**信息安全等级保护（二级）建设方案**

**2016年3月**

目录

[1. 项目概述 4](#_Toc446373342)

[1.1. 项目建设目标 4](#_Toc446373343)

[1.2. 项目参考标准 4](#_Toc446373344)

[1.3. 方案设计原则 6](#_Toc446373345)

[2. 系统现状分析 7](#_Toc446373346)

[2.1. 系统定级情况说明 7](#_Toc446373347)

[2.2. 业务系统说明 7](#_Toc446373348)

[2.3. 网络结构说明 7](#_Toc446373349)

[3. 安全需求分析 8](#_Toc446373350)

[3.1. 物理安全需求分析 8](#_Toc446373351)

[3.2. 网络安全需求分析 8](#_Toc446373352)

[3.3. 主机安全需求分析 9](#_Toc446373353)

[3.4. 应用安全需求分析 9](#_Toc446373354)

[3.5. 数据安全需求分析 9](#_Toc446373355)

[3.6. 安全管理制度需求分析 9](#_Toc446373356)

[4. 总体方案设计 9](#_Toc446373357)

[4.1. 总体设计目标 9](#_Toc446373358)

[4.2. 总体安全体系设计 10](#_Toc446373359)

[4.3. 总体网络架构设计 12](#_Toc446373360)

[4.4. 安全域划分说明 12](#_Toc446373361)

[5. 详细方案设计技术部分 13](#_Toc446373362)

[5.1. 物理安全 13](#_Toc446373363)

[5.2. 网络安全 13](#_Toc446373364)

[5.2.1. 安全域边界隔离技术 13](#_Toc446373365)

[5.2.2. 入侵防范技术 13](#_Toc446373366)

[5.2.3. 网页防篡改技术 14](#_Toc446373367)

[5.2.4. 链路负载均衡技术 14](#_Toc446373368)

[5.2.5. 网络安全审计 14](#_Toc446373369)

[5.3. 主机安全 15](#_Toc446373370)

[5.3.1. 数据库安全审计 15](#_Toc446373371)

[5.3.2. 运维堡垒主机 15](#_Toc446373372)

[5.3.3. 主机防病毒技术 16](#_Toc446373373)

[5.4. 应用安全 16](#_Toc446373374)

[6. 详细方案设计管理部分 16](#_Toc446373375)

[6.1. 总体安全方针与安全策略 17](#_Toc446373376)

[6.2. 信息安全管理制度 18](#_Toc446373377)

[6.3. 安全管理机构 18](#_Toc446373378)

[6.4. 人员安全管理 18](#_Toc446373379)

[6.5. 系统建设管理 19](#_Toc446373380)

[6.6. 系统运维管理 19](#_Toc446373381)

[6.7. 安全管理制度汇总 21](#_Toc446373382)

[7. 咨询服务和系统测评 22](#_Toc446373383)

[7.1. 系统定级服务 22](#_Toc446373384)

[7.2. 风险评估和安全加固服务 22](#_Toc446373385)

[7.2.1. 漏洞扫描 22](#_Toc446373386)

[7.2.2. 渗透测试 22](#_Toc446373387)

[7.2.3. 配置核查 22](#_Toc446373388)

[7.2.4. 安全加固 22](#_Toc446373389)

[7.2.5. 安全管理制度编写 24](#_Toc446373390)

[7.2.6. 安全培训 24](#_Toc446373391)

[7.3. 系统测评服务 24](#_Toc446373392)

[8. 项目预算与配置清单 25](#_Toc446373393)

[8.1. 项目预算一期（等保二级基本要求） 25](#_Toc446373394)

[8.2. 利旧安全设备使用说明 26](#_Toc446373395)

# 项目概述

## 项目建设目标

为了进一步贯彻落实教育行业信息安全等级保护制度，推进学校信息安全等级保护工作，依照国家《计算机信息系统安全保护等级划分准则》、《信息系统安全等级保护基本要求》、《信息系统安全保护等级定级指南》等标准，对学校的网络和信息系统进行等级保护定级，按信息系统逐个编制定级报告和定级备案表，并指导学校信息化人员将定级材料提交当地公安机关备案。

本方案中，通过为**满足物理安全、网络安全、主机安全、应用安全、数据安全**五个方面基本技术要求进行技术体系建设；为**满足安全管理制度、安全管理机构、人员安全管理、系统建设管理、系统运维管理**五个方面基本管理要求进行管理体系建设。使得学校信息系统的等级保护建设方案最终既可以满足等级保护的相关要求，又能够全方面为学校的业务系统提供立体、纵深的安全保障防御体系，保证信息系统整体的安全保护能力。

