达州中医药职业学院

校园升级改造工程信息化建设项目需求书

目录

[第一章 本单位已建信息化项目建设现状 3](#_Toc132179213)

[第二章 整体建设依据 6](#_Toc132179214)

[2.1 信息安全建设依据 6](#_Toc132179215)

[2.2 机房建设依据 7](#_Toc132179216)

[2.3 整体软件建设依据 7](#_Toc132179217)

[第三章 信息安全建设需求 10](#_Toc132179218)

[3.1 整体建设策略 10](#_Toc132179219)

[3.1.1 信息安全技术体系总体策略 10](#_Toc132179220)

[3.1.2 安全管理体系总体策略 12](#_Toc132179221)

[3.1.3 安全运营体系总体策略 13](#_Toc132179222)

[3.2 整体建设架构图 14](#_Toc132179223)

[3.3 安全技术方案设计 14](#_Toc132179224)

[3.3.1 安全通信网络 14](#_Toc132179225)

[3.3.2 安全区域边界 20](#_Toc132179226)

[3.3.3 安全计算环境 41](#_Toc132179227)

[3.4 安全管理体系设计 64](#_Toc132179228)

[3.4.1 安全管理制度 64](#_Toc132179229)

[3.4.2 安全管理机构 68](#_Toc132179230)

[3.4.3 安全管理人员 72](#_Toc132179231)

[3.4.4 安全运维管理 74](#_Toc132179232)

[3.5 安全运营体系设计 83](#_Toc132179233)

[3.5.1 安全运营体系总体设计 83](#_Toc132179234)

[3.5.2 安全运营体系详细设计 84](#_Toc132179235)

[第四章 等保测评需求 100](#_Toc132179236)

[1、项目背景 100](#_Toc132179237)

[2、适用范围 101](#_Toc132179238)

[3、标准和规范 101](#_Toc132179239)

[4、测评范围 102](#_Toc132179240)

[5、技术规范 102](#_Toc132179241)

[5.1、测评及评估原则 102](#_Toc132179242)

[5.2、实施要求 103](#_Toc132179243)

[5.3、测评及评估方法 103](#_Toc132179244)

[5.4、等级保护测评内容 104](#_Toc132179245)

[第五章 模块化机房建设需求 107](#_Toc132179246)

[5.1 建设必要性 107](#_Toc132179247)

[5.2 机房装修装饰设计 107](#_Toc132179248)

[5.2.1 机房平面布局和功能室的划分 107](#_Toc132179249)

[5.2.2 吊顶 108](#_Toc132179250)

[5.2.3 墙面和地面 108](#_Toc132179251)

[5.2.4 门 109](#_Toc132179252)

[5.2.5 防尘处理 109](#_Toc132179253)

[5.2.6 防火处理 109](#_Toc132179254)

[5.2.7 防水处理 110](#_Toc132179255)

[5.2.8 防鼠处理 110](#_Toc132179256)

[5.2.9 保温设计 110](#_Toc132179257)

[5.2.10 机房场地的特殊处理 110](#_Toc132179258)

[5.3 精密空调与新排风系统 110](#_Toc132179259)

[5.3.1 系统要求 110](#_Toc132179260)

[5.3.2 精密空调系统 111](#_Toc132179261)

[5.3.3 数据空调制冷量计算 111](#_Toc132179262)

[5.3.4 空调给排水 112](#_Toc132179263)

[5.3.5 新排风系统 112](#_Toc132179264)

[5.4 综合布线系统 112](#_Toc132179265)

[5.4.1 概述 112](#_Toc132179266)

[5.4.2 电气防护、接地及防火要求 113](#_Toc132179267)

[5.4.3 桥架部分 113](#_Toc132179268)

[5.5 门禁和视频监控系统 115](#_Toc132179269)

[5.5.1 门禁系统 115](#_Toc132179270)

[5.5.2 视频监控系统 115](#_Toc132179271)

[5.6 UPS系统 116](#_Toc132179272)

[5.6.1 概述 116](#_Toc132179273)

[5.6.2 UPS供电系统的要求 116](#_Toc132179274)

[5.6.3 UPS主机设计 116](#_Toc132179275)

[5.6.4 UPS容量的确定 117](#_Toc132179276)

[5.6.5 UPS电池配置要求 117](#_Toc132179277)

[5.7 供配电系统 117](#_Toc132179278)

[5.7.1 概述 117](#_Toc132179279)

[5.7.2 配电设计方案 118](#_Toc132179280)

[5.7.3 低压配电系统 118](#_Toc132179281)

[5.8 防雷接地系统 119](#_Toc132179282)

[5.9 消防报警系统 119](#_Toc132179283)

[5.9.1 设计范围及内容 119](#_Toc132179284)

[5.9.2 火灾自动报警系统 119](#_Toc132179285)

[5.9.3 气体灭火系统 120](#_Toc132179286)

[5.10 环境集中监控系统 121](#_Toc132179287)

[5.10.1 系统概述 121](#_Toc132179288)

[5.10.2 系统需求设计 121](#_Toc132179289)

[5.11 机柜 122](#_Toc132179290)

[5.11.1 机柜 122](#_Toc132179291)

[第六章 教务管理系统建设需求 123](#_Toc132179292)

[6.1 教务管理系统建设必要性 123](#_Toc132179293)

[6.2 教务管理系统功能要求 124](#_Toc132179294)

[6.2.1 基础信息 124](#_Toc132179295)

[6.2.2 学籍管理 125](#_Toc132179296)

[6.2.3 新生管理 128](#_Toc132179297)

[6.2.4 课程资源管理 128](#_Toc132179298)

[6.2.5 教学计划(培养方案)管理 129](#_Toc132179299)

[6.2.6 开课及免听考勤管理 130](#_Toc132179300)

[6.2.7 排课及调停补课管理 133](#_Toc132179301)

[6.2.8 选课管理 134](#_Toc132179302)

[6.2.9 教室管理 135](#_Toc132179303)

[6.2.10 教材管理 136](#_Toc132179304)

[6.2.11 实验教学管理 137](#_Toc132179305)

[6.2.12 实习实训管理 138](#_Toc132179306)

[6.2.13 考务管理 139](#_Toc132179307)

[6.2.14 成绩及缓补考免重修管理 141](#_Toc132179308)

[6.2.15 教学质量评价 143](#_Toc132179309)

[6.2.16 毕业审核管理 147](#_Toc132179310)

[6.2.17 教职工服务 148](#_Toc132179311)

[6.2.18 学生服务 149](#_Toc132179312)

[6.2.19 系统管理 151](#_Toc132179313)

[6.2.20 数据挖掘服务 152](#_Toc132179314)

[6.2.21 微信服务平台 153](#_Toc132179315)

[第七章 OA系统建设需求 155](#_Toc132179316)

[7.1 OA系统建设必要性 155](#_Toc132179317)

[7.2 OA系统功能要求 155](#_Toc132179318)

[第八章 学工一体化系统建设需求 162](#_Toc132179319)

[8.1 学工一体化系统建设必要性 162](#_Toc132179320)

[8.2 学工管理系统 162](#_Toc132179321)

[8.2.1 学工管理[PC端] 162](#_Toc132179322)

[8.2.2 学工管理[移动端] 185](#_Toc132179323)

[8.3 宿舍管理系统 193](#_Toc132179324)

[8.3.1 宿舍管理[PC端] 193](#_Toc132179325)

[8.3.2 宿舍管理[移动端] 197](#_Toc132179326)

[8.4 疫情管理平台 199](#_Toc132179327)

[8.4.1 健康填报管理（日常填报） 199](#_Toc132179328)

[8.4.2 返校监控管理 201](#_Toc132179329)

[8.4.3 体温监控管理 202](#_Toc132179330)

[8.4.4 体温填报监控 202](#_Toc132179331)

[8.4.5 风险地区管理 202](#_Toc132179332)

[8.4.6 到校生管理 203](#_Toc132179333)

[8.4.7 疫苗接种管理 203](#_Toc132179334)

[8.4.8 核酸检测管理 203](#_Toc132179335)

[8.5 系统管理 204](#_Toc132179336)

[8.5.1 学院管理 204](#_Toc132179337)

[8.5.2 专业管理 204](#_Toc132179338)

[8.5.3 年级管理 204](#_Toc132179339)

[8.5.4 学期设置 204](#_Toc132179340)

[8.5.5 火车站点维护 204](#_Toc132179341)

[8.5.6 重置密码 204](#_Toc132179342)

[8.5.7 预制数据管理 204](#_Toc132179343)

[8.5.8 权限管理 204](#_Toc132179344)

[8.5.9 系统日志 205](#_Toc132179345)

[8.6 数据集成 205](#_Toc132179346)

[第九章 教务管理系统、OA系统、学工一体化系统等硬件需求 206](#_Toc132179347)

[9.1 教务管理系统、OA系统硬件需求 206](#_Toc132179348)

[9.2 学工一体化平台硬件需求 206](#_Toc132179349)

[9.3 高职平台硬件需求 207](#_Toc132179350)

[第十章 原有防火墙升级 207](#_Toc132179351)

[第十一章 教学资源库升级 207](#_Toc132179352)

# 本单位已建信息化项目建设现状

达州中医药职业学院成立于2019年，是经四川省人民政府批准、教育部备案、达州市人民政府举办的公办全日制普通高等职业院校。学院现有直属附属医院----达州市中西医结合医院，该院是集医疗、教学、科研、预防、保健、康复于一体的国家三级甲等医院。还与达州市中心医院、南充市中医院、宣汉县中医院、达川区中医院、新天泰药业、成都地奥集团天府药业有限公司等32家单位签订了实习实训合作框架协议，为学生提供多层次、多渠道的实习实训基地。学院坚持“中西医并重，促进中医药教育全面发展，发扬中医药特色优势，服务人民健康”的大政方针，为中医药卫生事业、中药产业和医养、康养产业培养高素质技能人才，是读书治学的理想之地。

达州中医药职业学院现有业务系统包括教务系统、一卡通系统、网站系统等，基本实现教育信息化的建设。

随着信息技术在教育行业的广泛应用和深度融合，在教育系统、教育设备、教育环境等纷纷融入信息化元素的同时，也加大了攻击者对于教育行业相关教育数据的关注程度和攻击面，使支撑教育教学的底层网络系统、业务系统等在网络安全面临的威胁也持续加大。

近年来，黑客入侵教务管理平台窃取或倒卖学生学籍信息、篡改学校网站造成不良影响、植入勒索病毒到大量校园网电脑终端等信息安全事件逐渐增多，部分案例甚至造成了很大的社会影响。

在此安全背景下，下一阶段的校园信息化建设应重点关注信息安全工作的投入及成果，并结合业务实际情况，制定切实可行的安全保障机制，降低系统攻击面、增强安全防范能力，整体提高校园网基础信息网络和重要信息系统的信息安全保护能力、水平及全生命周期的安全处置能力。

校园网由于其业务涉及面广、信息量大、环境复杂、人员变化快等问题, 对信息安全的保护需求更高。2019年上半年，网络攻击数量总体呈上升趋势，网站态势依然严峻，教育行业的网站漏洞数量发现最多。从勒索病毒攻击目标来看，教育成为勒索病毒的主要目标行业，总占比达到21%。同时，从挖矿木马攻击的行业分布来看，黑产更倾向于攻击教育行业，挖矿病毒感染分布教育行业占比21%。此外，由于教育往往与科研密不可分，因此也成为很多以窃取科技情报为目的APT攻击者的重点攻击目标，根据调研分析得出，教育行业主要有以下几个行业特性：

* **业务与网络架构复杂**

一个学校的网络需要划分多个域，包括视频监控区、一卡通区、DMZ区、学生宿舍区、核心服务器区、运维管控区、甚至还有云平台区域等等，由于整个校园范围较大，各个终端、区域之间的网络安全域划分策略和权限控制相对复杂。

* **网站安全性较低**

据不完全统计，2018年教育培训类网站是检测出网站漏洞最多的行业，总计为555.3万次网站漏洞；共扫描检测出高危漏洞16.89万次，数量排行第二，网站安全状况不容乐观。

* **数据类型密集**

随着教育信息化的深入，越来越多纸张上的数据向硬盘存储和网络变革，无论学籍档案、成绩管理、教职员工信息，还是学术文献资料，这些教育关键数据都在向IT系统转移。大到国家级别的教育资源和管理公共服务平台，小到院、校级别的各种数字教学平台，都汇聚存储了教育管理、教学支持领域的海量知识和用户信息。

* **外部面临威胁大**

教育行业是一个包含巨大信息流的行业，有效利用这些数据信息将能够进一步指导教学，实现国家对教学资源的科学管理。而且，越是高等级、研究深入的教育机构产生的信息越是机密，也越有价值。但也正因此，学校也一直是数据泄露最频繁的地方，尤其是强调自由开放的学校网络，经常成为外部攻击者攻击的目标。

* **教育行业受监管**

自从《网络安全法》颁布实施后，教育行业中的重要系统就确定了其关键基础设施的地位，需要受到外部较高的安全监管要求。

* **内部编制较少**

相对于其他行业而言，各高校安全人员由于编制受限、技术要求较高、技术迭代速度较快等等各种制约条件所限制，导致高校目前专职安全人手大多处于一个相对缺乏的地位，直接导致了一定程度上的安全运维操作颗粒度不到位，安全策略更新不及时等等安全风险。

* **安全监控能力较弱**

由于高校的网络架构和业务流程均相对复杂，导致很难由单一的手段统一发现整个网络中的安全问题，故安全监控能力相对较低。

# 整体建设依据

## 信息安全建设依据

本方案的设计过程中将按照国家的相关法律标准展开，在方案的设计过程中，既考虑满足合规要求，又符合单位的实际安全建设需求，主要依据的标准文件包含如下：

|  |  |
| --- | --- |
| 指导思想 | 教技〔2015〕2 号《教育部、公安部关于全面推进教育行业信息安全等级保护工作的通知》 |
| 教技厅〔2017〕3号教育部办公厅关于印发《教育行业网络安全综合治理行动方案》的通知 |
| 教技厅〔2019〕2号教育部办公厅关于印发《2019年教育信息化和网络安全工作要点》的通知 |
| 《中华人民共和国网络安全法》 |
| 《网络安全等级保护管理条例》（征求意见稿） |
| 等级保护 | GB/T 25070-2019 信息安全技术 网络安全等级保护安全设计技术要求GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求GB/T -2019 信息安全技术 网络安全等级保护实施指南 |
| 系统定级 | GB/T -2019 信息安全技术 网络安全等级保护定级指南 |
| 技术方面 | GB/T 20270-2006 信息安全技术 网络基础安全技术要求GB/T 20271-2006 信息安全技术 信息系统通用安全技术要求GB/T 20272-2006 信息安全技术 操作系统安全技术要求GB/T 20273-2006 信息安全技术 数据库管理系统通用安全技术要求GA/T671-2006 信息安全技术 终端计算机系统安全等级技术要求GA/T 709-2007 信息安全技术 信息系统安全等级保护基本模型  |
| 管理方面 | GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求ISO/IEC 27001 信息系统安全管理体系标准 |
| 方案设计 | GB/T 25070-2019 信息安全技术 网络安全等级保护安全设计技术要求 |
| 方案架构 | IATF 信息保障技术框架 |

## 机房建设依据

设备和系统的设计、制造、安装、运行、材质、工艺等所有相关内容均须符合本章内所标注的规范/标准，若现行有关标准、规范高于上述标准、规范或有最新标准、规范，均按照现行或最新标准、规范执行。

* 学院相关要求
* 《数据中心设计规范》GB50174-2017
* 《电力调度通信中心工程设计规范》（GB/T50980-2014）
* 《数据中心基础设施施工及验收规范》（GB50462-2015）
* 《计算机场地通用规范》（GB/T2887-2011）
* 《计算机场地安全要求》（GB/T9361-2011）
* 《智能建筑设计标准》（GB 50314-2015）
* 《低压配电设计规范》（GB50054-2011）
* 《供配电系统设计规范》（GB50052-2009）
* 《防静电工程施工与质量验收规范》（GB 50944-2013）
* 《工业建筑供暖通风与空气调节设计规范》（GB 50019—2015）
* 《综合布线系统工程设计规范》（GB/T50311-2016）
* 《综合布线系统工程验收规范》（GB 50312-2016）
* 《民用建筑电气设计规范》（JGJ/16-2008）

## 整体软件建设依据

《教育信息化2.0行动计划》

《教育信息化2.0行动计划》提出为深入贯彻落实党的十九大精神，加快教育现代化和教育强国建设，推进新时代教育信息化发展，培育创新驱动发展新引擎，结合国家“互联网+”、大数据、新一代人工智能等重大战略的任务安排，必须站在新的历史起点，必须聚焦新时代对人才培养的新需求，强化以能力为先的人才培养理念，将教育信息化作为教育系统性变革的内生变量，支撑引领教育现代化发展，推动教育理念更新、模式变革、体系重构，使我国教育信息化发展水平走在世界前列，发挥全球引领作用，为国际教育信息化发展提供中国智慧和中国方案。

《中国教育现代化2035》

《中国教育现代化2035》提出要加快信息化时代教育变革。建设智能化校园，统筹建设一体化智能化教学、管理与服务平台。利用现代技术加快推动人才培养模式改革，实现规模化教育与个性化培养的有机结合。创新教育服务业态，建立数字教育资源共建共享机制，完善利益分配机制、知识产权保护制度和新型教育服务监管制度。推进教育治理方式变革，加快形成现代化的教育管理与监测体系，推进管理精准化和决策科学化。

2035年主要发展目标是：建成服务全民终身学习的现代教育体系、普及有质量的学前教育、实现优质均衡的义务教育、全面普及高中阶段教育、职业教育服务能力显著提升、高等教育竞争力明显提升、残疾儿童少年享有适合的教育、形成全社会共同参与的教育治理新格局。到2035年，总体实现教育现代化，迈入教育强国行列，推动我国成为学习大国、人力资源强国和人才强国，为到本世纪中叶建成富强民主文明和谐美丽的社会主义现代化强国奠定坚实基础。

《职教20条》

《国家职业教育改革实施方案》（简称“职教20条”）。在以习近平新时代中国特色社会主义思想指引下，为了贯彻党的十九大精神和全国教育大会精神，全面贯彻落实习近平总书记关于教育的重要论述，推进新时代职业教育改革发展，经中央深改委第五次会议审议，2019年1月国务院印发了《国家职业教育改革实施方案》，方案明确提出“深化复合型技术技能人才培养培训模式改革，借鉴国际职业教育培训普遍做法，制定工作方案和具体管理办法，启动1+X证书制度试点工作。”

方案还指出建立健全学校设置、师资队伍、教学教材、信息化建设、安全设施等办学标准，引领职业教育服务发展、促进就业创业。落实好立德树人根本任务，健全德技并修、工学结合的育人机制，完善评价机制，规范人才培养全过程。深化产教融合、校企合作，育训结合，健全多元化办学格局，推动企业深度参与协同育人，扶持鼓励企业和社会力量参与举办各类职业教育。推进资历框架建设，探索实现学历证书和职业技能等级证书互通衔接。

《深化新时代教育评价改革总体方案》

《深化新时代教育评价改革总体方案》提出全面贯彻党的教育方针，坚持社会主义办学方向，落实立德树人根本任务，遵循教育规律，系统推进教育评价改革，发展素质教育，引导全党全社会树立科学的教育发展观、人才成长观、选人用人观，推动构建服务全民终身学习的教育体系。

《职业教育提质培优行动计划（2020-2023年）》

《职业教育提质培优行动计划（2020-2023年）》提出以习近平新时代中国特色社会主义思想为指导，贯彻党的十九大和十九届二中、三中、四中全会精神，牢固树立新发展理念，落实高度重视、加快发展的工作方针，坚持服务高质量发展、促进高水平就业的办学方向，坚持职业教育与普通教育不同类型、同等重要的战略定位，着力夯实基础、补齐短板，着力深化改革、激发活力，加快构建纵向贯通、横向融通的中国特色现代职业教育体系，大幅提升新时代职业教育现代化水平和服务能力，为促进经济社会持续发展和提高国家竞争力提供多层次高质量的技术技能人才支撑。

《四川省“十四五”教育发展规划》

《四川省“十四五”教育发展规划》在“五、强化教育高质量发展支撑保障”的“（二）推进教育信息化”提到“4.提升教育信息化管理与服务水平。”，加速教育治理数字化转型,实现各类信息系统互联互通、数据有序流动和开放共享。建立教育政务信息资源大数据,推动应用“互联网十政务服务”平台,实现管理服务“简流程、减证明、减时间”,让“数据多跑路、群众少跑腿”。推动运用“互联网十监管”平台,支持“双随机、一公开”监管和非现场监管,加强知识产权保障,完善教育服务消費者权益保障机制。推进学校管理智能化,加强智能教学系统、智能教学助手、智能学伴、人工智能教师等新技术 应用。将教育信息化资源与服务纳入地方政府购买服务指导性目录,鼓励社会力量参与信息化建设,引导社会资本支持“互联网十教育”发展。

# 信息安全建设需求

## 整体建设策略

### 信息安全技术体系总体策略

为满足校园网所面临的信息安全相关法律法规及监管要求，着力改善校园网信息安全基础建设薄弱的现状，以及网站及数据防护重点，并考虑到安全建设是一个需要不断优化的过程，故本方案以安全体系总体架构为指引，从安全技术体系、安全管理体系、安全运营体系三方面来实现校园网的信息安全建设。



安全防护体系架构图

本项目规划和建设，应严格遵循信息安全等级保护2.0标准，建设以“一个中心、三重防护、三个体系”为核心指导思想，构建集防护、检测、响应、恢复于一体的全面的安全保障体系。其中：

“一个中心”是指安全运营管理中心，即构建先进高效的安全运营管理中心，实现针对系统、产品、设备、策略、信息安全事件、操作流程等的统一管理；

“三重防护”是指构建安全区域边界、安全计算环境、安全通信网络三维一体的技术防御体系；

“三个体系”是指形成安全技术体系、安全管理体系、安全运营体系三个体系，三个体系相互融合、相互补充，形成一个整体的安全防御体系。其中，安全管理体系是策略方针和指导思想，安全技术体系是纵深防御体系的具体实现，安全运营体系是支撑和保障。

* + 1. 安全技术体系

安全技术体系设计内容主要涵盖到 “一个中心、三重防护”。即安全运营管理中心、计算环境安全、区域边界安全、通信网络安全。

* 1. 安全运营管理中心

安全管理中心是安全技术体系的核心和中枢，集安全监测中心、安全运维中心、安全防御中心和安全响应中心的功能为一体。

安全监测中心：其中主要包括对系统、设备安全监测和报警，并提供基于人工或工具的多层次的安全监测服务。

安全防御中心：在构建整体的技术防御体系的基础上，通过安全防御中心加强协调联动，进行积极主动防御，提升整体安全防御水平。

安全运维中心：实现安全运维操作的流程管理和标准化管理，实现自动化安全运维，实现运维策略可视化。

安全响应中心：采用本地服务+云端服务+专家的新型工作模式，结合云端的威胁情报、大数据提供及时的技术保障服务。

* 1. 三重防护

计算环境安全：为智慧校园安全建设打造一个可信、可靠、安全的计算环境。从系统、应用的身份鉴别、访问控制、安全审计、数据机密性及完整性保护、资源控制等方面，全面提升智慧校园安全建设平台在系统及应用层面的安全；

区域边界安全：从加强网络边界的访问控制粒度、网络边界行为审计以及保护网络边界完整等方面，提升网络边界的可控性和可审计性；

通信网络安全：从保护局域网和广域网的数据传输安全、整体网络架构可靠可用等方面保障网络通信安全。

* + 1. 安全管理体系

仅有安全技术防护，无严格的安全管理相配合，难以保障整个系统的稳定安全运行。在系统建设、运行维护、日常管理中都要重视安全管理，制定并落实安全管理制度，明确责任权力，规范操作，加强人员、设备的管理以及人员的培训，提高安全管理水平，同时加强对紧急事件的应对能力，通过预防措施和恢复控制相结合的方式，使由意外事故所引起的破坏减小至可接受程度。

* + 1. 安全运营体系

由于安全技术和管理的复杂性、专业性和动态性，智慧校园安全建设平台安全的规划、设计、建设、运行维护均需要有较为专业的安全服务和运营队伍支持。基础的安全运营服务包括系统日常维护、安全加固、应急响应、安全评估、安全培训和安全咨询等工作；在系统建设上线后，需要逐步完善安全运营体系，确保系统运行安全。

信息系统维护上目前投入了大量的硬件管理平台和人力进行管理，但对资产的管理上目前没有相关的管理制度；其次在设备的密码管理制度上没有形成规范；信息系统的变更与备份目前没有相关的管理制度约束，但有相关人员进行管理，没有形成纸质的规范；网络、系统的维护目前有专人进行管理，已形成了相关的值班制度、账号管理制度，但没有形成相关的体系文件，整个系统运维的管理制度上不够完善。

技术体系策略如下：

1、以校园内网学籍系统为例，作为保障对象，参照以《网络安全等级保护基本要求》中三级保护要求为控制要求，建设基础安全技术体系框架。

2、安全技术体系建设覆盖物理环境、通信网络、区域边界、计算环境和安全管理中心五个方面。

3、通过业界成熟可靠的安全技术及安全产品，结合专业技术人员的安全技术经验和能力，系统化的搭建安全技术体系，确保技术体系的安全性与可用性的有机结合，达到适用性要求。

4、建设集中的安全管理平台，实现对安全系统的集中管控、分权管理。

### 安全管理体系总体策略

1、建立信息安全领导小组和信息安全工作组，形成等级保护基本要求的信息安全组织体系职责。

2、建立信息安全管理制度和策略体系，形成符合等级保护基本要求的安全管理制度要求。

3、建立符合系统生命周期的安全需求、安全设计、安全建设和安全运维的运行管理要求。

4、系统安全建设过程应落实等级保护定级、备案、建设整改、测评等管理要求。

5、系统安全运营过程应落实等级保护监督检查的管理要求。

### 安全运营体系总体策略

1、通过互联网等领域所形成的新技术适当提升安全能力，强化风险应对（监测、预警、防护、处置、溯源等）能力。

2、建立规范的信息化安全运营体系，以安全视角规范信息系统安全运营的整个过程，形成安全业务标准与流程。

3、建立信息安全运营中心，安全运营实行分级保障，加强安全运营的可持续性建设。

## 整体建设架构图



## 安全技术方案设计

本次安全技术方案参照 《信息安全技术 网络安全等级保护安全设计技术要求》GB/T 25070-2019和《信息安全技术 网络安全等级保护基本要求》GB/T 22239-2019标准进行设计，具体技术包括安全通信网络、安全区域边界、安全计算环境。

### 安全通信网络

#### 安全网络架构

为了对达州中医药职业学院实现良好的安全保障，参照等级保护的要求对系统安全区域进行划分设计，实现内部办公、数据共享交换与外部接入区域之间的安全隔离，并对核心区域进行冗余建设，用以保障关键业务系统的可用性与连续性。

##### 安全域划分原则

安全域是由安全保护对象中安全计算环境和安全区域边界的综合组成，根据安全域的描述可以把保护对象进行进一步的划分，同时使整个网络逻辑结构清晰。

安全域可以根据其更细粒度的防护策略，进一步划分成安全子域，其关键是能够区分防护重点，形成重要资源重点保护的策略。

安全域的理论和方法所遵循的根本原则：

* 业务保障原则：

安全域方法的根本目标是能够更好的保障网络上承载的业务。在保证安全的同时，还要保障业务的正常运行和运行效率。

* 适度安全原则：

在安全域划分时会面临有些业务紧密相连，但是根据安全要求（信息密级要求，访问应用要求等）又要将其划分到不同安全域的矛盾。是将业务按安全域的要求强性划分，还是合并安全域以满足业务要求？必须综合考虑业务隔离的难度和合并安全域的风险（会出现有些资产保护级别不够），从而给出合适的安全域划分。

* 结构简化原则：

安全域方法的直接目的和效果是要将整个网络变得更加简单，简单的网络结构便于设计防护体系。比如，安全域划分并不是粒度越细越好，安全域数量过多过杂可能导致安全域的管理过于复杂和困难。

* 等级保护原则：

安全域的划分要做到每个安全域的信息资产价值相近，具有相同或相近的安全等级安全环境安全策略等。

* 立体协防原则：

安全域的主要对象是网络，但是围绕安全域的防护需要考虑在各个层次上立体防守，包括在物理链路网络主机系统应用等层次；同时，在部署安全域防护体系的时候，要综合运用身份鉴别访问控制检测审计链路冗余内容检测等各种安全功能实现协防。

* 生命周期原则：

对于安全域的划分和布防不仅仅要考虑静态设计，还要考虑不断的变化；另外，在安全域的建设和调整过程中要考虑工程化的管理。

##### 达州中医药职业学院网络安全域划分

根据达州中医药职业学院网整体安全需求并结合《网络安全等级保护基本技术要求》和《网络安全等级保护安全设计技术要求》中的相关要求，区域划分如下：

（1）互联网接入区

包含于Internet通信的路由设备和网络安全边界设备，与DMZ区、核心网络区有通信，向外联接Internet，向内连接外网DMZ区，负责达州中医药职业学院网络信息系统对Internet的接入。

（2）DMZ服务器区

包含DMZ交换机和对外应用服务器，向外与专网其他单位有通信，直接连接专网接入区的边界设备，向内与安全管理区有通信。

（3）核心网络区

包含核心交换机和安全设备，对网络信息系统起数据通讯支撑作用。向外连接互联网接入区，负责内部网络与互联网的数据交互；向内连接业务服务器区、安全管理区、办公终端区等，主要负责这各区域间的通信。这样部署提高了网络通讯新能，增加网络可靠性和安全性，为今后网络信息系统扩展提供了一个基础网络平台。

（4）安全管理区

包含网络管理系统、防病毒系统、补丁升级系统、IDS管理端、漏洞扫描系统等，与所有的区域都有通信，连接核心网络区。

（5）业务服务器区

向外联接核心网络区，与核心网络区通信，这样调整增加了服务器区网络的稳定性同时具备更好的扩容能力。

（6）业务终端区

包含楼层接入交换机，与业务服务器区和DMZ区有通信，连接核心网络区。

##### 安全隔离与信息交换系统功能需求

1. 具有外网主机模块、内网主机模块和隔离交换模块，内外端主机为网络协议终点，彻底阻断各种网络协议；包含数据库同步、文件交换、数据库访问、邮件访问、安全浏览、安全FTP、定制模块、工控访问、防病毒等功能模块；
2. 应用层吞吐不低于450Mbps，3年设备质保；内网侧：≥6个10/100/1000Base-T端口，≥2个USB口；外网侧：≥6个10/100/1000Base-T端口，≥2个USB口
3. 为提高运维效率，产品内、外网主机分别具有独立液晶屏，能够显示产品品牌型号、CPU/内存占用率、网络接口状态等信息；
4. .支持双系统冗余架构，可通过WEB页面进行主备系统切换，当主系统发生故障或需要升级时可切换至备系统进行工作。
5. 支持配置智能备份功能，可灵活设置备份周期，备份个数，为节省磁盘空间占用，当配置无变化时，不进行重复备份。
6. 支持文件断点续传功能，同时支持文件并发数量设置，大幅度提升文件传输性能，充分利用硬件资源；文件传输支持文件名过滤、文件类型过滤、文件内容过滤、文档重建、病毒过滤功能。
7. 数据库同步支持无客户端方式同步，无客户端方式同步由网闸主动发起并完成，不需要第三方软件支持（无需在数据库安装任何第三方软件，可以在网闸系统上完成数据库同步配置）。
8. 支持垃圾邮件过滤，支持对邮件附件及其附件类型进行过滤控制，邮件内容过滤、文档重建、病毒过滤。
9. 安全FTP支持最大并发连接数、单个IP最大并发数设置，灵活限制数据通道是否在1024以下端口使用。
10. 支持TCP、UDP业务数据统计，可按照秒、分钟展示发送速率、接受速率、连接数，并且可按照图表进行展示。
11. 支持安全审计能力，可通过自定义时间、任务名称 、文件名称、文件类型、文件大小类型、源目的文件路径、源目IP等详细字段追溯业务数据流向，可自定义配置查询条件，查询条件策略可以自定义设置。
12. 支持异构双引擎病毒模块，可根据用户需求选择需要的病毒引擎，支持云查杀模式，可联动云端文件鉴定中心，预判文件安全风险，防止恶意文件通过网闸进入内网，提供高中低不同级别阻断策略。
13. 支持弱口令防护功能，针对网闸隔离保护的服务器，防止暴力破解密码。

