山西药科职业学院

网络安全等级保护建设方案

安洽科技
ANQIA TECHNOLOGY CO.,LTD

www.anqia.com

版本：V1.0

2020 年 10 月

目　　录

一、前言 1

1.1 安全形势 1

1.2 安全现状 2

1.2.1 网站缺乏安全防护与审计 ..... **错误!未定义书签。**

1.2.2 业务系统缺乏安全防护与审计 3

1.2.3 缺少系统的病毒防护措施 3

1.3 等级保护 4

二、安全设计 5

2.1 安全模型 5

2.2 安全框架 6

2.3 安全体系 7

2.4 设计原则 8

三、安全目标 ..... **错误!未定义书签。**

3.1、健全安全防护体系 ..... **错误!未定义书签。**

3.2、筑牢等级保护基础 ..... **错误!未定义书签。**

3.3、提升威胁感知能力 ..... **错误!未定义书签。**

3.4、增强安全响应能力 ..... **错误!未定义书签。**

3.5、强化安全风险意识 ..... **错误!未定义书签。**

四、服务亮点 ..... **错误!未定义书签。**

五、安全规划 9

5.1 建设概述 9

5.2 安全产品 10
5.3 分析平台 ..... **错误!未定义书签。**
5.4 建设价值 10
六、安全服务 ..... **错误!未定义书签。**
6.1、资产统计服务 ..... **错误!未定义书签。**
6.2、安全设备巡检 ..... **错误!未定义书签。**
6.3、安全渗透测试 ..... **错误!未定义书签。**
6.4、安全防护加固 ..... **错误!未定义书签。**
6.4.1、操作系统加固 ..... **错误!未定义书签。**
6.4.2、密码复杂性检查 ..... **错误!未定义书签。**
6.4.3、漏洞防护与修复 ..... **错误!未定义书签。**
6.4.4、文件上传防护 ..... **错误!未定义书签。**
6.4.5、防暴力破解 ..... **错误!未定义书签。**
6.4.7、远程登录防护 ..... **错误!未定义书签。**
6.4.7、抗 CC 攻击 ..... **错误!未定义书签。**
6.5、持续性服务 ..... **错误!未定义书签。**
6.5.1、安全巡检 ..... **错误!未定义书签。**
6.5.2、应急处置 ..... **错误!未定义书签。**
6.5.3、安全值守 ..... **错误!未定义书签。**
6.5.4、技术咨询 ..... **错误!未定义书签。**
6.5.6、业务迁移 ..... **错误!未定义书签。**
6.5.6、安全预警 ..... **错误!未定义书签。**

6.5.7、应急演练.....**错误!未定义书签。**

6.6、网络安全培训.....**错误!未定义书签。**

七、预算清单.....11

八、方案总结.....12

一、前言

1.1 安全形势

随着信息技术日新月异的发展，各行业在信息化应用和要求方面逐步提高，信息网络覆盖面也越来越大，网络的利用率稳步提高，利用网络技术与业务系统相结合，可有效地提高工作效率。然而信息化技术给我们带来便利的同时，各种网络与信息系统安全问题也逐渐暴露出来，由于计算机网络所具有多样性、开放性、互连性等的特点，造成网络易受攻击，有来自黑客，也有其他诸如计算机病毒等形式的攻击，具体的攻击是多方面的。

从国家层面上来看，中国在现代化发展的过程当中，一直非常重视网络安全方面的建设工作。

2014 年 2 月 27 日，中央网络安全与信息化领导小组正式成立，由习近平总书记任组长，并且伴随着中央网络安全与信息化领导小组的成立，国家相继制定了相应的工作规范制度，习总书记也在“419 讲话”中强调“没有网络安全就没有国家安全”。

2003 年 9 月，中共中央颁布了《国家信息化领导小组关于加强信息安全保障工作的意见》（中办发【2003】27 号文件），提出要在 5 年内建设中国信息安全保障体系。

2004 年 9 月，公安部、国家保密局、国家密码管理委员会办公室、国务院信息化工作办公室联合颁布了《关于信息安全等级保护工作的实施意见》（公通字【2004】66 号文件），明确了信息安全等级保护的基本原则、基本内容、职责分工和实施计划。

2007 年 6 月,《信息安全等级保护管理办法》(公通字【2007】43 号文件) 正式出台,文件对国家关于信息安全等级化的相关政策、标准和规范作出了详细说明。

