；
3. 建立运维操作授权机制，仅授权核心管理员执行策略更改。

## （二）数据安全保护

**技术措施**：

1. 加强数据库加密机制

对患者身份证号、诊断记录、费用明细等敏感字段进行字段级加密，密钥管理采用分权管控，防止单点泄密。

1. 建立访问控制分级体系

对HIS数据库、PACS图像系统等进行按“岗位+数据类别”划分的最小权限配置，设置只读/查询/下载等访问粒度。

1. 接入集中审计日志平台

数据库与文件访问操作统一接入安全日志平台，启用对高敏感数据的访问行为记录、告警和追溯能力。

1. 优化图像访问与传输机制

PACS系统图像传输使用SSL/TLS加密，图像文件访问引入水印与脱敏浏览功能，防止非法截屏和重构。

1. 强化数据备份安全性

主用数据定期异地备份，采用数据校验机制检测备份完整性，确保在遭遇勒索病毒等攻击下的快速恢复能力。

**管理措施：**

1. 制定敏感数据分级分类管理制度，明确不同级别数据的访问审批流程与存储方式；
2. 建立数据访问授权审批制度，关键岗位如财务、医技人员的数据访问需双人审批；
3. 安排季度脱敏机制自查及数据库安全配置审计，并输出整改报告；
4. 实施数据备份保密等级归档策略，重要备份数据定期加密归档至离线介质并记录流转情况。

## （三）身份认证与访问控制

**技术措施：**

1. 部署多因素认证机制（MFA）

面向所有医护人员和关键岗位运维账号启用MFA，结合手机动态验证码、硬件令牌或USB Key，提高身份校验强度。

1. 强制实施口令复杂度与周期策略

账号密码策略设置为：最小8位、必须包含大小写字母、数字及特殊字符，密码有效期不超过90天，超期强制修改。

1. 接入统一身份认证平台（LDAP/AD）

所有业务系统用户纳入统一认证体系，实现账号生命周期集中管理、角色自动同步、集中授权回收。

1. 加强登录行为审计与告警

所有系统登录行为（成功/失败）统一接入日志审计平台，设定异常登录告警策略，如多地登录、夜间频繁尝试等。

1. 构建动态权限管控机制

根据岗位职责自动分配权限，临时权限申请需审核批准并限定时效，结束后自动回收。

**管理措施：**

1. 建立账号全生命周期管理制度，包括账号申请、审批、启用、权限变更、离职注销等完整流程；
2. 与人力资源系统对接，实现员工状态变更自动触发账号回收或锁定；
3. 制定高权限账号使用审批与操作记录要求，关键操作应双人操作或录像备查；
4. 定期开展账号权限清查，尤其是对长期未登录账户进行停用或清理；
5. 开展员工信息安全意识培训，强调“账号即责任”的安全理念。

## （四）应用系统安全加固

**技术措施：**

1. 全面输入校验与输出编码

后端统一采用白名单校验框架，防止 SQL 注入、XSS 等常见攻击。前端增加参数合法性检查并对错误输入进行反馈限制。

1. 部署 Web 应用防火墙（WAF）

拦截注入、跨站脚本、文件包含等高频攻击；对高危 URI、参数开启虚拟补丁规则。

1. 强化 Session 管理

登录失败 5 次锁定账号；空闲 15 min 自动注销；Cookie 启用 HttpOnly+Secure。

1. 终端安全加固

医护工作站禁用 U 盘自动运行并安装 EDR（终端检测与响应）并强制操作系统及浏览器补丁定期自动推送。

1. 代码安全审计与静态扫描

上线前进行 SAST/DAST 双重扫描；发现高危漏洞立即修复后方可发布。

**管理措施：**

1. 建立开发安全生命周期（SDL），将安全编码规范、漏洞检查纳入版本评审；
2. 制定补丁管理流程，关键补丁 48 小时内完成全量推送；
3. 运维变更工单与回滚策略必须包含安全回归测试记录；
4. 对所有上线应用保存源代码与变更记录，备份不少于两年。

## （五）安全监控与态势感知

**技术措施：**

1. 集中日志采集与留存

所有服务器、数据库、网络设备日志实时发送 SIEM；日志采用链式哈希防篡改，保留 ≥ 180 天。

1. 威胁情报与规则自动更新

IDS/IPS 与云端情报订阅接口对接，规则库每日自动同步；对0-day 攻击启用基于行为的检测引擎。

1. 安全事件联动阻断

配置 IDS/IPS 与防火墙 API，对高危事件实现 30 秒内自动封禁 IP 或账号；SOC 大屏实时展示安全态势热力图。

1. 异常检测与告警

建立机器学习模型，识别异常流量、异常时间段登录、内部横向移动等行为，识别后的告警信息通过短信/邮件/IM 多渠道推送至值班人员。

**管理措施：**

1. 制定《安全事件分级响应流程》，明确 T0/T1/T2 不同级别处置时限；
2. 安排 7×24 h 值守班表，关键时段需不少于两名安全分析员在线；
3. 每月输出《安全运营报告》，评估 IDS 告警命中率与误报率，持续调优；
4. 对重大告警进行 Root-Cause 分析并形成经验教训库。