本项目建设将完成以下目标：

**1、以学校信息系统现有基础设施，建设并完成满足等级保护二级系统基本要求的信息系统，确保学校的整体信息化建设符合相关要求。**

**2、建立安全管理组织机构。成立信息安全工作组，学校负责人为安全责任人，拟定实施信息系统安全等级保护的具体方案，并制定相应的岗位责任制，确保信息安全等级保护工作顺利实施。**

**3、建立完善的安全技术防护体系。根据信息安全等级保护的要求，建立满足二级要求的安全技术防护体系。**

**4、建立健全信息系统安全管理制度。根据信息安全等级保护的要求，制定各项信息系统安全管理制度，对安全管理人员或操作人员执行的重要管理操作建立操作规程和执行记录文档。**

**5、制定学校信息系统不中断的应急预案。应急预案是安全等级保护的重要组成部分，按可能出现问题的不同情形制定相应的应急措施，在系统出现故障和意外且无法短时间恢复的情况下能确保生产活动持续进行。**

**6、安全培训：为学校信息化技术人员提供信息安全相关专业技术知识培训。**

## 项目参考标准

我司遵循国家信息安全等级保护指南等最新安全标准以及开展各项服务工作，配合学校的等级保护测评工作。本项目建设参考依据：

|  |  |
| --- | --- |
| 指导思想 | 中办[2003]27号文件（关于转发《国家信息化领导小组关于加强信息安全保障工作的意见》的通知）  公通字[2004]66号文件（关于印发《信息安全等级保护工作的实施意见》的通知）  公通字[2007]43号文件（关于印发《信息安全等级保护管理办法》的通知）  公信安[2009]1429《关于开展信息安全等级保护安全建设整改工作的指导意见》  全国人大《关于加强网络信息保护的决定》  国发[2012]23号《国务院关于大力推进信息化发展和切实保障信息安全的若干意见》  国发[2013]7号《国务院关于推进物联网有序健康发展的指导意见》  公信安[2014]2182号《关于加强国家级重要信息系统安全保障工作有关事项的通知》（ 公信安[2014]2182号） |
| 等级保护 | GB 17859-1999 计算机信息系统安全保护等级划分准则  GB/T25058-2010 信息系统安全等级保护实施指南 |
| 系统定级 | GB/T 22240-2008 信息安全技术 信息系统安全保护等级定级指南 |
| 技术方面 | GB/T25066-2010 信息安全产品类别与代码  GB/T17900-1999 网络代理服务器的安全技术要求  GB/T20010-2005 包过滤防火墙评估准则  GB/T20281-2006 防火墙技术要求和测试评价方法  GB/T18018-2007 路由器安全技术要求  GB/T20008-2005 路由器安全评估准则  GB/T20272-2006 操作系统安全技术要求  GB/T20273-2006 数据库管理系统安全技术要求  GB/T20009-2005 数据库管理系统安全评估准则  GB/T20275-2006 入侵检测系统技术要求和测试评价方法  GB/T20277-2006 网络和终端设备隔离部件测试评价方法  GB/T20279-2006 网络和终端设备隔离部件安全技术要求  GB/T20278-2006 网络脆弱性扫描产品技术要求  GB/T20280-2006 网络脆弱性扫描产品测试评价方法  GB/T20945-2007 信息系统安全审计产品技术要求和测试评价方法  GB/T 21028-2007 服务器安全技术要求  GB/T25063-2010 服务器安全侧评要求  GB/T 21050-2007 网络交换机安全技术要求（EAL3）  GB/T28452-2012 应用软件系统通用安全技术要求  GB/T29240-2012 终端计算机通用安全技术要求与测试评价方法  GB/T28456-2012 IPsec协议应用测试规范  GB/T28457-2012 SSL协议应用测试规范 |
| 管理方面 | GB/T20269-2006 信息系统安全管理要求  GB/T28453-2012 信息系统安全管理评估要求  GB/T20984-2007 信息安全风险评估规范  GB/T24364-2009 信息安全风险管理指南  GB/T20985-2007 信息安全事件管理指南  GB/T20986-2007 信息安全事件分类分级指南  GB/T20988-2007 信息系统灾难恢复规范 |
| 方案设计 | GB/T25070-2010 信息系统等级保护安全设计技术要求 |
| 等保测评 | GB/T28448-2012 信息系统安全等级保护测评要求  GB/T28449-2012 信息系统安全等级保护测评过程指南 |

## 方案设计原则

针对本次项目，等级保护整改方案的设计和实施将遵循以下原则：

* 保密性原则：我司对安全服务的实施过程和结果将严格保密，在未经用户方授权的情况下不会泄露给任何单位和个人，不会利用此数据进行任何侵害客户权益的行为；
* 标准性原则：服务设计和实施的全过程均依据国内或国际的相关标准进行；根据等级保护二级基本要求，进行分等级分安全域进行安全设计和安全建设。
* 规范性原则：我司在各项安全服务工作中的过程和文档，都具有很好的规范性（《南宁市学家科技有限公司安全服务实施规范》），可以便于项目的跟踪和控制；
* 可控性原则：服务所使用的工具、方法和过程都会在深信服与用户方双方认可的范围之内，服务进度遵守进度表的安排，保证双方对服务工作的可控性；
* 整体性原则：服务的范围和内容整体全面，涉及的IT运行的各个层面，避免由于遗漏造成未来的安全隐患；
* 最小影响原则：服务工作尽可能小的影响信息系统的正常运行，不会对现有业务造成显著影响。
* 体系化原则：在体系设计、建设中，深信服充分考虑到各个层面的安全风险，构建完整的立体安全防护体系。
* 先进性原则：为满足后续不断增长的业务需求、对安全产品、安全技术都充分考虑前瞻性要求，采用先进、成熟的安全产品、技术和先进的管理方法。
* 分步骤原则：根据用户方要求，对用户方安全保障体系进行分期、分步骤的有序部署。
* 服务细致化原则：在项目咨询、建设过程中深信服将充分结合自身的专业技术经验与行业经验相结合，结合用户方的实际信息系统量身定做才可以保障其信息系统安全稳定的运行。