2017 年 6 月《中华人民共和国网络安全法》颁布，明确要求各业务系统需要按照信息安全等级保护标准建设。

2020 年，网络安全形势已然更加复杂，网络攻击手段更为多样，尤其受新冠肺炎影响，各类安全事件频发。根据公安部门有关数据显示，今年出现了各种新型网络攻击：电脑版“新型冠状病毒”悄然蔓延、无文件勒索病毒开始传播、境外黑客组织攻击我国视频监控网络、某厂商设备多个 0day 漏洞的爆发、51 万台路由器和物联网设备的 Telnet 账号密码泄露、APT 组织已利用“双星”漏洞开展攻攻击。

从国家层面来说,为了更有效的抵御当前复杂的网络入侵攻击、全面提升我国关键信息基础设施的网络安全防护能力,公安部及省、市各级公安机关每年的年中都会以实战攻防的形式开展网络演习工作。

2020 年，由于新冠疫情的影响，相较 2019 年的攻防演习活动时间稍有推迟，但仍旧会照常组织开展，而演习的重点目标就包括了军事、政府、金融、能源、医疗、通讯等重要行业领域,这就对单位自身的网络安全能力提出了更为严格的要求。

1.2 安全现状

近年来,国内各级高校对于信息化建设的重视程度日渐提高,但是就目前的情况来看，对于信息化发展过程中的安全性问题考虑却并不是特别周全。

大部分高校虽然都已经进行了高校信息化建设,但是在信息安全管理方面的意识和管理水平还存在严重的不足之处,部分高校在建设了信息化之后,仍然采用传统的管理方式,对于信息化建设管理非常不利。高校必须加强对信息安全问题的重视和对信息化建设的安全管理,若不加强信息管理。高校大学生极强的人员流动性、学校网络的应用非限制性都将使高校的信息管理系统和学校各项信息数据面临毁坏和泄露的威胁。

1.2.1 业务系统缺乏安全审计

随着山西药科职业学院校园网信息化的逐步深入，教学业务系统逐渐增多，教学信息管理系统等信息化业务系统均已逐步上线运行,而这些系统由于管理及防护不到位，面临着较严重的安全威胁：

1）业务系统缺乏必要的安全手段，随着学校网络规模扩张迅速，网络带宽及处理能力都有很大的提升,但是管理和维护人员方面的投入明显不足,没有条件管理和维护内部计算机的安全，一旦受到黑客攻击，无法及时发现攻击源；

2）校园网数据中心内的系统应用众多、服务器众多，管理及维护方式也不尽相同，无法做到所有的系统实施统一的漏洞管理政策；

3）对于存在安全隐患的配置检查，缺乏自动化的高运维监控手段；

4）业务系统的访问权限控制不合理，有很大的安全隐患。

1.2.2 缺少系统的病毒防护措施

2017 年 5 月份开始爆发的勒索病毒席卷全国，高校成为重灾区，不仅是电脑，被高校中的电子屏、阅览室也都成为勒索病毒攻击的对象，一时间高校纷纷谈“毒”变色。

网络在提供给大家的方便的同时，也变成了病毒传递的最快捷的途径。随着网络飞速发展、网络病毒的编制者水平的提高以及近几年网络病毒和黑客软件的结合，网络病毒的爆发直接导致用户的隐私和重要数据外泄。同时还极大的消耗了网络资源；造成网络性能急剧下降；从近期的“勒索病毒”、“挖矿木马”等网络恶意代码的爆发中可以看出，网络病毒的防范任务越来越严峻。而病毒防范的措施也不能仅仅靠原来单机的方式，必须是一种集中管理，统一升级，统一监控的针对网络的防病毒体系。

1.3 等级保护

网络安全等级保护制度是国家网络安全领域的基本国策、基本制度和基本方法，地位特殊，意义重大。网络安全等级保护制度从 2007 年大规模开展至今已有十二年，开展前还在社会各界大力支持下进行了十几年的研究工作，它是中国网络安全保障工作的伟大创举，是维护国家安全、社会秩序和公共利益的根本保障。依据网络安全等级保护制度开展网络安全等级保护工作是保护信息化发展、维护网络安全的根本保障，是网络安全保障工作中国家意志的体现。

2019 年 5 月 13 日，网络安全等级保护制度 2.0 版本（简称等保 2.0）正式公开发布，等保 2.0 覆盖大数据、云计算等新技术新应用，为全面落实信息系统安全工作提供了方向和依据。