## （六）安全管理体系

**技术措施：**

1. 堡垒机强制运维审计

所有生产环境登录必须经过堡垒机，录屏+命令双审计；高危操作需双人授权。

1. RBAC 权限模型落地

结合岗位矩阵，细化到系统、功能、数据三层级；按“先职位后权限”继承。

1. 自动化策略合规扫描

对服务器、数据库、网络设备定期执行基线合规检测，输出整改清单。

**管理措施：**

1. 完善《信息安全管理制度》《运维操作规范》，并在每季度安全例会审定更新；
2. 建立岗位职责矩阵，明确“谁审批、谁执行、谁复核”；
3. 开展年度安全培训与考试，覆盖新员工、在岗人员、外包人员；
4. 对严重违规操作实行问责，纳入绩效与奖惩体系。

## （七）应急响应与业务连续性

**技术措施：**

1. 建立双活或热备容灾架构

关键数据库采用双机热备；业务系统部署灾备节点，支持一键切换。

1. UPS 远程监控与告警

UPS 支持 SNMP 监控，电池健康度、温度、电量低下实时告警；配置自动关机脚本防止硬关机。

1. 自动化备份及恢复演练

数据日增量、周全量，本地+异地双份；

**管理措施**

1. 制定《信息安全应急预案》、《业务连续性计划》，细化角色分工、通知链路与决策权限；
2. 建立多部门联合应急演练机制（信息中心、医务科、后勤、电力）；
3. 定期评估应急资源（备用机房、备件、人员）可用性并补充；
4. 重大事件结束后 5 个工作日内完成事件复盘报告并更新预案。

# 参考文献

[1] 李洪民.浅谈网络安全等级保护信息建设方案[J].现代工业经济和信息化, 2016(13):4.DOI:10.16525/j.cnki.14-1362/n.2016.13.32.

[2] 顾敏.基于等级保护的移动应用安全评估体系研究[C]//第七届全国网络安全等级保护技术大会.中国电子科技集团公司第三研究所, 2018.

[3] 张弢,慕德俊,任帅,等.一种基于风险矩阵法的信息安全风险评估模型[J].计算机工程与应用, 2010, 46(5):3.DOI:10.3778/j.issn.1002-8331.2010.05.028.

[4] 阎春平,刘飞,郭风.数字化企业的信息安全体系及实施方案[J].重庆大学学报, 2010, 33(2):36-41.DOI:10.11835/j.issn.1000-582x.2010.02.006.

[5] 何伟.基于网络安全等级保护2.0的医院综合网络防护探究[J].网络安全技术与应用, 2020(9):3.DOI:CNKI:SUN:WLAQ.0.2020-09-072.

[6] 张旭辉.某民办高校网络信息安全方案的设计与实现[D].西安电子科技大学,2015.DOI:10.7666/d.D01065406.

# 附录

## 风险矩阵

**（1）安全事件发生可能性矩阵：**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 脆弱性严重程度/威胁发生频率 | 1 | 2 | 3 | 4 | 5 |
| 1 | 1 | 2 | 3 | 4 | 5 |
| 2 | 6 | 7 | 8 | 9 | 10 |
| 3 | 11 | 12 | 13 | 14 | 15 |
| 4 | 16 | 17 | 18 | 19 | 20 |
| 5 | 21 | 22 | 23 | 24 | 25 |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 安全事件发生可能性的值。 | 1-2 | 3-8 | 9-14 | 15-20 | 21-25 |
| 安全事件发生可能性的等级 | 1 | 2 | 3 | 4 | 5 |

**（2）安全事件影响矩阵**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 脆弱性严重程度/资产价值 | 1 | 2 | 3 | 4 | 5 |
| 1 | 1 | 3 | 6 | 11 | 16 |
| 2 | 2 | 5 | 10 | 15 | 17 |
| 3 | 4 | 9 | 14 | 16 | 20 |
| 4 | 7 | 13 | 15 | 19 | 23 |
| 5 | 12 | 14 | 18 | 21 | 25 |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 安全事件影响值 | 1-5 | 6-10 | 11-15 | 16-20 | 21-25 |
| 安全事件影响程度 | 1 | 2 | 3 | 4 | 5 |

**（3）风险矩阵**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 安全事件发生可能性/安全事件影响 | 1 | 2 | 3 | 4 | 5 |
| 1 | 1 | 3 | 5 | 7 | 9 |
| 2 | 2 | 4 | 6 | 8 | 10 |
| 3 | 11 | 13 | 15 | 17 | 19 |
| 4 | 12 | 14 | 16 | 18 | 20 |
| 5 | 21 | 22 | 23 | 24 | 25 |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 风险值 | 1-3 | 4-11 | 12-17 | 18-22 | 23-25 |
| 风险等级 | 1 | 2 | 3 | 4 | 5 |