##### 安全管理交换机

1. 交换能力不低于598Gbps；包转发速率不低于222Mpps；
2. 配置可插拔双电源；
3. 支持防火墙等高性能OAP模块插卡，扩展安全板卡须具备中国网络安全审查技术与认证中心EAL4增强级别。

#### 通信传输安全

1、安全风险

随着远程办公、移动办公的普及，越来越多的学校内部的师生通过互联网接入内部办公系统，此外，随着业务规模的扩大，分校区的增加，不同地域的分校区往往需要通过互联网进行网络互联。

达州中医药职业学院由于业务需要，存在大量远程用户，这些用户通过互联网访问内部应用系统，远程方式为用户使用带来了很大便利，但是，也带来了安全风险，如果师生使用移动办公设备传输数据时发生了篡改、或者敏感数据发生泄漏的话，后果将会非常严重。所以如何保证移动办公的远程传输安全、数据安全和身份安全等是单位需要考虑的重中之重。

2、控制要求

等级保护标准在“安全通信网络”中明确要求：

* “应采用校验技术或密码技术保证通信过程中数据的完整性；”（8.1.2.2 a））
* “应采用密码技术保证通信过程中数据的保密性”。 （8.1.2.2 b））

在“安全计算环境”中针对数据保护要求：

* “应采用校验技术或密码技术保证重要数据在传输过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等；” （8.1.4.7 a））
* “应采用密码技术保证重要数据在传输过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要个人信息等”。 （8.1.4.8 a））

并且在对终端（包括移动终端）访问系统时要求：

* “对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；” （8.1.4.1 a））
* “采用口令、密码技术、生物技术等两种或两种以上组合的鉴别技术对用户进行身份鉴别，且其中一种鉴别技术至少应使用密码技术来实现”。 （8.1.4.1 d））

3、控制措施

通过部署安全接入网关（SSL VPN）可以实现远程用户的安全访问，从用户接入身份的安全性、终端设备的合法性、访问业务系统的权限合法性、业务数据传输的安全性等多个层面保障用户跨互联网远程接入的安全。主要控制措施如下：

（1）采用密码技术，符合国家密码管理相关要求。为确保密码算法的安全性，远程传输加密的设备或组件除了需要支持AES、DES、3DES、RSA等多种国际主流的商用加密算法之外，还需要支持国密算法，包括 SM1、SM2、SM3、SM4等。

（2）数据远程传输加密保护。远程办公终端连接VPN以后，远程终端与网关之间采用加密传输协议进行数据传输，从而实现数据的保密性。

（3）数据远程传输完整性保护。远程办公终端在传输数据的过程中，通过采用校验码技术或密码技术对传输数据的完整性进行验证和保护。

（4）多因素认证，确保身份安全。能够采用多种认证方式的多因素组合认证，包括用户名密码方式、数字证书认证、AD认证、LDAP认证、指纹认证、Radius认证、动态口令等多种身份认证方式，支持采用密码技术的身份认证需求。

5、产品部署

在互联网区通过防火墙（SSL VPN），实现非可信链路的传输层加密，确保信息通过互联网传输时的机密性和完整性。作为互联网远程接入解决方案的门户，为实现高可用性，可采用双机热备方式，根据实际业务场景选择主从或主主业务模式。

#### 安全通信防护架构

安全防护基本要求：安全审计、传输加密、网络健壮





### 安全区域边界

#### 边界访问控制

##### 边界防护与访问控制

1、安全风险

边界是信息安全的第一道防线，所有访问内部应用的数据均会通过网络边界进入内部网络，随着攻击手段的不断演进，边界所面临的安全风险越来越高，频发突发、隐蔽性强、手段多样、实施体系化的复合型攻击，已经成为当前网络边界威胁的主要特征。事实证明，每一次网络攻击的成功，都是攻击者通过技术手段数次突破网络边界防线的过程，传统的边界防御技术已经不能满足新的边界安全防护的需求。

2、控制要求

等级保护标准在“安全区域边界”中明确要求：

* “应保证跨越边界的访问和数据流通过边界设备提供的受控接口进行通信；”（8.1.3.1 a）
* “应在网络边界或区域之间根据访问控制策略设置访问控制规则，默认情况下除允许通信外受控接口拒绝所有通信；”（8.1.3.2 a）
* “应删除多余或无效的访问控制规则，优化访问控制列表，并保证访问控制规则数量最小化；”（8.1.3.2 b）
* “应对源地址、目的地址、源端口、目的端口和协议等进行检查，以允许/拒绝数据包进出；”（8.1.3.2 c）
* “应能根据会话状态信息为进出数据流提供明确的允许/拒绝访问的能力；”（8.1.3.2 d）
* “应对进出网络的数据流实现基于应用协议和应用内容的访问控制。”（8.1.3.2 e）

3、控制措施

针对新的边界安全威胁，边界访问控制已经成为基本安全措施，必不可少，但为了更加有效的应对当前的网络威胁，防火墙设备应当更加智能化、联动化，以满足安全有效性和防御实时性的切实需求。

当前，下一代防火墙技术已经逐步成熟，通过相关功能实现及策略配置，可实现上述要求，防火墙主要功能及配置要求如下：

（1）访问控制

能够基于IP、安全域、VLAN、时间、用户、地理区域、服务协议及应用等多种方式进行访问控制，一条安全策略可配置应用控制、入侵防护、URL过滤、病毒检测、内容过滤、网络行为管理等高级访问控制功能。能对HTTP、SMTP、POP3、IMAP、FTP、TELNET协议进行细粒度的控制，过滤不受信任的网络行为。

（2）应用层访问控制

能实现文件过滤、URL过滤、邮件过滤等、实现针对主要的应用协议如HTTP、FTP、POP3、SMTP、IMAP等的双向内容传输过滤，可预定义或自定义敏感信息库进行敏感信息定义。

（3）入侵防范

对于主要攻击能进行防护，包括：Flood（SYN Flood、ICMP Flood、UDP Flood、IP Flood）、恶意扫描（禁止tracert、IP地址扫描攻击、端口扫描）、欺骗防护（IP欺骗、DHCP监控辅助检查）、异常包攻击（Ping of Death、Teardrop、IP选项、TCP异常、Smurf、Fraggle、Land、Winnuke、DNS异常、IP分片、ICMP管控（禁止ICMP分片、禁止路由重定向报文、禁止不可达报文、禁止超时报文、ICMP报文大小限制）、应用层Flood（DNS Flood、HTTP Flood）、SYN Cookie等。

（4）负载均衡

作为主要的链路设施，能实现基于IP、ISP、应用、用户、服务等的多链路负载均衡，DNS流量的负载均衡，基于服务器地址的负载均衡。

（5）高可靠性

具备双机热备功能，在路由和透明模式下能支持“主-备”、“主-主”模式，能实现接口联动，链路探测。

（6）动态QoS功能

可配置带宽限制策略。策略类型包括共享型和独享型，用户优先级分为高、中、低，服务类型包括应用层的多种协议。在用户都满足保证带宽情况下，高优先级用户将抢占中、低优先级用户带宽，中优先级用户将抢占低优先级用户带宽。当网络中存在空闲带宽时，防火墙系统会根据当前网络带宽分配情况，自动将空闲带宽分配给重要业务，保证重要业务的正常访问。

（7）支持IPv6

能够支持完整的双栈协议，支持IPv6下的多种功能，包括网络功能和安全功能，包括IPv6接口、IPv6路由、IPv6认证管理、IPv6日志管理、IPv6 VPN、IPv6安全功能及安全策略等。

（8）虚拟防火墙

具备虚拟系统功能，即将防火墙虚拟成多个相互隔离并独立运行的虚拟防火墙，每一个虚拟系统都可以为用户提供定制化的安全防护功能，并可配备独立的管理员账号。

（9）协同联动

能够与终端安全管理系统、云端的URL库、病毒库、应用识别库等资源进行联动，提升对已知威胁的识别效率，并能对在终端发现的威胁从网络层及时阻断。

（10）日志管理

对各类日志，如流量日志、威胁日志、URL过滤日志、邮件过滤日志、行为日志等进行分析和日志外发，能基于IP、用户、接口、地区、应用等过滤条件搜索自定义时间段内的历史日志。

各安全区域都应针对自身业务特点设定访问控制策略，下表表述了各安全区域之间的访问控制关系，在对各网络安全区域设置安全策略时，可以此为参考原则进行设置：

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 目的源 | 核心交换区 | DMZ区 | 移动互联接入区 | 安全管理区 | 业务服务器区 | 业务终端区 |
| 核心交换区 | — | 互通 | 互通 | 互通 | 互通 | 互通 |
| DMZ区 | 互通 | — | 互通 | 禁止 | 禁止 | 禁止 |
| 移动互联接入区 | 互通 | 互通 | — | 禁止 | 互通 | 互通 |
| 专网接入区 | 互通 | 互通 | 禁止 | 互通 | 禁止 | 禁止 |
| 共享交换区 | 互通 | 禁止 | 禁止 | 禁止 | 禁止 | 互通 |
| 安全管理区 | 互通 | 禁止 | 禁止 | — | 互通 | 互通 |
| 业务服务器区 | 互通 | 禁止 | 互通 | 互通 | — | 互通 |
| 业务终端区 | 互通 | 禁止 | 互通 | 互通 | 互通 | — |

访问控制策略应根据网络及业务变化和单位的安全基线进行合理配置和及时调整，及时删除多余或无效的访问控制规则，优化访问控制列表，并保证访问控制规则数量最小化。

4、产品部署

防火墙一般部署在各安全域边界，在互联网接入边界、安全管理区边界、核心业务区边界均建议需单独部署防火墙设备，设置严格的访问控制规则，并定期进行策略的检查和优化。

##### 边界防火墙功能需求

1. 网络处理不低于12Gbps，并发连接数不低于300万，每秒新建连接数不低于20万/秒；配置：≥8个10/100/1000Base-T电接口，≥2个千兆光接口，≥2个万兆光接口，≥2个业务扩展槽；配置：≥16个SSLVPN 并发用户数，≥16个IPsecVPN 并发隧道数，3年设备质保和3年威胁情报数据订阅服务、应用识别库、URL分类特征库、病毒防护特征库、入侵防御特征库升级服务。
2. 支持基于策略的路由负载，支持根据应用和服务进行智能选路。
3. 支持路由模式、透明模式的HA高可靠性部署，可工作于主备、主主模式，会话、用户、配置可实时同步；HA高可靠性部署支持接口联动；HA高可靠性部署支持配置接口权重；支持链路探测。
4. 支持配置基于IPv6地址的安全策略，并在一条策略中可同时启用入侵防御、反病毒、URL过滤、应用识别、反间谍软件等安全功能；支持针对IPv6流量通过HTTP、HTTPS实现Web认证，用户身份信息可存储在本地或Active Directory\Radius\TACACS+\POP3等第三方服务器；通过HTTPS实现Web认证支持使用本地CA颁发的证书同时使用证书验证身份。
5. 支持虚拟防火墙功能，在虚系统内独立配置病毒防护、漏洞利用防护、间谍软件防护、URL过滤、文件过滤、内容过滤、邮件过滤、行为管控等安全功能，并可支持对本虚系统内产生的日志进行独立审计。
6. 支持漏洞防护功能，同时将漏洞防护特征库分类，至少包括缓冲区溢出、跨站脚本、拒绝服务、恶意扫描、SQL注入、WEB攻击等六种分类；漏洞防护支持日志、阻断、放行、重置等执行动作,可批量设置针对某一分类或全部攻击签名的执行动作；支持基于FTP、HTTP、IMAP、OTHER\_APP、POP3、SMB、SMTP等应用协议的漏洞防护。
7. 产品的漏洞防护特征库及间谍软件库包含高危漏洞攻击特征，至少包括“永恒之蓝”、“震网三代”、“暗云3”、“Struts”、“Struts2”、“Xshell后门代码”以及对应的攻击的名称、CVEID、CNNVDID、CWEID、严重性、影响的平台、类型、描述、解决方案建议等（CVEID、CNNDID、CWEID等信息在漏洞攻击特征中体现）详细信息。
8. 支持IPv4和IPv6流量的HTTPS、POP3S、SMTPS、IMAPS协议进行解密，支持配置基于源安全域、目的安全域、源地址、目的地址、SSL协议服务的解密策略，动作可以设置解密或不解密，并可基于安全域、IPv4和IPv6地址进行例外设置，同时支持将解密后流量镜像到其他设备进行分析统计。
9. 支持基于主机或威胁情报视图，统计网络中确认被入侵、攻破的主机数量，至少可查看被入侵、攻破的时间、威胁类别、情报来源、威胁简介、被入侵、攻破的主机IP、用户名、资产等信息；并对威胁情报发现的恶意主机执行自动阻断。
10. 支持接收针对突发重大安全事件的“应急响应消息”，并至少在界面显示安全事件名称、类型、当前防护状态、处置状态以及相应的操作等信息；并可根据设备安全配置的变化动态显示应急响应的处理结果。
11. 支持资产管理，能够通过设置资产监控、VPN、源安全域来控制资产识别范围，支持scanner或onvif类型的扫描方式和网段，实现自动或手动资产扫描；支持通过设置IP地址、MAC地址、资产类型、生效市场、厂商、位置等信息来制定黑/白名单，方便日常资产管理，支持通过设置IP地址、MAC地址、资产类型、操作系统、应用、开放的端口和访问的端口等信息来制定资产指纹库。
12. 支持将告警信息以SNMP Trap、邮件、声音、短信等形式通知管理员，告警信息的范围至少包括配置变更、病毒事件、攻击事件、异常事件、失陷主机告警、并发数告警、CPU利用率、内存利用率、硬盘利用率、接口带宽利用率、NAT端口池利用率等。
13. 支持业务接口下Netflow功能，能够通过Netflow实现对网络进行监控，对接口流量进行抓包，并在可将Netflow抓包文件数据外发。

##### 数据中心防火墙功能需求

1. 冗余电源，网络处理能力不低于45Gbps，并发连接数不低于450万，每秒新建连接数不低于35万/秒；配置：≥4个10/100/1000Base-T电接口，≥4个千兆光接口，≥4个万兆光接口（满配光模块），≥4个业务扩展槽；配置：≥32个SSLVPN 并发用户数，≥32个IPsecVPN 并发隧道数；3年设备质保和3年威胁情报数据订阅服务、应用识别库、URL分类特征库、病毒防护特征库、入侵防御特征库升级服务。
2. 支持基于策略的路由负载，支持根据应用和服务进行智能选路。
3. 支持路由模式、透明模式的HA高可靠性部署，可工作于主备、主主模式，会话、用户、配置可实时同步；HA高可靠性部署支持接口联动；HA高可靠性部署支持配置接口权重；支持链路探测。
4. 支持配置基于IPv6地址的安全策略，并在一条策略中可同时启用入侵防御、反病毒、URL过滤、应用识别、反间谍软件等安全功能；支持针对IPv6流量通过HTTP、HTTPS实现Web认证，用户身份信息可存储在本地或Active Directory\Radius\TACACS+\POP3等第三方服务器；通过HTTPS实现Web认证支持使用本地CA颁发的证书同时使用证书验证身份。
5. 支持虚拟防火墙功能，在虚系统内独立配置病毒防护、漏洞利用防护、间谍软件防护、URL过滤、文件过滤、内容过滤、邮件过滤、行为管控等安全功能，并可支持对本虚系统内产生的日志进行独立审计。
6. 支持漏洞防护功能，同时将漏洞防护特征库分类，至少包括缓冲区溢出、跨站脚本、拒绝服务、恶意扫描、SQL注入、WEB攻击等六种分类；漏洞防护支持日志、阻断、放行、重置等执行动作,可批量设置针对某一分类或全部攻击签名的执行动作；支持基于FTP、HTTP、IMAP、OTHER\_APP、POP3、SMB、SMTP等应用协议的漏洞防护。
7. 产品的漏洞防护特征库及间谍软件库包含高危漏洞攻击特征，至少包括“永恒之蓝”、“震网三代”、“暗云3”、“Struts”、“Struts2”、“Xshell后门代码”以及对应的攻击的名称、CVEID、CNNVDID、CWEID、严重性、影响的平台、类型、描述、解决方案建议等（CVEID、CNNDID、CWEID等信息在漏洞攻击特征中体现）详细信息。
8. 支持IPv4和IPv6流量的HTTPS、POP3S、SMTPS、IMAPS协议进行解密，支持配置基于源安全域、目的安全域、源地址、目的地址、SSL协议服务的解密策略，动作可以设置解密或不解密，并可基于安全域、IPv4和IPv6地址进行例外设置，同时支持将解密后流量镜像到其他设备进行分析统计。
9. 支持基于主机或威胁情报视图，统计网络中确认被入侵、攻破的主机数量，至少可查看被入侵、攻破的时间、威胁类别、情报来源、威胁简介、被入侵、攻破的主机IP、用户名、资产等信息；并对威胁情报发现的恶意主机执行自动阻断。
10. 支持接收针对突发重大安全事件的“应急响应消息”，并至少在界面显示安全事件名称、类型、当前防护状态、处置状态以及相应的操作等信息；并可根据设备安全配置的变化动态显示应急响应的处理结果。
11. 支持资产管理，能够通过设置资产监控、VPN、源安全域来控制资产识别范围，支持scanner或onvif类型的扫描方式和网段，实现自动或手动资产扫描；支持通过设置IP地址、MAC地址、资产类型、生效市场、厂商、位置等信息来制定黑/白名单，方便日常资产管理，支持通过设置IP地址、MAC地址、资产类型、操作系统、应用、开放的端口和访问的端口等信息来制定资产指纹库。
12. 支持将告警信息以SNMP Trap、邮件、声音、短信等形式通知管理员，告警信息的范围至少包括配置变更、病毒事件、攻击事件、异常事件、失陷主机告警、并发数告警、CPU利用率、内存利用率、硬盘利用率、接口带宽利用率、NAT端口池利用率等。
13. 支持业务接口下Netflow功能，能够通过Netflow实现对网络进行监控，对接口流量进行抓包，并在可将Netflow抓包文件数据外发。
14. 原防火墙特征库升级服务。（出口防火墙的硬件质保、入侵检测、反病毒、URL过滤许可、云沙箱检测许可1年）

#### 边界入侵防范

##### 边界入侵防御

1、安全风险

随着教育信息化2.0的普及，针对校园网络攻击的活动也愈演愈烈，而网络攻击造成的破坏性因信息化程度的高度集中也越来越大。主要呈现如下趋势：网络应用越来越复杂，单纯的依靠端口识别应用以达到攻击检测的目的不再有效；网络带宽的快速增长给入侵防护系统的处理能力带来挑战，仅依靠防火墙这样的边界防护设备实现网络攻击检测已经远远不能满足要求，具备大流量业务并发处理能力的专业设备尤其重要；除具备针对网络层/传输层的基础攻击防护外，针对应用层深度识别和防御能力越发重要。

因此，如何有效的对网络攻击行为、异常行为进行监测防御，是边界安全的重要一环。

2、控制要求

根据等级保护的要求，针对“安全区域边界”和“安全计算环境”的防护要求包括：

* “应在关键网络节点处检测、防止或限制从外部发起的网络攻击行为；” （8.1.3.3 a）
* “应在关键网络节点处检测、防止或限制从内部发起的网络攻击行为；” （8.1.3.3 b）
* “检测到攻击行为时，记录攻击源IP、攻击类型、攻击目标、攻击时间，在发生严重入侵事件时应提供报警” 。（8.1.3.3 d）
* “应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。” （8.1.4.4 f）

3、控制措施

在网络区域的边界处，需要通过部署入侵防御设备对网络攻击行为进行检测与阻断，并及时产生报警和详尽的报告。

入侵防御设备需要具备以下功能：

（1）具备新一代检测分析技术

新一代检测引擎能结合异常检测与攻击特征数据库检测的技术，同时也包含了深层数据包检查能力，除了检查第四层数据包外，更能深入检查到第七层的数据包内容，以阻挡恶意攻击的穿透，同时不影响正常程序的工作。

（2）多层多类型攻击检测

可以检测多层多种类型攻击，如应用型攻击：包括Web cc、http get flood、DNS query flood等攻击；流量性攻击：包括SYN Flood、UDP Flood、ICMP Flood 、ARP Flood、Frag Flood、Stream Flood等攻击；蠕虫连接型攻击；普通常见攻击：包括ipspoof、sroute、land、TCP标志位攻击、fraggle攻击、winnuke、queso、sf\_scan、null\_scan、xmas\_scan、ping-of-death、smurf、arp-reverse-query、arp-spoofing等。

（3）双向攻击检测

通过对进出网络的流量进行采集分析，可对由内向外发起的网络攻击行为和由外向内发起的网络攻击行为均进行检测和告警。

（4）日志告警和阻断

网络入侵防御系统除了需要能检测辨别出各种网络入侵攻击，保护网络及服务器主机的安全外，还需要提供完整的取证信息，提供客户追查黑客攻击的来源，这些信息包括黑客攻击的目标主机、攻击的时间、攻击的手法种类、攻击的次数、黑客攻击的来源IP地址等，并提供包括Email/SNMP trap/声音等方式的告警。对于在线部署模式，可以对攻击行为进行实时阻断。

（5）高可用性

对于在线部署模式的设备，当出现软件故障、硬件故障、电源故障时，系统bypass电口自动切换到直通状态以保障网络可用性，能够避免单点故障，不会影响业务。

4、产品部署

入侵防御系统支持在线部署和旁路部署，针对校园内网的网络环境及业务需求，通过在互联网接入边界部署入侵防御系统，实现对网络事件的检测，入侵防御系统采用串接方式部署在防火墙和核心交换机之间，能够有效检测和阻断入侵攻击。

###### 入侵检测系统功能需求

1. 入侵检测系统，网络层吞吐量不低于10Gbps，IDS吞吐量不低于5Gbps,并发连接不低于200万，每秒新建连接数不低于15万/秒，≥1TB硬盘，≥6个10/100/1000M自适应电口，扩展槽≥2个，Console口≥1个，支持液晶屏；3年硬件维保服务，3年入侵检测特征库升级服务；
2. 支持显示系统最近1小时、24小时、1周、1个月的入侵攻击事件趋势图，支持显示系统最近10分钟、1小时、24小时的上下行流量趋势、总流量、总流量占比，并支持趋势图和关联用户；
3. 支持显示系统入侵攻击源地址TOP10和入侵攻击目的地址TOP10；
4. 支持实时显示用户流量TOP10，支持最近10分钟、1小时、24小时跨度的应用统计，统计指标包括：平均速率（上行、下行、双向、双向占比）、实时速率、实时包速率、连接数，并支持一键跳转显示趋势图、关联用户、关联会话。
5. 支持实时显示系统CPU使用率、流量内存使用率、系统内存使用率、硬件存储使用率、CPU温度。
6. 支持导入、导出配置文件；支持配置下次启动的配置文件；支持不少于10个本地配置文件留存，可按需调用配置文件；
7. 支持本地DNS解析、DDNS动态域名；
8. 可实现基于IP地址、服务端口、IP协议、物理端口、DSCP值、IP优先级、TOS值、TTL值、ICMP类型、分片状态、TCP状态、时间等安全策略的状态包过滤，支持源地址、目的地址的取反操作；
9. 支持黑名单，根据报文的源IP地址、掩码进行报文过滤，并对黑名单解禁时间进行自定义；
10. 支持白名单，根据报文的源IP地址、掩码让报文通过，支持IPS业务、防垃圾邮件、防病毒、应用安全和流量控制五个业务；
11. 支持对单个攻击事件保存其原始报文以供取证分析；
12. 支持口令暴力破解检测，支持弱口令检测；
13. 支持按源地区和目的地区展现进行查询；支持地图上展现的威胁类型包括：病毒、入侵攻击、僵木蠕；支持最近一个小时、一天和一个月进行详细查询；支持光标指向该地域的名称及攻击数，点击该地域跳出详细信息列表；支持通过颜色区分威胁严重程度；

##### 未知威胁攻击检测

1、安全风险

大学作为中国高端人才培养和科学技术研究的重要基地，其除了肩负繁重的“教学”职能外还承担着大量的国家级“科研”项目。极易成为行业中最典型的“网络安全攻击目标”。校园内大量邮箱密码泄露，图书馆账号被黑客利用，作为攻击源向校内投放垃圾钓鱼邮件，从而控制校内师生电脑终端，发动下一轮针对性攻击。

在这种情况下，依靠已知特征、已知行为模式进行检测的IDS、IPS在无法预知攻击特征、攻击行为模式的情况下，理论上就已无法检测未知攻击。

未知威胁的隐蔽性、持久性和复杂性远超普通的网络攻击行为，且针对的往往是校园内的关键应用系统。由于未知威胁的这些特点，其造成的破坏性往往也是巨大的，使学校网络安全、学生隐私数据安全、科研项目成果安全面临严峻挑战，必须采用专门的技术措施对这类攻击进行检测、发现和分析，并能够追踪溯源。

2、控制要求

面对新的安全威胁形势，新等级保护标准中除了对边界攻击检测能力提出要求外，还明确提出了对高级威胁攻击和未知攻击的检测、发现能力，具体要求如下：

* “应采取技术措施对网络行为进行分析，实现对网络攻击特别是新型网络攻击行为的分析。” （8.1.3.3 c）

3、控制措施

通过部署专业的未知威胁检测设备，实现对新型网络攻击行为的发现、分析、追溯的能力，设备所需具备的功能包括：

（1）未知威胁发现

由于未知威胁的复杂性和背景的特殊性，仅依赖于单一企业的数据经常无法有效的发现未知威胁，难以做到真正的追踪溯源，而从互联网数据进行发掘和分析，由于任何攻击线索都会有相关联的其他信息被互联网数据捕捉到，所以从互联网进行挖掘可极大提升未知威胁和未知威胁的检出效率，而且由于数据的覆盖面更大，可以做到攻击的更精准溯源。

（2）未知威胁定位、溯源与阻断

用威胁情报的形式对各种攻击中常出现的特点和背景信息进行记录和传输，而威胁情报将通过统一的规范化格式将攻击中出现的多种攻击特征进行标准化，可对未来扩展攻击特征并进行精准攻击定位和溯源提供支撑。

对未知威胁的定位、溯源和阻断离不开专业的安全分析团队，需要能够针对用户网内发现的未知威胁攻击等行为进行深度挖掘和分析，减少损失。

（3）未知恶意代码检测

针对新型攻击和病毒，需要采用机器学习等人工智能算法，通过恶意代码智能检测技术，对海量程序样本进行自动化分析，解决大部分未知恶意程序的发现问题。

（4）未知漏洞攻击检测

可采用基于轻量级沙箱的未知漏洞攻击检测引擎对客户端应用中已知漏洞和未知0day漏洞的攻击利用进行检测。

4、产品部署

未知威胁检测设备旁路部署在核心交换机上，对用户网络中的流量进行全量检测和记录，所有网络行为都将以标准化的格式保存于数据平台，云端威胁情报和本地文件威胁鉴定器分析结果与本地分析平台进行对接，为用户提供基于情报和文件检测的威胁发现与溯源的能力。

###### 高级威胁态势感知系统功能需求

1. 2U标准上架设备；内存：≥32G；硬盘：≥1TB；网口：≥6千兆网口；配置3年设备质保服务和3年特征库升级服务（特征库至少包含：威胁情报、webshell检测规则、网页漏洞利用规则、网络攻击检测规则）；
2. 支持常见协议识别并还原网络流量，用于取证分析、威胁发现，支持：http、dns、smtp、pop3、imap、webmail、DB2、Oracle、MySQL、sql server、Sybase、SMB、FTP、SNMP、telnet、nfs等；
3. 支持自定义协议和端口，满足特殊场景下的流量抓取；
4. 支持基于流量实时IOC匹配功能，设备具备主流的IOC，情报总量不低于254万条；
5. 支持基于工具特征的WEBSHELL检测，能通过系统调用、系统配置、文件的操作来及时发现威胁；
6. 支持基于webshell函数的攻击检测，如文件包含漏洞、任意文件写入、任意目录读取、任意文件包含、preg\_replace代码执行等；
7. 支持通过设备对流量进行抓包分析，可定义抓包流量双向或单向、数量、IP地址、端口或协议类型；
8. 支持基于网络请求的语义分析检测，能够将网络请求拆分后从请求头、响应头、请求体、响应体四方面详细展示请求内容，并能提升对未知威胁检测能力；
9. 支持自定义弱口令字典，支持HTTP、HTTPS、Telnet、FTP、POP、SMTP、IMAP等协议的自定义弱口令检测；
10. 支持旁路HTTPS解密、威胁检测；
11. 支持以攻击者的维度进行分析，对攻击者进行画像，画像内容包括地理位置信息、国家信息、所属组织、使用的攻击手段、攻击的所有资产；
12. 支持系统安全的细分维度包括：暴力破解、弱口令、未授权访问、挖矿行为；
13. 支持与云端威胁情报中心联动，可对攻击IP、C&C域名和恶意样本MD5进行一键搜索，查看基本信息、相关样本、关联URL、可视化分析、域名解析、注册信息、关联域名、数字证书等；
14. 支持语境关联分析技术，通过语义实时检测和拦截攻击行为。
15. 支持与云端安全运营中心联动。在云端分析并撰写威胁分析报告下发到设备上；设备离线时，可将关键数据离线导出上传到云端安全运营中心，安全专家进行分析撰写威胁分析报告；

###### 高级威胁态势感知系统展示屏需求

1. ≥75"，4K 超高清显示屏 ，顺滑防眩钢化玻璃，低书写高精度红外触控技术。支持双系统，配置ops模块，ops模块：≥4核心，≥8G内存，≥128GSSD,屏幕比例:≥16:9,响应时间:不高于6ms，接口支持USB2.0、USB3.0,对比度：大于等于4000:1，支持HDR显示，支持无线、有线连接。

#### 边界完整性检测

##### 网络安全准入

1、安全风险

目前大多数学校构建的还是开放式的网络，这种开放网络给学校业务开展确实能够带来便捷，但也有严重的安全风险，开放的内部网络访问已经严重影响到学校IT基础设施的稳定运行和数据安全，因此需要构建新一代的内部终端准入安全防御体系。

为了防止学校网络资源不受非法终端接入所引起的各种威胁，在有效管理用户和终端接入行为的同时，需采用技术手段保障终端入网的安全可信，同时达到了规范化地管理计算机终端的目的。

2、控制要求

等级保护标准在“安全区域边界”中要求：

* “应能够对非授权设备私自联到内部网络的行为进行检查或限制”。 （8.1.3.1 c）

即需要对学校的内部网络边界进行管控，对非授权的连接行为能够发现和限制。

3、控制措施

针对网络层的非授权连接行为管控可以通过网络安全准入系统（NAC）进行控制，网络安全准入系统可实现以下功能：

（1）安全管理与访问控制

利用网络安全准入系统的动态检测技术和安全策略管理，可针对接入用户和终端进行网络访问控制功能。不符合安全策略的计算机终端进行隔离，并友好提示，提供向导式的安全修复指引。拦截可疑的计算机终端或设备、恶意尝试认证的用户，支持强制下线和账号锁定功能。对接入用户进行动态VLAN的分配管理，有效的对网络访问权限进行控制。