为了顺应当前信息技术的发展和网络安全形势的变化，等级保护 2.0 标准在 1.0 的基础上，更加注重全方位的主动防御、动态防御、整体防控和精准防护，实现了对云计算、大数据、物联网、移动互联和工业控制信息系统等保护对象的全覆盖，以及除个人及家庭自建网络之外的领域全覆盖。

因此，为了适应当前国际化的信息安全形势，我国网络安全等级保护制度体系化建设做出了进一步完善，这同时也对信息系统的运营者、尤其是关键信息基础设施的运营单位，提出了更高的安全建设要求。

二、安全设计

2.1 安全模型

我们选择 P2DR 安全模型为本次方案的支撑模型，该模型从 Policy(策略)、Protection(防护)、Detection(检测)和 Response(响应)四个方面，对安全建设的全过程进行了阶段性划分，在整体的安全策略的控制和指导下，综合运用安全防护手段(如防火墙、入侵防御、通信加密等)的同时，利用安全检测技术(如漏洞评估、入侵检测等)了解和评估系统的安全状态，通过适当的反应将系统调整到“最安全”和“风险最低”的状态。防护、检测和响应组成了一个完整的、动态的安全循环，在安全策略的指导下保证信息系统的安全，能够满足本次方案实施的总体安全规划需求。

（1）策略：定义系统的监控周期、确立系统恢复机制、制定网络访问控制策略和明确系统的总体安全规划和原则。

（2）防护：通过修复系统漏洞、正确设计开发和安装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脆弱性；通过培训等手段，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、监视等手段来防止恶意威胁。采用的防护技术通常包括数据加密、身份认证、访问控制、授权和虚拟专用网（VPN）技术、防火墙、安全扫描和数据备份等。

（3）检测：是动态响应和加强防护的依据，通过不断地检测和监控网络系统，来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。当攻击者穿透防护系统时，检测功能就发挥作用，与防护系统形成互补。

（4）响应：系统一旦检测到入侵，响应系统就开始工作，进行事件处理。响应包括紧急响应和恢复处理，恢复处理又包括系统恢复和信息恢复。

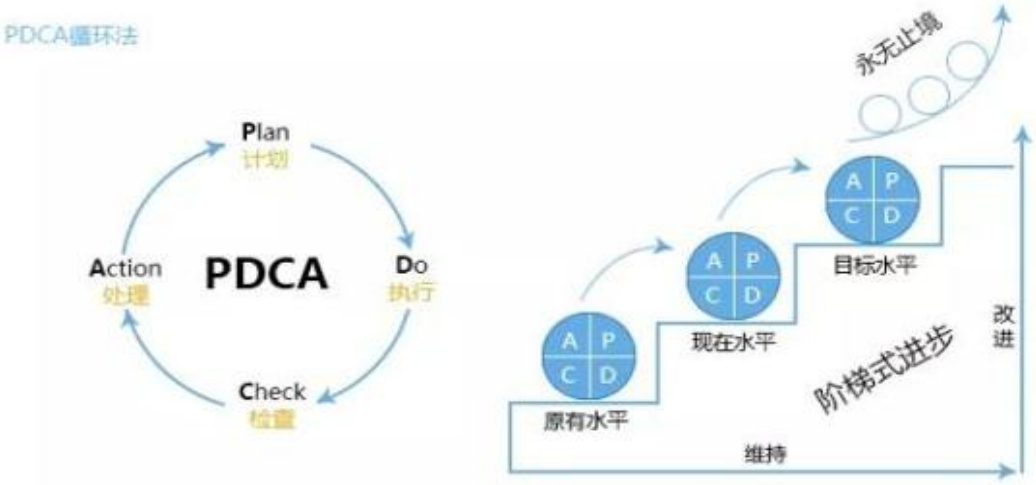
2.2 安全框架

针对总体安全框架的设计，我们将根据现有信息系统信息化建设的实际需求，同时结合新的安全形势下等保 2.0 标准指出的“一个中心，三重防护”的整体安全防护理念，针对现有信息系统的安全管理中心、计算环境安全、区域边界安全和通信网络安全进行安全合规的总体框架设计，建立以计算环境安全为基础，以区域边界安全、通信网络安全为保障，以安全管理中心为核心的信息安全整体保障框架体系，并且通过安全监测预警、安全主动防御、及时安全响应、有效安全恢复的技术手段，努力将信息系统构建成具备主动防御、多级防护、纵深防控、整体保护能力的安全、可靠信息系统。