# 系统现状分析

## 系统定级情况说明

学校综合考虑了学校信息系统、学校信息系统的业务信息和系统服务类型，以及其受到破坏时可能受到侵害的客体以及受侵害的程度，经学校省公安厅的批准，已将学校系统等级定为等级保护第二级（S2A2G2），整体网络信息化平台按照二级进行建设。

## 业务系统说明

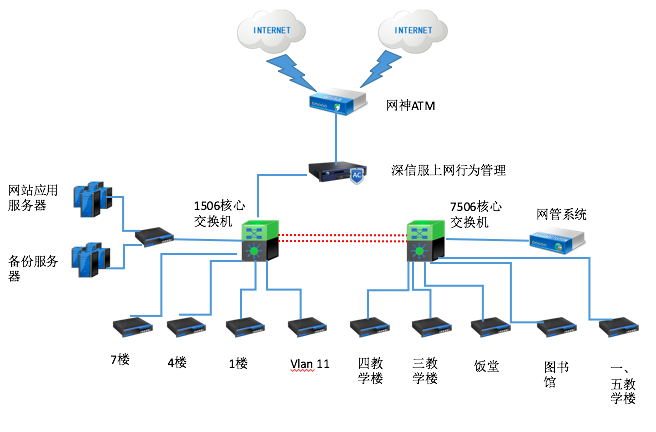
学校本次参加整改的共有X个信息系统，分别是学校系统、学校系统、学校系统、学校系统，具体情况介绍如下：

学校门户网站系统：2012年门户网站（网络版）历经系统开发、模拟测试、网络、硬件设备安装部署，在试点和实施过程当中发现系统仍有不足之处，需要对系统进行深入完善和改进，主要考虑到由于门户网站（网络版）作为学校集中部署的网络化重要业务系统，其具有应用面广、用户规模大，并涉及到学校对互联网形象，以及基于公众网上部署的特性，因此系统自身和运行环境均存在一定的安全风险，在数据传输、安全加密、网络监控、防入侵等方面的必须要建立一套更有效更完善的安全保护体系和措施。

学校OA系统：目前学校旧OA系统准备停用，并且已经开发和准备上线新的业务系统，新的业务系统目前准备对公网直接公开访问，因此涉及到的能够访问到业务系统的规模比较大，而且整个网络相对会比较复杂、流量多变，所以系统任有较多不足，在本次建设过程中应该加强安全建设，系统自身和运行环境均存在一定的安全风险，在数据传输、安全加密、网络监控、防入侵等方面的必须要建立一套更有效更完善的安全保护体系和措施。