（2）终端安全合规检查

网络安全准入系统的安全检查策略会检测终端入网安全状态，能快速定位发现入网计算机终端的安全合规状态，并利用其本地防火墙隔离管控技术立即将这个设备与网络上的其它设备隔离起来，只能够访问修复区，同时依照策略进行引导修复。对于已授权合规终端，如发现运行阶段又不符合安全检查策略，可调用周期检查或定时检查引擎，对该终端的安全状态进行二次检查，期间如发现不合规进行再次隔离，禁止其访问企业核心资源，可提供安全检查结果详情和全网安全状态统计等日志报表。

（3）访客注册申请

针对外来人员临时性的访问需求，能够进行访客入网管理，包括访客用户注册申请、访客认证、用户审批流程，经管理员审批或系统自动审批后才能认证入网，审批结果可邮件通知用户。

（4）第三方认证源联动

能够实现多种认证源认证方式，包括本地用户、AD认证、LDAP认证、Email认证、Http认证适应用户不同网络环境，满足用户实名制认证、集中统一管理的入网需求。

（5）认证绑定管理

支持多种条件绑定认证，即用户和终端、交换机、VLAN、交换机端口等进行绑定认证、提高入网安全强度。

（6）设备例外管理

用户网络中存在大量的哑终端设备，如：网络打印机、视频会议系统等设备，并分散在各地，能够提供设备的白名单管理，当添加到白名单的合法设备可以直接接入网络，反之非法设备不允许接入，此方式可适应于多种认证技术方式，如：Portal和802.1X认证方式。

（7）强制隔离

用户正常的802.1x认证成功后，如果认证会话没有过期网络会持续可用，系统专有的认证客户端可以实时接收认证服务器的控制指令，管理员可以在任何时候强制在线的用户和终端下线、注销当前登录的网络，确保非正常情况下可对终端入网进行控制和强制隔离处理。

4、产品部署

网络安全准入系统采用旁路部署，通过监听来发现和评估哪些终端入网是否符合遵从条件，判断哪些终端是否允许安全访问企业核心资源，不符合会被自动拦截要求认证或安装客户端才能进行访问，并可配置入网安全检查策略，不符合进行隔离和修复，达到合规入网的管理规范要求。

##### 违规外联检测

1、安全风险

互联网的开放性、交互性、延伸性为校内师生快速获取知识、即时沟通以及跨地域跨校区交流提供了极大的便利；与此同时，互联网的便利性与虚拟性也成为各种不和谐行为滋生的温床，网络恶搞、诽谤中伤、侵犯隐私、色情泛滥等问题，就像打开了潘多拉盒子，对国家安定、社会和谐、学习效率、青少年成长等提出了严峻的挑战。如果不对校内的互联网访问行为加以控制，内网主机在师生安全意识薄弱的情况下违规访问互联网，或者被黑客放置木马反向连接互联网，将导致学校的敏感数据、业务面临安全风险。

2、控制要求

等级保护标准中明确要求：

* “应能够对内部用户非授权联到外部网络的行为进行限制或检查”。 （8.1.3.1 b）
* 应能对远程访问的用户行为、访问互联网的用户行为等单独进行行为审计和数据分析。（8.1.3.5 d）

因此，不仅要对私自接入内部网络的终端进行发现和阻断，还要对内部用户的非授权连接外网的行为进行检查和限制。

3、控制措施

对于终端的非法外联可以通过终端安全管理系统或者采用专业的上网行为管理设备进行控制。终端安全管理系统可对终端的外联端口、外联能力进行检查和阻断，上网行为管理设备通过在网络出口处进行安全策略的配置，限制单位用户的外联访问行为，具体功能如下：

* 上网行为管理系统

（1）URL访问审计与过滤

采用URL分类数据库，通过管理员配置基于URL分类的控制策略（策略条件可包括用户、部门、时间段、访问类别、URL关键字、网页内容关键字、下载文件类型等），进行WEB访问控制，发现非法访问可进行阻断、记录或报警。

（2）应用控制

通过应用特征与行为特征对应用进行识别。所谓应用特征，是指在成序列的数据包的应用层信息中，存在有规律的字节特征，它可以唯一地标识某种应用协议，行为特征，是指连续多个包或者多个并发的网络连接表现出来的某种行为模式具有一定规律性，通过这些行为模式可以识别特征值不明显的应用类型。通过精细化的控制策略设置，可以实现对单位应用访问的精细化管理。

（3）内容审计和过滤

对内容的审计可以有效控制信息的传播范围，控制敏感信息的泄露，避免可能引起的安全风险，内容审计和过滤包括邮件收发审计和过滤、论坛发帖审计和过滤、搜索引擎关键字审计和过滤、HTTP文件传输审计和过滤、FTP文件传输审计和过滤等。

（4）共享接入监控

共享接入是指使用NAT等技术将一个网络出口共享到多个主机，共享接入监控能够对接入网络的设备做观察、控制，能够检测到一个用户或IP所共享的终端数量，并可以对数量做策略控制，以达到掌控用户终端数量的目的，在监控到用户使用的终端数后，可以对此进行控制，屏蔽该用户的上网流量。

 （5）日志审计

能够完整地记录内网用户网络访问的日志，包括上网时间、网络流量、Web访问记录、接收与发送的邮件等等。为进一步的查询统计与报表分析提供了完整的基础信息。

* 终端安全管理系统

为了防止计算机终端用轻易通过拨号、私设代理、多网卡通讯等非法外联手段，造成内部机密外泄的情况发生，终端安全管理系统提供非法外联管控功能，可根据探测类型，使用对应的技术手段如域名解析，对传入的ip或是网址进行连接，如果连接成功则根据策略处理措施，进行对应的提示、断网或关机处理。

（1）外联设备控制（可以禁用终端上可能运行的外联设备——冗余有线网卡、移动数据网卡、MODEM设备、ISDN设备、ADSL设备、WIFI及SSID例外）

（2）外联能力探测（选择探测方式发现终端是否具有外联能力）

（3）外联控制措施（发现终端具有外联能力后的处理措施——提示、断网、关机）

4、产品部署

上网行为管理系统可以串接和旁路镜像部署在学校的互联网出口处，在串接模式下，串接方式能实现对上网行为的控制，并完整审计所有上网数据。串接包括网桥和网关两种模式，采用网桥模式时，当学校拥有两个互联网出口，且学校内部不同子网需要通过不同的互联网出口连接互联网时，上网行为管理系统可提供双入双出，双网桥的部署模式。通过一台设备即可同时管控两条链路内的用户互联网行为。

#### 边界恶意代码检测

1、安全风险

当前，病毒的产生速度、种类、危害程度已经发生了巨大的变化，电子邮件和互联网已经成为网络病毒传播的主要途径，由于网络传播的快速性，对于越来越多的混合型病毒和未知病毒更加难以防范，影响范围也更大，而病毒一旦进入网络内部植入主机，往往已经对学校造成了损失，因此，需要在网络边界处入手，及时检测处病毒，并切断传播途径，采取更积极主动的防病毒措施。

2、控制要求

根据等级保护要求“应在关键网络节点处对恶意代码进行检测和清除，并维护恶意代码防护机制的升级和更新”。 （8.1.3.4 a）

3、控制措施

下一代防火墙一般均具有专业的AV模块，能在网络重要节点处（如互联网入口）进行病毒的检测和清除，但考虑到部分学校已有的防火墙性能不高，也可以采用专业的防病毒网关，在网络边界处进行病毒的检测和阻断。

下一代防火墙通过启用一体化安全防护策略，将反病毒、漏洞防护、防间谍软件、恶意URL防护等功能集成到一条策略，并基于优越的架构设计保障高性能的安全能力。

通过在互联网边界启用下一代防火墙的漏洞防护、防间谍软件、反病毒、URL过滤等功能，基于本地安全引擎，能高效拦截常见漏洞入侵、间谍软件、病毒、木马、钓鱼网站、恶意URL访问等网络威胁。

同时，防火墙通过云端协同可以极大提升特征库数量级，补充本地识别库，并提升防火墙对高级威胁的识别能力，提高防火墙拦截的精确度和高效性。

防火墙的特征库能够支持自动升级，定期进行病毒库的升级和系统的更新。

4、产品部署

为实现对病毒的实时阻断，在互联网边界需串接防火墙，开启AV模块，或在防火墙后串接专业的防病毒网关，实现从网络层检测和阻断恶意代码。

#### 网络安全审计

1、安全风险

随着《网络安全法》的颁布实施，安全审计已经成为网络安全建设的必要措施，随着威胁的多样化，传统信息安全以“防”为主的思路已经发生重大转变，在攻击防不胜防的情况下，持续的监测、快速响应并追踪溯源成为新等级保护体系下的主要思想，因而，安全审计变得尤为重要。

自《网络安全法》实施以来，已经有许多学校因为安全审计没有达到合规要求而面临处罚，因此，新等级保护制度下，安全审计措施的缺失不仅仅将使学校存在安全防护短板，更将会给学校带来严重的合规风险。

2、控制要求

《网络安全法》第二十一条之（三）规定“采取监测、记录网络运行状态、网络安全事件的技术措施，并按照规定留存相关的网络日志不少于六个月”。

等级保护标准中针对网络安全审计的要求包括：

* “应在网络边界、 重要网络节点进行安全审计，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；” （8.1.3.5 a）
* “审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；” （8.1.3.5 b）
* “应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等；”（8.1.3.5 c）
* “应能对远程访问的用户行为、访问互联网的用户行为等单独进行行为审计和数据分析”。 （8.1.3.5 d）

3、控制措施

网络安全审计系统通过镜像获取通过核心交换机上流量数据可对整个网络的流量进行审计分析，可对用户的行为进行审计。包括：

（1）对用户的HTTP、邮件、FTP、TELNET等应用进行审计。

（2）对远程桌面、QQ远程等远程访问行为进行审计。

（3）对用户的互联网访问行为进行审计。

（4）本地日志可以FTP、USB等方式导出，支持将日志发送至外置日志存储系统，确保日志记录满足合规要求。

网络安全事件的踪迹一般都分布在网络的边界设备、安全设备、访问控制设备的日志中，除对网络流量中用户的行为进行审计分析外，发现网络安全事件也是网络安全审计的重要目标，集中安全审计系统通过收集网络设备、安全设备、服务器、应用系统等的日志信息，结合网络流量日志进行关联分析，可以快速发现网络安全事件，并进行定位和报警，相关功能描述可参见“集中安全运营与管理”部分。

4、产品部署

网络安全审计系统通过旁路部署在核心交换机，通过分析网络流量进行用户行为的分析审计。

##### 日志收集与分析系统功能要求

1. 标准1U机架式设备，冗余电源，事件处理性能不低于6000EPS，配置≥6个千兆电口，≥2个万兆光口，≥2个扩展插槽，配置不少于50个节点授权许可，不低于4T硬盘；3年硬件质保。
2. 支持对IT资源中构成业务信息系统的各种网络设备、安全设备、安全系统、主机操作系统、虚拟化、云计算、数据库、中间件以及各种应用系统的日志、事件、告警等安全信息进行全面的审计。
3. 支持通过Syslog、Syslog-NG、SNMP Trap、Netflow V5、JDBC、Agent代理、WMI、(S)FTP、NetBIOS、文件\文件夹读取、Kafka等多种方式完成各种日志的收集功能。
4. 支持对资产日志进行过滤，设置允许接收和拒绝接收日志，并可以对资产设置一定时间范围内未收到事件后进行主动告警。
5. 支持对资产IP地址（含内网IP）的地理信息进行管理，设置单IP及IP段行政区及经纬度，支持地图显示。
6. 内置日志解析不少于130个字段，属性字段可扩展，用户可根据审计需要自行创建字段，字段类型包括IP、字符串、整型等6种，可设定字段长度、选择字段操作符集，选择映射函数等。内置及新增的所有字段均可参与查询、关联分析和报表统计。
7. 支持机器学习对原始日志进行聚类分析，能够对原始日志结构模式进行自动识别(无须范化)，使审计人员清晰了解采集的日志构成。
8. 支持自动识别收集的日志并自动选择范化策略，也可由人工设置设备的范化策略。针对匹配的多条范化策略，系统支持用户手工设置策略匹配优先级。
9. 支持提供安全运维报告，帮助运维人员快速生成日常日志分析和运维报告
10. 具备完善的基于规则的关联分析引擎，支持对关联规则进行监控，了解该规则命中历史情况。

#### 安全区域边界防护架构

安全防护基本要求：安全防护、威胁检测、审计分析、纵深防御



### 安全计算环境

#### 身份鉴别与访问控制

##### 主机身份鉴别与访问控制

1、安全风险

学校应用数据的安全性问题，主要是由于缺乏用户身份验证或者强度不足，对于常见的身份鉴别方式，如用户名+密码，采用字典攻击等手段进行破解仅仅需要几分钟甚至更短。对于校内主机访问权限的制定不够完善，并且未能对学校数据实施有效的访问与隔离措施，给学校重要的业务系统及敏感信息带来严重的安全隐患。

现代学校除了部署办公必需的邮件、OA、学籍、一卡通系统外，也在逐步部署更丰富的学校级应用。诸多应用的引入，不仅给学校信息管理员带来了对各类应用管理、用户权限管理等方面的诸多问题。同时，繁多的应用账号和密码信息也给用户带来了使用的不便。

如学籍管理系统的主机环境涵盖了服务器、终端和网络设备操作系统、系统软件、应用系统、数据库等。这些设备和系统用户在登录时，应进行身份鉴别，并对系统进行最小化授权。学籍管理系统所有涉及的系统用户应当具备仅供其个人或单独使用的独一无二的标识符（即用户ID），以便跟踪后续行为，从而责任到人。

2、控制要求

等级保护制度在“安全计算环境”中，对包括终端和服务器设备操作系统在内的保护对象统一提出了安全保护要求，包括身份鉴别和访问控制要求。

身份鉴别要求包括：

* “应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；” （8.1.4.1 a）
* “应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；” （8.1.4.1 b）
* “应采用口令、密码技术、生物技术等两种或两种以上组合的鉴别技术对用户进行身份鉴别，且其中一种鉴别技术至少应使用密码技术来实现”。 （8.1.4.1 d）

访问控制要求包括：

* “应对登录的用户分配账号和权限；” （8.1.4.2 a）
* “应重命名或删除默认账户，修改默认账户的默认口令；” （8.1.4.2 b）
* “应及时删除或停用多余的、过期的账户，避免共享账户的存在；” （8.1.4.2 c）
* “应授予管理用户所需的最小权限，实现管理用户的权限分离。” （8.1.4.2 d）
* “应由授权主体配置访问控制策略，访问控制策略规定主体对客体的访问规则；” （8.1.4.2 e）
* “访问控制的粒度应达到主体为用户级或进程级，客体为文件、数据库表级；” （8.1.4.2 f）
* “应对重要主体和客体设置安全标记，并控制主体对有安全标记信息资源的访问。” （8.1.4.2 g）

3、控制措施

针对主机的双因素身份鉴别一般可采用专业的终端安全登录产品，终端安全登录产品所使用的密码设备应符合国家密码管理相关要求。

针对主机访问控制的要求，采用服务器加固系统，并进行以下安全配置：

* 启用访问控制功能，依据安全策略控制用户对资源的访问；
* 根据管理用户的角色分配权限，实现管理用户的权限分离，仅授予管理用户所需的最小权限；
* 严格限制默认帐户的访问权限，重命名系统默认帐户，修改这些帐户的默认口令；
* 及时删除多余的、过期的帐户，避免共享帐户的存在；
* 对重要信息资源设置敏感标记；
* 依据安全策略严格控制用户对有敏感标记重要信息资源的操作。

对重要的主机系统采用专业的主机安全加固系统对主机进行整体安全防护，设置强制安全访问控制策略，从而使操作系统达到B1级高安全级别。对数据库进行安全配置，对于存储大量敏感数据的数据库采用安全数据库或数据库防火墙进行保护。

4、产品部署

终端安全登录产品分为服务器端和客户端，服务器端作为重要的管理端设备一般部署在安全管理区，客户端部署在各业务终端上。

##### 应用身份鉴别与访问控制

1、安全风险

智慧校园是高校信息化的高级形态，是对数字校园的进一步扩展与提升，将学校物理空间和数字空间有机衔接起来，基于新型通信网络技术构建业务流程、资源共享、智能灵活的教育教学环境。使师生办公学习不局限于固定位置，而是可以在任何时间、任何地点处理与教学相关的任何事情，从而打造智慧教育新模式。

移动教学给师生带来方便的同时，随之而来的就是移动教学安全问题，如何防范终端安全威胁、保障身份安全、管理用户权限、保护数据安全是每个学校所重点关注的，也是每个安全厂商急需解决的问题。

2、控制要求

根据等级保护要求，在主机操作系统以及应用和数据等多个层面都有对身份鉴别的安全要求。针对应用系统要求

* “应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；” （8.1.4.1 a）
* “应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；”（8.1.4.1 b）
* “应采用口令、密码技术、生物技术等两种或两种以上组合的鉴别技术对用户进行身份鉴别，且其中一种鉴别技术至少应使用密码技术来实现。” （8.1.4.1 c）

3、控制措施

因此，需要实现对应用系统访问的双因素认证，采用身份认证服务系统可以实现对用户身份的统一管理和多种方式组合的强身份认证。

身份认证服务系统可以与安全接入网关（SSL VPN）共同构建应用身份解决方案，该解决方案主要实现以下功能：

（1）多因素身份认证

根据不同的应用场景，可以提供动态口令、数字证书、指纹、二维码等身份安全机制。

（2）口令传输安全加密

身份认证系统与终端间传输的认证信息进行加密处理，加密算法采用RSA、DES、3DES、AES等多种加密算法组合。为了满足国家信息安全的需要，系统同时支持SM系列国密算法，大大降低了认证信息被劫持、被破译的风险。

（3）数据传输加密

在用户通过认证接入SSL VPN后，客户端和服务端通信，默认使用TLS协议创建的安全通道进行数据传输，确保用户账号密码、动态秘钥、应用数据传输的高安全性及稳定性。同时支持移动终端隧道控制策略，实现移动终端连接VPN以后，移动终端数据只能走VPN，不能访问互联网，从而实现防止数据泄密。

同时，为了满足国密办信息安全的相关规定，加强密码算法的安全性。SSL VPN完整支持国密算法，包括 SM1、SM2、SM3、SM4。

（4）访问控制

为不同职责人员匹配不同业务应用，精细化访问控制技术能够细粒度控制接入可以到用户级、资源级，甚至下到URL和文件级的权限，这样不同的用户拥有不同的访问权限。

（5）虚拟工作区

为防止工作区的数据遗落到个人数据区，SSL VPN采用虚拟工作区进行数据分离。个人数据与企业数据进行隔离，落地数据加密，第三方应用或转发到其它设备当中无法打开查看。 启用虚拟工作区之后，终端数据落地加密，数据采用AES256或者SM4加密算法，防止终端数据被拷贝出去而造成数据泄密。

当VPN客户端被卸载、设备进行了Root或者设备超过一定时间不能连接上网关的情况下，移动终端数据可以远程擦除，防止数据泄密。

(6) 终端杀毒

为了保障移动终端免受病毒木马侵扰，避免移动终端被攻击者利用成为渗透学校内网的跳板，身份认证服务系统应当拥有完善的病毒防护体系，不但具备查杀病毒的能力，同时还要能对新生病毒和恶意软件也能够第一时间进行防御，为用户的移动设备提供严密保护。

(7) 用户权限和认证管理

为保证业务系统的安全性，防止越权行为，身份认证服务系统应支持对用户组进行权限分配，将权限一致的人员编入同一组，然后对该组进行权限分配。用户登录时，会根据用户的组查询用户的相关应用策略的分配情况，以决定授予用户哪些服务资源。同时，可以将动态口令认证、AD域认证、LDAP认证、RADIUS认证、数字证书认证等通用认证方式组合使用，以满足客户特定应用的强身份认证需求。

4、产品部署

身份认证系统分为两部分组成：硬件平台与客户端APP。硬件平台采用旁路部署在企业内网，与用户的业务系统/认证系统做到网络可达即可，客户端兼容支持PC、平板、手机（android与ios）。

###### 运维安全管理系统需求

1. 采用专用千兆多核硬件平台和安全操作系统，配置≥6个千兆电口；内置硬盘容量≥4T，预留≥2个业务扩展插槽，配置不少于100个资产管理授权许可，支持不少于150路图形会话或400路字符会话并发；3年设备质保服务；
2. 支持IPv6网络环境下的运维、操作审计；
3. 支持SSH、RDP、VNC、Telnet、FTP、SCP、SFTP、DB2、MySQL、Oracle、SQL Server、Rlogin等协议；
4. 支持通过应用发布实现对MySQL、SQL Server、Oracle、IE、Firefox、Chrome、VNC Client、SecBrowser、VSphere Client、Radmin、dbisql等应用程序/客户端的扩展支持，且图形界面支持分辨率设置。
5. 支持按IP范围、端口进行资源设备自动发现，实现快速批量添加资源设备；
6. 支持云主机资源批量添加，包括阿里云、百度云、华为云、腾讯云、Ucloud、AWS、Azure云平台的资源。
7. 支持不限操作客户端系统类型，无需安装任何客户端插件，使用H5即可直接运维windows、Linux、网络设备等资源；
8. 支持运维过程中会话协同，可邀请其他用户参与、协助操作；会话协同过程中，参与者可以控制会话，创建者强制获取控制权；
9. 设备应符合脆弱性评定且不具有高中风险的安全脆弱性问题；
10. 支持多因子认证，方式包括手机令牌、谷歌认证、360ID、FreeOTP、手机短信、动态令牌、USBKey、微信小程序等多因子认证；
11. 支持对MySQL和Oracle数据库的访问操作控制，可基于库、表、命令实现对数据库操作的细粒度访问控制；
12. 支持工单审批时，可以设置多人审批模式或会签审批模式；
13. 支持用户水印功能，避免数据泄露无法追责；
14. 支持修改系统自身对外提供服务的默认端口，支持页面展示系统负载、内核、内存、网卡、路由表、ARP信息、磁盘使用信息等状态信息；

#### 入侵及恶意代码防范

##### 系统脆弱性评估与检测

1、安全风险

漏洞是系统固有的弱点，是由软硬件开发设计缺陷导致的，而这些设计缺陷往往是不可避免的，只能尽可能消除却无法完全避免，这些漏洞有些是人为的，有些是技术能力所限，但一旦这些漏洞被恶意人员利用，都将给系统带来巨大威胁，而有目的的攻击组织行为往往利用未被公开的漏洞进行恶意攻击，造成的后果往往是灾难性的，因此，单位不许持续发现和关注系统内的漏洞，尤其是高危漏洞，并及时地修补漏洞或者采取其他措施规避风险。

2、控制要求

按照等级保护的要求，主机系统应定期进行漏洞评估并进行安全配置，这些要求包括：

* “应能发现可能存在的已知漏洞， 并在经过充分测试评估后，及时修补漏洞；” （8.1.4.4 e）
* “应关闭不需要的系统服务、默认共享和高危端口”。 （8.1.4.4 b）

3、控制措施

漏洞扫描系统针对传统的操作系统、网络设备、防火墙、远程服务等系统层漏洞进行渗透性测试。测试系统补丁更新情况，网络设备漏洞情况，远程服务端口开放等情况并进行综合评估，在黑客发现系统漏洞前提供给客户安全隐患评估报告，提前进行漏洞修复，提前预防黑客攻击事件的发生。

通过部署漏洞扫描系统，可以帮助用户快速建立针对自己网络的安全风险评估体系。

（1）发现内部资产

帮助用户快速发现内部资产，避免未知资产带来的安全风险，实现内部IT资产的标识和分类管理，方便安全扫描策略的部署何风险评估的进行

（2）实现针对内部网络的脆弱性评估

通过漏洞知识库以及多样的漏洞扫描策略，针对网络设备、系统主机、应用程序等存在的漏洞和风险进行有效评估，并生产完善的评估报告，帮助用户建立起高效的安全漏洞管理解决方案。

（3）建立完善的漏洞管理和风险评估体系

通过定期的漏洞扫描和漏洞验证帮助用户形成规范的全网漏洞管理体系，并辅以风险报表以及解决方案建议，为用户提供了完整的从漏洞发现、验证、修复建议的流程。

（4）解决漏洞原因造成的安全问题

实时漏洞扫描，定期安全漏洞评估帮助用户及时修复当前系统中存在的漏洞，避免漏洞问题造成的安全威胁和带来的安全隐患。

4、产品部署

漏洞扫描系统可旁路部署在待评估网络中的核心交换机上，网络可达待评估的主机、网络设备和系统软件。

###### 漏洞扫描系统功能需求

1. 配置3年漏洞特征库升级，3年硬件维修服务；
2. Web扫描域名无限制，Web扫描任务并发数不少于8个域名。系统扫描IP地址支持不低于1024个，支持扫描A类、B类、C类地址，系统扫描支持不低于100个IP地址并行扫描；
3. 具备操作系统、数据库、网络设备等主流系统的漏洞库列表，支持对主流的数据库软件的漏洞检查，支持Oracle、MySQL、SQL server、DB2等数据库的安全漏洞检查；
4. 支持同时下发系统扫描、Web扫描、弱口令扫描任务，无需单独下发扫描任务，扫描目标可以是IP、域名、URL的任一格式；
5. 支持针对已有任务做任务复制，快速生成一个相同任务，支持对复制出来的任务进行再编辑，包括：基本信息、策略、目标范围、调度、扫描参数；
6. 支持检测的漏洞数大于60000条以上，涵盖漏洞标准包含CVE、CVSS、CNVD、CNNVD、CNCVE、Bugtraq6种，CVSS覆盖CVSS2和CVSS3版本；
7. 支持SSH、SMB、TELNET、RDP、POP、POP3、IMAP、FTP协议的登录扫描；支持批量导入登录信息、批量登录验证；
8. 支持操作系统的配置核查，能够对主流操作系统进行安全配置进行检查，支持windows、linux、unix等主流操作系统；
9. 具备漏洞验证工具，支持通用验证方式，提供GET、Post、Put、Delete等多种验证方式；
10. 支持漏洞数据高级检索及分析，支持按照目标IP或URL、操作系统、MAC地址、资产评分、漏洞等级、漏洞名称、漏洞类别、漏洞评分、开放端口查看漏洞分布情况，并将检索结果导出；
11. 支持Web登录扫描，支持Cookie认证、Form认证、Basic认证、NTLM认证、Session认证、Digest认证、SSL，并支持Web登陆验证，确保Web登录成功；
12. 支持不少于3种漏洞验证方式如浏览器验证、注入验证、通用验证；
13. 支持扫描任务完成后发送告警，告警方式包含邮件告警、短信告警、SNMPtrap告警、SYSLOG告警、FTP告警；
14. 在脆弱性扫描能力方面，能够扫描到浏览器漏洞、SMTP/FTP/WEB/DNS/SNMP/RPC服务的漏洞，能够扫描到windows操作系统共享、用户、口令、注册表等漏洞；

##### 服务器加固

1. 安全风险
2. 服务器漏洞

当前国内使用的操作系统主要是来自国外（如Windows/Linux/Unix），系统漏洞一直影响操作系统的安全，每一次大规模蠕虫病毒的爆发，都提醒人们要居安思危，打好补丁，做好防范工作。对于机器众多的用户，繁杂的手工补丁安装已经远远不能适应大规模网络的管理，必须依靠新的技术手段来实现对操作系统的补丁自动修补。

1. 信息泄露

恶意软件、数据滥用和社会工程学等造成学生学籍信息泄露事件，多类群体中，学生信息堪称“最没有安全保障”的一类， “新鲜出炉”、“没有卖过”的一手学生数据，售价约1到2元每条，大量采购还有优惠。学生数据存放在很多地方，学校、招生办、教育机构等等。目前中小学数据教育部会提供统一平台，但大学数据，则存储在各个大学自己手中。数据存储渠道的多样，增加了接触数据人员的数量，也无限放大了内部人员泄密的风险。减少泄密的风险，首先，要保障私有云安全，保障操作系统安全是防止信息泄密的基础。

1. 资产难掌握

校方难以掌握自身所有资产的安全运营情况。多少资产暴露在互联网？内网又有多少资产？都是什么？获取资产属性的手段单一，掌握的资产信息少、不准确，资产信息靠人工填报，无法掌握资产的变化。

1. 攻防演练常态化

2018年6月，部级：参与护网单位100+，目标业务系统300+ ，爆发0day漏洞8个，未披露的更多。2018年奇安信集团安服团队应急响应救援教育行业50起。2019年上半年应急响应教育行业救援服务29起，上半年教育行业应急同比增加48.3%，其中应急影响范围内部服务器、数据库占比31%，外部、内部网站占比24%。与此同时，攻防演练以及敏感时期重保过程中，大部分高校对自身服务器安全大多缺乏自信，敏感时期果断断网。

1. 控制要求

按照等级保护的要求以及《关键信息基础设施安全保护条例》要求，服务器应定期进行漏洞防护、入侵防御、恶意代码免疫以及进行相关访问安全配置，这些要求包括：

* + - “应关闭不需要的系统服务、默认共享和高危端口；”（8.1.4.4 b）
		- “应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；”（8.1.4.4 c）
		- “应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；”（8.1.4.4 d）
		- “应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞；” （8.1.4.4 e）
		- “应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。”（8.1.4.4 f）
		- “应采用免受恶意代码攻击的技术措施或主动免疫可信验证机制及时识别入侵和病毒行为，并将其有效阻断。” （8.1.4.5）
1. 控制措施

服务器安全加固系统应跨平台支持Windows及Linux双操作系统，以操作系统内核加固技术、web访问控制技术作为核心防御体系，针对操作系统核心资源，如注册表、网络连接、系统文件、进程等进行有效防护。应可有效帮助网站服务器发现并抵御CC攻击、SQL注入、XSS跨站、漏洞利用、病毒、木马、后门等黑客入侵行为。

1. 操作系统加固

针对操作系统核心资源，如注册表、网络连接、系统文件、进程等资源进行有效防护。包括：禁止将非管理员组账户添加到管理员组；禁止在系统目录下对可执行类型文件进行写操作；禁止修改host文件；禁止添加启动项；禁止磁盘低级操作；禁止加载没有数字签名的驱动。

1. 服务器漏洞修复

该功能可以扫描服务器系统，列出未修复的不同级别的漏洞补丁和已过期的补丁。用户可以根据漏洞的严重程度和必要性选择是否修复，针对一些暂不需要更新的补丁则可以进行忽略，当需要更新时取消忽略即可更新。应支持虚拟补丁。

1. 风险识别

通过对业务系统持续学习，自动发现并跟踪业务信息资产的变更，包括：服务器、服务器上运行的软件、网站、及web应用类型等，自动识别安全风险，包括：危险端口、安全漏洞、恶意代码、敏感信息泄露等，进而缩短Attack free 时间窗，避免Shadow IT带来的安全风险。

1. 风险跟踪

通过系统持续自动化跟踪管理的每台服务器安全状态，为每台服务器建立风险档案及风险评分，帮助管理员更好的了解整个业务系统当前的安全状态。通过持续性对业务系统进行安全评估，结合本地服务端，云管理平台双重扫描发现应用漏洞，系统漏洞，风险端口，恶意代码等，并以事件形式展现。

1. 资产管理

应支持自动识别出信息资产，包括服务器、服务器上运行的软件、中间件、网站、甚至网站使用的应用系统类型。通过动态拓扑图的方式展示业务系统服务器间内在关联，便于用户掌握自身所有资产的安全运营情况。