2.3 安全体系

安全体系化建设，通常需要从信息安全组织体系、管理体系、技术体系三个方面着手建立统一的安全保障体系，力保网络信息安全；组织体系着眼于人员组织架构，像岗位设置、职责授权、人员任用、绩效考核等；管理体系侧重在制度的梳理，制定安全计划并持续改进，制定运行、维护、监控制 度，明确审计的内容和程序等；技术体系分成准备、预防、检测、保护、响应、监控、评价七个阶段，根据用户需求采用相应的安全防护技术。

安全体系化建设必须遵循 PDCA 原则，即计划(Plan)、实施(Do)、检查(Check)、调整(Adjustment)，不断改善，重点遵循等保、分域管理、应急响应。



三、设计原则

1、等级保护标准性原则

构建信息系统的安全防护体系，必须坚持遵循相关的安全标准，本方案从设计到产品选型都以国家网络安全等级保护相关标准为设计原则。

2、需求、风险、代价平衡的原则

我们将针对网络现状及安全需求进行实际分析(包括任务、性能、结构、可靠性、可用性、可维护性等)，并对网络面临的威胁及可能承担的风险进行定性与定量相结合的分析，然后制定规范和措施，确定安全策略。

3、综合性、整体性、易操作性原则

完整信息系统的整体安全性取决于其中安全防范最薄弱的一个环节，必须提高整个信息系统的安全性以及系统中各个环节之间的严密安全逻辑关联的强度，才能保证组成安全防护体系的各个位置间协调一致地运行。安全措施则需要人为去完成，因此必须满足易操作性原则，措施过于复杂，对人的要求过高，本身就降低了安全性。

4、先进性、成熟性与无缝接入原则

安全产品的选择，既要考虑先进性，还要考虑产品的技术成熟性。先进意味着技术、性能方面的优越，而成熟性表示可靠与可用。同时，安全产品的部署、运行，应不改变网络原有的拓扑结构，并且不会对网络传输造成通信“瓶颈”。

5、保护原有投资原则

进行信息安全防护体系建设时，应充分考虑原有投资，充分利用已有的信息化建设基础、安全产品、防护措施，统一规划信息化建设的整体安全体系和灾难恢复系统。

四、安全规划

网络安全等级保护安全保护环境的设计目标是：落实《信息安全技术 网络安全等级保护基本要求》对信息系统的安全保护要求，在安全保护环境的基础要求上，通过实现基于安全策略模型和标记的强制访问控制以及增强系统的审计机制，使得系统具有在统一安全策略管控下，保护敏感资源的能力。

我们严格依照国家网络安全等级保护的相关标准，通过满足物安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心五个方面的基本技术要求进行技术体系建设，满足安全管理制度、安全管理机构、安全管理人员、安全建设管理、安全运维管理五个方面基本管理要求进行管理体系建设，使得建设完成后的信息系统最终既可以满足网络安全等级保护的相关要求，又能够全方面为单位的业务系统提供立体、纵深的安全保障防御体系。

5.1 建设概述

（1）针对整个核心业务系统区域的安全审计和运维，主要通过采用以下的防护措施：部署**日志审计系统**，对网络系统内的各类设备的日志信息（服务器、网络设备、操作系统系统等）进行统一的管理和安全分析，并能够实现对日志信息六个月以上的留存；通过部署**运维堡垒主机**，对网络设备和服务器设备的访问连接进行访问过程的记录留存与审计，便于意外发生时的追踪溯源使用；上述审计设备全部采用旁路部署，旁挂在核心交换机上。

（2）从终端安全与主机安全的层面来说，建议在终端电脑与服务器中安装**网络版杀毒软件**，并选用一台独立的服务器部署杀毒软件的**统一控制中心**，对网络杀毒软件进行统一的管理，提升系统整体的防病毒能力。

5.2 安全产品

序号	产品	数量	功能	备注
1	日志审计系统	1 台	集中采集信息系统中的系统安全事件、用户访问记录、系统运行日志、系统运行状态等各类信息，经过规范化、过滤、归并和告警分析等处理，实现对日志的全面审计	等保三级安全管理中心建设要求旁路部署
2	运维堡垒主机	1 台	实时收集和监控网络环境中每一个组成部分的系统状态、安全事件、网络活动	等保三级安全管理中心建设要求旁路部署
3	网络版杀毒软件	1 套	统一防护信息系统内的恶意代码和网络病毒	等保三级安全计算环境建设要求需要服务器上部署杀毒控制中心