## 网络结构说明

学校信息系统网络拓扑图现状如下：



# 安全需求分析

## 物理安全需求分析

目前在机房建设方面还存在如下问题：

1. 物理访问控制；
2. 防雷击；
3. 防火墙；
4. 防水防潮；
5. 温湿度控制；

## 网络安全需求分析

边界入侵防范：该信息系统无法实现对边界的访问控制，需要部署下一代署防火墙等安全设备来实现。

防web攻击和网页防篡改：该信息系统无法实现对边界的访问控制，需要部署下一代署防火墙等安全设备来实现。

安全域边界安全审计：该信息系统无法实现对边界的访问控制，需要部署署网络安全审计等安全设备来实现。

## 主机安全需求分析

主机防病毒：该信息系统缺少主机防病毒的相关安全策略，需要配置网络版主机防病毒系统，从而实现对全网主机的恶意代码防范。

数据库审计：该信息系统缺少针对数据的审计设备，不能很好的满足主机安全审计的要求，需要部署专业的数据库审计设备。

运维堡垒机：该该信息系统无法实现管理员对网络设备和服务器进行管理时的双因素认证，需要部署堡垒机来实现。

漏洞扫描：需要部署漏洞扫描实现对全网漏洞的扫描。

## 应用安全需求分析

通信完整性和保密性：该信息系统无法实现对边界的访问控制，需要部署SSL VPN等安全设备来实现。

## 数据安全需求分析

备份与恢复：该该信息系统没有完善的数据备份与恢复方案，需要制定相关策略。同时，该信息系统没有实现对关键网络设备的冗余，建议部署双链路确保设备冗余。

## 安全管理制度需求分析

根据前期差距分析结果，该单位还欠缺较多安全管理制度，需要后续补充。

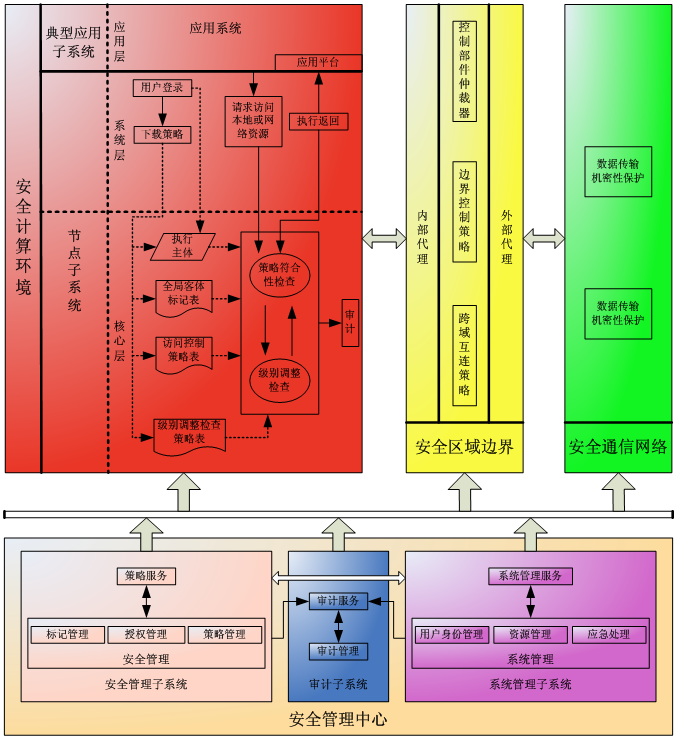
# 总体方案设计

## 总体设计目标

学校的安全等级保护整改方案设计的总体目标是依据国家等级保护的有关标准和规范，结合学校信息系统的现状，对其进行重新规划和合规性整改，为其建立一个完整的安全保障体系，有效保障其系统业务的正常开展，保护敏感数据信息的安全，保证学校信息系统的安全防护能力达到《信息安全技术 信息系统安全等级保护基本要求》中第二级的相关技术和管理要求。

## 总体安全体系设计

本项目提出的等级保护体系模型，必须依照国家等级保护的相关要求，利用密码、代码验证、可信接入控制等核心技术，在“一个中心三重防御”的框架下实现对信息系统的全面防护。整个体系模型如下图所示：



* **安全管理中心**

安全管理中心是整个等级保护体系中对信息系统进行集中安全管理的平台，是信息系统做到可测、可控、可管理的必要手段和措施。依照GB/T25070-2010 信息系统等级保护安全设计技术要求中对安全管理中心的要求，一个符合基于可信计算和主动防御的等级保护体系模型的安全管理中心应至少包含以下三个部分：

系统管理

实现对系统资源和运行的配置。控制和管理，并对系统管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行系统管理操作，并对这些操作进行审计。

安全管理

实现对系统中的主体、客体进行统一标记，对主体进行授权，配置一致的安全策略，确保标记、授权和安全策略的数据完整性，并对安全管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行安全管理操作，并进行审计。

审计管理

实现对系统各个组成部分的安全审计机制进行集中管理，包括根据安全审计策略对审计记录进行分类；提供按时间段开启和关闭相应类型的安全审计机制；对各类审计记录进行存储、管理和查询等；对审计记录应进行分析，根据分析结果进行处理。此外，对安全审计员进行身份鉴别，只允许其通过特定的命令或操作界面进行安全审计操作。

此外，安全管理中心应做到技术与管理并重，加强在安全管理制度、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方面的管理力度，规范安全管理操作规程，建立完善的安全管理制度集。

* **安全计算环境**

参照基于可信计算和主动防御的等级保护模型，安全计算环境可划分成节点和典型应用两个子系统。在解决方案中，这两个子系统都将通过终端安全保护体系的建立来实现。

信息安全事故的源头主要集中在用户终端，要实现一个可信的、安全的计算环境，就必须从终端安全抓起。因此，依照等级保护在身份鉴别，访问控制（包括强制访问控制）、网络行为控制（包括上网控制、违规外联的控制）、应用安全、数据安全、安全审计等方面的技术要求，可充分结合可信计算技术和主动防御技术的先进性和安全性，提出一个基于可信计算和主动防御的终端安全保护体系模型，以实现从应用层、系统层、核心层三个方面对计算环境的全面防护。

* **安全区域边界**

为保护边界安全，本解决方案针对构建一个安全的区域边界提出的解决手段是在被保护的信息边界部署一个“应用访问控制系统”。该系统应可以实现以下功能：信息层的自主和强制访问控制、防范SQL注入攻击和跨站攻击、抗DoS/DDoS攻击端口扫描、数据包过滤、网络地址换、安全审计等。由于国内外在这一方面的相关技术非常成熟，因此，在本次系统整改总体设计中更多的是考虑如何将防火墙、防病毒网关、网络安全审计系统、IDS、IPS、网管系统等有机地结合在一起，实现协同防护和联动处理。

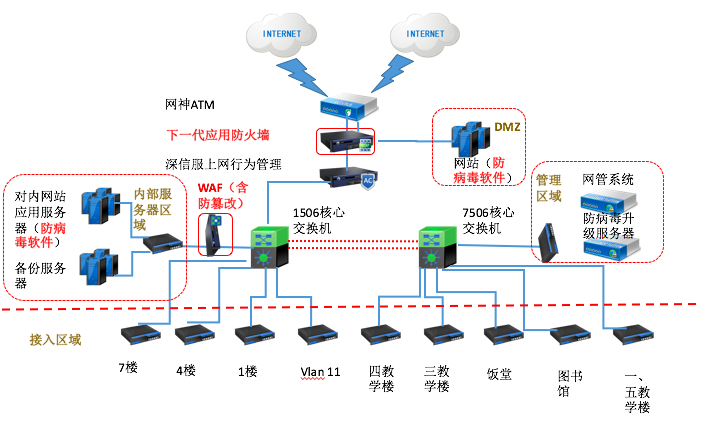
此外，对于不同安全等级信息系统之间的互连边界，可根据依照信息流向的高低，部署防火墙或安全隔离与信息交换系统，并配置相应的安全策略以实现对信息流向的控制。

