信息安全等级保护(二级）建设方案

201 6 年 3 月

目录

1. 项目概述

1.1. 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。

1.2.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 17859-1 999 计算机信息系统安全保护等级划分准则 GB/T2 5058-2010 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/T 28452-2012 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

1.3.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。

2. 系统现状分析

2.1. 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。

2.2. 业务系统说明

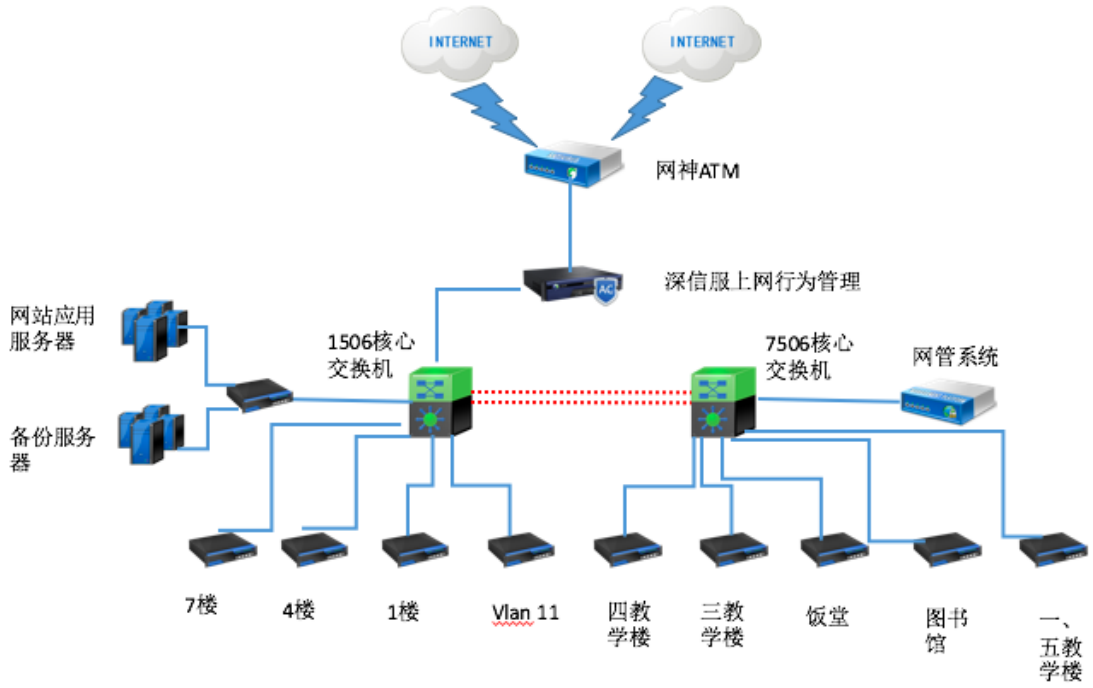
学校本次参加整改的共有 X 个信息系统,分别是学校系统、学校系统、学校系统、学校系统,具体情况介绍如下：

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。

2.3. 网络结构说明

学校信息系统网络拓扑图现状如下:



3. 安全需求分析

3.1. 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;

3.2. 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。

3.3. 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。

3.4. 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 S SL VPN 等安全设备来实现。

3.5. 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。

3.6. 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。

4. 总体方案设计

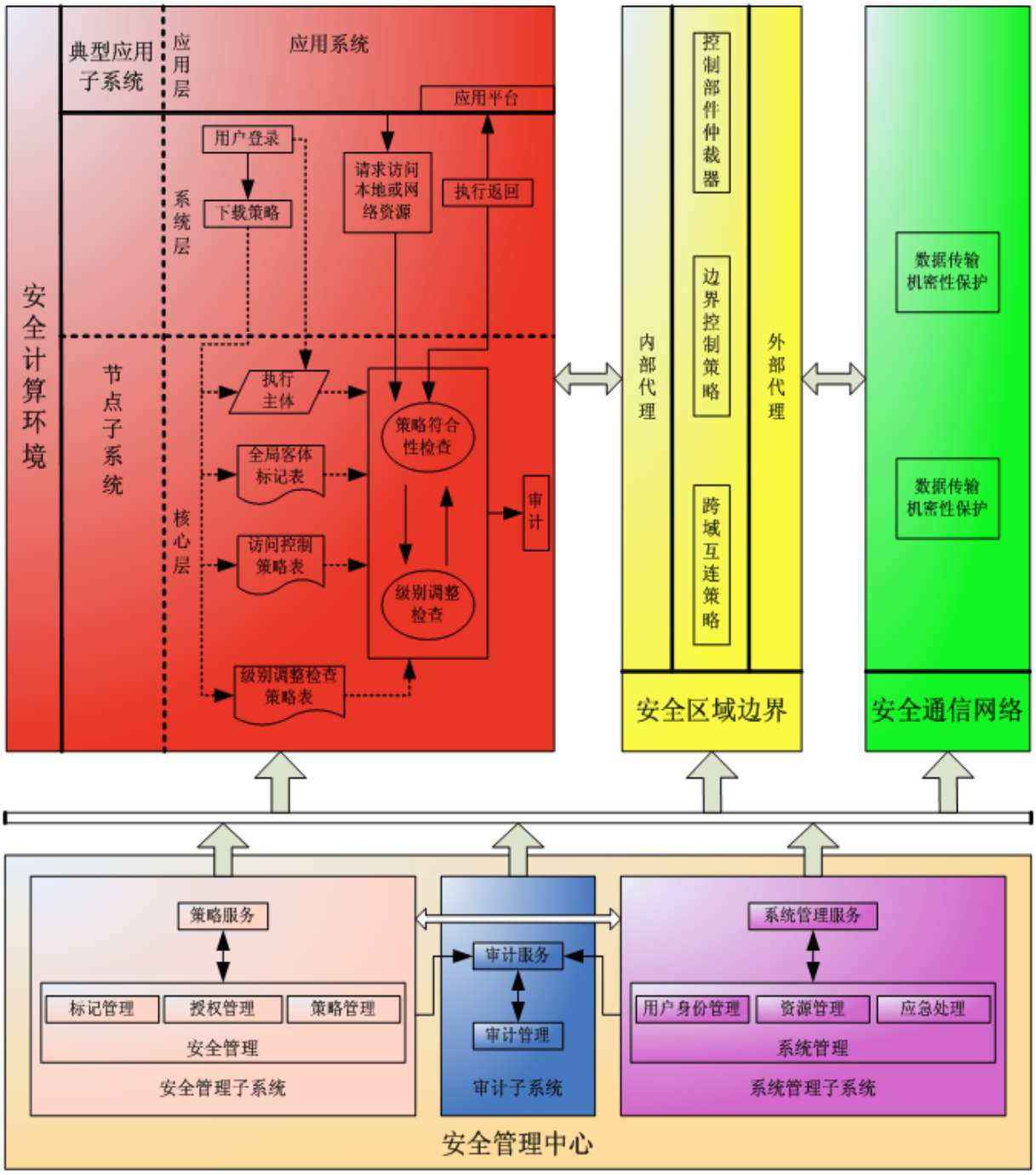
4.1. 总体设计目标

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。

--

4.2. 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。