1. 产品部署

在内部网络搭建私有云中心，部署管理监测平台，在私有云业务信息系统和应用服务器上安装部署服务器加固客户端，在内部PC机安装管理控制端，对所有服务器进行管理控制。

##### 终端安全防护

1、安全风险

系统内部面临的各种威胁，尤其是大量的终端系统，校园内的多媒体教室、计算机教室等面临来自病毒木马的入侵、各种类型设备接入不同网络区域不易管理、容易引发泄密等所带来的问题、需要人工维护各类系统进行补丁升级等工作所带来的巨大工作量……，这一系列问题都为单位终端安全管理带来的极大的挑战。

而随着校园安全建设的推进，由于受条件和其它因素限制，在针对上述解决问题制定解决方案的时候，学校往往采取了分而治之的方式，某一类问题就采用一套独立的系统解决问题。现在再回顾的话，学校内部可能部署了多套系统，而这些系统甚至来自不同的厂商，彼此独立完成不同的功能。同时，这些各种各样的安全系统也给企业安全带来了一些新的问题：

（1）终端被各种软件占据，资源耗费巨大

各系统均有独立的数据库、内存加载项、数据扫描行为等一系列资源需求，包括对磁盘存储需求、内存需求、CPU需求等，这些资源需求往往处于自身软件设计的考虑，极易导致对整体终端系统资源的较大消耗，影响用户实际使用体验，干扰用户正常业务工作。

（2）系统之间容易产生冲突

终端安全软件实现方式往往采用进程注入、API挂载、驱动挂载等系统级的处理方式，使得安全软件之间的兼容性，安全软件与其它软件的兼容性出现问题。譬如某软件安装后，其它软件出现功能无法使用、软件无法启动、系统蓝屏等问题。由于终端系统的复杂性，这种兼容性所带来的问题往往都比较难以处理。

（3）系统之间独立，无法联动

安全从过去的孤立针对某个方面的防护已经全面进入大数据阶段，通过各种数据的整合、分析、处置是应对新型威胁的有效办法。而过去安全建设所产生的多种安全防护体系彼此孤立，无论从系统层面还是数据层面都无法进行有效整合，从而造成实际防护效果大打折扣，在应对未知威胁时捉襟见肘。

（4）管理维护困难

多个安全系统的存在意味着针对每个系统要有不同的运维管理的工作量，如系统的安全策略的定义、细化、调优、更改，系统的更新，系统日志管理、数据库管理等一系列工作。这无疑给安全管理人员提出来非常高的要求，这不仅仅是增加了工作量，而且要求管理员在不同的系统之间进行管理切换必须充分了解每个系统之间细微的差别，以确保对系统的设置不会出错。

2、控制要求

除了终端身份鉴别和访问控制外，等级保护对终端的安全防护主要从以下几个方面进行要求：

* “应采用免受恶意代码攻击的技术措施或主动免疫可信验证机制及时识别入侵和病毒行为，并将其有效阻断；” （8.1.4.5）
* “应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；” （8.1.4.3 a）
* “审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；” （8.1.4.3 b）
* “应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等；” （8.1.4.3 c）
* “应对审计进程进行保护，防止未经授权的中断。” （8.1.4.3 d）
* “应对安全策略、恶意代码、补丁升级等安全相关事项进行集中管理”。 （8.1.5.4 e）

3、控制措施

综合分析学校面临的终端安全风险，需要一个综合的终端安全管理系统，以应对不同层面的安全需求，满足合规要求，而满足这些安全需求的同时，又不会割裂这些系统之间的关系，使得他们能在统一的安全环境里执行一致的安全策略，并互相协同，发挥最大的安全防护效率。

采用终端安全管理系统作为终端合规管控一体化解决方案。通过建设恶意代码防范体系、落实终端安全管理技术措施、启用统一终端运维、开启安全审计功能，来建设终端合规一体化体系，一体化终端安全管理的建设内容如下：

（1）终端恶意代码防护

全网部署终端安全管理系统客户端代理，通过集中管理端实现对病毒查杀策略、病毒库的统一升级管理。通过采用云查杀引擎、未知病毒检测等新技术，解决传统防病毒软件本地特征库对新型病毒查杀效果不明显的问题。

（2）终端统一安全管控

在终端安全管理系统的控制中心制定策略，进行全网终端的流量监控、非法外联监控、应用程序黑白名单控制、外设管控、桌面安全加固等。

（3）终端软件管理

通过策略配置和日志报表功能，管理员可以掌握网内软件使用情况，及时发现异常，保证校园内部网软件的正常运行和软件安全性，支持校园软件的统一分组、定时分发，并可实现自动安装应用以及强制卸载应用，帮助管理员按照校园规定管理终端用户软件的安装。

（4）统一补丁升级和管理

教学及办公网络中存在各种不同类型的操作系统及不同版本的操作系统都需要进行全面的补丁管理，终端安全管理系统控制中心对全网计算机进行漏洞扫描把计算机与漏洞进行多维关联，根据终端或漏洞进行分组管理，并且能够根据不同的计算机分组与操作系统类型将补丁错峰下发，并能实现对补丁库的统一升级和管理。

（5）终端统一安全运维

终端安全管理系统统一运维功能，实现全网终端硬件资产管理，并且通过远程协助功能，当终端需要远程帮助的时候，运维人员向终端用户发送远程控制请求，等终端用户确认后，协助IT维护人员高效的完成终端运维工作。

（6）终端综合审计

终端安全管理系统通过综合审计功能，对终端用户的行为进行审计，审计内容包括软件使用日志、外设使用日志、开关机日志、系统帐号日志、文件操作日志、文件打印日志、邮件记录日志等；并提供报表功能，对终端安全日志、漏洞修复、病毒日志、木马查杀、插件清除、安全配置、文件及应用日志、终端事件告警等信息进行报表统计。

4、产品部署

在网络内部部署终端安全管理系统控制中心和终端，终端通过控制中心连接到升级服务器进行升级、更新等。终端根据控制中心制定的安全策略，进行杀毒、修复漏洞、运维管控、移动存储管理等安全操作。

###### 终端安全管理系统功能需求

1. 配置不少于500点位Windows或国产操作系统终端至少包含病毒查杀、补丁管理、主机防火墙、终端管控功能的授权；不少于25点位Windows Server或国产服务器操作系统至少包含多引擎协同，对病毒、木马、恶意软件等查杀功能授权；不少于5点位Linux Server至少包含对病毒、木马、恶意软件等查杀功能授权；上诉授权点位数量可按照实际情况随意拆分 windows或国产操作系统终端授权、信创终端授权；特征授权配置3年升级服务；
2. 控制中心采用B/S架构管理端，根据客户端点数的增加支持横向扩展；
3. 支持根据分组、计算机名称、IP地址、操作系统、在线状态等条件的组合筛选出符合条件的终端进行管理；
4. 支持定时公告功能，可配置开机显示、周期显示和立即推送；
5. 管理控制中心当登录账号输入密码错误次数超过锁定阈值后账号将被锁定，同时应支持双因子认证登录方式，提高安全性；
6. 客户端主程序、病毒库版本支持按分组和多批次进行灰度更新，保持在低风险中完成终端能力更新。支持设置不同终端类型设置和每批次观察时长。
7. 支持终端密码保护功能，支持终端“防退出”密码保护、“防卸载”密码保护、防安装密码保护；
8. 病毒防护日志包含：病毒查杀日志、查杀任务日志、攻击防护日志、系统防护日志、按分组、按终端、按时间；
9. 支持扫描资源占用设置，可设置不限制、均衡型、低资源三种模式；
10. 支持自动阻止远程登录行为，防护黑客远程爆破和拦截恶意的远程登录；
11. 支持开启自动修复漏洞，包括开机时修复，并支持随机延迟执行、间隔修复和按时间段修复，可设置延迟时间、间隔修复时间和修复时间段；
12. 支持对外设进行多维度的放行，包括设备名称、PID/VID、实例路径，通过添加实现例外或加黑；
13. 支持国产操作系统安全防护，包括银河麒麟、中标普华、一铭、红旗、中标麒麟、深度、中科方德等，支持飞腾、龙芯、兆芯、申威等国产cpu，实现了与国产各平台的无缝对接。

##### WEB应用安全防护

1、安全风险

2019年上半年，网络攻击数量总体呈上升趋势，网站态势依然严峻，教育行业的网站漏洞数量发现最多。关键时间节点，如高考报名及公布成绩期间，重大节假日期间，学校网站面临ddos攻击和网页被恶意篡改风险。对于校园网来说，校内拥有大量的教育网公网地址，缺省情况下，互联网用户都可以访问到这些地址，因此学校内部老师或者学生私自创建了大量的科研、学术、生活类网站。再加上服务器部署时间长、人员更迭，服务器的应用情况很难摸清。

Web服务器端是Web安全防护的重要环节，虽然Web服务器做了相关的安全防护。但服务器端的安全设置较为专业、复杂，一旦设置不合理，就使得Web服务器端很容易成为恶意攻击入侵的对象。

2、控制要求

在等级保护要求中对于计算环境的安全防护明确要求：

* “应能发现可能存在的已知漏洞， 并在经过充分测试评估后，及时修补漏洞；” （8.1.4.4 e）
* “应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。” （8.1.4.4 f）

3、控制措施

可以采用WEB应用防火墙及web安全云防护对WEB应用进行安全防护。WEB防火墙可针对WEB应用实现以下防护功能。

（1）漏洞防护

Web应用防火墙能够对SQL注入、跨站脚本、代码执行、目录遍历、脚本源代码泄露、CRLF注入、COOKIE篡改、URL重定向等多种漏洞攻击进行有效防护。

（2）攻击防护

Web应用防火墙能够对用户请求提供多重检查机制和智能分析，确保对高安全风险级别攻击事件的准确识别率。针对Flood攻击、SQL注入、跨站脚本、目录遍历等主要攻击手段， WAF系统提供了有效识别、阻断并告警。

（3）网页代码检查

Web应用防火墙能够对用ASP、ASPX、JSP、PHP、CGI等语言编写的页面，对用SQL Server、MySQL、Oracle等数据构建的网站进行检查，能够在客户网站被挂马之前发现网站的脆弱点，从而使客户可以未雨绸缪，避免挂马事件的发生。

（4）访问加速

Web应用防火墙通过在现有的互联网中增加一层新的网络架构，将网站服务器内容缓存到系统内存中，使用户可以就近取得所需内容，降低服务器的压力，解决互联网拥挤的状况，提高用户访问服务器的响应速度。从而解决由于网络带宽小、用户访问量大、网点分布不均等原因所造成的用户访问网站响应速度慢的问题。

（5）挂马检测

多数攻击者在成功入侵并不采取直接的网站篡改，为了获取更多的经济利益往往采取比较隐蔽的方式，其最终目的是为了盗取用户的敏感信息，如各类账号密码，甚至使用户电脑沦为攻击者的“肉鸡”。一旦网站服务器成为传播病毒木马的“傀儡帮凶”，将会严重影响到网站的公众信誉度

（6）网页防篡改

Web应用防火墙内置有网页防篡改监控平台，可以对网页防篡改客户端进行实时监控。当网页防篡改客户端与Web应用防火墙的网络中断时，网页文件会被自动锁定，所有“写”的权限进行封锁，只有“读”的权限。当网络恢复中，所有相关权限会自动下发，网站正常恢复更新。

4、产品部署

部署采用纯透明串行接入模式，交换机上串行接入Web应用防火墙，所有Web请求和恶意访问攻击均由Web应用防火墙来承担处理，清洗、过滤后Web应用防火墙向真实的服务器提交请求并将响应进行整形、压缩等处理后送交给请求客户端。这样可以很好的防范来自互联网的威胁，保护网站的安全、稳定、高性能运行。

安域则部署在云端，它大大利用了云端的资源优势。当DDOS攻击远远超过用户带宽的时候，出口已经被打死，流量清洗设备完全失去效果，安域云平台可以依靠云端的带宽储备进行流量的负载与清洗。在有紧急事件发生时，安域在云端进行防护策略的更新，没有时间延迟，除此之外，安域还具备对网站的加速与监控能力，在页面加速与问题发现的能力上都要比本地设备有效。

###### WEB应用防火墙功能需求

1. 专业性WEB应用防火墙设备，配置≥6个10/100/1000M自适应电口，≥2个千兆SFP光接口，≥2组bypass端口，Web安全保护不少于8个站点；网络吞吐量不低于5Gbps，应用层处理能力不低于500Mbps，网络并发连接数不低于50万，HTTP并发为不低于22万，3年设备质保及WAF特征库升级；
2. 支持旁路部署对镜像流量分析的同时实现阻断功能，产品具备专门的阻断接口设置和对端MAC地址设置功能；
3. 支持对HTTP、HTTPS协议的代理网关功能，支持透明代理、反向代理、负载均衡等模式；
4. 支持SQL注入、XSS跨站攻击防御策略，支持特征检测与语义算法检测；
5. 支持Web业务控制防御功能，提供针对爬虫、黑链、内网代理以及盗链的防护功能；支持Web业务加固防御功能，提供人机识别、弱密码检测、会话安全、CGI安全、跨站请求伪造以及业务流程控制的防御功能；
6. 支持敏感信息检测防护，检测类型包括：中间件信息保护，数据库信息保护，敏感文件保护，代码错误信息保护，隐私信息保护；
7. 具备蜜罐防御功能，提供伪造的后台管理系统页面防御功能；
8. 支持自定义每天、每周、每月自动化对资产识别探测；
9. 支持检测TCP并发链接数，TCP新建链接数，TCP带宽（c2s），UDP带宽（c2s），ICMP带宽（c2s），HTTP GET 速率，HTTP POST 速率，HTTP 其他请求速率，DNS 查询请求速率，并发IP数量等单用户和总量进行自定义阈值配置；
10. 支持检测并抵御IP，TCP，UDP，ICMP，DNS，HTTP协议的20多种DDoS攻击类型；
11. 支持检测漏洞后门类攻击，包括漏洞利用、后门攻击、文件包含、缓冲溢出、目录遍历，shellcode等；支持检测僵木蠕类攻击，包括木马、蠕虫病毒、僵尸网络等；
12. 支持安全态势大屏实时展示，可通过产品自带的实时态势监测模块进行攻击态势地图展示，至少包含对源地域、目标资产、安全防护攻击类型、攻击趋势、HTTP并发请求及实时事件统计；
13. 支持日志综合统计分析，可对源IP、目的IP，源地域，攻击类型，级别，处理动作，协议类型，客户端设备类型，客户端操作系统，客户端浏览器类型进行综合统计分析，并通过饼图、曲线图及柱图等对分析结果进行图形化统计。

#### 数据完整性与保密性

##### 数据加密与保护

1、安全风险

学生数据是学校的核心资产，是攻击者的最终目标，存在学生学籍信息被泄露风险。数据分布在学校信息系统的各个组件中，被大量终端用户进行访问和处理，数据的分散性和流动性导致数据在产生、处理、流转、存储等生命周期中各个环节都面临着巨大的安全风险，必须系统的全面地对数据安全风险进行分析，并采取有效的措施保护数据安全。

2、控制要求

等级保护制度中，对于数据安全的防护要求主要是从完整性和保密性进行规范的，并主要定义了数据在传输和存储环节的安全要求，包括：

* “应采用校验技术或密码技术保证重要数据在传输过程中的完整性， 包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等；”（8.1.4.7 a）
* “应采用校验技术或密码技术保证重要数据在存储过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等。” （8.1.4.7 b）
* “应采用密码技术保证重要数 据在传输过程中的保密性，包括但不限于鉴别数据 、重要业务数据和重要个人信息等；” （8.1.4.8 a）
* “应采用密码技术保证重要数据在存储过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要个人信息等。” （8.1.4.8 b）

3、控制措施

数据的完整性和保密性保护措施可以在应用系统开发过程中同步采取基于密码技术的相关功能实现，但数据保护是个复杂的过程，由于数据的分散性和流动性，在终端、网络、数据库等各层面也需要采用相关的数据防护措施。

建议通过以下具体的技术保护手段，在数据和文档的生命周期过程中对其进行安全相关防护，确保内部数据在整个生命周期的过程中的安全。

（1）加强对于数据的分级分类管理

对关键敏感数据须设置标记，对于重要的数据应对其本身设置相应的认证机制。

（2）加强对于数据的授权管理

对文件系统的访问权限进行一定的限制；对网络共享文件夹进行必要的认证和授权。除非特别必要，可禁止在个人的计算机上设置网络文件夹共享。

（3）数据和文档加密

保护数据和文档的另一个重要方法是进行数据和文档加密。数据加密后，即使别人获得了相应的数据和文档，也无法获得其中的内容。

网络设备、操作系统、数据库系统和应用程序的鉴别信息、敏感的系统管理数据和敏感的用户数据应采用加密或其他有效措施实现传输保密性和存储保密性。

当使用便携式和移动式设备时，应加密或者采用可移动磁盘存储敏感信息。

（4）加强对数据和文档日志审计管理

使用审计策略对文件夹、数据和文档进行审计，审计结果记录在安全日志中，通过安全日志就可查看哪些组或用户对文件夹、文件进行了什么级别的操作，从而发现系统可能面临的非法访问，并通过采取相应的措施，将这种安全隐患减到最低。

（5）进行通信保密

用于特定业务通信的通信信道应符合相关的国家规定，密码算法和密钥的使用应符合国家密码管理规定。

4、产品部署

对于存在大量敏感信息的系统，还可针对信息系统和数据在使用过程中面临的具体风险进行整体地分析，采用专业的数据防泄密系统（DLP）对数据进行全生命周期防护。

##### 数据访问安全审计

1、安全风险

学校大量敏感数据都保存在数据库中，数据库存在的安全风险主要表现在：

（1）无法通过本地部署访问控制，及时发现或阻断超级用户对数据发起的访问。

（2）分布式技术的部署，导致用户对数据的真实存储位置不可知。

（3）虚拟化技术的运用，使用户难以获知正与哪个或者哪些其他用户共享相同的存储或处理设备，对于提供商在解决数据隔离保护问题方面部署措施的有效性更是难以获得充分、可信的信息。

2、控制要求

新等级保护要求对计算环境中包括数据库在内的保护对象有着明确的审计要求，包括以下：

* “应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；”（8.1.4.3 a）
* “应对审计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审计操作，并对这些操作进行审计；”（8.1.5.2 a）
* “应通过审计管理员对审计记录进行分析，并根据分析结果进行处理，包括根据安全审计策略对审计记录进行存储、管理和查询等。”（8.1.5.2 b）

3、控制措施

数据库审计系统能够对业务网络中的各种数据库进行全方位的安全审计，具体包括：

（1）数据访问审计：记录所有对保护数据的访问信息，包括文件操作、数据库执行SQL语句或存储过程等。系统审计所有用户对关键数据的访问行为，防止外部黑客入侵访问和内部人员非法获取敏感信息

（2）数据变更审计：统计和查询所有被保护数据的变更记录，包括核心业务数据库表结构、关键数据文件的修改操作等等，防止外部和内部人员非法篡改重要的业务数据

（3）用户操作审计：统计和查询所有用户的登录成功和失败尝试记录，记录所有用户的访问操作和用户配置信息及其权限变更情况，可用于事故和故障的追踪和诊断

（4）违规访问行为审计：记录和发现用户违规访问。支持设定用户黑白名单，以及定义复杂的合规规则，支持告警。

4、产品部署

一般情况下，数据库审计系统旁路部署在服务器区，对数据库访问行为进行审计。

###### 数据库审计功能要求

1. 采用专用硬件平台和安全操作系统，事件处理不低于30000条/秒，不低于4TB磁盘存储空间，≥6个千兆自适应电口，≥2个扩展槽位，支持液晶屏，3年软件升级和硬件质保服务；
2. 支持Oracle、SQL-Server、DB2、Informix、Sybase、MySQL、PostgreSQL、达梦、人大金仓kingbase、南大通用Gbase，hadoop架构下Hbase，支持后关系型数据库Cache的审计；
3. 支持旁路阻断功能（非串联方式），阻断两种模式，宽松模式：对单一会话危险操作阻断；严格模式：源IP操作的所有请求直接阻断；
4. 支持B/S、C/S应用系统三层架构http应用审计，可提取包括应用系统的应用层帐号、数据库帐号、操作系统用户名、客户端主机名、客户端IP、客户端MAC等身份信息，精确定位到人，并可获取XML返回结果；
5. 支持C/S架构COM、COM+、DCOM组件的审计，可提取应用层工号（账号）的身份信息，精确定位到人；
6. 内置疑似SQL注入、跨站脚本攻击、字段猜测、代码更改、等近500种风险审计规则库，无需单独配置，直接调用；
7. 支持重复操作的统计审计规则，可根据在一定的时间内，重复某项操作达到设定的统计次数进行规则审计告警；
8. 具备翻译功能：实现对SQL语句转换成中文自然语言的描述功能，便于非技术人员理解报警内容；
9. 提供用户界面告警、Syslog告警、SNMP告警、邮件告警、短信系统、短信猫等多种告警方式；
10. 支持全文检索数据库solr的审计，可审计到solr的查询、插入行为的操作信息；
11. 支持操作语句系列的组合审计规则，可根据某一客体的操作行为序列，连续操作了设定的语句序列时进行规则审计告警；
12. 支持事件进行关联综合分析，并能够通过阈值设定筛选潜在危害事件，能够通过用户活动、系统资源使用情况、网络通讯连接数等多种异常情况进行异常事件分析；

## 安全管理体系设计

### 安全管理制度

#### 安全策略和制度体系

1、建设思路

安全技术措施的有效实施需要安全管理制度的助力，同样，安全管理制度的落实也常常需要技术措施的支撑，两者是相辅相成，相互关联的，等级保护对于单位安全制度体系的建设要求参照了ISO 27001的相关标准，即安全管理制度体系自上而下分为安全策略、管理制度和操作规程、记录表单，单位需要建设符合单位实际情况的管理制度体系，应覆盖物理、网络、主机系统、数据、应用、建设和运维等管理内容，并对管理人员或操作人员执行的日常管理操作建立操作规程。

2、建设内容

单位网络安全管理制度体系应结合实际业务需要，建立符合本单位实际情况的安全制度体系，需包括网络安全方针、安全策略、安全管理制度、安全技术规范以及流程等，如下所示。



图 7‑1安全管理制度体系图

（1）安全方针和策略。

最高方针，纲领性的安全策略主文档，陈述本策略的目的、适用范围、网络安全的管理意图、支持目标以及指导原则，网络安全各个方面所应遵守的原则方法和指导性策略。

（2）安全管理制度和规范

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，是必须具有可操作性，而且必须得到有效推行和实施的。

技术标准和规范，包括各个安全等级区域网络设备、主机操作系统和主要应用程序的应遵守的安全配置和管理的技术标准和规范。技术标准和规范将作为各个网络设备、主机操作系统和应用程序的安装、配置、采购、项目评审、日常安全管理和维护时必须遵照的标准，不允许发生违背和冲突。

安全管理制度和规范包括如下表：（示例）

|  |  |  |
| --- | --- | --- |
| 序号 | 类型 | 制度组成 |
| 1 | 总体方针、安全策略 | 《网络安全总体方针和安全策略》 |
| 2 | 安全管理机构 | 《网络安全组织及职责管理规定》 |
| 3 | 《重大事项授权和审批管理规定》 |
| 4 | 安全制度管理 | 《网络安全制度管理规定》 |
| 5 | 人员安全管理 | 《内部人员安全管理规定》 |
| 6 | 《外部人员安全管理规定》 |
| 7 | 信息系统建设管理 | 《信息系统建设安全管理办法》 |
| 8 | 系统运维管理 | 《机房环境安全管理规定》 |
| 9 | 《办公环境安全管理办法》 |
| 10 | 《信息资产安全管理办法》 |
| 11 | 《介质管理办法》 |
| 12 | 《信息资产运行维护安全管理办法》 |
| 13 | 《网络安全管理规定》 |
| 14 | 《系统安全管理规定》 |
| 15 | 《防病毒管理办法》 |
| 16 | 《口令管理办法》 |
| 17 | 《信息系统变更管理规定》 |
| 18 | 《备份与恢复管理规定》 |

（3）安全流程和操作规程

为网络安全建立相关的流程，保证安全运营可以遵照标准流程制度执行，主要的内容包括：

流程制定：建立健全流程管理制度，主要包括的流程有：安全事件处置流程、安全风险评估流程、安全事件应急响应流程、安全事件溯源取证流程、安全设备上线交割流程等；

流程变更维护：定期的维护和修订相关的管理制度；

流程发布：根据需要，定期发布变更后的全套流程到相关的组织范围内，并对发布的流程进行相关的培训。

（4）安全记录单

安全记录单是落实安全流程和操作规程的具体表单，根据不同等级信息系统的要求可以通过不同方式的安全记录单落实并在日常工作中具体执行。主要包括日常操作的记录、工作记录、流转记录以及审批记录等。

#### 制度文件管理

1、建设思路

制度文件需要正式发布并进行定期评审修订和版本控制。网络安全管理制度应该得到单位负责人的签发和认可，只有被正式发布并真正落实的管理制度才能促使单位安全管理能力的提升和安全技术措施的有效运行。

2、建设流程

网络安全管理制度体系是不断改进和完善的过程，包括以下：

（1）制定和发布

安全制度系列文档制定后，必须有效发布和执行。发布和执行过程中除了要得到管理层的大力支持和推动外，还必须要有合适的、可行的发布和推动手段，同时在发布和执行前对每个人员都要做与其相关部分的充分培训，保证每个人员都知道和了解与其相关部分的内容。

安全制度在制定和发布过程中，应当实施以下安全管理：

* 安全管理制度应具有统一的格式，并进行版本控制；
* 安全管理制度应通过正式、有效的方式发布，并进行版本控制；

必须要注意到这是一个长期、艰苦的工作，需要付出艰苦的努力，而且由于牵扯到许多部门和绝大多数员工，可能需要改变工作方式和流程，所以推行起来的阻力会相当大；同时安全策略本身存在的缺陷，包括不切实可行，太过复杂和繁琐，部分规定有缺欠等，都会导致整体策略难以落实，需要不断改进。

（2）评审和修订

应定期对安全管理制度的合理性和适用性进行论证和审定，对存在不足或需要改进的安全管理制度进行修订。。同时应指定网络安全职能部门每年审视安全策略系列文档，具体检查内容包括：

网络安全策略中的主要更新；

网络安全标准中的主要更新。网络安全标准不需要全部更新，可以仅对因变更而受影响的部分进行更新；如果必要，可以使用年度审视／更新流程对网络安全标准做一次全面更新。

* 安全管理组织机构和人员的安全职责的主要更新；
* 操作流程的主要更新；
* 各类管理规定、管理办法和暂行规定的主要更新；
* 用户协议的主要更新等等。

### 安全管理机构

#### 网络安全组织机构及职责

1、建设思路

网络安全管理机构是行使单位网络安全管理智能的重要机构，一般由网络安全管理领导机构和执行机构构成，网络安全领导机构需确保整个组织贯彻单位的网络安全方针、策略和制度等。等级保护制度中明确规定“单位应成立指导和管理网络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担任或授权。”并设立网络安全管理的职能部门。

2、建设内容

单位应根据管理工作需要设立安全管理机构，但至少应包括网络安全领导小组和网络安全管理职能部门，其工作职责分工如下：

（1）网络安全领导小组

网络安全领导小组是公司网络安全工作的最高领导决策机构，负责公司网络安全工作的宏观管理，其最高领导由单位主管领导担任或授权，职责如下：

* 贯彻执行国家关于网络安全工作的方针、政策，组织落实公司网络安全体系建设工作的目标、方针、政策。
* 审定网络安全相关策略、规范及管理规定。
* 监督、检查网络安全相关制度的落实与执行情况。
* 协调指挥网络安全重大突发事件的应急处理。
* 完成上级单位交办的有关工作。

2、网络安全管理部门

网络安全管理部门负责落实网络安全领导小组各项决策，协调组织公司各项网络安全工作，具体职责如下：

* 负责网络安全日常工作的协调和处理。
* 负责网络安全总体规划设计与实施。
* 组织网络安全管理规定的编制；
* 督促网络安全重大突发事件应急预案的落实。
* 组织网络安全培训的相关工作。
* 完成网络安全领导小组交办的有关事项。

#### 岗位职责及授权审批

1、建设思路

网络安全管理应落实岗位安全责任，网络安全组织机构及职责明确了组织层面的管理职责，但管理职责的落实需要层层落实到人，等级保护中明确要求要“设立安全主管、安全管理各个方面的负责人岗位，并定义各负责人的职责”，并设立系统管理员、审计管理员和安全管理员，并明确岗位工作职责。

2、建设内容

根据单位实际情况，设立相关的网络安全管理岗位，但至少应包括安全主管以及“三员”（系统管理员、审计管理员和安全管理员），且“三员”工作职责需分工明确，互相监督，安全管理员需专职，不得兼任其他岗位工作。

三员的岗位职责建议如下：

（1）安全管理员

安全管理员不能兼任网络管理员、系统管理员，其职责是：

* 组织信息系统的安全风险评估工作，并定期进行系统漏洞扫描，形成安全现状评估报告；
* 定期编制网络安全状态报告，向网络安全领导小组报告公司的网络安全整体情况；
* 负责核心网络安全设备的安全配置管理工作；
* 编制网络安全设备和系统的运行维护标准；
* 负责信息系统安全监督及网络安全管理系统、补丁分发系统和防病毒系统的日常运行维护工作。
* 负责沟通、协调和组织处理网络安全事件，确保网络安全事件能够及时处置和响应。

（2）系统管理员

系统管理员不能兼任安全管理员，其职责是：

* 负责网络及网络安全设备的配置、部署、运行维护和日常管理工作；
* 负责编制网络及网络安全设备的安全配置标准；
* 能够及时发现、处理网络、网络安全设备的故障和相关安全事件，并能根据流程及时上报，减少网络安全事件的扩大和影响；
* 负责服务器的日常安全管理工作，确保服务器操作系统的漏洞最小化，保障服务器的安全稳定运行；
* 负责编制服务器操作系统的安全配置标准；
* 能够及时发现、处理服务器和操作系统相关安全事件，并能根据流程及时上报，减少网络安全事件的扩大和影响。

（3）安全审计员

安全审计员的职责是：

* 定期审计网络安全制度执行情况，收集和分析信息系统日志和审计记录，及时报告可能存在的问题；
* 对安全、网络、系统、应用、数据库管理员的操作行为进行监督，对安全职责落实情况进行检查。

单位可根据实际管理需要进行岗位职责的细化，如将系统管理和网络管理工作分别由不同的人负责，对重要的应用系统设置业务系统管理员，对机房、数据库、信息资产进行专门的管理，设置机房管理员、数据库管理员、信息资产管理员等，并明确岗位职责。

在明确岗位职责过程中，单位需梳理在网络安全管理过程中需要授权审批的事项，并根据各个部门和岗位的职责明确授权审批部门和批准人等，对于系统变更、重要操作、物理访问和系统接入等重要事项建立审批程序，按照审批程序执行审批过程， 对重要活动建立逐级审批制度，并定期审查，及时更新相关信息。

#### 内部沟通和外部合作

1、建设思路

网络安全管理工作不是孤立的，在单位业务工作中离不开安全管理工作的保障，同样，网络安全管理工作也离不开单位业务部门的配合，要使网络安全管理工作顺利开展，需“加强各类管理人员、组织内部机构和网络安全管理部门之间的合作与沟通，定期召开协调会议，共同协作处理网络安全问题”，加强内部沟通。