* **安全通信网络**

目前，在通信网络安全方面，采用密码等核心技术实现的各类VPN都可以很有效的解决这类问题，达到在满足等级保护相关要求的同时，可灵活提高通信网络安全性的效果。

## 总体网络架构设计

学校网络架构整体设计如下：



## 安全域划分说明

安全域的划分是网络防护的基础，事实上每一个安全边界所包含的区域都形成了一个安全域。这些区域具有不同的使命，具有不同的功能，分域保护的框架为明确各个域的安全等级奠定了基础，保证了信息流在交换过程中的安全性。

在本项目中，将严格按照信息系统的重要性和网络使用的逻辑特性划分安全域，将划分如下确定的安全域：

* 互联网出口域，该区域说明如下：
* 专网出口域，该区域说明如下：主要承载互联网出口，出口主干需要部署相应的安全边界产品。
* 终端接入域，该区域说明如下：主要是无线和有线终端接入；
* 对外服务器域，该区域说明如下：该区域主要承载对外发布服务器，比如学校的网站；
* 内部服务器域，该区域说明如下：主要承载对内的服务器和存储，比如OA和学校专业先关零时性的试验服务器。
* 安全管理域，该区域说明如下：主要承载网络管理先关设备，比如网管系统，防病毒升级服务器等。

# 详细方案设计技术部分

## 物理安全

根据GB/T25070-2010 信息系统等级保护安全设计技术要求中物理安全的要求，应从以下方面进行整改：

## 网络安全

## 安全域边界隔离技术

根据《信息系统安全等级保护基本要求》，应该在学校各安全域的边界处部署防火墙设备，保证跨安全域的访问都通过防火墙进行控制管理。因此，在互联网出口域边界部署下一代防火墙，在内网服务器区域边界部署WEB应用防火墙。

## 入侵防范技术

根据等级保护基本要求，二级业务系统应该在互联网出口处实现入侵防范功能，因此，在互联网出口的下一代防火墙上启用入侵防御模块非常有必要。二级业务系统应该在互联网出口处部署网络层防病毒设备，并保证与主机层防病毒实现病毒库的异构。因此，在互联网出口的下一代防火墙上启用防病毒模块非常有必要。

## 网页防篡改技术

学校网站承载了学校等重要职责，暴露在互联网上，随时会面临网页被篡改及黑客攻击的危险，因此，在互联网出口的下一代防火墙上启用网页防篡改功能非常有必要。

## 链路负载均衡技术

根据等级保护基本要求，二级业务系统应该在互联网出口处进行优化控制，保证用户访问选择最优的链路。因此，建议在二期部署一套专业的链路负载均衡设备非常有必要。

## 网络安全审计

针对用户访问业务系统带给我们的困扰以及诸多的安全隐患，必须部署一套日志审计系统利用实时跟踪分析技术，从发起者、访问时间、访问对象、访问方法、使用频率各个角度，提供丰富的统计分析报告，帮助用户在统一管理互联网访问日志的同时，及时发现安全隐患，协助优化网络资源的使用。

根据公安部等级保护基本要求，所有信息系统都需要部署日志审计系统，并保存3个月的日志，学校拥有庞大的网络海量的数据交换，目前还没有部署日志审计系统。因此，建议在二期部署一套日志审计系统对全网行为进行监控、日志进行记录。

**部署设计：**

日志审计系统旁路部署在核心交换上，实现全网的网络行为的统一审计，收集网络设备、安全设备、主机系统等设备的运行状况、网络流量、用户行为等日志信息，并对收集到的日志信息进行分类和关联分析，并可根据审计人员的操作要求生成统计报表，方便查询和生成报告，为网络事件追溯提供证据。

## 主机安全

## 数据库安全审计

建议在二期部署数据库审计系统，实现对用户行为、用户事件及系统状态加以审计，范围覆盖到每个用户，从而把握数据库系统的整体安全。

**部署设计：**

数据库审计部署于数据库前端交换机上，通过端口镜像收集信息。

## 运维堡垒主机

对运维的管理现状进行分析，我们认为造成这种不安全现状的原因是多方面的，总结起来主要有以下几点：

* 各IT系统独立的帐户管理体系造成身份管理的换乱，而身份的唯一性又恰恰是认证、授权、审计的依据和前提，因此身份的混乱实际上造成设备访问的混乱。
* 各IT系统独立管理，风险分散在各系统中，各个击破困难大，这种管理方式造成了业务管理和安全之间的失衡。
* 核心服务器或设备的物理安全和临机访问安全通过门禁系统和录像系统得以较好的解决，但是对他们的网络访问缺少控制或欠缺控制力度，在帐号、密码、认证、授权、审计等各方面缺乏有效的集中管理技术手段。

目前，学校使用数量众多的网络设备、服务器主机来提供基础网络服务、运行关键业务、数据库应用、ERP和协同工作群件等服务。由于设备和服务器众多，系统管理员压力太大等因素，越权访问、误操作、滥用、恶意破坏等情况时有发生，这严重影响信息系统的运行效能，另外黑客的恶意访问也有可能获取系统权限，闯入部门内部网络，造成不可估量的损失。如何提高系统运维管理水平，跟踪服务器上用户的操作行为，防止黑客的入侵和破坏，提供控制和审计依据，降低运维成本，满足相关标准要求，越来越成为信息系统关心的问题，因此建议在学校二期安全建设有必要部署一套运维堡垒主机来实现账户的安全维护。