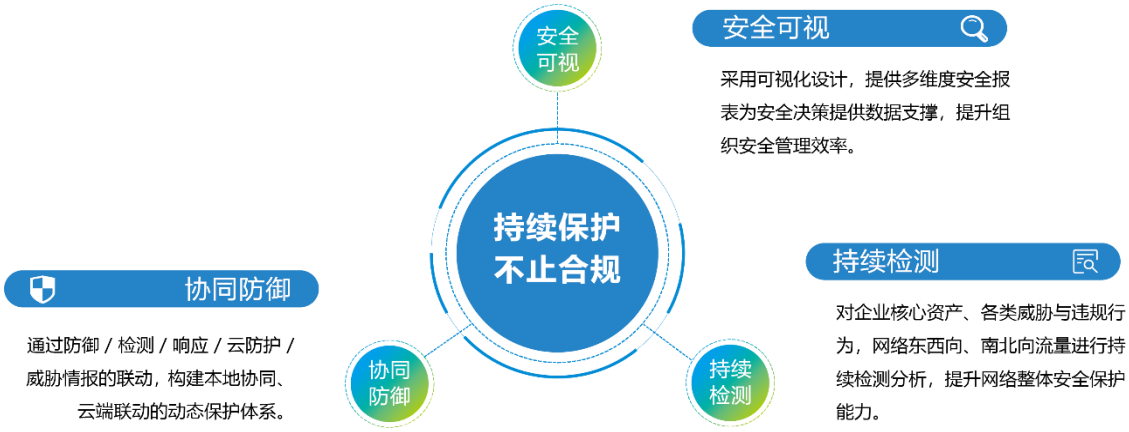
5.3 建设价值

符合行业需求，体现组织利益，投资节省，实现重点保护

我们的等级保护整改建设方案，结合业内信息安全最佳实践，形成了一套以安全策略为核心，以组织保障为基础，以技术措施为工具，以运行维护为支撑的等级保护方法论。在满足国家等级保护政策前提下，结合业务需求保障信息系统安全可靠，不仅合规，还要简单有效，体现组织利益，投资节省，实现重点保护。

体系化精细化安全优化，全面提高信息安全保障水平

以等级保护为标准开展安全建设，可以让安全建设更加体系化精细化，通过从物理、网络、主机、应用和数据等多个方面成体系地进行安全建设，打破了传统头痛医头、脚痛医脚的建设状况，对单位的安全建设提出整体的规划和思路。通过等级保护整改建设，发现单位系统内部存在的安全隐患和不足，通过安全整改之后，全面提高信息系统的信息安全防护能力，降低系统被各种攻击的风险。



五、方案总结

山西安洽科技股份有限公司是以软件研发、网络安全服务及安全产品集成为一体的高科技公司，同时也是公安部第一研究所山西服务中心、山西省网络安全协会理事单位 、太原市互联网协会副会长单位。

公司目前致力于传统信息服务和信息安全的资源技术整合，公司拥有专业的软件研发、安全服务、系统集成技术团队，已拥有中国网络安全审查技术与认证中心（CCRC）颁发的风险评估、安全集成、安全运维资质，获得了质量管理体系认证、高新技术企业认证、3A 级诚信示范单位认证与软件企业认证，并已承接多项相关项目。