同时，单位的网络安全工作也需要得到外部专家和技术力量的支持，包括监管部门、供应商、业界专家及其他安全组织等。

2、建设内容

聘请专家和外部顾问成员，这些成员需要对网络安全或相关领域有丰富地知识和经验，如安全技术、电子政务、等级保护或质量管理等。专家和外部顾问负责对网络安全重要问题的决策提供咨询和建议。

同时加强与供应商、业界专家、专业的安全公司等安全组织的合作和沟通。建立外联单位联系列表，包括外联单位名称、合作内容、联系人和联系方式等信息。

#### 安全审核与检查

1、建设思路

网络安全管理工作是否有效，安全制度和规范是否得到落实需要单位网络安全管理部门定期进行检查，以便及时发现问题，持续改进和提升网络安全管理能力。按照等级保护的要求，单位网络安全检查可分为定期常规安全检查和定期全面安全检查，安全检查工作需进行认真准备，保留记录。

2、建设内容

单位可根据实际情况，进行安全检查工作安排。包括：

（1）定期进行常规安全检查，检查内容包括系统日常运行、系统漏洞和数据备份等情况；

（2）定期进行全面安全检查，检查内容包括现有安全技术措施的有效性、安全配置与安全策略的一致性、安全管理制度的执行情况等；由于单位人员及安全技术能力有限，全面安全检查可请专业的安全厂商协助完成。

（3）制定安全检查表格实施安全检查，汇总安全检查数据，形成安全检查报告，并对安全检查结果进行通报。单位也可参照上级单位或自行制定安全检查评价指标，以便量化考核安全工作的执行情况。

### 安全管理人员

#### 内部人员安全管理

1、建设思路

人是网络安全工作的主体，也是网络安全威胁的主要来源，调查发现，越来越多的网络安全事件是由内部人员的恶意或工作疏忽导致，因此，加强人员安全管理是网络安全管理工作的重中之重，其中，尤其需要加强对内部人员的安全教育和审核。

2、建设内容

针对内部人员的安全管理需从人员的录用、安全培训和教育、技能考核和调用、离岗审核等全过程进行安全管理，具体管理要求包括：

（1）录用前

* 指定或授权专门的部门或人员负责人员录用；
* 应对被录用人员的身份、安全背景、专业资格或资质等进行审查， 对其所具有的技术技能进行考核；
* 与被录用人员签署保密协议，与关键岗位人员签署岗位责任协议。

（2）工作期间

* 对各类人员进行安全意识教育和岗位技能培训，并告知相关的安全责任和惩戒措施；
* 针对不同岗位制定不同的培训计划，对安全基础知识、岗位操作规程等进行培训；
* 定期对不同岗位的人员进行技能考核；

（3）调离岗

（1）及时终止离岗人员的所有访问权限，取回各种身份证件、钥匙、徽章等以及机构提供的软硬件设备；

（2）办理严格的调离手续，并承诺调离后的保密义务后方可离开。

#### 外部人员安全管理

1、建设思路

在日常业务工作中，单位越来越多地与外部单位人员进行业务合作和往来，外部人员包括指软件开发商，硬件供应商，系统集成商，设备维护商和服务提供商，以及实习生、临时工、调用人员等。这些人员由于工作需要需临时或短期访问单位内部网络，进出单位工作场所，非内部人员由于流动性强，背景情况不明，给单位信息系统的安全带来较大隐患，必须建立严格的物理和网络访问授权审批制度，并有效执行。

2、建设内容

单位应制定外部人员物理访问和网络接入的管理制度，并记录相关内容，具体要求如下：

（1）在外部人员物理访问受控区域前先提出书面申请，批准后由专人全程陪同，并登记备案；

（2）在外部人员接入受控网络访问系统前先提出书面申请，批准后由专人开设账户、分配权限，并登记备案；

（3）外部人员离场后及时清除其所有的访问权限；

（4）获得系统访问授权的外部人员应签署保密协议，不得进行非授权操作，不得复制和泄露任何敏感信息。

### 安全运维管理

按照等级保护要求，日常安全运维管理主要从环境管理、资产管理、介质管理、资产维护管理、漏洞和风险管理、网络和系统安全管理、防病毒管理、配置管理、密码管理、变更管理、备份与恢复管理、安全事件处置管理、应急预案管理、外包运维管理几个方面进行考虑。

#### 环境管理

1、建设思路

环境是指信息系统所处的物理环境，包括机房、配线间、办公场所等，加强对环境的安全管理主要是为了防止非授权物理访问导致的对信息系统的破坏，一般来说，机房作为重要信息设备集中放置的场所应重点加强防护，重要办公区域也需要加强物理防护。

2、建设内容

所有的服务器和核心网络设备均按照要求放置在机房中，指定专门的部门或人员负责机房安全，对机房出入进行管理，定期对机房供配电、空调、温湿度控制、消防等设施进行维护管理；

制定机房安全管理制度，对有关物理访问、物品带进出和环境安全等方面的管理作出规定；

制定办公环境安全管理制度，并对以下方面进行规定：办公室的网络安全要求；办公终端网络安全保密要求；办公终端使用规范等。

#### 资产管理

1、建设思路

信息资产是构成网络和信系统的基础，是系统各种服务功能实现的提供者和信息存储的承载者，应明确单位信息资产的种类、数量、责任人等，并建立清单，定期盘点，对重要信息资产应重点保护。

2、建设内容

编制并定期更新与被保护对象相关的资产清单，包括各类硬件、软件、数据、介质、文档等，确定并标识资产责任部门、重要程度和所处位置等内容；

根据资产的重要程度对资产进行标识管理，针对重要信息资产制定专门的管理措施；

对信息分类与标识方法作出规定，并对信息的使用、传输和存储等进行规范化管理。

#### 介质管理

1、建设思路

介质作为信息的载体，在信息的存储、传递过程中发挥着重要作用，同时，也是恶意代码传播的重要手段、且容易导致信息泄露。

单位需要制定严格的介质管理制度，规范介质的使用行为，对个人介质更加需要严格的管理。

2、建设内容

需制定介质安全管理制度，规定介质的使用范围、介质标识、介质保存等方面的内容。

对于单位介质，需将介质存放在安全的环境中，对各类介质进行控制和保护，实行存储环境专人管理，并根据存档介质的目录清单定期盘点；

对介质在物理传输过程中的人员选择、打包、交付等情况进行控制，并对介质的归档和查询等进行登记记录。

#### 设备维护管理

1、建设思路

信息设备在日常工作中存储和处理业务信息，设备的可用性和安全性对网络安全至关重要，要加强对信息设备日常的管理，包括设备日常维护、外带、报修、报废等。

2、建设内容

对各种设备（包括备份和冗余设备）、线路等指定专门的部门或人员定期进行维护管理；

对配套设施、软硬件维护管理做出规定，包括明确维护人员的责任、维修和服务的审批、维修过程的监督控制等；

信息处理设备必须经过审批才能带离机房或办公地点，含有存储介质的设备带出工作环境时其中重要数据必须加密；

含有存储介质的设备在报废或重用前，应进行完全清除或被安全覆盖，保证该设备上的敏感数据和授权软件无法被恢复重用。

#### 漏洞和风险管理

1、建设思路

网络安全漏洞是信息系统脆弱性的主要表现，易被攻击者利用进而入侵系统进行破坏，对漏洞的发现和修补除了需采取必要的技术措施外，加强对系统的日常安全评估，并及时进行整改修复，也是降低网络安全风险的重要手段。

2、建设内容

定期开展安全评估，形成评估报告，对发现的漏洞等安全问题及时通报，并限定整改时间；

定期开展安全测评，形成安全测评报告，对发现的问题制定整改方案，采取措施应对发现的安全问题，相关内容形成记录。

#### 网络和系统安全管理

1、建设思路

网络和系统作为信息系统的基础性设施，为各个业务系统和办公应用提供连通和数据传输，实现信息共享，网络和系统应进行更细分更专业的管理，对重要的业务系统还需要指定专门的管理人员。

2、建设内容

按照等级保护的要求，对网络和系统的安全管理包括：

（1）划分不同的管理员角色进行网络和系统的运维管理，明确各个角色的责任和权限。可以指定专门的网络管理员、系统管理员、数据库管理员等，对网络设备、操作系统、数据库等进行专业化管理。

（2）指定专门的部门或人员进行账户管理，对申请账户、建立账户、删除账户等进行控制。对重要服务器、数据库、业务应用等的管理账户应更加严格管理。

（3）建立网络和系统安全管理制度，对安全策略、账户管理、配置管理、 日志管理 、日常操作、升级与打补丁、口令更新周期等方面作出规定；

（4）制定重要设备的配置和操作手册，依据手册对设备进行安全配置和优化配置等；

（5）详细记录运维操作日志，包括日常巡检工作、运行维护记录、参数的设置和修改等内容；

（6）指定专门的部门或人员对日志、监测和报警数据等进行分析、统计，及时发现可疑行为；

（7）严格控制变更性运维，经过审批后才可改变连接、安装系统组件或调整配置参数，操作过程中应保留不可更改的审计日志，操作结束后应同步更新配置信息库；

（8）严格控制运维工具的使用，经过审批后才可接入进行操作，操作过程中应保留不可更改的审计日志，操作结束后应删除工具中的敏感数据。

（9）严格控制远程运维的开通，经过审批后才可开通远程运维接口或通道，操作过程中应保留不可更改的审计日志，操作结束后立即关闭接口或通道；

（10）保证所有与外部的连接均得到授权和批准，应定期检查违反规定无线上网及其他违反网络安全策略的行为。

#### 防病毒管理

1、建设思路

对于病毒的防范需要采取必要的安全技术措施，但技术措施的有效性需要安全管理制度进行保障，病毒防范作为单位重要的网络安全基础性工作，必须确保提高全员的防病毒意识，确保技术手段的有效落实。

2、建设内容

（1）制定防病毒管理办法，明确防恶意代码软件授权使用、恶意代码库升级、定期汇报等流程，明确对外来计算机或存储设备接入系统前进行恶意代码检查。

（2）定期验证防范恶意代码攻击的技术措施的有效性；

（3）组织全员的网络安全意识培训，提高全员对病毒的防范意识。

#### 配置管理

1、建设思路

信息系统的配置基线管理是重要的日常运维管理工作，良好的配置管理是系统安全可靠运行的基础，配置基线应结合等级保护的要求，进行相关配置信息的保存、更新和变更控制。

2、建设内容

单位日常配置管理包括：

（1）记录和保存基本配置信息，包括网络拓扑结构、各个设备安装的软件组件、软件组件的版本和补丁信息、各个设备或软件组件的配置参数等；

（2）将基本配置信息改变纳入变更范畴，实施对配置信息改变的控制，并及时更新基本配置信息库。

（3）建立安全配置基线，对设备、操作系统、数据库等制定安全基线，并定期维护安全基线。

#### 密码管理

1、建设思路

根据等级保护的要求，单位在网络安全建设过程中需遵循密码相关国家标准和行业标准，使用国家密码管理主管部门认证核准的密码技术和产品。

2、建设内容

确保在系统中使用的密码相关产品获得有效的国家密码管理主管部门规定的检测报告或密码产品型号证书。

#### 变更管理

1、建设思路

网络安全风险是“动态”的主要因素之一，就是网络和信息系统是会发生变化的，为了加强防范由于网络和系统变化对整体安全现状的影响，规避变更产生的风险，需进行变更管理。

2、建设内容

变更管理建设的内容包括：

（1）明确变更需求，变更前根据变更需求制定变更方案，变更方案经过评审、审批后方可实施；

（2）建立变更的申报和审批控制程序，依据程序控制所有的变更，记录变更实施过程；

（3）建立中止变更并从失败变更中恢复的程序，明确过程控制方法和人员职责，必要时对恢复过程进行演练。

#### 备份与恢复管理

1、建设思路

按照等级保护要求，三级信息系统需具备实时的数据备份能力，并能进行异地备份，对于单位信息系统容灾备份能力的建设，除了建设备份与恢复技术措施外，对备份策略的制定和管理，备份与流程的制定以及备份恢复能力的演练是单位系统实现高可用的重要保证。

2、建设内容

制定单位备份与恢复管理制度，体现的内容包括：

（1）指定责任部门，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；

（2）定义备份信息的备份方式、备份频度、存储介质和保存期等；

（3）根据数据的重要性和数据对系统运行的影响，制定数据的备份策略和恢复策略，备份策略须指明备份数据的放置场所、文件命名规则、介质替换频率和将数据离站运输的方法；

（4）建立备份和恢复流程，对备份过程进行记录，所有文件和记录应妥善保存；

（5）建立演练流程，定期对恢复程序进行演练，检查和测试备份介质的有效性，确保可以在恢复程序规定的时间内完成备份的恢复。

##### 容灾备份系统功能需求

1. 配置2颗八核至强处理器（主频不低于2.1GHz）、内存不低于32G、网卡不低于4个千兆，2个万兆（含光模块）、硬盘配置不低于2\*480GB SSD+5\*8TB SATA企业级磁盘。
2. 配置不低于21个持续数据保护CDP软件许可，不限CDP数据保护容量；配置不限容量和不限节点数量的定时备份软件许可；配置不限容量和不限节点数量的整机备份软件许可。
3. 支持字节级别的实时复制功能，可实现任意历史点数据快速恢复，时间精度达到微秒级别。
4. 实时备份采用真实CDP技术，历史数据恢复的时间精度最小可达到微秒级别。
5. CDP至少包含按“数据增量做快照”、“细粒度快照的时间间隔”、“连续CDP保留”等；CDP连续保留天数≥999天。
6. 提供带宽及数据流控制功能，每个复制任务可根据时间动态调整带宽限制功能。
7. 支持数据一致性比对验证功能，做到数据复制过程中实时比对或自定义校验计划任务 。
8. 支持数据防误删除保护，灾备端同步删除操作前支持将误删除文件归档保存, 可恢复。
9. 支持不同操作系统间的数据复制, 同时要求灾备端文件和数据保留文件属性信息，严格保证数据的完整性和可用性。
10. 支持过滤特定文件或目录功能，同时支持按照文件后缀和类型进行文件过滤；支持数据一致性验证功能，做到数据复制过程中实时比对、或自定义校验计划任务。
11. 实时备份数据格式和生产机数据格式保持一致, 在灾备端可直接使用。
12. 支持灵活的规则管理策略，支持定制CDP数据合并策略，在磁盘空间和CDP恢复时长之间取得有效平衡。
13. 支持从灾备数据副本中全部恢复或选择性恢复单个文件和目录。
14. 支持文件增加前缀后缀操作，同时支持大小写转换，满足客户特殊场景的使用；支持数据镜像前后的脚本检测，满足特殊场景需求。
15. 提供多种代理模式，至少支持一级代理和二级代理来满足NAT和堡垒机的网络环境。
16. 提供统一监控面板,包括针对生产节点CPU、内存、网络、磁盘IO进行图形化的监控展示。
17. 支持多种恢复方式，包括但不限于“即时恢复“、”CDP恢复”、“快照恢复。
18. 支持文件级和块级整机备份，针对不同的操作系统情况选择不同的备份方式；备份数据格式支持原格式文件、QCOW2、VMDK虚拟磁盘文件。
19. 兼容SUSE Linux 、Redhat、CentOS、Debian和Windows，兼容中标麒麟、银河麒麟和红旗等国产操作系统。
20. 支持但不限于Hyper-V、VMware、KVM、OpenStack、FusionCompute等虚拟化平台。

#### 安全事件处置和应急管理

1、建设思路

新等级保护制度强调了单位对于网络安全事件处置能力和应急管理的能力，在当前网络安全威胁形势下，各类安全事件频发，网络安全保障的思路已经从传统的以防为主，转换为更加关注单位威胁检测能力以及快速的响应和处置能力。

2、建设内容

针对网络安全事件需要建设以下内容：

（1）及时向安全管理部门报告所发现的安全弱点和可疑事件；在安全事件报告和响应处理过程中，分析和鉴定事件产生的原因，收集证据，记录处理过程，总结经验教训；

（2）制定安全事件报告和处置管理制度，明确不同安全事件的报告、处置和响应流程，规定安全事件的现场处理、事件报告和后期恢复的管理职责等；

（3）对造成系统中断和造成信息泄漏的重大安全事件应采用不同的处理程序和报告程序。

此外，对单位应急管理需要从总体制度层面加以规范和明确，并按照国家应急管理的相关规定明确流程，定期演练，包括：

（1）规定统一的应急预案框架，包括启动预案的条件、应急组织构成、应急资源保障、事后教育和培训等内容。

（2）制定重要事件的应急预案，包括应急处理流程、系统恢复流程等内容；

（3） 定期对系统相关的人员进行应急预案培训，并进行应急预案的演练；

（4）定期对原有的应急预案重新评估，修订完善。

## 安全运营体系设计

只有安全技术体系和安全管理体系，并不能充分保障达州中医药职业学院系统的安全性，这是因为：一方面，无论是技术控制措施还是管理制度，都需要人来落地操作，这类事情就是运营工作；如果出现不会操作、操作不好或违规操作的情况，而且安全管理者也没有能力对操作行为进行监控，那就必将导致技术体系无法真正发挥威力，也会导致管理体系难以落地；另一方面，技术体系的控制措施，主要通过软硬件系统来实现；然而，还有不少技术控制措施，需要通过人的专业服务来实现；专业安全服务是一类特殊的安全操作，也属于运营体系范畴。总之，安全运营体系的作用是支撑、连通技术体系和管理体系，使之真正发挥效能。

达州中医药职业学院系统上线运行后，将面临新的安全威胁以及较繁重的安全运营工作，传统安全防御体系与安全运维模式已经不能应对新形势下的安全事件监测、响应与处置需求，未知风险对业务系统及数据信息的威胁巨大，如何有效对应安全威胁动态变化、安全意识整体薄弱、安全技能相对缺乏的现状，如何能够不断加强安全运营体系的适用性、高效性、可扩展性，确保业务的连续性以及信息系统抗风险的能力，已成为单位即将面临的重大课题。

紧跟信息化发展趋势，充分利用安全产品、网络产品的数据收集、关联、分析等自动化分析能力，结合企业云端大数据资源及安全威胁情报信息，形成一套规范有序、高效运转、快速响应的安全运营体系，提升对未知威胁感知和防御能力，有效防御各种新型攻击，是新形势下网络安全保障工作的重要环节。

### 安全运营体系总体设计

根据网络安全现状与安全运营需求，开展安全运营体系建设工作，安全运营体系如下图所示。



等级保护安全运营体系图

### 安全运营体系详细设计

#### 日常安全运营

##### 风险管控

###### 互联网资产发现

1、安全风险

近年来联网信息系统的风险形势一直很严峻，并且每一次联网信息系统风险被恶意者利用后导致的损失都较为严重。形势尽管如此严峻，但是大量应急响应案例表明：大量组织未全面掌握暴露在互联网上的IT资产，这就造成了组织的防御边界出现了盲区，成为整个网络安全体系的重要短板。甚至，在一些真实案例中，我们看到组织一方面在竭尽全力检测、分析、抑制攻击，而另一方面，新的攻击却从一些“陌生资产”源源不断爆发出来。这些“陌生资产”就像黑洞一样，平时不可见、无防备，关键时刻却吸引了大量攻击流量、造成整个防御体系的失效。

2、控制措施

互联网资产发现服务是通过平台结合人工分析的方式，针对某一组织，进行互联网资产梳理与暴露面筛查的综合服务。

3、服务方式

通过工具平台和人工梳理相结合的方式，远程进行服务。建议每月或每季度进行一次服务，及时掌握互联网资产的暴露情况。

4、服务交付

服务交付通常包括如下内容：

* 《资产信息库列表》
* 《资产画像》
* 《项目实施方案》
* 《项目实施计划》
* 《服务实施授权书》

###### 基础安全评估

1、安全风险

信息系统是一个复杂系统，覆盖从网络层到数据层的多层结构，容易出现自身的脆弱性问题，包括：标准网元组件（网络设备、操作系统、中间件、数据库）本身的漏洞，以及不合理配置问题，这些脆弱性问题是黑客入侵的基础性条件，给整个信息系统带来了重大风险；同时，信息系统是由人来设计、实施、运营的，人无法做到如机器般的高可靠性，这就意味着脆弱性问题是信息系统始终伴生的问题，必须予以重视和控制。

2、控制措施

采用基础安全评估服务可以对系统进行脆弱性问题进行客观评估，主要包括如下内容：

（1）漏洞扫描

漏洞扫描主要是通过漏洞扫描工具以本地扫描的方式，对评估范围内的终端设备进行主动扫描，从内网和外网两个角度，来查找网络结构、网络设备、服务器主机、数据等安全对象目标存在的安全漏洞。漏洞扫描工作涉及了如下三个层面的安全问题：

* 网络层安全：该层的安全问题主要包括网络设备自身的安全性、网络资源的访问控制、域名系统的安全性等；
* 系统层安全：该层的安全问题主要来自操作系统，包括：UNIX、Linux、Windows以及专用操作系统等。安全性问题主要表现在操作系统本身的不安全因素，包括身份认证、访问控制、系统漏洞等；
* 应用层安全：该层的安全考虑应用系统和数据的安全性，包括：数据库、Web服务、电子邮件系统、业务应用系统等。

（2）基线检查

安全基线是指为满足安全规范要求，各网元设备（网络设备、操作系统、中间件、数据库等）的安全配置必需达到的标准。基线检查就是对各网元设备的安全配置进行人工检查，判断其是否满足安全基线要求，检查内容主要包括了账号配置安全、口令配置安全、授权配置、日志配置、IP 通信配置等方面内容，这些安全配置直接反映了系统自身的安全脆弱性。

* 网络及安全设备基线检查

针对交换机、路由器、防火墙、入侵防御系统、VPN等网络及安全设备进行设备配置的人工检查，尽量减少网络设备因配置不当产生的安全弱点，提升网络设备自身及网络整体的抗攻击能力。

* 操作系统基线检查

针对Windows、Linux、Unix、AIX等操作系统进行系统配置的人工检查，尽量减少服务器因操作系统设置不当生的安全弱点，提升服务器自身的抗攻击能力，并根据应用系统的不同情况，提供定制式安全策略建议，使操作系统的安全级别达到较理想状态。

* 数据库基线检查

针对MYSQL、SQLServer、ORACLE、INFORMIX等数据库进行系统配置的人工检查，尽量减少数据库系统因配置不当产生的安全弱点，提升数据库系统的安全性。

* 中间件基线检查

针对IIS、TOMCAT、WEBLOGIC、Apache、JBoss等中间件进行人工配置检查，利用系统自身的安全功能提高中间件的安全性。

基础安全评估服务可以带来如下价值：

* 提高信息系统的安全脆弱性识别能力；
* 提供丰富完善的安全脆弱性现状分析；
* 提供有针对性的脆弱性问题整改方案；避免因“脆弱性被利用”而产生的安全损失。

3、服务方式

现场提供服务。使用漏洞扫描器、基线检查脚本、基线检查checklist等服务工具。服务周期建议为每月或每季度周期进行。

4、服务交付

服务交付通常包括如下内容：

* 《安全评估报告》
* 《项目实施方案》
* 《项目实施计划》
* 《服务实施授权书》

###### 应用系统安全检测

1、安全风险

除了标准网元组件（网络设备、操作系统、中间件、数据库）本身的脆弱性问题外，购买或开发的各类应用系统也有不少脆弱性问题，而且应用系统和标准网元组件相比，具有更强的个性化特征，也和业务绑定更加紧密；这都造成难以通过漏洞扫描器、基线检查脚本等工具来准确检测应用系统的脆弱性问题。

2、控制措施

针对应用系统的脆弱性检测包括黑盒和白盒两种方式，黑盒方式的检测通过渗透测试服务来实现，白盒方式的检测通过代码安全检测服务来实现。

（1）渗透测试服务

渗透测试服务是在客户授权前提下，依托威胁情报和技术资源，融合原厂工程师、第三方测试人才，融合远程和现场服务，人工模拟黑客可能使用的攻击技术和漏洞发现技术，对目标应用系统的安全性做深入的探测，尽可能广泛、深入地人工挖掘应用系统“真实可被利用”的漏洞并验证，特别是应用漏洞和业务逻辑漏洞。

在服务的过程中，通过实名认证、双因子身份验证、全流量审计等多种管理和技术手段，保障测试过程安全可监控、可审计、可追溯。

（2）代码安全检测服务

代码安全检测是由具备丰富编码经验，并对安全编码原则及应用安全具有深刻理解的安全服务人员，对信息系统或软件源代码及软件架构的安全性、可靠性进行全面的安全检查。

代码安全检测服务的目的在于充分挖掘当前源代码中存在的安全缺陷以及规范性缺陷，从而让开发人员了解其开发的应用系统可能会面临的威胁，并指导开发人员正确修复程序缺陷；从而提高源代码的可靠性，从底层保障应用系统本身的安全性。

代码安全检测服务通过对系统开发框架、应用程序、客户端程序、接口及第三方组件和应用配置这五个方面进行深入的安全分析，从而发现系统源代码存在的安全缺陷，并采用安全测试等技术手段进行漏洞验证。



代码安全检测内容

代码检测服务可以带来如下价值：

* 减少应用系统的安全漏洞和缺陷隐患，从而提高源代码的质量和可靠性；
* 从源头上有效降低应用系统安全风险，保障业务的连续性。

3、服务方式

（1）渗透测试服务

渗透测试服务以远程渗透为主，辅以现场报告解读环节。在交付模式上，采用双交付模式，平衡了交付及时性和交付完整性之间的矛盾。

渗透测试操作在“可信生产环境”中进行，通过在生产环境部署全流量分析系统、SSL VPN、防火墙等完善的安全控制措施，实现对整个渗透过程的事前认证、事中监控、事后审计溯源，将生产风险最大程度降低。

（2）代码安全检测服务

代码安全检测通常在代码权属方指定的安全地点进行。

代码安全检测操作，在“代码检测专用设备”上进行，并禁止连接互联网。专用设备具有公安部颁发的“计算机信息系统安全专用产品销售许可证”，证明公安部已对专用设备的“安全性”进行过安全检测、并获其认可；专用设备是服务方购买的正版产品，并且具有国家版权局颁发的“计算机软件著作权登记证书”。

4、服务交付

（1）渗透服务交付通常包括如下内容：

* 《渗透测试报告》（项目整体性报告）
* 《单个漏洞报告》（通过SaaS系统交付）
* 《项目实施方案》
* 《项目实施计划》
* 《服务实施授权书》

（2）代码安全检测服务交付通常包括如下内容：

* 《源代码安全检测报告》
* 《源代码检测服务方案》
* 《项目实施计划》
* 《服务实施授权书》

###### Web失陷检测

1、安全风险

目前，攻击者的主流特点是隐秘地侵入目标系统、获取关键数据或潜伏等待攻击时机，特别是Web系统，因其部署在网络最外侧提供服务；所以，面临的这类风险最为严重，一旦Web系统失陷，那么攻击者就会以此为跳板，逐渐渗透进内网的各类系统。

2、控制措施

Web失陷检测服务依托安全大数据能力，通过对Web应用访问日志，进行空间和时间维度的关联分析，发现内网中潜在的失陷主机，然后基于大数据溯源技术，找到问题发生的根本原因。攻击者威胁情报中包含了该攻击者在不同时间段使用的IP，并可以根据攻击者不同的技能能力制定不同的技术防御策略，或者使用边界安全防护类设备对IP进行实时的阻断。

Web失陷检测服务可以带来如下价值：

（1）确诊Web应用是否遭受攻击

通过对失陷主机的特征和痕迹进行调查，确诊Web应用是否已被攻击者入侵，并对发现的安全事件进行分析和取证。

（2）还原攻击流程

发生安全事件后仍需要亡羊补牢，该服务会提供入侵事件完整的攻击路线图，包括安全事件中涉及的所有的安全漏洞，可以按图索骥，进行有针对性的修复。

（3）评估安全事件造成的影响

针对已经发生的安全事件，安全工程师会根据攻击者的行为进行事件影响研判。

（4）提升组织的安全对抗能力

利用攻击者威胁情报中的IP和IOC，可以在时间维度上极大地扩充事件调查范围，将不同的攻击来源合并为同源攻击者，完整地看到攻击者的所有攻击手段和相关安全事件。

3、服务方式

工程师现场提取数据，结合软件工具、威胁情报进行人工分析。分析工作在远程或现场均可进行。

建议每月或每季度进行一次分析，及时发现、分析安全威胁和安全事件。

4、服务交付

服务交付通常包括如下内容：

* 《Web失陷检测服务报告》（含整改建议）
* 《项目实施方案》
* 《项目实施计划》
* 《服务实施授权书》

##### 安全运维

###### 应急响应

1、安全风险

由于攻防的不对称性，面对APT类攻击、新型未知攻击，任何安全防御体系都有可能被击穿，这时面临的安全风险既包括系统可用性风险，更有数据失窃或被篡改的风险。因此，应急响应服务至关重要，能及时将网络安全事件带来的损失降至最低，及时“止损”。

2、控制措施

应急响应是针对已经发生或可能发生的安全事件进行检测、分析、协调、处理，保护资产安全属性的活动。应急响应的目标包括：采取紧急措施恢复业务到正常服务状态，调查安全事件发生的原因、避免同类安全事件再次发生等。

应急响应服务突出了组织的协同力量、IT平台的支撑力量，以“快速响应、力保恢复”为行动指南，通过在遇到突发安全事件后采取专业的安全措施和行动，并对已经发生的安全事件进行监控、分析、协调、处理工作，保障网络安全，最大程度地减少安全事件所带来的经济损失以及恶劣的社会负面影响。

（1）应急响应不应是一个部门单兵作战的模式，而应是协同多部门联合开展应急处置工作，形成指挥中心统一调度下的一线、二线多部门联动的大兵团作战模式。

（2）应急响应后端以高效的应急响应系统IT平台以及遍览全国安全事件的“应急响应监控指挥调度中心”作为支撑。为在发生安全事件时，第一时间作出有效决断，提供了强大的后台保障。

应急响应服务可以带来如下价值：

* 系统地响应安全事件，以采取适当的步骤；
* 帮助迅速有效地从安全事件中恢复过来，并将信息丢失、被窃以及服务被破坏的程度降到最低；
* 利用从安全事件处理过程中获得的信息，做好更充分的准备，以处理未来的安全事件并对系统和数据进行更强的保护；
* 建立安全事件响应机制，协同建立有效的防御策略来抵御网络安全威胁。

3、服务方式

现场提供服务，后端以高效的应急响应系统IT平台以及遍览全国安全事件的“应急响应监控指挥调度中心”作为支撑。

4、服务交付

服务交付通常包括如下内容：

* 《应急响应报告》

###### 安全巡检

1、安全风险

安全技术体系的控制措施和安全管理体系的管理制度，有很大一部分是要通过基础运维操作来落地实现。没有好的基础运维操作，技术控制措施就会流于形式，处于“不会用”、“用不好”的尴尬状态。同样，没有好的基础运维操作，管理制度也会流于形式，出现制度、操作两张皮的局面。好的基础运维操作来自于人的专业能力、敬业精神，以及组织的严格管理。基础运维需求的控制措施主要有驻场运维服务、安全巡检服务；其中，安全巡检服务提供相比驻场运维服务，技术难度更高的增强服务，提升对安全软硬件产品的运维能力。