**部署设计：**

运维审计系统部署在安全管理域，通过交换机的访问控制策略限定只能由堡垒主机内控管理平台直接访问服务器的远程维护端口。维护人员对网络设备、安全设备和服务器系统进行远程维护时，首先以 Web 方式登录运维审计系统，然后通过运维审计系统上展现的访问资源列表直接访问授权资源。

## 主机防病毒技术

学校目前网络内所有终端使用免费的杀毒软件，基本满足等级保护二级的要求，但是现在主要服务器并没有部署专业的杀毒软件，建议第一期部署杀毒软件。

**部署设计**

软件客户端部署在内外防服务器上面，通过管理区域防病毒升级服务器对病毒规则库进行升级。

## 应用安全

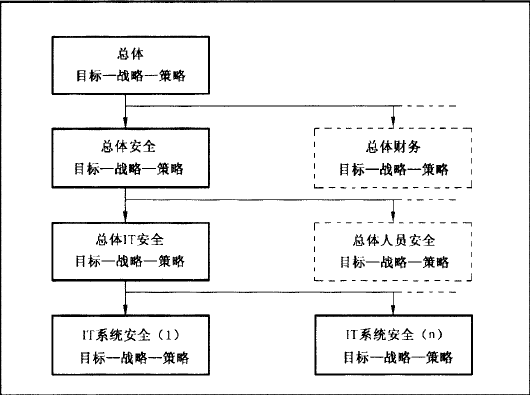
根据等级保护的要求，二级业务系统必须加密传输，因此需要部署SSL VPN技术实现应用系统远程访问的加密，如果后期OA系统需要实现出差老师或则在外网的人能够访问需要上SSL VPN设备。

**部署设计：**

SSL VPN旁路部署于核心交换机上。

# 详细方案设计管理部分

安全管理体系的作用是通过建立健全组织机构、规章制度，以及通过人员安全管理、安全教育与培训和各项管理制度的有效执行，来落实人员职责，确定行为规范，保证技术措施真正发挥效用，与技术体系共同保障安全策略的有效贯彻和落实。信息安全管理体系主要包括组织机构、规章制度、人员安全、安全教育和培训等四个方面内容。



## 总体安全方针与安全策略

总体安全方针与安全策略是指导用户方所有信息安全工作的纲领性文件，是信息安全决策机构对信息安全工作的决策和意图的表述。总体安全方针与安全策略的作用在于统一对信息安全工作的认识，规定信息安全的基本架构，明确信息安全的根本目标和原则。本次项目中深信服将协助用户方确定安全管理体系的层次及建立方式，明确各层次在安全管理体系中的职责以及安全策略，建立具有高可操作性的考核体系，以加强安全策略及各项管理制度的可落实性。

我方为用户方设计的总体安全方针与安全策略将具备以下特性：

* 安全策略紧紧围绕行业的发展战略，符合用户方实际的信息安全需求，能保障与促进信息化建设的顺利进行，避免理想化与不可操作性。
* 总体安全方针与安全策略中将明确阐述用户方所有信息化建设项目在规划设计、开发建设、运行维护和变更废弃等各阶段，应遵循的总体原则和要求。
* 安全策略在经过用户方信息安全决策机构批准之后，将具备指导和规范信息安全工作的效力。
* 安全策略中将规定其自身的时效性，当信息系统运行环境发生重大变化时，我方将协助用户方及时对总体安全策略进行必要的调整，并将调整后的策略提交用户方信息安全决策机构批准。

## 信息安全管理制度

根据安全管理制度的基本要求制定各类管理规定、管理办法和暂行规定。从安全策略主文档中规定的安全各个方面所应遵守的原则方法和指导性策略引出的具体管理规定、管理办法和实施办法，是具有可操作性，且必须得到有效推行和实施的制度。

制定严格的制定与发布流程，方式，范围等，制度需要统一格式并进行有效版本控制；发布方式需要正式、有效并注明发布范围，对收发文进行登记。

信息安全领导小组负责定期组织相关部门和相关人员对安全管理制度体系的合理性和适用性进行审定，定期或不定期对安全管理制度进行评审和修订，修订不足及进行改进。

## 安全管理机构

根据基本要求设置安全管理机构的组织形式和运作方式，明确岗位职责；

设置安全管理岗位，设立系统管理员、网络管理员、安全管理员等岗位，根据要求进行人员配备，配备专职安全员；成立指导和管理信息安全工作的委员会或领导小组，其最高领导由单位主管领导委任或授权；制定文件明确安全管理机构各个部门和岗位的职责、分工和技能要求。

建立授权与审批制度；

建立内外部沟通合作渠道；

定期进行全面安全检查，特别是系统日常运行、系统漏洞和数据备份等。

## 人员安全管理

人员安全管理主要包括人员录用、离岗、考核、教育培训等内容。

一般单位都有统一的人事管理部门负责人员管理，这里的人员安全管理主要指对关键岗位人员进行的以安全为核心的管理，例如对关键岗位的人员采取在录用或上岗前进行全面、严格的安全审查和技能考核，与关键岗位人员签署保密协议，对离岗人员撤销系统帐户和相关权限等措施。