CCRC

信息安全服务资质认证证书

证书编号:CCRC-2017-ISV-SI-561

兹证明

山西安洽科技股份有限公司

统一社会信用代码:911401006666324859

的信息系统安全集成服务资质符合

CCRC-ISV-C01:2018《信息安全服务 规范》

三级服务资质要求。

注册地址：山西综改示范区太原学府园区东渠路西二巷6号智创城A座1708-1710室

办公地址：山西综改示范区太原学府园区东渠路西二巷6号智创城A座1708-1710室

颁证日期：2017年4月20日　　有效期至：2021年4月19日

中国网络安全审查技术与认证中心

中国·北京·朝外大街甲10号（100020）　www.isccc.gov.cn　证书通过此网站查询

S 005824


CCRC

信息安全服务资质认证证书

证书编号:CCRC-2017-ISV-RA-207

兹证明

山西安洽科技股份有限公司

统一社会信用代码:911401006666324859

的信息安全风险评估服务资质符合

CCRC-ISV-C01:2018《信息安全服务 规范》

三级服务资质要求。

注册地址：山西综改示范区太原学府园区东渠路西二巷6号智创城A座1708-1710室

办公地址：山西综改示范区太原学府园区东渠路西二巷6号智创城A座1708-1710室

颁证日期：2017年4月20日　　有效期至：2021年4月19日

中国网络安全审查技术与认证中心

中国·北京·朝外大街甲10号（100020）　www.isccc.gov.cn　证书通过此网站查询

S 006184


高新技术企业

证书

企业名称：山西安洽科技有限责任公司　　证书编号：GR201714000413

发证时间：2017年11月09日　　有效期：三年

批准机关：


软件企业证书

经评估，山西安洽科技股份有限公司　　符合《进一步鼓励软件产业和集成电路产业发展的若干政策》和《软件企业评估标准》（T/SIA002 2017）的有关规定，评估为软件企业，特发此证。

证书编号：晋RQ-2019-0047

有效期：一年

评估机构：山西软件产业协会

日期：2019-09-05


CCRC

信息安全服务资质认证证书

证书编号:CCRC-2020-ISV-SM-1015

兹证明

山西安洽科技股份有限公司

统一社会信用代码:911401006666324859

的信息系统安全运维服务资质符合

CCRC-ISV-C01:2018《信息安全服务 规范》

三级服务资质要求。

注册地址：山西综改示范区太原学府园区东渠路西二巷6号智创城A座1708-1710室

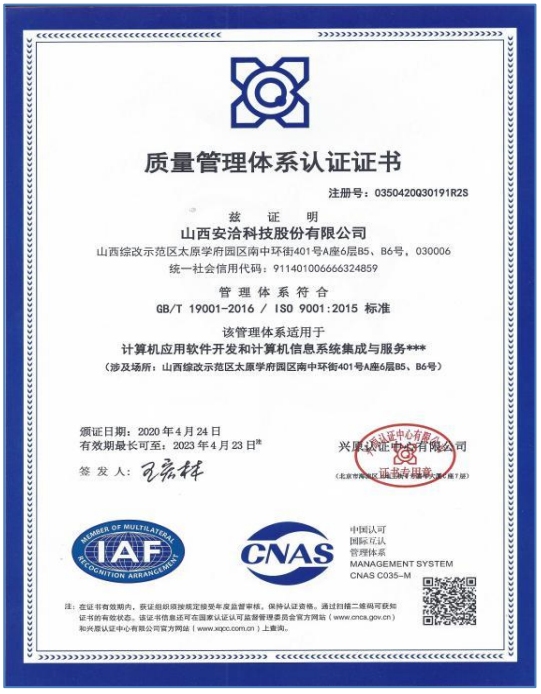
办公地址：山西综改示范区太原学府园区东渠路西二巷6号智创城A座1708-1710室

颁证日期：2020年5月21日　　有效期至：2021年5月20日

中国网络安全审查技术与认证中心

中国·北京·朝外大街甲10号（100020）　www.isccc.gov.cn　证书通过此网站查询

S 005825


质量管理体系认证证书

注册号：0350420Q30191R2S

兹　证　明

山西安洽科技股份有限公司

山西综改示范区太原学府园区南中环街401号A座6层B5、B6号，030006

统一社会信用代码：911401006666324859

管理体系符合

GB/T 19001-2016 / ISO 9001:2015 标准

该管理体系适用于

计算机应用软件开发和计算机信息系统集成与服务***

（涉及场所：山西综改示范区太原学府园区南中环街401号A座6层B5、B6号）

颁证日期：2020年4月24日

有效期最长可至：2023年4月23日

签发人：

兴原认证中心有限公司

CNAS

中国认可 国际互认 管理体系 MANAGEMENT SYSTEM CNAS C035-M

通过对学校当前信息整体情况的分析，我们提出了合理、有效，并具有针对性的网络安全等级保护建设方案。

上述针对信息系统的安全规划建议、相关安全建设管理体系的完善建议以及结合多种先进信息技术手段的网络安全解决方案，整体上可以实现：对信息机房的整体保护、对核心业务应用系统的保护、对数据和网络中心的保护，并且能够大大降低信息机房运维管理人员的工作量，大幅提升工作效率。

整体上，确保在围绕信息化建设总体思路不变的基础上，加强了整体信息系统的信息安全保障工作，参照国家信息系统等级保护制度的相关要求，结合可信计算、深度防御的思想，使信息系统整体上具备了多级防护、整体防御的安全保障体系。