2、控制措施

安全巡检服务包括如下内容：

（1）漏洞扫描

根据的实际需要，对确定的巡检范围内的数据库系统、主机系统、网站系统进行漏洞扫描，并导出、保存漏洞扫描记录。

（2）策略检查

根据的实际需要，对确定的巡检范围内的安全设备、网络设备、服务器，以人工的方式，结合业务状况，进行策略的合理性和有效性检查，记录、保存检查结果。

（3）日志审计

根据的实际需要，对确定的巡检范围内的服务器、数据库系统、网站系统的日志，采用人工和自动化工具相结合的方式，对日志进行审计分析，记录保存日志审计结果。

安全巡检服务可以带来如下价值：

通过专业、严谨的巡检服务，保障IT环境的安全性和稳定性；降低运维风险和运维成本；从繁琐的IT运维中解脱出来，更加的关注核心业务，提高工作效率。

3、服务方式

周期性现场服务。服务周期建议为：每月或每季度一次。

4、服务交付

服务交付通常包括如下内容：

* 《安全设备巡检记录表》
* 《安全设备配置变更记录表》
* 《安全设备配置备份记录表》
* 《安全设备故障维修记录表》
* 《安全设备升级记录表》

###### 态势感知与安全运营平台基础运营

1、安全风险

态势感知与安全运营平台是安全运营工作的中枢平台，是一个复杂的多组件平台，它接入多探针数据进行关联分析，并在平台上流转多种安全业务操作，包括资产管理、漏洞管理、事件流程管理等。所以，态势感知与安全运营平台的基础运营工作，本身就比较复杂，想要做好，对人员有一定的专业性要求。如果基础运营工作做不好，就无法发挥平台的价值，也难以为安全运营体系运转提供有力支撑。

2、控制措施

态势感知与安全运营平台基础运营服务是基于平台提供的专业服务，内容包括：

（1）资产管理

运营人员通过调研、工具收集，充分利用系统的资产管理功能。能够管理网络中的主机设备、终端（办公主机）、网络设备、安全设备、应用系统等），协助建立完整的资产档案信息，管理资产分组、分域的统一维护。支持以资产树的形式显示不同关系。

（2）安全监控

安全监控包括负责平台日常监控工作，筛选过滤告警日志，记录并统计告警信息，协助告警信息的通告下发，定期跟踪事件处置情况，高危安全事件的通告工作等。

（3）漏洞管理

漏洞扫描是发现漏洞的主要手段，网络中重要的主机系统、网络设备都会出现安全漏洞，漏洞的存在会影响着网络的安全性，如果不对其发现和处置，则会成为潜在的安全风险。运营人员利用系统提供了漏洞管理模块，实现对重要主机系统和网络设备漏洞信息的收集和管理。

（4）事件流程管理

威胁处置是一个复杂的流程，需要多级、多人的协同配合。运营人员通过监控、分析、通告传递给达州中医药职业学院相关情况，协助利用平台将告警和漏洞情况通过工单统一跟踪。并将多个人的分析处置结果通过工单统一跟踪和记录，从而使得威胁的处置可追踪。保障每一个威胁都能够通过工单进行及时有效的跟踪，强化了安全威胁的闭环管理，协助做好评价与考核工作，确保安全事件有人盯、有人查、有人管。

（5）平台巡检

态势感知与安全运营平台是由传感器、分析器等多个复杂构建组成，承载着实时收集数据、实时关联数据、实时分析数据的任务。确保平台健康平稳的运行，定期进行技术性维护是运营人员的重要工作。包括各项功能检查、传感器、分析器等多功能组件检查等。

态势感知与安全运营平台基础运营服务可以带来如下价值：

（1）充分地运用平台发挥应有的作用

人、数据、工具、流程，共同的组合成了安全运营，优秀的安全产品亦需要优秀的驾驭者。贴身、专业化的运营服务，能够更专业化地发挥安全设备效能、增加安全收益。

（2）良好的运营更好发挥出产品应有的价值

态势感知与安全运营平台不同于其他类安全防护设备，它接收来自主机、应用、终端、安全设备等各类专业化系统的日志，收集网络中的流量，并进行关联分析。态势感知与安全运营平台的运营可以加强达州中医药职业学院事前与事中的安全保障能力，避免发生“中看不中用”的情况，真正体现出平台的安全中枢价值。

3、服务方式和服务交付

服务方式分驻场服务和计次服务：

（1）驻场服务

一线驻场服务+二线专家远程支持的服务模式；

提供：资产管理、安全监控、威胁分析、事件流程管理、漏洞管理、平台巡检服务；

交付物：日报、周报、月报、年度报告、事件深度分析报告、安全事件通告等。

（2）计次服务

按需到现场进行服务，同时二线专家提供远程支持；

提供：资产管理、威胁分析、平台巡检服务；

交付物：《安全事件分析报告》等。

#### 重大事件保障

1、安全风险

重大事件、重要时期的安全保障工作，是我国安全运营工作的“重头戏”，可以说是“准战时”的工作。在此期间，国内外黑客、特别是国外反动势力的攻击动力大幅提升，组织面临的安全威胁陡然升高；而安全事件一旦发生，其后果通常也远超过日常安全运营阶段。在如此严峻的压力下，如果组织平时的安全运营工作松懈，存在失控资产、各种脆弱性问题，甚至已经被黑客入侵进来，那将面临极大的安全风险，发生安全事件的可能性也较高。

2、控制措施

重要时期安全保障服务（以下简称 “重保服务”）是在重要时期为关键信息系统提供：组织架构设计、积极防御、实时检测、响应处置、攻击预测等安全服务，以提高组织的网络安全保障能力，保障重大活动的顺利进行。

重保服务整体工作分成备战阶段服务、临战阶段服务、实战阶段服务、决战阶段服务四个阶段服务，其中备战阶段服务、临战阶段服务是在重大活动或者会议开始前为安全保障工作做准备；实战阶段服务和决战阶段服务是为重大活动或者会议过程中安全保障工作提供技术支撑。

重保服务可以带来如下价值：

* 保障国家重大活动时期网络网络安全；
* 协助监管单位发现重大活动期间本区域或本行业网络建设存在的问题及安全隐患；
* 全面构建重保期重要单位信息系统的积极防御体系、加强应用系统生命周期安全管理、全面建立重要单位主动运营机制、提升重要单位数据驱动的威胁对抗能力。

3、服务方式

现场为主、结合远程的综合服务交付方式。通常会成立重保领导小组，重保领导小组由达州中医药职业学院分管网络安全领导及服务方重保负责人联合组成，主要负责安全保障工作中关键问题的决策，以及为重保工作的顺利开展协调充足的资源。重保领导小组下设达州中医药职业学院重保工作小组和服务方重保工作小组，主要负责重保工作中的具体安保工作的执行以及双方在重保工作中的配合与沟通。

4、服务交付

服务交付通常包括如下内容：

* 《重要时期安全保障服务工作总结》
* 《重要时期安全保障服务方案》
* 《项目实施计划》
* 《服务实施授权书》

#### 运营赋能

##### 安全培训服务

1、服务内容

依据国家等级保护相关标准及等级保护的实施要求，结合团队丰富的等保实施经验，提供等保培训服务。培训主要通过循序渐进的方式，从浅显的基础到等级保护的实战经验，使学员能够更容易的由浅入深掌握等级保护的相关内容。

主要涉及的培训为三部分，由浅入深分别为等级保护基础篇、等级保护深入篇及等级保护实战篇：

* 等级保护基础篇：讲解等级保护由来、等级保护政策及制度等内容；
* 等级保护深入篇：讲解等级保护技术、管理等方面的详细内容；
* 等级保护实战篇：讲解等级保护定级、差距分析、整改等方面的实操技能。

2、服务方式

服务方式为现场培训。

3、服务交付

* 各类培训课件。

##### 网络安全运营及服务需求

* + - 1. 支持通过关联主体发现、域名探测、主机IP探测、站点探测、组件探测、端口服务探测等方式快速发现全网的域名、站点、IP、服务、数字证书、等资产信息，并结合资产的业务属性动态进行安全标记，形成资产台账进行管理，全方面识别用户数字资产暴露面；
			2. 支持按风险检测任务展示风险的检测情况，包括新增检测结果及修复结果。风险检测包含WEB漏洞、主机漏洞、安全事件、文件泄露、可用性、弱口令、高危服务等。支持算法自动评估风险值，提供风险值变化趋势分析及资产风险值TOP排名；
			3. 支持AI自动化将用户资产与风险关联，将暴露面转化为攻击面，采用验证式漏洞检测技术，对资产进行漏洞扫描发现和验证，通过模拟真实攻击行为，根据上下文智能判断漏洞是否真实存在。支持对用户进行多种协议的弱口令爆破（可自定义弱口令库），检测出攻击者能够爆破利用的弱口令；
			4. 支持展示当前最新的检测结果中新增WEB/主机漏洞和本次被修复的WEB/主机漏洞、新增弱口令和本次被修复的弱口令；支持展示客户当前环境的主机中存在的高危端口服务的检测结果；支持展示用户安全事件发现的变化趋势；
			5. 支持对单个或多个风险创建工单。支持管理员查看任意漏洞历史产生的工单详情；
			6. 支持采用 VPT（漏洞优先级技术）并结合国家标准，自动化计算风险问题的威胁概率（通过风险利用难度、风险影响范围、风险等级等方面），协助用户发现最易被攻击风险点，安全运营专家结合实际业务情况，研判风险利用危害，明确风险响应优先级并进行排序；
			7. 支持按照工单处置流程，对关键基础设施、重要资产的失陷事件。提供处置建议，协助客户进行病毒查杀，安全加固。
			8. 支持对用户暴露在互联网上的站点进行持续的安全监测，提供站点可用性监测（监测站点的服务状态）；安全事件监测（包含如暗链、隐私泄露、页面篡改、恶意连接、死链等）；
			9. 情报扩展来源提供包括公开漏洞库、威胁情报源以及来自第三方的数据风险及供应链安全情报，实现对文件、代码等敏感数据信息泄露监测，对漏洞事件、威胁事件、行业安全事件等攻击情报与暴露面相结合进行预警。
			10. 可阻断已失陷资产与攻击者之间的恶意网络通信，避免机器进一步的数据失窃、系统被破坏，或者被勒索加密等安全事故。
			11. 通过线上工单流程引擎，安全运营人员可协助用户实现从风险的发现、风险的修复到风险的复验全风险生命周期的闭环管理。帮助客户了解企业资产所面临风险的实时状态，挂图作战提高攻击面的收敛效率。
			12. 基于资产情况及安全风险，通过暴露面与攻击向量的聚合分析，提供攻击面分析报告、资产清单、漏洞清单，定期生成月报。
			13. 结合关联分析规则产生的告警，经过安全专家分析研判，将真实的告警信息生成安全事件，并提供处置建议。关基、重要资产的安全事件生成工单，由T1工程师联系客户进行远程或者现场处置。
			14. 提供安全巡检服务，并提供全面的巡检服务报告，给出存在的安全风险并提供对应的修复建议，最终输出《安全巡检报告》。
			15. 提供安全渗透测试服务，在得到授权的前提下，以模拟黑客攻击的方式，对授权业务系统的安全漏洞、安全隐患进行全面检测，最终输出《渗透测试服务报告》。
			16. 提供应急响应服务，当发生黑客入侵、系统崩溃或其它影响业务正常运行的安全事件时，提供第一时间协助对安全事件进行应急响应处理，协助在最短时间内恢复正常运行，并协助查找入侵来源，最终输出《应急响应服务报告》。
			17. 提供重要时期安全保障服务，在重大会议、节假日等特殊时期内，派出安全攻防经验丰富的安全专家，协助对目标系统进行远程安全值守和保障，最终输出《重要时期安全保障服务报告》。
			18. 支持以旁路部署的方式对网络流量进行实时采集，利用多类分析引擎和威胁情报，聚合情报分析、流量分析、异常分析，从海量数据中，快速发现和控制威胁，并进行综合预警，单机最高支持不低于10Gbps网络流量的采集、分析和处理能力。
			19. 需要与本次安全设备以及原有安全设备兼容，实现统一的管理以及安全策略下发。

##### 网络安全运营展示屏

1. ≥75"，4K 超高清显示屏 ，顺滑防眩钢化玻璃，低书写高精度红外触控技术。支持双系统，配置ops模块，ops模块：≥4核心，≥8G内存，≥128GSSD,屏幕比例:≥16:9,响应时间:不高于6ms，接口支持USB2.0、USB3.0,对比度：大于等于4000:1，支持HDR显示，支持无线、有线连接。

# 等保测评需求

技术要求

## 1、项目背景

达州中医药职业学院依据《中华人民共和国网络安全法》的相关要求，拟对本单位的信息系统进行网络安全等级保护测评工作。

本次信息安全等级保护测评涵盖安全技术内容包括：安全技术测评：包括安全物理环境、安全通信网络、安全区域边界、安全计算环境和安全管理中心等五个方面的安全测评。安全管理测评：包括安全管理制度、安全管理机构、安全管理人员、安全建设管理和安全运维管理等五个方面的安全测评。依据相关的测评准则，结合系统的构成特点，确定具体的测评对象，制定测评方案，通过访谈、检查、测评和系统分析等方式判断其安全技术和安全管理的各方面是否达到了相应等级的国家信息系统等级保护要求，找出信息系统中存在的安全隐患，对安全性进行整体评估，制定相关的信息安全整体安全策略和中长期的安全规划，以便对被测系统进行安全方面的调整和改进，确保其安全防护水平达到信息系统安全等级保护相应能力的要求。

## 2、适用范围

本技术规范提出的是最低限度的技术要求。凡本技术规范中未规定，但在相关国家标准中有规定的规范条文，应按相应标准的条文进行服务供应说明。

如果没有以书面形式对本技术规范的条文提出异议，则认为提供的服务完全符合本技术规范。

本技术规范所建议使用的标准如与所执行的标准不一致，应按更严格标准的条文执行或按双方商定的标准执行。

## 3、标准和规范

下列文件中的条款通过本规范的引用而成为本规范的条款，除本技术规范书特别规定外，所提供的测评标准均应遵循公安部相关文件要求和的相关文件要求。

《中华人民共和国网络安全法》

《信息安全等级保护管理办法》（公通字[2007]43号）

《GB/T22239-2019信息安全技术 网络安全等级保护基本要求》

《GB/T22240-2020信息安全技术 网络安全等级保护定级指南》

《GB/T25058-2010信息安全技术 信息系统安全等级保护实施指南》

《GB/T28448-2019信息安全技术 网络安全等级保护测评要求》

《GB/T28449-2018信息安全技术 网络安全等级保护测评过程指南》

## 4、测评范围

|  |  |
| --- | --- |
| **被测评系统名称** | **安全保护等级** |
| 教务系统 | 三级 |
| 财务系统 | 二级 |
| 一卡通系统 | 二级 |

## 5、技术规范

### 5.1、测评及评估原则

**保密性原则：**项目实施方应与签订保密协议，对测评的过程数据和结果数据严格保密，未经授权不得泄露给任何单位和个人，不得利用此数据侵害的权益，否则有权追究的责任。

**标准性原则：**测评及评估方案的设计与实施应依据国家的相关标准进行。

**规范性原则：**项目实施方工作中的过程和文档，应具有规范性，便于项目跟踪和控制。

**可控性原则：**项目的进度应符合进度安排，保证对测评工作的可控性。

**整体性原则**：测评及评估的范围和内容应系统、全面、规范，满足等级保护的相关基本要求。

**最小影响原则：**技术测评及评估工作应尽可能小的影响在线系统和网络的正常运行，不能对现有运行系统造成影响。在线测评及评估应在许可的条件下进行。

### 5.2、实施要求

应详细描述信息系统安全等级保护测评的整体实施方案，包括项目概述、等保测评方案、项目实施方案、时间安排、阶段性文档提交和验收标准等。应详细描述测评及评估人员的组成、资质及各自职责的划分。应配置经验丰富的测评及评估人员进行信息系统安全等级保护测评工作。 本次测评拟排的项目负责人，应具有信息安全等级测评师（高级）证书、信息系统项目管理师证书（高级），拟排的项目经理，应具有信息安全等级测评师（中级）证书、COBIT Foundation信息系统审计认证证书、重要信息系统保护人员CIIP-A（可信计算）证书、ISO27001 Foundation信息安全管理体系认证证书、计算机技术与软件专业技术人员资格证书（信息安全工程师）、信息技术应用创新考试评价证书（信息安全工程师）、ISTQB国际软件测试工程师证书、ITILFoundation管理认证证书，拟派的质量主管，应具有信息安全等级测评师（中级）证书、CISAW信息安全保障人员证书、ITILFoundation管理认证证书、ISTQB国际软件测试工程师证书、信息技术应用创新考试评价证书（信息安全工程师）、CCSC网络安全能力认证证书。

### 5.3、测评及评估方法

测评及评估方法包括访谈、检查和测试三种方法，可细化为文档审查、配置检查、工具测试和实地察看等多种方法。

如需对系统安全等级保护测评实施过程中采用在线测评工具，各种工具软件由项目实施方推荐，经确认后由项目实施方提供并在工作中使用。

安全测评工具软件运行可能需要的硬件平台（如笔记本电脑、PC、工作站等）和操作系统软件等由项目实施方推荐，经确认后由项目实施方提供并在测评中使用。

### 5.4、等级保护测评内容

根据国家等级保护相关标准，本次项目的安全等级保护测评应包括以下内容：

安全技术测评：包括安全物理环境、安全通信网络、安全区域边界、安全计算环境和安全管理中心等五个方面的安全测评；

安全管理测评：包括安全管理制度、安全管理机构、安全管理人员、安全建设管理和安全运维管理等五个方面的安全测评。

#### 5.4.1、安全物理环境

安全物理环境针对物理机房提出了安全控制要求，主要对象为物理环境、物理设备和物理设施等；涉及的安全控制点包括物理位置的选择、物理访问控制、防盗窃和防破坏、防雷击、防火、防水和防潮、防静电、温湿度控制、电力供应、安全等级保和电磁防护。

#### 5.4.2、安全通信网络

安全通信网络针对网络架构和通信传输提岀了安全控制要求。主要对象为广域网、城域网、局域网的通信传输以及网络架构等；涉及的安全控制点包括网络架构、通信传输和可信验证。

#### 5.4.3、安全区域边界

安全区域边界针对网络边界提出了安全控制要求，主要对象为系统边界和区域边界等；涉及的安全控制点包括边界防护、访问控制、入侵防范、恶意代码防范、安全审计和可信验证。

#### 5.4.4、安全计算环境

安全计算环境针对边界内部提出了安全控制要求，主要对象为边界内部的所有对象，包括网络设备、安全设备、服务器设备、终端设备、应用系统、数据对象和其他设备等；涉及的安全控制点包括身份鉴别、访问控制、安全审计、入侵防范、恶意代码防范、可信验证。

#### 5.4.5、安全管理中心

安全管理中心针对整个系统提出了安全管理方面的技术控制要求，通过技术手段实现集中管理；涉及的安全控制点包括系统管理、审计管理、安全管理和集全等级。

#### 5.4.6、安全管理制度

安全管理制度测评是对信息系统的安全管理制度体系和制度内容、制定和发布流程、评审和修订机制等情况进行测评。

#### 5.4.7、安全管理机构

安全管理机构测评是对信息系统的安全管理组织和岗位设置、人员配备、授权和审批、沟通和合作、审核和检查等情况进行测评。

#### 5.4.8、安全管理人员

人员安全管理测评是对信息系统相关内部人员的人员录用、人员离岗、人员考核、安全意识教育和培训，以及外部人员访问管理等情况进行测评。

#### 5.4.9、安全建设管理

系统建设管理测评是对信息系统建设过程中的系统定级、安全方案设计、产品采购和使用、自主软件开发、外包软件开发、工程实施、测试验收、系统交付、系统定级备案、等级测评、安全服务商选择等情况进行测评。

#### 5.4.10、安全运维管理

系统运维管理测评是对信息系统运行维护过程中的环境管理、资产管理、介质管理、设备管理、监控管理和安全管理中心、网络安全管理、系统安全管理、恶意代码防范管理、密码管理、变更管理、备份与恢复管理、安全事件处置、应急预案管理等情况进行测评。

# 模块化机房建设需求

## 建设必要性

我院目前有业务系统包括教务系统、一卡通系统、网站系统等，基本实现教育信息化的建设，投入运行后，几大系统纵横交错，构成了庞大的计算机网络系统。我院网络系统覆盖全院的每个部门，涵盖全院师生，10000多台终端设备同时运行，支持各方面的管理，成为教务教学的重要业务平台，教育信息系统的安全稳定性直接关系到学校工作的正常运行，一旦网络瘫痪或数据丢失，将会给全院师生带来巨大的灾难和难以弥补的损失。因此，建设一个安全稳定的数据中心机房非常必要。

## 机房装修装饰设计

目前我院已经建设单排7柜的模块化机房，还有一个网络机房，为方便统一管理，决定在在大楼2层新建一个模块化机房，把原有机房迁移过来，在配两排机柜模块化机房，其中新主机房面积约64㎡，层高3.6m，梁下净高3.1m，机房设计采用模块化机房进行设计，按B类安全机房和国家相关标准设计，核心包括：机房装修装饰子系统；机房精密空调与新排风子系统；机房综合布线子系统；机房门禁和视频监控子系统；机房UPS子系统；机房供配电子系统；机房消防报警子系统；机房防雷与接地子系统；机房环境集中监控子系统等，具体需求如下：

### 机房平面布局和功能室的划分

机房按主要功能具体划分为：主机房、观察区等。

根据规范，机房室内装修应采用非燃烧材料（燃烧性能为A级）或难燃材料（燃烧性能为B1级）。

满足相关规范，选材和工艺上应注意防尘、防火，防鼠和防水等对材料的基本要求。满足装修整体效果的要求。

考虑经济实用，选用性能价格比较高产品。

机房平面布局和功能室划分

|  |  |  |  |
| --- | --- | --- | --- |
| 房间名称 | 吊顶 | 墙 | 地面 |
| 主机房 | 微孔铝板 | 彩钢板 | 防静电活动地板 |
| 观察区 | 微孔铝板 | 彩钢板 | 防静电活动地板 |

### 吊顶

吊顶采用600X600mm微孔铝板。吊杆必须采用高度可调节的螺杆，吊杆距副龙骨端部不超过100mm,吊杆间距不大于1200mm，吊点按设计图要求布置；

U型38副龙骨吊杆间距不大于1200mm；

安装微孔铝板应在龙骨平直条件下进行，安装时应从一个方向开始，依次安装，不可多点同时进行，避免结合不良；

吊顶施工时，吊顶上的风口、灯具、火灾探测器、消防喷头可在吊顶板就位后进行安装；

天棚上层空间其四壁和顶面应保持平整、光滑、清洁，缝隙处应采用粘接剂嵌平及密封；

微孔铝板四周墙面及灯孔周边经裁割后，应采取压缩密封措施，活动式板的下表面不允许有翘角和出现明显的缝隙。

### 墙面和地面

墙面：主机房采用彩钢板墙面，板后作网格接地处理，达到抗干扰和防静电的效果。其余房间采用墙面乳胶漆等。

地面：主机房安装防静电活动地板，架设高度300mm；性能指标如下：

●规格：600\*600

●材质：钢质

●集中负荷之变形≤2.0mm

●集中载荷≥8880N

●分布负荷≥16000N/m2

●系统阻抗：≥109Ω

●阻燃级别：B1级

●产品寿命长，长期使用无变形、褪色现象。

地面承重计算：

 本次模块化机房（含精密空调、UPS模块、机柜）总重量约为4200kg，服务器、存储、网络设备总重量约为2000kg，设备总重量约为6200kg。根据本次实际配置14个模块化机柜，分别每排7个机柜，中间通道为1.2m，每个机柜的尺寸为0.6m\*1.4m\*2m（长、宽、高），模块化机柜的设备占地面积为：0.6m\*1.4m\*16+0.6m\*1.2m\*8=17.28m²，根据测算本次配置每平方重量为：6200kg/17.28m²=358.79kg/m²

### 门

主机房配置1500\*2100甲级防火防盗门；

### 防尘处理

为保机房的洁净度，除主材选用不起尘的材料外，要做到机房的外围护结构及进出的管道要密封处理；抗静电地板下的地面及墙面要刷地面漆做防尘处理；顶面和墙面要刷乳胶漆防尘。采用新风机保持机房的正压，机房内的空调采用精密空调，含初、中效两级过滤。

### 防火处理

本次设计耐火等级为二级。

主材为非燃性或难燃性外，其它材料尽可能选用难燃性材料，其它辅助材料也主要考虑防火材料。

地面：采用全钢抗静电活动地板，防火等级应该达到B级。

墙面：内填保温防火岩，棉面饰彩钢板；机房内隔断防火等级为B级。

门：采用钢质甲级防火防盗门；防火等级为B级。

其他：木制材料都要刷防火涂料。

### 防水处理

目前空调是机房中容易出现漏水隐患的几个地方之一，因此空调的下水管在安装时要严格检查安装，做到没有渗漏。并且设计在挡水线内布置漏水检测系统，重点检测空调四周。

空调的外机安装在大楼屋顶，管道的进出造成对屋面的破坏，要对破坏处做防水处理。

### 防鼠处理

机房墙上的管道进出处需密封。电线、电缆采用金属桥架。空调的下水管道口用金属网包覆。所有地板下设备的角钢支撑架要用金属网包覆。

### 保温设计

模块化机房设计，机房外围环境无需设置保温措施。

### 机房场地的特殊处理

* 所有外围隔断均包封到顶；
* 进出机房的管洞必须封堵；
* 对窗区域采用双鉴探测器进行安全防护

## 精密空调与新排风系统

### 系统要求

1、精密空调是保证机房环境的重要手段，为满足机房设备及环境的需求，主机房采用精密空调。

根据《计算机场地安全要求》计算机房的环境包括：温度、湿度、尘粒等都必须达到IT设备安全运行的要求，计算机机房内有严格的温、湿度要求，机房内须按相关规定，机房的温湿度应达到B级机房标准要求。

根据机房的实际需求，由于机房内将安装大量服务器、网络设备、存储设备和IT辅助设备，这些设备是机房的主要发热源，由于设备长期处于运行工作状态，其发热量非常大。在计算机机房中发热源主要包括：设备负荷（计算机及机柜热负荷）、机房照明负荷、建筑维护结构负荷、补充的新风负荷、人员的散热负荷等。

为能满足上述要求，保持整个机房的环境应控制在恒定的范围内，采用精密空调实施机房内的环境精确控制。

2、计算机机房必须维持一定的正压，与其他房间的压差不小于4.9Pa,与室外静压差不应小于9.8Pa。为维持机房一定的正压和机房工作人员补充新鲜空气，设置新风系统系统。

### 精密空调系统

精密空调区域划分的原则是提供机房主要设备的环境条件，确保机房安全、可靠地运行。根据GB50174－2017《数据中心设计规范》要求，空调双路电源需进行末端切换，因此在末端配置一套转换开关，从双市电输出上引入两路电源，一路市电为主路，一路为备用电源。空调机组需与消防进行联动。由于大楼场地因素，本次按两路市电设计。

### 数据空调制冷量计算

根据Q＝0.6Q1+Q2

式中Q 数据机房空调总制冷量需求

Q1 主机房设备功率，本次按照每个机柜2KW估算，共28KW。

Q2 主机房建筑热负荷（180W\*机房面积）

Q＝0.5\*机房设备功耗+机房面积\*0.18

Q1=28KW

Q2=9KW

本次使用模块化机房设计，模块内使用2套12.5KW行间精密空调制冷，本配置1+1冗余。

观察区配置1台3P柜机；

### 空调给排水

精密空调的给水水源根据大楼现场实际情况就近引入，给水管从大楼外侧直接进入风冷热泵。

 在2台空调机组的下方地坪做一个集中的15厘米高挡水围堰，以防漏水或积水向机房中部蔓延。围堰内设排水管，接至室外平台落水管。围堰内地坪向排水管处做0.5%坡度。

### 新排风系统

空调系统的新风量依据机房设计规范应取以下三项中的最大值：室内总送风量的 5%；保证工作人员每人 40M3/H;维持室内正压：即主机房相对于室外 9.8Pa，其他房间相对于室外 4.9Pa。为维持机房正压，中心机房设置变频独立新风系统。中心机房与其他房间、走道的压差不小于4.9Pa，与室外压差不小于9.8Pa。相应设置变频独立排风系统，以保证送排风平衡。新风机组的进排风需与消防进行联动，并加装消防防火阀。

考虑10－20%漏风系数，选择一套400 m3/h的机房专用新风机组，标准配置初效/中效/亚高效/离子净化过滤器，洁净新风引入，保持室内正压，保持室内高洁净度。

相应按此风量选择一套400 m3/h的机房专用排风机，以保证送排风平衡。

## 综合布线系统

### 概述

本项目综合布线系统是一个高标准的布线系统，是连接信息系统主机房内所有机房内部及外部语音、数据及多媒体信号的传输通道，它不但必须满足当前的业务处理需求，更需要考虑今后的通讯及宽带网络发展需求。

本次综合布线系统采用5类4对非屏蔽系统及光纤系统，呈星型结构，将为机房的各种网络提供独立的物理链路支持。

机房内的墙面不考虑信息点，走线方式采用上走线，上走线梯架机柜上固定。具备高速大容量的信息传输能力，支持宽带计算机网络，多媒体音视像、语音等可靠的信号传输。

整个网络系统要求具有实用性、灵活性、可扩充性，以及真正的开放性。一次性布线，保证在15年内其系统性能不会下降，功能不会落后，不会因为网络配置的变化而如旧布线方法那样重复土木工程。破坏建筑物原有的结构，增加不必要的投资，真正地达到一次性投资，长年受益。

### 电气防护、接地及防火要求

1. 综合布线区域内存在电磁干扰场强大于3V/m时，应采取防护措施。
2. 综合布线电缆与附近可能产生高平电磁干扰的电动机、电力变压器等电气设备之间应保持必要的间距。综合布线、电缆、光缆及管线与其他管线的间距要求如表。

综合布线系统电缆与电器设备之间间距要求

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 管线类别 | 最小平行净距（mm） | 最小交叉净距（mm） |
| 1 | 闭雷引下线 | 1000 | 300 |
| 2 | 保护地线 | 50 | 20 |

### 桥架部分

1. 桥架敷设：

制作好桥架应平整，内部光洁、无毛刺，加工尺寸准确。

桥架采用焊接连接时应牢固，不应有显著变形。

桥架采用螺栓连接或固定时，宜用平滑的半圆头螺栓，螺母应在桥架的外侧，应固定牢固。

桥架的安装应横平竖直，排列整齐，其上部与顶棚之间应留有便于操作的空间。垂直排列的桥架拐弯时，其弯曲弧度一致。

桥架与桥架之间、桥架与仪表箱之间、桥架与盖之间、盖与盖之间的连接处，应对合严密。

所有弱电线槽皆有警示及鉴别标志或铭牌，子系统共槽采用槽内分割，并良好接地。

线槽配线利用率低于60％。

采用的桥架材料符合GB716—1983《普通碳素结构钢冷轧钢带》的冷轧板，钢板厚度：2mm。表面已进行酸洗、磷化及热镀锌处理，镀锌层厚度：60mm。外观光滑，不起泡，无裂纹。

桥架设计与制造符合CECS 31：9l《钢制电缆桥架工程设计规范》。

1. 桥架接地要求

为确保线路的安全，应使管线有良好的接地端。金属线槽、金属软管、电缆桥架及各配线机柜均需整体连接，然后接地。

就接地系统设计提出以下建议：

镀锌冷轧金属线槽的规格为2米/节，建议在线槽与线槽用连接片连接时加入有效的接地体（连接导线），该接地导线线径不应小于6平方毫米。弱电线槽应统一接入弱电系统的接地电极。

镀锌钢管的规格为6米/根，建议在管与管连接时增加有效的接地体（跨接导线），该接地导线线径不应小于6平方毫米。整个大厦弱电线槽应统一接入大厦的弱电系统的接地电极。

镀锌钢管与镀锌冷轧金属线槽之间的连接也应加入有效的接地连接导线，并接入大厦弱电系统的接地电极。金属线槽与机柜也用跨接导体连接。

各个信息点的出线盒和管路系统内的分线盒，与线管的连接应加入有效的接地连接导线，并接入大厦弱电系统的接地电极。

为防止电磁干扰，弱电线缆管路与强电线缆管路平行走向之间距离应相距20cm以上，即<2KVA应大于127mm；2-5KVA应大于305mm；>5KVA应大于610mm。