只有注重对安全管理人员的培养，提高其安全防范意识，才能做到安全有效的防范，因此需要对各类人员进行安全意识教育、岗位技能培训和相关安全技术培训。培训的内容包括单位的信息安全方针、信息安全方面的基础知识、安全技术、安全标准、岗位操作规程、最新的工作流程、相关的安全责任要求、法律责任和惩戒措施等。

具体依据标准《基本要求》中人员安全管理，同时可以参照《信息系统安全管理要求》等。

## 系统建设管理

系统建设管理的重点是与系统建设活动相关的过程管理，由于主要的建设活动是由服务方，如集成方、开发方、测评方、安全服务方等完成，运营使用单位人员的主要工作是对之进行管理，应制定系统建设相关的管理制度，明确系统定级备案、方案设计、产品采购使用、软件开发、工程实施、验收交付、等级测评、安全服务等活动的管理责任部门、具体的管理内容和控制方法，并按照管理制度落实各项管理措施，完整保存相关的管理记录和过程文档。

具体依据标准《基本要求》中系统建设管理。

## 系统运维管理

1. 环境和资产安全管理制度

环境包括计算机、网络机房环境以及设置有网络终端的办公环境，明确环境安全管理的责任部门或责任人，加强对人员出入、来访人员的控制，对有关物理访问、物品进出和环境安全等方面作出规定。对重要区域设置门禁控制手段，或使用视频监控等措施。

资产包括介质、设备、设施、数据、软件、文档等，资产管理不等同于设备物资管理，而是从安全和信息系统角度对资产进行管理，将资产作为信息系统的组成部分，按其在信息系统中的作用进行管理。应明确资产安全管理的责任部门或责任人，对资产进行分类、标识，编制与信息系统相关的软件资产、硬件资产等资产清单。

具体依据标准《基本要求》中系统运维管理，同时可以参照《信息系统安全管理要求》等。

2、设备和介质安全管理制度

明确配套设施、软硬件设备管理、维护的责任部门或责任人，对信息系统的各种软硬件设备采购、发放、领用、维护和维修等过程进行控制，对介质的存放、使用、维护和销毁等方面作出规定，加强对涉外维修、敏感数据销毁等过程的监督控制。

具体依据标准《基本要求》中系统运维管理，同时可以参照《信息系统安全管理要求》等。

3、日常运行维护制度

明确网络、系统日常运行维护的责任部门或责任人，对运行管理中的日常操作、账号管理、安全配置、日志管理、补丁升级、口令更新等过程进行控制和管理；制订设备操作管理、业务应用操作管理、变更控制和重用管理、信息交换管理相应的管理制度；制定与信息系统安全管理相配套的规范和操作规程并落实执行；正确实施为信息系统可靠运行而采取的各种检测、监控、审计、分析、备份及容错等方法和措施，对运行安全进行监督检查。

具体依据标准《基本要求》中系统运维管理，同时可以参照《信息系统安全管理要求》等。

4、集中安全管理制度

第二级以上信息系统应按照统一的安全策略、安全管理要求，统一管理信息系统的安全运行，进行安全机制的配置与管理，对设备安全配置、恶意代码、补丁升级、安全审计等进行管理，对与安全有关的信息进行汇集与分析，对安全机制进行集中管理。

具体依据标准《基本要求》中系统运维管理，同时可以参照《信息系统等级保护安全设计技术要求》和《信息系统安全管理要求》等。

1. 事件处置与应急响应制度

按照国家有关标准规定，确定信息安全事件的等级。结合信息系统安全保护等级，制定信息安全事件分级应急处置预案，明确应急处置策略，落实应急指挥部门、执行部门和技术支撑部门，建立应急协调机制。落实安全事件报告制度，第二级以上信息系统发生较大、重大、特别重大安全事件时，运营使用单位按照相应预案开展应急处置，并及时向受理备案的公安机关报告。组织应急技术支撑力量和专家队伍，按照应急预案定期组织开展应急演练。

具体依据标准《基本要求》中系统运维管理，同时可以参照《信息安全事件分类分级指南》和《信息安全事件管理指南》等。

1. 灾难备份制度

要对第二级以上信息系统采取灾难备份措施，防止重大事故、事件发生。识别需要定期备份的重要业务信息、系统数据及软件系统等，制定数据的备份策略和恢复策略，建立备份与恢复管理相关的安全管理制度。

具体依据标准《基本要求》中系统运维管理和《信息系统灾难恢复规范》。

1. 安全监测制度

开展信息系统实时安全监测，实现对物理环境、通信线路、主机、网络设备、用户行为和业务应用等的监测和报警，及时发现设备故障、病毒入侵、黑客攻击、误用和误操作等安全事件，以便及时对安全事件进行响应与处置。

具体依据标准《基本要求》中系统运维管理。

8、其他制度

对系统运行维护过程中的其它活动，如系统变更、密码使用等进行控制和管理。按国家密码管理部门的规定，对信息系统中密码算法和密钥的使用进行分级管理。

## 安全管理制度汇总

制定安全检查制度，明确检查的内容、方式、要求等，检查各项制度、措施的落实情况，并不断完善。定期对信息系统安全状况进行自查，第二级系统每两年自查一次，第三级信息系统每年自查一次，第四级信息系统每半年自查一次。经自查，信息系统安全状况未达到安全保护等级要求的，应当进一步开展整改。

具体依据标准《基本要求》中安全管理机构，同时可以参照《信息系统安全管理要求》等。最终提交安全制度包括但不限于以下内容：

* 总体安全策略（组织、流程、策略、技术）
* 岗位安全责任制度
* 第三方安全管理制度
* 系统日常安全管理工作制度
* 系统安全评估管理办法
* 机房建设运行标准
* 安全区域划分及管理规定
* 管理信息区域网管制度
* 系统建设管理制度
* 设备入网安全管理制度
* 系统软件和补丁管理制度
* 备份与恢复管理制度
* 账号和口令及权限管理制度
* 介质管理
* 加密技术使用管理办法
* 应急预案管理制度
* 安全事件报告和处置管理制度
* 安全审计管理

# 咨询服务和系统测评

## 系统定级服务

协助用户单位，依据《信息系统安全等级保护定级指南》，确定信息系统的安全保护等级，准备定级备案表和定级报告，协助用户单位向所在地区的公安机关办理备案手续。

## 风险评估和安全加固服务

通过漏洞扫描、配置核查和渗透测试等技术手段发现系统中的漏洞，这些漏洞不能由安全设备解决，只能有安全加固解决。

### 漏洞扫描

利用业界领先的多种扫描工具检查整个网络内部网络的主机系统与数据库系统的漏洞情况，并用人工对扫描结果进行误报分析，结果整理。目标是发掘网络内部网络的安全漏洞，包括但不局限于：操作系统漏洞、网络设备漏洞、中间件漏洞、数据库漏洞、脆弱账户等，并提出漏洞修补建议

### 渗透测试

模拟黑客的真实攻击方法对系统和网络进行非破坏性质的攻击性测试，旨在发现目标系统这里，所有的渗透测试行为将在客户的书面明确授权和监督下进行。通过远程渗透测试全面检测信息系统清单中的系统（网站）直接暴露在互联网上的安全隐患，并提供实际可行的安全修复建议。

### 配置核查

通过配置核查工具和安全专家人工检查想结合的方式，逐项检查系统的各项配置和运行状态，评估对象应包括各主机的操作系统、网络设备和数据库，并出具评估报告。

### 安全加固

根据漏洞扫描、配置核查和渗透测试的结果，对用户单位提供安全加固建议（包括主机安全加固、网络设备安全加固服务、安全设备安全加固优化服务、数据库系统安全加固服务、管理制度完善），并对具体的安全加固提供指导咨询。

主机安全加固

主要对用户单位所有主机系统（含虚拟机）进行安全加固，内容如下:

* 检查主机系统的补丁管理；
* 账号及口令策略；
* 网络与服务
* 文件系统；
* 日志审核；
* 防火墙策略；
* 系统钩子；
* 木马、后门及rookit；
* 安全性增强；

网络安全加固

主要对用户单位所涉及的网络设备进行安全加固，内容如下:

* 网络设备的补丁管理及版本；
* 账号及口令策略；
* 访问控制；
* 网络与服务；
* 日志审核

信息安全设备加固

安全设备是否配置最优，实现其最优功能和性能，保证网络系统的正常运行、是否存在漏洞或后门、自身的保护机制是否实现、检查安全设备的补丁管理、账号及口令策略、访问控制、网络与服务、日志审核，主要内容如下：

* 关闭不必要系统服务
* 开启系统各项审计功能
* 配置账号、组策略
* 配置注册表相应的安全项
* 配置文件系统的权限
* 评估新补丁对操作系统及应用系统的影响，在不影响系统正常使用的情况下，升级系统补丁
* 升级防病毒软件的版本

数据库系统安全加固

数据库系统主要从系统版本、用户账号、口令管理、传输情况、文件系统、日志审核等方面进行安全加固，主要内容如下：

* 数据库组件安装优化
* 适度应用数据库补丁程序
* 数据库服务运行权限改善
* 清理数据库默认配置无用账号
* 改善程序包权限设置
* 改善登录认证方式设置
* 改善传输加密协议配置
* 设置客户端连接IP限制策略
* 禁用Extproc功能
* 清理不必要的存储过程
* 增强数据库日志审计功能

### 安全管理制度编写

为用户单位完成编写信息安全管理制度，并保障该制度适合客户方的需求，以及便于落地。具体制度详细见详细方案设计管理部分。

### 安全培训

根据用户单位要求，除了提供产品方面培训，将着重定制化与日常工作相关的安全培训,具体的培训内容将根据客户提出的要求具体执行。

## 系统测评服务

为用户选择满足国家要求的测评机构（在本省等包办推荐目录下且在本省备案的测评机构），完成对用户单位信息系统的等级保护测评。

# 项目预算与配置清单

## 项目预算一期（等保二级基本要求）

请参照附表

## 利旧安全设备使用说明

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **产品** | **部署位置** | **利旧说明** |
|  | 网神SecGate 3600 | 互联网出口路由部署 | 用于访问控制 |
|  | 深信服上网行为管理 | 互联网出口透明部署 | 用于应用访问控制，流量管理和网络行为审计 |
|  | 网管系统 | 安全管理区域 | 网络管理 |