在机房中的所有弱电机柜均使用6mm2的多芯绝缘铜线直接与弱电接地端子连接，以确保抗静电活动地板支架构成有效的等电位。

## 门禁和视频监控系统

### 门禁系统

#### 概述

门禁管理系统包括主机房通道门、冷通道前后共3个门禁点。

系统由门禁管理工作站、通讯转换器、门禁控制器、电锁、读卡器、出门按钮等组成。

整个门禁系统应该由UPS提供220V交流电，保证用电安全。

门禁管理工作站设于操作室，门禁控制器根据门禁点位置就近设于地板下，读卡器门旁明装。

#### 门禁身份识别模式

模式：指纹+密码（感应卡）+人脸识别

使用者在门外出示经过授权的指纹+密码（感应卡）+人脸识别，经读卡器识别确认身份后，控制器驱动打开电锁放行，并记录进门时间。使用者离开机房时，按出门按钮，控制器驱动打开电锁放行，并记录出门时间。

### 视频监控系统

#### 系统设计

电视监控系统由前端视频信号采集设备部分、线路传输部分、中心图象控制处理部分以及图象信息的储存和显示部分组成。各部分中包含各相关设备的具体部件。

* 监控点位设计

摄像机为整个监控系统的前端视频采集部分。监控范围为对各机柜正面通道及主要入口通道,共设计3个摄像头，

* 摄像机的供电

摄象机采用UPS集中供电，采用POE交换机集中供电。

* 传输部分

传输部分采用网线沿吊顶内穿电气导管敷设至观察区内的监控控制台内，与相关设备进行连接。

* 监控中心设计

系统监控中心主要由硬盘录像机、显示器构成，系统构成后将一方面进行全实时录像，另一方面可以在监视器上进行各种画面显示。

## UPS系统

### 概述

UPS（不间断电源）是所有网络不间断运行的重要组成部分。考虑到机房信息与数据的安全性，选用UPS不间断电源来保护信息与数据是科学的决策。

### UPS供电系统的要求

UPS按照要求应该向负载提供稳压精度高、稳频、波形失真度小的高质量电源，并且在与静态旁路切换时可以做到供电无间断。在设计的时候要考虑以下几个方面：

1、前级供电系统电源质量不宜太差，电压及频率应稳定在正常范围。

2、前级供电系统中不应当带有别的频繁启动负载，比如经常使用的电梯等。

### UPS主机设计

根据负载容量及性质，选择适当的UPS，既可保证UPS的供电质量，降低故障率，又可节省投资，提高经济效益。一般来说，UPS容量的确定主要是要满足当前负载的需要，同时，也要考虑几个因素：

（1）负载性质对UPS输出功率的影响。

（2）UPS容量较负载不宜过大，使其过度轻载运行。

### UPS容量的确定

本次工程新建UPS设备为机房设备及应急照明供电。总计满配功耗为54KW，其中机房设备45KW；其他设备9KW。

根据GB50174规范要求，UPS设备容量为

S1＝nP1/cos

S1为UPS容量（单位：KVA）

n为UPS安全容量系数(取1.2)

P1为机房IT设备功耗

UPS容量计算：

S1＝ (机房设备功耗+其他设备)/0.8

S1＝(45+9)\*1.2/0.98＝66KVA

结合实际使用情况，本次工程UPS容量确定为60KVA，1个小时延时。

### UPS电池配置要求

为保证电网停电时，也能利用UPS电源继续向计算机提供高质量供电，后备电池的配置尤为重要。

电池容量选择应遵循以下原则：即电池必须在后备时间内供电给逆变器，且在额定负载下，电池组电压不应下降到逆变器所允许的最低电压以下。电池组安装在电池柜内，美观、整洁、散热性好。

## 供配电系统

### 概述

机房电源按照要求应该为一级负荷，按一类供电考虑，保证机房内设备与系统可靠运行。

机房的设备供电应按设备总用电量进行适当的预留。

### 配电设计方案

机房的整个供配电系统都采用具有高度容错功能的冗余式的供配电方案，以确保在市电电网出现故障时，计算机设备能安全可靠的运行。

### 低压配电系统

本次工程配电详见下表。

本项目配电系统，采用放射状系统模式。

UPS配电系统，采用N+1系统设计，采用1+1方式；

精密空调和照明采用市电供电；

照明系统，照明设正常照明和应急照明，应急照明采用UPS电源供电；

机房防雷接地系统、配电系统配置浪涌保护，接地采用联合接地。

应急情况下UPS给机房设备和应急照明供电。

#### 照明系统

满足国家标准JGJ/T16-2008《民用建筑电气设计规范》、《电子信息系统机房设计规范》规定。光线明亮且柔和，适合人们的生理需要；灯具布置合理，为工作人员创造良好的工作环境。

机房中心应设置正常照明和备用照明，主机房及网管监控中心照度为500LX，辅助区为300LX，支持区及行政管理区的照度标准值应满足现行国家标准《建筑照明设计标准》GB 50034的有关规定。

中心机房应设置应急照明，备用照明的照度值应达到一般照明照度值的10%以上，设计照度值50LX; 设置通道疏散照明及疏散指示标志灯，设计照度值5 LX。应急照明系统由蓄电池供电，应急照明灯均匀布置无死角，以保证人员紧急处理以后撤离。

采用600\*600LED光源灯。

## 防雷接地系统

本次工程接地采用联合接地方式，机房防雷接地系统，工作地、保护地采用三地合一的方式，其接地电阻小于1欧姆，如大楼接地电阻大于1欧姆需进行接地整改。

本次工程所有电源设备均采用TN-S接地系统进行保护。利用建筑预留接地扁钢为接地体，作为保护接地、防雷接地、弱电系统接地的共同接地体，接地排引至接地体的点位至少不少于两点。

数据中心内除采用TN-S接地系统，三相五线制，PE线与N线严格分开；所有插座回路均应有专用接地线（PE）；所有设备的金属外壳、各类金属管道、金属线槽等必须进行等电位联结并接地。

联合接地系统包括：主机房直流接地、UPS输出端中性点工作接地、电气设备保护接地、等电位接地、弱电系统直流接地及其它电子设备的直流接地合用同一接地体。机房防静电地板下设置30×3铜排接地网，与所经结构柱内的主钢筋可靠联结。

本项目机房内电源防雷采用逐级防雷。总电源进线处安装一级电源防雷模块，SPD标称放电电流60KA；UPS电源进线处安装二级电源防雷模块，SPD标称放电电流40KA；UPS末端至机柜处建议采用有防雷功能PDU。SPD能够承受8/20µs波型，采用限压型N+1的方式的浪涌保护器

## 消防报警系统

### 设计范围及内容

本项目主机房按规范属于二级保护对象，设计火灾自动报警系统和消防灭火系统。

### 火灾自动报警系统

1）保护等级及系统组成

机房为二级保护对象，采用区域报警系统。

2）火灾探测器的选择

机房的火灾探测器选用点型感烟探测器和点型感温探测器相结合。

3)消防主电源、备用电源供给方式，接地及接地电阻要求

火灾自动报警系统的主电源应采用消防电源，直流备用电源采用火灾报警控制器的专用蓄电池或集中设置的蓄电池。当直流备用电源采用消防系统集中设置的蓄电池时，火灾报警控制器应采用单独的供电回路，并应保证在消防系统处于最大负载状态下不影响报警控制器的正常工作。

火灾自动报警系统接地装置采用共享接地装置，接地电阻值不应大于1Ω。

4) 线路选型及敷设方式

火灾自动报警系统的传输线路选用电压等级不低于交流 500V的铜芯绝缘阻燃导线，线芯截面积 1.5mm2，敷设方式采用穿金属管暗设。

### 气体灭火系统

（1）根据防火保护区的结构特点及相关规范，采用管网式气体灭火系统对防护区进行保护。

（2）根据《气体灭火设计规范》GB50370规定，本工程机房的设计灭火浓度为8%，喷射时间为小于8s，浸渍时间为5min。

（3）详见灭火系统平面图。

灭火及控制方式

（1）本设计采用全淹没灭火系统的灭火方式，即在规定时间内向防护区喷射一定浓度的七氟丙烷灭火剂，并使其均匀地充满整个防护区，此时能将其区域里任何一部位发生的火灾扑灭。

（2）灭火系统的控制方式为自动、手动2种方式。

自动控制：正常状态下,气体灭火控制器的控制方式选择在"自动"位置，灭火系统处于自动控制状态。当保护区发生火情，火灾探测器发出火警信号，火灾报警控制器（或气体灭火控制器）即发出声、光报警信号，同时发出联动命令，关闭空调、风机、防火卷帘等通风设备，经过30秒延时（此时防护区内人员必须迅速撤），输出DC24V/1.5A灭火电源信号驱动启动瓶电磁阀，释放出的控制气体打开对应区域的选择阀，继而打开灭火剂贮瓶上的瓶头阀，释放七氟丙烷实施灭火。

手动控制：在防护区有人工作或值班时，控制方式选择"手动"位置，灭火系统处于手动控制状态。若某保护区发生火情，按下火灾报警灭火控制器(或气体灭火控制器)面板上的"启动"按钮，即可按"自动"程序启动灭火装置，实施灭火。也可在确认人员已经全部撤离的情况下,按下该区门口设置的"紧急启动"按钮，即可立即按"自动" 程序启动,释放七氟丙烷实施灭火。

## 环境集中监控系统

### 系统概述

根据监控中心实际情况，需要实现对机房设备环境的集中监控，机房所监控的智能设备或子系统主要包括：精密空调监控、UPS监控、供配电、机房的温湿度监测、漏水监测等。系统建立可以扩充的整体平台，能够实现子系统之间的联动，实现语音报警或手机短信等各种报警，并且在满足现有需求的同时，可以方便地满足今后系统扩容的需求。

### 系统需求设计

监控系统结构

选用专业监控软件，采用国内外专业的采集前端、工控主机、及相关的硬件，确保系统稳定性。监控软件应该将所有设备环境监控信息，包括视频、设备运行参数、报警信号等集成在同一的平台上，以方便机房管理人员的操作管理维护，而且达到用户可以在任意网络上实现对机房的全面监控的效果。

本地监控站

本地监控系统由监控主机、智能模块、协议转换模块、信号处理模块、智能设备等组成。接收各种实时信息、报警信息和视频信息、显示监控画面和视频内容、处理所有的报警信息、发送管理人员的控制命令、记录报警事件，存储及保存监控数据，完成各种控制任务，实现子系统之间联动等。

远程WEB浏览站

为便于管理人员随时随地了解机房的实际工作状况，实现管控一体化，系统应该提供内嵌于IE浏览器的远程监控模块,方便用户的远程管理。系统可采用管理站或浏览站的客户软件实时查看用户的各分站点机房设备实时运行情况，还可方便地查看各分站点的实时视频及历史视频，还可进行远程数据的存储功能。

智能模块

智能模块用于采集及输出模拟量、开关量等信号，将信号传输给现场本地站，并接受现场本地站的控制信号输出给相应的设备进行控制功能。智能模块分为四种，即智能模拟量采集模块，智能开关量采集模块，智能控制输出模块。智能模块采用RS485通讯接口，可以长距离远传。

各监控系统功能描述

监控对象及内容：根据机房需要，暂定主要监控内容包括：供配电、UPS、空调、新风、温湿度、漏水、防雷设备、消防、门禁、保安等。

## 机柜

### 机柜

根据相关标准，机柜采用服务器专用机柜，42U高，

机房机柜共2列，共14个机柜（其中包含服务器机柜、综合柜）服务器机柜尺寸为600mm\*1400mm\*2000mm。

# 教务管理系统建设需求

## 教务管理系统建设必要性

信息社会的高科技，商品经济化的高效益，使计算机的应用已普及到经济和社会生活的各个领域。计算机虽然与人类的关系愈来愈密切，但是还有人由于计算机操作不方便继续用手工劳动。为了适应现代社会人们高度强烈的时间观念，随着信息技术在管理上越来越深入而广泛的应用，管理信息系统的实施在技术上已逐步成熟。管理信息系统是一个不断发展的新型学科，任何一个单位要生存、要发展、要高效率地把内部活动有机地组织起来，就必须建立与自身特点相适应的管理信息系统。这对于正在迅速发展的各大高校而言，同样有着重要意义。

现如今高校为适应社会的需求以及自身办学的需要，扩建、扩招已在寻常不过。自然就会有更多的学生信息需要处理。如果只靠人力来完成，必然是一项非常繁琐、复杂的工作，而且还会出现很多意想不到的错误，这不仅会给教学及管理带来了很大的不便，也不益于学校全面快速发展的需要。

众所周知，作为高校日常教学中的主要管理工作之一的教务管理，它涉及到院校、专业、师生等诸多方面。特别是目前国家的教育体制也正处在不断改革、创新的阶段，教育部门充分吸取国外优秀的教学模式，结合国内多年的办学经验，逐步探索出了适合中国特色的教学形式，国家教育部面向各级各类学校开展了全面学分制改革。同时，随着选课制的展开和深入，教务日常管理工作也日趋繁重、复杂，如何把教务工作信息化、模块化、便捷化便成为了现代高校发展的重点。所以总的来说，教务管理软件应实现教务信息的集中管理，使传统的教务管理朝数字化、无纸化、智能化、综合化的方向发展，并为进一步实现完善的计算机教务管理系统和全校信息系统打下良好的基础。在高校中，教务管理工作具有举足轻重的地位，教学质量直接取决十教务管理水平。现如今教务管理信息系统的开发与实施可谓日新月异。

在数字校园理论逐步应用的过程中，各高校一方面不断投资购建各种硬件、系统软件和网络，另一方面也不断开发实施了各类教学、科研、办公管理等应用系统，形成了一定规模的信息化建设体系。

教务管理系统是一个庞大而复杂的系统，它包括对学生信息的注册、修改，学生选课及课程管理和学生的四六级考试及计算机等级考试的管理；对教师课程的管理以及对选课学生评分的管理；和管理员对教师、各类考试的综合管理等主要的功能。教务管理系统运行的状况将直接影响到学校里的主要工作，一旦此系统出错，不仅学校的教学进度安排会受到一定程度的影响，而且还会危及到每一个在校学生的切身利益。所以设计一个功能相对完整、操作简单以及界面友好的教务管理系统变得非常必要。

## 教务管理系统功能要求

### 基础信息

* + - 1. 公共资源管理

教学基础资源是高校教学运行的基础保障，需要根据变化情况及时更新。教学资源管理应提供的功能：

* + - * 1. 设置行政结构信息：设置或从数字化校园平台接收学校信息、校区信息、单位信息，包括行政处室及下属科室信息、院系及下属系(教研室)/研究所(室)/行政班信息；支持按照树状结构直观显示学校行政结构示意图。
				2. 设置教学场所：设置或从数字化校园平台接收教学场所信息，包括教学功能区信息、教学楼信息、教室信息。支持自定义教室类型字典表，包括：普通教室、多媒体教室、语音室等。可设置教室距离权重(自动排课时安排就近楼层或楼号)、座位数、有效排课座位数及序号、考试可用座位数及序号。支持批量修改教室的各项属性，如：教室类型、座位数、所属教学楼等。支持批量修改允许是否可借用、排课，以及批量时间锁定功能。
				3. 设置专业信息：能根据学校招生模式的不同按照专业大类、专业、校内专业、专业方向、辅修专业分别进行管理，专业信息包括学制、培养层次、培养对象、所属学科、修读年限等。能够支持校内专业与国标专业的二元化管理(即对内按照校内专业管理，对外按照国标专业管理)。
				4. 设置学年学期：能设置学年学期信息，支持二学期制、三学期制、多学期制的管理。
				5. 班级管理：能根据学年制、学年学分制、完全学分制的信息化管理需要，支持不同类型班级的管理，包括行政级、辅修班级、教学班等，能批量或单个对行政班进行快速拆班、合班处理，及合班后再进行拆班的操作，一个学生可以同时分属多个不同的班级。可设置行政班级的固定教室、班级花名册、所属专业、班主任、辅导员等信息, 支持行政班、辅修班、教学班等等各种类型的班级管理及其开课、排课、课表管理功能(班级类别说明)。支持对班级的管理单位、所在校区进行分学期管理，用户可以分别设置班级各个学期的管理单位和所在校区。
				6. 设置校历功能，管理人员可以设置各学期的校历，指定各学期的开学、放假时间，同时也可以指定特殊的节假日，其中节假日的设定可以同时在课表中进行体现，管理人员在管理课表时能够自动提醒用户。能够对校历中节假日进行批量调课，并在学生及教师的校历页面中进行标注显示，在微信平台中进行提示。
				7. 教职工信息，设置或从数字化校园平台接收教职工信息，包括教师姓名、所在单位、职称、岗位状况、是否外聘等信息；增加外聘教师申请功能，对各学期学校新进的教师或外聘教师，由各院系相应管理人员在网页端或微信平台中提交教师信息新增申请，通过上传文件或拍照等方式提交上传相关材料。

### 学籍管理

学籍管理模块是教学服务系统中多个管理模块的输入端口，也是整个教务系统的基础信息模块，同时它又要求能接受来自教学服务系统以外的数据信息(如：学工管理系统中的奖励信息，招生系统的新生基本信息，财务收费系统的学生缴费情况)。学籍管理模块要能提供学生从入学到离校整个过程中各方面表现的详细记录，主要包括学籍基本信息、学生学籍预警、学籍异动管理、专业分流、方向分流等。

* + - * 1. **学籍基本信息**

学籍基本信息要求包括：学生基本信息(学号：入学到毕业唯一号，自动生成，不重复号)、身份证(默认18位，不对系统提示，也可录港澳身份证或护照号码)、是否师范专业及对应的师范班级、学位授予门类(如：艺术学、管理学)、层次、年制、所在年级、专业代码、毕业年份、是否辅修专业、是否双学位、姓名、姓名拼音、性别、民族、政治面貌、出生日期、生源地、籍贯、联系电话、通信地址、入学年份、所属院系、专业、班级、照片等等)，学生个人简历，家长信息(姓名、身份证号、联系方式)，奖励处分情况，异动信息，注册信息等。要求提供新增、修改、删除学籍基本信息的功能，能够按照多个组合字段对学籍信息进行综合查询，能够导出打印查询结果。

学籍信息导入：要求提供多种格式文件(excel、dbf)的学籍信息导入功能，学籍照片分为录取照片和学生近照，可按学生学号或身份证号命名的照片进行批量导入。照片是.jpg格式。录取照片和学生近照可由管理员统一导入，学生近照也可由学生自行上传，由相关管理员控制上传权限及审核，作为今后开发电子学籍表或电子学生证功能，及人脸识别功能的基础数据。

提供学籍信息更新导入功能，用户可以通过上传excel的方式表把学生信息的追加更新到教务系统。

学籍信息导出：要求能提供多种格式文件(excel、dbf)的学籍信息导出功能，能根据具体需要自定义导出表格的显示字段；支持按照多种照片命名方式(以学号命名、以身份证号命名、以考生号命名)导出系统中的学生照片。

学籍信息网上核对：学生的基本信息采集(导入、录入)到学生信息库中后，学生可以在管理人员的控制下，网上对自己的信息进行校对，管理员可控制学生的范围(年级、专业等)、校对的起止时间、限制学生可修改的字段。学生可提交修改申请，经管理员审批通过后，系统会自动更新到学生信息库中去，某些字段可授权院系具体负责人修改、审核。如：学生的政治面貌。提供院系导出、打印可选多字段的班级核对签名表。

学生的奖惩信息、家庭信息、学生简历、学生异动信息等，通过管理员授权后，可指派到具体负责人来完成日常管理。可给学生设置学籍标签，如拔尖人才、留学生、民族生、交流生、港澳台生、体育特长生等学生标签。

管理员也可以通过本系统生成电子注册上报数据、高基表、基本状态数据、学籍异动汇总表、学生人数统计表、学籍表、学生名册等。公共查询、导出、打印：提供灵活的实时学生人数报表统计、导出、打印。如在校生人数(不含休学、退学、保留学籍、借读、外出借读交流等异动学生)，在校班级数及各班级人数，实时班级花名册，报表(可按性别、院系、年级、专业、层次、班级字段筛选生成报表)，将学生核对完成的学籍表打印纸质存档，并生成相关在校生人数、专业分布等数据统计图表，直观显示学校办学概况。

学期注册信息，与财务系统对接学生学费缴费情况，对学生各学期的注册情况进行管理，可以有针对性的设置未注册学生不允许使用系统或部分功能。

教师系统提供学生监护人信息采集功能，可以收集监护人姓名、证件号码等各项信息。

* + - * 1. **异动**

提供各类学籍异动(转专业、休学、复学、退学、保留学籍、保留入学资格等)的管理功能，要求能根据实际需要自定义扩展学籍异动的类型，能设置异动申请审核的流程。可由学籍管理人员直接进行学籍异动操作，也可按照异动流程由学生在网页端或微信平台中上传相关证明材料，提交异动申请进行各级审批处理后完成异动。提供学籍异动情况的查询统计报表，可生成图表显示统计时间内的学籍异动人数数量、异动原因等。

学籍预警：提供学业成绩结果预警与学籍处理的功能，能针对各种学籍处理类型(如：一级、二级、三级学业预警)设置预警条件，能够在网页及微信平台中及时推送送预警消息给相关用户，如院系领导、班主任，辅导员，学生本人及其家长，并可对多次达到学业预警的学生进行统计。

与考勤系统对接后，对迟到或旷课达到一定数量的学生信息推送给相关用户，可按院系、课程等条件生成相关统计报表，以图形化或表格形式呈现考勤情况，提供学业过程预警。

针对按学科大类招生的要求，能确定需要分流的专业，将需要分流的学生分流到对应专业及相应班级。专业分流时，可由学生从网上进行申请，然后由各院系进行审批与调整，从而形成专业分流后的班级学生名单。针对在分方向的专业，提供专业方向分流的功能，可由学生从网上进行申请，然后由各院系进行审批与调整，从而形成专业方向分流后的班级学生名单。对于分流后的学生，可在培养方案中显示新旧培养方案的课程变动情况，专业方向课程能够以不同颜色标注。

学籍异动后，对一些关联模块会产生影响，系统提供相应的异动联动处理功能，包括：异动后的成绩处理、异动后选课处理、异动后考试安排的处理等。提供学籍异动自动处理功能：在异动完成后，能够按照规则分别对转专业、休学、复学、退学等各类异动学生的培养计划、上课任务自动进行处理。

学生奖励信息，由相应权限管理员维护学生的奖励信息，获奖记录、文号等信息，可上传文件附件。

学生处分信息，由相应权限管理员维护学生的处分信息，处分情况、说明、文号及处分解除情况，可上传文件附件。

学生缴费情况，存储学生缴费情况，提供财务系统同步或导入功能。

学期注册信息，对学生各学期的注册情况进行管理，可以有针对性的设置未注册学生不允许使用系统或部分功能(如报名选修课、查询成绩等)。

### 新生管理

对生源信息进行管理，可增加/修改/删除/查询/导入/导出/更新，批量上传/导出照片，设置招生专业，自动编班等，生成统计报表、班级报表等。

可扫描新生的条形码或输入考生号，进行报到或注册。

按专业、省市、学院，综合统计报到学生信息。

按班级查询新生转在校生。

按设置的规则给新生编排学号。

### 课程资源管理

* + - * 1. 课程管理用于管理和维护课程库基本信息，包括课程编号、课程名称、英文名称、学科门类；课程建设信息，包括课程简介、课程大纲、发展规划、课程改革、综合评估等各项内容。
				2. 课程平台管理，依据课程的学时(包括总学时，理论、实践、实验、实习实训等各个教学环节的学时)、学分、开课单位、授课内容不同划分不同的课程平台，不同的课程平台对应不同的教学大纲；课程平台包括如下几项内容：

课程简介：包括课程中文简介和英文简介。

课程大纲: 对课程讲授的内容进行详细的量化管理，包括每次课的教学环节、学时数、要求使用的教学功能区、教学模式、授课内容等。

指导教材：管理该课程平台使用的指导教材，以便在开设各学期课程时自动指定；具有相同课程编号时，高学时学分的课程平台可以自动覆盖低学时学分(含相同学时学分)课程平台的培养要求，从而实现成绩的自动替代功能(如转专业后)。

课程平台可以指定适用专业年级范围，只允许指定范围内的专业年级使用本课程平台。

### 教学计划(培养方案)管理

培养计划管理总体要求：

教学计划管理功能既能满足传统的按专业进行的人才培养计划管理，同时也需要满足未来学分制改革情况下多样化、个性化的人才培养计划管理，培养计划形式灵活多样，一个学生可以同时对应多份不同的培养计划，从而支持和满足教学改革发展的要求。

**培养计划制定：**支持学年制、学分制及学年学分制情况下各种类型培养计划的混合管理，如专业培养计划、辅修专业计划、模块选修课计划、定向培养计划、兴趣班计划、拔尖人才培养计划等各种类型的培养计划。

支持按学生个人制定的培养计划，支持一个学生多份培养计划同时存在，培养计划制定过程中支持快速批量选用往年计划课程，支撑方便快速制定培养计划。模块选修课计划支持由任课教师或学院教学秘书在线提交申请，审核后生成模块选修课计划流程，学生需选修相应模块选修课到达学分要求后，才能通过毕业审核。

教学计划制定，制定各年级教学计划(包括课程设置表、培养要求、学分要求以及其它毕业要求)，支持各种教学计划制订、变更的流程化管理；在教学计划中设置的学分要求标准能作为毕业审核的依据进行审核。

学生可以依据该标准随时进行毕业自审，查看自已的学习完成情况，在教学计划查询页面中，以不同颜色标识直观显示已通过课程、未通过课程、未修读课程。

提供教学计划之间、教学计划与版本之间相互比对功能，快速比对出变更过的课程；学生转专业前可与新教学计划进行课程对比，转专业后用不同颜色标识学生有变更的课程，包括需要补修的课程。

培养方案生成版本/选用版本功能：具备培养方案版本管理功能，能提供在不同年度或不同专业培养方案(含辅修专业培养方案)之间进行快速生成版本/选用版本的功能，或是不同专业培养方案的相互复制功能。

培养方案要求设置：设置培养方案的修读学分、学时等要求，可录入专业代码及专业名称、学制、培养目标、培养方案等详细说明，支持在线的word文本编辑器，支持直接拷贝或上传电子版的培养方案文档到编辑器中。

修改培养方案功能：能单个或者批量修改培养方案课程信息。

培养方案审核流程管理：系统中要能自定义培养方案审核的流程，支持由院系教务管理人员在系统中编制各专业的培养方案，并提交院系领导或教务处进行审核审批，审核通过后培养方案才能生效并公开发布使用。

执行计划生成：要求系统能自动根据培养方案生成每个年级每个专业的教学执行计划。

执行计划锁定功能，对于执行过的计划，可以进行锁定，锁定后禁止用户进行修改。

计划变更功能：要求在培养方案执行过程中，提供变更的功能，以应对实际教学安排过程中的一些变动(如：增开课程、停开课程、修改课程等)，系统提供变更审核的流程自定义，变更需要审核后才能生效，系统需要保留变更情况的历史记录，并能按照学期、专业、变更类型等进行查询。停开课程及修改课程应在相应学期进行提示，供排课人员进行排课操作。

培养方案的查询和输出：系统提供查询和打印的功能，培养方案要按学校的格式显示，并提供导出打印的功能。

支持课程跨学期开课功能，一门课程可以开设多个学期，可分别设置该课程每个学期的总学时、理论学时、实践学时、考核方式等内容，各学期的成绩可以按比例合并后计一次学分，如形势政策课开多个学期只计一次学分，且分上下学期录入成绩。

### 开课及免听考勤管理

开课任务管理，由课程开设单位从全校教师中确定任课教师、进行合拆班、填报教学日历、管理学生名单、登分册、课堂考勤表的导出打印功能允行管理人员对执行过程中的开课任务进行锁定，锁定后的开课任务不允许合拆班，更改教学日历，更改学时、考核方式、变更课程负责人等操作。

提供开课学时校验功能：教务处管理人员可以分学期统计各门课程实际开课学时与课程应开学时比对功能，可以方便统计出课程少开或多开学时，课程应开学时默认为该课程学时分配到对应学期的具体信息。

教学进程管理，各学生院系管理人员可以设置学院管辖班级在本学期各个教学周的整体安排情况，如第1-8周理论教周、第12周社会实践周、第19-20周为考试周等整体教学进程安排情况，支持采用各种自定义符号命名各种教学环节，支持通过复制、导入等各种方式快速制定班级教学进程表，依据教学进程表可以快速明确班级在哪些教学周可以排课、哪些教学周不能排课。

提供班级教学进度汇总功能：分别按班级统计出每学期各教学周安排进度总学时及外出实习周次是否安排了理论课进度。

教学进度(周学时平衡)生成管理，依据班级教学进程，系统能够按照周学时平衡的原则自动生成班级每门课在各个教学周的学时分配情况。

提供按照教学进度自动生成教学日历功能。

教学日历管理，依据教学进度中分配的周学时情况，系统能够提供录入、导入excel、沿用以往学期、按大纲生成等各种方式；减轻教师每学期录入教学日历表的录入压力；提供按课次进行分轮或分组管理的功能，一次课可以分成多个小组或多个轮组进行安排。

学生考勤管理，提供管理人员录入或导入学生上课考勤情况，并可与学校已有考勤系统进行免费对接，共享排课数据学生名单和考勤签到数据。

加开课申请管理，对于部分特殊课程,学生可以网上提交加开课申请，由管理人员汇总统计申请人数后确认是否需要额外增加开课任务，加开课申请应对学生申请增加课程范围进行限制。

学生免听管理，对于部分重修学生，如果存在课表冲突或其它学生手册上允许的不上课情况，学生可以在网上或微信平台中选择预设免听理由，提交免听申请，免听申请通过后考勤时可以自动忽略该学生。

教学工作量统计模块：可以快速、准确的实时统计出教学工作量，其中包括理论课、实践课、上机课、实习实训、排练、课程设计等各个教学环节的工作量换算和计算，统计内容中包括：教师职称、课程类别、学生人数及超人数系数、班级数、教学模式(双语、全英、智慧课堂、翻转课堂)、授课内容重复次数等；工作量统计形式可以按学院、教研室，按职称、按教师或者是按教师课程，分别统计出所承担的理论、排练、上机、实践学时。

支持各种分项目、分级教学等各种特殊类型的教学安排活动，满足体育分项目、英语分等级教学要求。

支持补修、重修学生网上报名功能，管理人员设置补、重修报名时间和限选数量后，学生可通过系统选择跟班班级，当要跟读班级上课人数达到教室容纳人数后，禁止学生加入。

学生在进行重修报名时，选择报名课程后，根据系统设置的专业学分收费标准进行计算需缴费金额弹出二维码，用支付宝进行扫码缴费，缴费成功后则报名成功，并且支持退费功能，在学生缴费记录里可以申请退费，由管理人员审核通过后，返回审核结果告诉学生到财务处办理退费手续，成功办理退费手续后，在系统的退费按钮进行确认退费。

在设置重修报名安排时，要求有按专业设置每学分的收费标准

重修报名开放以后，学生在自己个人界面选择需要重修的课程，选择报名课程后，在报名列表界面显示重修课程、学时、学分、修读方式、课程大类、教学班、是否缴费、缴费时间。

在每一门报名重修的课程中显示缴费按钮，点击以后弹出二维码，学生使用支付宝扫码支付，支付收款方对接学校财务处，成功支付后，更改缴费状态为成功缴费及显示缴费时间。

提供学生个人缴费记录的菜单给学生查询，在指定时间内，学生可以在缴费记录中对该学期报名的重修课程申请退费，填写申请理由，提交申请以后，由各个部门审核，最终审核结果及审核说明返回给学生，学生可以查看审核状态、审核结果说明，对审核成功的课程到学校财务处办理退费手续，办完退费手续以后，相关管理人员在系统上确认退费，退费手续办理完成。

管理员界面能查询汇总所有学生的缴费记录相关情况。

系统提供考勤信息录入、学生考勤状态查询、考勤情况汇总统计功能。提供管理人员按照开课信息单个或批量录入学生上课考勤状态（如正常上课、旷课、迟到、早退、病假、事假、免听等状态信息）。

系统支持按学年学期、学生院系、开课院系、专业、年级、班级、课程等进行学生到课情况查询，查询到每个学生的具体出勤状态。可以通过列表的数字链接，查询到课程明细。

提供考勤信息汇总及出勤率统计可视化分析表，支持按学年学期、院系、年级、专业、班级、考勤类型（可选）课程查询课堂的出勤率，输出直观统计分析数据表。

### 排课及调停补课管理

排课参数设置，支持各种自定义的排课参数设定，用户可以在排课时依据需要设定教师、教室、课程等各项实体相关的参数，如教师可集中排课时间、教师每天排课课上限、班级时间分散安排、班级教室就近安排、教师上课教室就近安排等；同时还可以设置教师其他工作时间、教室会议锁定时间、周四下午不排课等不排课时间。

自动编排课表，依据设定好的排课参数，系统自动统筹资源，安排合理的时间和地点。

课表编排能够尽可能综合考虑教师年龄与楼层，年龄大的教师优先排低楼层教室。

班级课表安排，提供多维度的课表安排功能，可按不同校区、不同课程类型(公共课、A校区每日10节课，每节40分钟、B校区每日11节课每节60分钟)，或按日、周时间，或按年级、班级在同一个页面进行课表安排，用户手工快速生成班级课表功能，用户可以通过拖拉教学日历的方式快速完成班级的安排，也可以通过拖拉班级已排课表进行上课时间或上课时间长度调整(提供权限开关)，拖动时自动检查班级时间、教师时间、教室时间冲突并进行提示。

教师课表安排，可以通过拖拉教师已安排教学日历的方式快速完成教师课表的安排；也可以通过拖拉教师已安排的课表进行课表调整，拖动时自动检查教师、班级、教室时间冲突并进行提示；为相应课程类型(如专业课)提供教师可自行增加学生名单的权限，并检查学生上课时间是否冲突。

教室课表管理，可以通过拖拉教室教学日历的方式快速完成教室课表的安排；也可以通过拖拉方式调整已安排的教室课表，拖动时自动检查教室、教师、班级上课时间冲突。

各类课表查询：提供全校总课表、教室课表、教师课表、学生个人课表等各种形式的周课表、月课表。

提供学期课表或周课表两种模式的课表管理功能，以便于多教师授课时能够精确显示具体上课情况，可导出复杂形式的课表，包括[教学进程表]、[教学安排表]、[课表]。

调、停、补课流程化管理功能，教师在网页或微信平台中提交调停补课申请，调停课申请审核通过后，系统自动更新相关联的教师、学生的课表(能通过系统消息提醒或微信平台通知老师、学生)。能区分课表调整的内容：调上课时间，教师，地点，能区分整体调课或部分调课。对于连排的课程调整，要求只做一次调课处理。提供对调课信息的分类统计：针对各院系课表调整的次数、学时总数、调课率分别进行统计，方便对各教学院系进行考核，提供课表冲突检查查询的功能。

课表显示支持周视图、月视图、列表视图等各种形式，能够将节次课表、天课表、周课表统一展示给学生和教师。

调课日志管理，系统自动记录调课日志，能够对记录的调课日志进行横向统计，比较各个学院学期调课数及其图形报表。

提供分级别、分时段排课功能，教务处和学院可以分级协作，在系统中进行课表编排，共同完成课表编排工作，高排课级别用户有权通过拖拉方式调整低排课级别用户排出的课表，反之则禁止操作。

提供课表冲突检查功能，可以快速定位班级、教师、教室各种类型的课表冲突情况。

若在排课完成后需要调整任课教师，院系排课管理员可按流程进行申请，审核通过后通过系统消息提醒或微信平台通知学生。

### 选课管理

选课类型：网上选课系统应支持不同的选课活动类别，包括：全校公共课选课、院系选修课选课、专业课选课、体育选项目等。每个学期可设置多个类别的选课活动，每次选课活动又可以根据需要分为多个轮次进行选课，如：预选、正选、补退选等；提供多种选课方式，如先到先得，积分选课，志愿选课，抽签等方式。

全校性公共选修课在线申报与审核：支持由教师于规定时间内在网上提交开课申请，包括填报多个上课时间(以供排课时安排)、计划开班数量、每堂课人数上限、周学时、面向对象、禁选对象、教室类型、先修课程。管理部门进行在线审核，审核流程可以自定义设置，审核进度以图形化显示在教师网页端或微信平台中以供查询。

对于该教师已开过的选修课，教师直接在申请页面课程名称中下拉菜单选择本人已开过的课程，按流程办理。

要能设置选课的开始时间与结束时间，以及该轮选课是否控制课程限选人数、是否允许学生退选课程。

限选控制，需要提供多种限选条件设置：可针对每门课程设置限选学生的培养层次、年级、院系、专业、班级、性别、先修课程等；可设置每个学生的限选课程门数、限选学分数量；针对模块选修课，可针对每个模块设置限选学分或门数。能批量设置多门课程的限选条件需要提供多种选课抽签方式：高年级优先、本专业优先、先选先得等。提供多种选课控制手段：要求在系统中可以设定没有完成上学期教学评价或上学期选修课缺考取消资格的学生不能选课；未注册或没有交费的学生，限制其选课。选课结束后，选课结果能自动发布，学生可查看到选中课程的课表，教师可打印选课学生的名单。

选课名单管理，管理员可以对单个课程增加或删除选课名单。可以设定课程开课条件，对于不符合开课条件的课程，可以将学生选课名单和排课信息删除并在网页和微信平台中进行提示。

学生选课记录查询：提供学生选课、退选的详细记录，可按照院系、专业、年级、学号、姓名、选课阶段、操作时间范围进行查询。能按照院系、专业、年级、学号、姓名、选课类别等条件查询学生已选中的所有课程归属具体模块和学分。

选课统计，选课情况查询统计：能按照院系、专业、年级、学号、姓名、选课类别等条件查询学生已选中的所有课程；能按照开课单位、课程名称、授课教师等条件查询选中该课程的学生名单；可查询每个学期未参加选课的学生名单；能按照年级或院系统计每门课程的选课人数；能统计每个学生的已选中课程的学分数和总门数。支持网络公选课成绩批量导入教务系统功能。支持学生选课时自动排除学生培养计划中的应修课程或是先修高级班不得再报名初级班。

支持完全学分制管理模式下的开放式选课功能，所有课程(含必修)都可以开放给学生进行选课，选课时自动检测学生个人课表与所选课程课表之间的冲突。

### 教室管理

教室信息管理，提供教室基本信息管理功能，记录教室所在教学楼、所属功能区、容纳上课人数及座位序号、考试人数及考试座位序号(设置优先、备用排考座位)、维护人、状态、是否可借用等基本信息，同时可对部分教室的时间进行锁定；提供课室平面布局照片上传功能，可供排课排考时参考，或由任课教师输出打印作为学生上课固定座位时使用。

教室使用情况查询：支持查询教室每天的课程安排、考试安排、借用等各种使用状态信息，同时可以查询每间教室当天的授课教师、授课内容、上课班级和人数。

支持在系统中自定义设置教室借用和调整的审核流程，包括审核的步骤层级、每级审核的人员、审核的时间范围；可控制用户最多能借未来多少天范围内的空闲教室；支持管理人员批量进行教室借用。可根据原上课教室的类型及容量匹配相应的空闲教室。

教室借用申请管理，提供空闲教室的查询、教室使用情况查询、教室借用流程管理的功能。

空闲教室查询：支持按照校区、教学功能区、教学楼、教室容纳人数范围、周次、星期、节次、学生年级(每年新生)等维度查询、导出空闲教室的信息。可按节次、天、周、月、学期、学年统计各类型教室申请情况。

教室借用单打印：系统需记录详细的教室借用日志信息，并支持从多个维度进行查询、导出。

支持查询教室每天的课程安排、考试安排、借用等各种使用状态信息，同时可以查询每间教室授课教师的课堂授课内容。

### 教材管理

教材征订管理流程如下：

首先由任课教师填报教材、之后有课程主管单位管理人员对教师录入教材进行审核，审核通过后即可开放给学生进行选订。

依据以上流程，教材管理模块应具备如下功能：

教材书目库管理，管理教材的ISBN号、教材名称、主编、出版社、版次、出版年月、单价等教材相关信息；

教材填报时间和选订时间控制功能， 允许管理人员设定教材填报起止时间和学生选课教材的起止时间。

教材填报功能：允许教师从教材书目库中选择要使用的教材或新增教材书目，同时上传自编讲义；为方便教师填报教材，允许教师从书目库中选择教材或是继续沿用以往学期使用过的教材；同时也允许教师提交个人用书申请。

教材审核流程，允许学院管理人员对教师录入的教材进行审核。

学生选订教材，学生依据个人上课任务，选择各自所需订购的教材。

生成并导出教材订购计划，依据教师用书和学生用书情况进行合并，对合并后的数据进行导出，提供给书商。导出时能同时导出教材订购汇总信息和明细信息，以便于书商按照学生订书明细进行发书。

对于新生用书，可以依据拟招生人数进行订购。

教材书目库提供两个字段标记库存的教材类型，分别是样书库库存和新购书库库存，填写库存的教材数量；

课程负责人安排课程所使用的教材，同时申请教师用书，选择课程需要使用的教材、申请的数量等信息后提交申请；

教师填报完教材由开课教研室、学院、教务处审核通过后认定为有领书资格；

入库：对书商提供具体的的教材、数量进行入库，分别更新到教材书目库中；

有领书资格的教师在线下领书，出库操作人可以选择从样书库或新购书库出库（每种教材在学校保留有少量样书即可，样书库存多则从样书库出库，否则从新购书库出库），新购书库库存可转换为样书库存；

退书规则：样书库不能退书。

### 实验教学管理

在系统上进行课表安排时，支持安排实验准备人员及实验项目，其中实验项目与课程、开课部门关联；在实验上课前提醒实验准备人员所负负责的实验，实验准备人员对相应的实验安排实验项目的实验器材、实验用品、使用数量等实验相关的前期准备

**普通实验课程：**

创建实验项目库管理，实验项目与课程关联，并且一个实验项目可对应多门课程，实验项目添加方式应支持手动单个增加及批量导入、批量删除、批量导出功能，实验项目支持实验项目导入，每个实验项目填写实验大纲；

在教学日历制定界面中，需支持对某些教学环节为实验教学的课程安排实验项目，并且一次课可以对应多个实验项目，实验项目可选范围为所属该课程的实验项目及其他不与课程有关联关系的是实验项目；

实验项目可以由项目承担单位管理实验项目及按开课单位进行管理实验项目，达到权限可分配管理；

在实验教学环节的课程当中，已经安排了实验项目的课程可以对该实验项目设置实验准备人员，并且一次实验课只允许安排一位实验准备人员；

计算工作量时，实验准备人员的工作量也需纳入计算，按每个教师所负责的实验西项目学时计算；

实验项目管理信息中可自定义设置该项目在实验过程中所用到的实验用品所需实验用品维护功能，在实际授课中，具体的实验相关器材用品数量由实验准备人员负责安排；

**开放实验项目：**

支持安排开放性实验项目，如：演示型、综合型、研究创新型等类型的实验项目

具体流程：

由开放实验项目总负责人制定实验项目的培养计划，每一份计划包含具体的实验项目，具体的项目由各个开设项目负责教师申报；

教师在申报实验项目时，每个实验开设的学时、项目开设学期、开设校区、项目可报名学生人数、可报名学生范围等相关信息可以由申报教师设定。

所有实验项目申报完成以后，由开放实验项目总负责人审核并开课，实验项目开设流程与普通课程开设流程雷同，在项目审核通过并开设后，由项目授课教师安排制定教学日历，制定每次课开设的时间地点、授课内容等信息；

开放实验总负责人设定每个项目的选了类型、选课时间、选课人数等信息给学生进行选课。

### 实习实训管理

实习单位管理：管理和维护所有实习单位，包括实习单位信息、容纳实习学生人数等信息。

实习见习管理：可以对实习见习教学任务进行具体分配，如安排带队教师、分配实习科室，统计已分配实习见习人员或未分配实习见习的人员。

提供批量安排实习见习功能：可以选择多门开课进行批量安排实习；

提供实习基地预约功能（选择实习单位）给学生自行申请；

提供实习请假功能，请假审批流程如下：辅导员 -- 系 -- 学工部、教务处-- 院领导审核。

提供实习基地转换申功能，由学生提出申请，审核通过以后去掉原实习任务，提供申请转换后的实习任务；

提供实习结束确认功能：对实习任务提出结束申请，申请后提示实习结束确认内容（由管理员设置），学生必须同意确认勾选后才可以成功提交申请。

提供实习简历信息填写（网页端填写、预览）功能，并支持批量导出pdf文件。

### 考务管理

考试安排管理能基于教学与非教学数据源，利用已有教学资源，来实现对考试内容、考试地点、考试时间、监考人员、巡考人员等的自动安排和人工指定。

支持随堂考、院系考、毕业专业考、学校统考等其他临时考试的安排管理，随堂考和院系考直接由各院系管理人员在系统中进行安排，统考集中自动安排。

考试任务管理，查询核对每学期的考试任务，允许用户设定各学期所开设课程的考核方式(考试、考查)、考核形式(笔试、机考、作业等)、考试安排类型(随堂考、院系考、统考)，依据不同的考试安排类型划分安排任务。

考务基础信息，管理人员可以设定考试场次信息、监考教师信息、考场信息,供自动编排考场时使用。

考试学生信息，查询要考试的学生，可以批量指定考试场次要求、考场要求、试卷编号等各项信息。

自动编排考场，编排各种类型的考试，包括正常考试、补考等，提供编排考场、编排监考、编排座位号功能；机考考试安排完以后，可按字段导出相应表格供考试系统使用。

提供考试安排调试功能，对于漏排考试的课程或学生，可以自动显示编排情况、漏排原因，供排课人员排查消除冲突。

考试安排查询，可以从多个角度查询考试安排结果，如学生考试安排、班级课程考试安排、考场考试安排、监考教师安排、教学班考试安排等；支持学生、教师、考场的转移与合并；安排完成或有调整的场次，应在系统提示或通过微信平台在考前进行提醒。

提供各种考试信息查询统计功能，如：按考生考场安排查询、主考监考查询、考试内容安排查询、准考证打印、考务分析统计等。

要求能提供灵活的排考参数设置，以适应不同的考试安排要求，包括：可针对一个学期设置多个考试轮次；设置监考老师要求(可设置同一教研室的老师不能同时监考同一考场、监考老师不能监考本院系学生等选项)；可设置查询考试安排结果的开关参数；能够强制将一个行政班安排在一个教室；能够设置每个考场容纳人数、容纳班数、容纳课程数等进行混合考场编排；可设置每个考场监控老师与学生的人数比例；是否需要整班排考；学生考试安排间隔方式等。

能自动编排考场、安排监考、编排座位号(顺序或乱序安排)并可输出打印以供张贴。

提供各种考试安排表：时间区段考试安排表，课程考试安排表，班级考试安排表，学生考试安排表，教室考试安排表，巡考人员巡考安排表，监考人员监考安排表。要求实现对监考人员监考场次的统计，作为发放监考费的标准。

考场违纪处理功能可以方便监考教师或巡考现场录入考场违纪作弊情况，可在微信平台内按预设步骤记录违纪作弊情况，通过查询本考场信息，选择该考生进行作弊、违规等处理，并对其行为进行描述或选择系统预设选项，拍照上传相关证据，推送信息给相同考场监考人员，选择或书写意见后提交。提交成功后，更新教师录入分数网页的学生成绩为作弊或违规，并可在同页面查询当时监考教师上传违纪作弊情况。

为了方便监考教师对考场考生情况汇报，教务手机微信端增加考场速报功能。教考教师可以在监考时使用此功能对作弊、违纪等情况的学生作登记汇报，汇报以后管理员可以针对这部分学生修改上课学生名单的成绩标志，方便录成绩教师录成绩时清楚考试学生的情况。具体流程包括:

监考教师进入教务微信端，打开考场速报界面；选择考试安排任务（可体现出哪门课、哪个考场、什么时间考试）;选择考试任务里的考生；;填写违纪作弊等情况;上传违纪证据（照片或附件）；提交；管理员界面增加考场速报统计功能，可在此界面针学生的情况对应上课学生名单成绩标志作出修改（如违纪、作弊、缺考等）

等级考试管理

在系统中能实现各类考级(大学英语四六级考试、计算机等级考试、普通话考试等)的报名工作，并能对考级的成绩进行管理。

能在系统中自定义各类等级考试的考级类别、考级等级。针对不同级别、不同考试类型的考级报名工作，提供设置报名条件(如：大学英语四级大于425分才允许报名大学英语六级)、设置报名时间范围、学生网上报名的功能，允许后台修改报名数据。

报名完成后，能批量导出学生报名信息(包含学生照片)，能维护学生的考试缴费信息。能按照校区、院系、专业等统计学生的报名情况。能提供上级考试部门需要的报名数据。

学生考级成绩公布后，需要将从考试院获取的成绩批量导入系统中，能对学生多次考级的成绩进行维护，学生可在系统中查询考级成绩。需要提供考级通过率报表统计功能，可按全校、按院系、按专业统计各类考级的通过率。

### 成绩及缓补考免重修管理

学生成绩指学生在校期间从入学到毕业各个学习环节的考核结果。学生成绩管理应具有的功能：

成绩录入：由任课教师、教务秘书或教务处成绩管理员，基于校园网/互联网简便、快捷地完成学生的课程成绩的录入与审核。支持手工在线录入与excel表格批量导入两种成绩录入的方式，提供成绩录入暂存功能，教师下次录入时可以继续录入上次未录完的成绩，能灵活设置课程总成绩的组成项目(如：平时成绩+期中考试+期末成绩，实践成绩+作业成绩+期中考试+期末成绩)，每个组成项目还可以再细分子项目，并能设置各项目所占总成绩的百分比。提供成绩录入进度查询功能，包括：课程人数、未录入成绩人数、是否录入完毕、是否审核通过等。系统提供批量导入成绩模板，提供过往学期成绩补录功能，方便类似分散学期上课，最后学期给成绩的课程成绩录入。总评成绩生成后，具有自定义成绩单打印和试卷分析功能，并生成相关成绩分布统计图表。对于由于出国学习、开会等各种原因迟录成绩的教师，可以单独为其开放成绩录入时间；教师可查询历年录入的成绩并可输出打印。

提供课程章节考试成绩录入或导入功能，各个章节考试成绩能够按比例合并为平时成绩或者是期未考试成绩。提供成绩录入时自动折算功能，教师在录入成绩时符合特定类型的学生成绩会依据管理人员设定的公式进行折算，如特长生的自动加分。

缓考管理：需要提供缓考的申请控制与审核功能，学生在规定时间范围内在网页或微信平台中提交缓考或免考的申请，上传相关证明附件照片，由二级学院和教务管理人员进行审核后生效。学生相应课程的成绩即会打上“缓考”成绩标识，在教师成绩录入界面该生成绩备注上有按钮可点击查看学生上传的相关证明材料，实行在线流程审核管理。

免修管理功能：支持未修免修和已修免修管理，实现无需人工干预的在线流程审核管理；由学生在网页或微信平台中提交已修免修或未修免修申请，上传相关证明附件照片，主管单位人员审核通过，审核通过后，自动为学生添加申请免修课程的成绩,如港澳台学生的思政课程自动标注免修。

成绩查询与统计：需要提供丰富的成绩查询条件字段，并能按各种组合条件进行成绩查询或按年级、行政班、课程成绩排名统计。提供多种多样的成绩统计报表，可计算总分、平均分、加权平均分、平均学分绩点、历年平均学分绩点，可设置学分绩点算法和规则，如重修补考成绩按分数范围设置不同绩点，奖励学分、缓考、免修等成绩可不纳入绩点计算，不及格公共选修课可不纳入绩点计算等。可打印的成绩单类型包括：学生中英文成绩单、班级成绩单、专业成绩单、课程成绩单、不及格门数统计、学分绩点统计、成绩通知单、不及格课程统计、不及格学生名单、缓考申请情况统计、学位课程平均分统计等。支持中英文成绩单的打印，支持输出PDF格式成绩单。班级、专业绩点排名,支持多种基于课程类型、课程模块等的绩点换算公式统计。学生可查询该课程平时成绩组成及分数，期末总评成绩需教师提交审核后学生才可查询。学分统计时能够按考试性质初修、补考、重修等各种性质统计学分，同时也能够按照修读方式必修、限选、任选进行分类统计学分。

提供对学生平均绩点的分段统计功能，如平均绩点1.0-2.0多少人，2.0-3.0多少人，3.0-4.0多少人，4.0以上多少人。

成绩复核管理：对于录入有误的成绩，需要提供成绩修改的功能，并要求经过流程的审批，只能由原来录入该学生成绩的教师在线提交成绩修改申请(针对单个学生单门课程的成绩)，其它人无法提交成绩修改申请。提交申请后，需要各级人员进行审核，审核通过后自动更新成绩总库中的成绩。提供成绩修改统计报表，统计各院系的成绩修改申请人数、修改比率，作为对院系的考核条件，同时必须提交纸质证明。

补考、重修、毕业清考管理：要求能审核补考、重修、毕业清考的学生名单，提供网上报名的功能，能控制学生报名的课程门数，单独设置重修、补考报名的起止时间。针对重修的学生，可以进行重修选课，对于重修时已不再开设的课程学生可以选择其它课程替代。补考、重修、毕业清考的学生名单可以直接在考务安排模块中进行排考、成绩录入。重修补考成绩录入时，与正常班级的课程任务分开，有专门的重修补考任务供教师录分。提供统计补考、重修、毕业清考学生人数的报表。设置补考，重修成绩的有效成绩，即打印成绩单显示成绩，但不影响实际数据。

重修、补修报名管理，提供时间及门数控制功能，学生可以在网上提交补修或重修申请，查询当前学期开设的课程，选择加入的教学班，可选择该课程不同的任课教师组别，同时可以查看要选的班级上课时间、考试时间是否与已有上课任务冲突，并且可以设置是否允许上课时间冲突或是超过教室容量选课；对于已有不及格成绩的报名，能够自动认定为重修，对于无成绩的报名应认定为补修。

成绩修改日志，成绩在修改时自动记录修改日志，以便于审计。

成绩数据防篡改：提供成绩加密存储功能，用户只能通过系统提供的合法途径修改成绩，合法途径修改的成绩会留下日志供审计。

成绩归档功能：对已毕业的学生，不再进行成绩处理，对在校生的成绩进行规则调整不影响已归档学生的成绩。

### 教学质量评价

系统需要提供学生评教、同行评教、领导评教、专家(督导)评教等多维度的教学评价方式，通过系统广泛获取评教样本，进行有效的评价数据处理，并形成多方位评教统计分析报表。

评价设置：能灵活设置评价课程类别、评价主体、评价内容(建议)。能控制各类评教活动的起止时间，指定学生、同行、领导、专家(督导)评教的参评人员，提供控制教师查看评估结果的开关参数；可通过二级权限配置，实现院(系、部)单独组织评教活动；对未参与教学评价活动的学生，可设置取消其选课、成绩查询等权限，促使其积极参加评教，保证学生参评率达到100%。

评价课程管理：系统可灵活的将需要评价的课程信息批量转入到不同的评价活动中，从而将评价指标与需要评价的课程建立关联；根据学校开课及多教师任课的实际情况，系统需要提供多种评价的方式，包括：每位任课教师仅评价一次、每个课堂的每个教师评价一次、每个课堂的某个学时评价一次、每个课堂评价一次。

过程性评价：设置相关指标，可在每节课后进行评价，简短的评价问题使学生在微信平台中可立即进行评价或提出建议，并可设置一定周期进行统计。设置对学生的评教数据“是否纳入学生平时成绩子项目”开关。

评价数据处理：能够对各项评价结果样本进行标准化处理，去掉一定比例(可自定义设置相应的比例)的最高分或最低分，对于参评率低于一定比例的样本设置为无效，并进行记录可供查询。

评价进度查询：能实时查询学生评教、同行评教、领导评教、专家(督导)评教)的进度情况，查询已评教人数、未评教人数、参评率等。可查询同行评教、领导评教、专家(督导)评教活动中具体的评价主体(个人)和对应的评价对象(个体)可查询并导出学生评教活动未评教学生名单并督促进行评教。

评价结果统计：能统计全校每个受评教师每门课程每个授课课堂的评价样本数、参评率、平均分；能按照教师/课程汇总统计评价的平均分、样本数、参评率、全校排名、学院(系、部)排名；能汇总统计每个教师的平均分、样本数、参评率、全校排名、学院(系、部)排名；能对教师各个指标项目的得分情况进行分析，与院(系、部)平均得分情况进行对比；能分院(系、部)统计各分数段的教师人数，统计院(系、部)的最高分、最低分、平均分，可自定义设置分数段等级范围(如：优秀为95～100分，良好为85～95分等等)。能汇总统计覆盖比例(指开展学生评教，同行、督导评教，领导评教的课程门次数占学年所有本科课程门次数的比例)，能分别统计学生评教，同行、督导评教，领导评教的优、良好、中、差的百分比。能统计教授主讲本科课程占教授总数比例、教授主讲本科课程占课程数比例(门次)、课程设置满意度、教授授课满意度、教育教学管理满意度等。

各个评价主体成员可登录系统，依据评价指标体系，对于相应评价范围内的课程任课教师进行评价。

专业技能课评价项目：针对学校专业技能课等一对一、一对二、小组课等形式的课程，可复制系统中已经设置好的评价指标，增加学生评教活动，将教师作为评教任务的对象，由任课教师本人或院(系、部)教学秘书将学生名单单个或批量增加到该教师评教任务中，或将项目开放给学生报名参与评价，学生可以在网页或微信平台中对该教师的任课情况进行评价。

教学评价管理人员、受评教师登录权限：可分别设置教学质量监控与评估中心“全校教学评价管理者(一级)”、各教学单位党政领导院(系、部)“教学单位管理者教学评价(二级)”、各教学单位教学秘书“教学单位教学评价工作人员(三级)”、“受评任课教师(四级)”相应可控制、过程性评价内容及评估结果的登录权限。

管理人员可以设计针对不同学院、教学形态的评价问卷表模板，同时设定问卷表模板，设定好模板后，学生评价时自动依据模板从指标库中动态抽取指标进行评价，同时也可以设定问卷表是否带印象分，由学生评价时给教师打印象分。

评价问卷表中的题目支持单选题、多选题、问答题、滑块题、星星题等多种类型。

提供动态问卷评价功能，学生在评价时，系统能够自动从指标库中抽取指标组成问卷表，学生评教时能够实现一人一问卷、一评一问卷，在减少学生评价指标的同时扩大教师被评覆盖面。

质量工程项目

**项目申报**

管理人员新建申报任务：

年度--项目类别--项目名称--起始时间

手动添加项目类型（重点项目、一般项目、专项项目等供教师选择）

手动添加项目细分（医药类、医药相关类、综合类等供教师选择）

手动添加设置申报书内容（研究意义、研究目标、研究内容、研究计划、预期成果等）

项目申报限制：同类别项目已立项未结项者不得申报

工作要求：要求可以填写本次申报任务的负责人要求，申报书填写格式，需要上传哪些支撑材料等等。

附件：附件可以传一些项目申报书，平台使用手册及本次任务的一些支撑性材料。

**教师申报：**

点击我要申报或者在线申报页面的申报按钮，教师可以进行申报项目，需要输入项目名称、负责人信息（由教务系统自动匹配，含年龄、职称、所在学院、联系电话等）、起始时间系统根据申报任务自动生成。

添加项目成员信息（校内人员直接输入姓名或工号搜索、校外人员手动添加姓名单位职务等）编辑成员承担工作

编辑申报书内容（研究意义、研究目标、研究内容、研究计划、预期成果等）

附件材料上传（文档或压缩文件）

提交完成申报

自动生成申报书（文档）

自动生成申报编号：年度+项目类别+系统编号

自动生成申请时间：教师申报提交申报材料的时间

**审核：**

教师提交项目后自动分入学院教学科待学院审核上报（教学科、分管教学院长）

学院审核无误后点击提交进入教务处管理端

**评审设置**

管理人员进行评审设置：

设置专家评审时间

手动添加评审指标保存后自动生成评审表

专家遴选（校内专家输入姓名或工号自动入选）

项目分配（可根据项目类别、项目细分、数量等选项自动分配项目，也可一一选择分配）

**专家评审：**

专家登录后显示评审任务，进入评审界面

逐项打分：按照评审指标一项一项进行打分，最后计算总分

综合打分：参照评审指标直接对项目打总分

不打分（给出是否立项意见）：不进行打分，只是参照评审指标给出专家意见。

专家评审完成点击保存、提交、汇总

**管理人员评审结果分析：**

根据专家评审结果统计拟会评（立项）比例

查看不同意立项项目，确定立项项目，自动生成立项编号：年度+项目类别+系统编号（仅最终确定立项项目），邮件提醒：项目通过后会邮件告知教师结果（通过/不通过），中期及结项管理。

**中期管理：**年末提交中期总结

**结项管理：**结项书提交，结项评审

**项目状态显示：**

在我的项目中，会显示不同的项目状态，项目状态代表不同的含义。

申报中：项目申报资料已部分填写，并未提交到审核流程中。

申报评审中：项目进入申报评审流程。

申报未通过：项目立项失败。

建设中：项目已立项，可进行建设。

中期评审中：项目已经进入中期审核流程。

结题评审中：项目已经进入结题审核流程。

已结题：项目已经结题。

### 毕业审核管理

毕业管理根据培养方案的规定，全面审查学生的学业修读情况，得出审查结论；可分别按学院、专业、班级、个人进行毕业审查并提供审查结论；毕业审查可以按照权限分别由教务处、院系发起，能分批次进行审查，实现毕业审查的系统化、自动化、日常化。

设置毕业审查条件：能设置每个专业的毕业条件、获得学位条件，如：学生取得学分达到所在年级/专业的毕业学分要求，历年学分绩点要求，学位英语成绩要求，专业毕业考成绩要求，必修课均需及格，计算机、外语达到相应等级要求，每个课程模块的修读学分等。能针对辅修/双学位等设置辅修毕业条件与获得双学位条件。

主、辅修毕业审核及学位审核：依据设置的毕业规定条件，能按批次自动智能审查学生的学业修读情况，得出学生的毕业结论和学位结论(包括主修毕业、获得学位、辅修专业毕业与获得双学位)，并可给出审查不通过学生的原因，分析未通过主修毕业、获得学位、获得双学位审核的原因。提供手工毕业结论修改功能。

对发生学籍异动的学生，能自动按最终专业的培养方案进行毕业审核，而不仅仅是计算学分，培养方案中要求的必修课必须全部完成，学分要求只计算培养计划匹配到的课程成绩。

能够快速一键完成毕业审核，对于不能毕业的学生，自动生成不能毕业的原因供用户查询。

依据学生平均绩点获得情况进行，能够自动完成普通学位审核。

提供荣誉学士学位管理功能，学生可以提交荣誉学士学位申请，经审核(支持工作流定制，用户可以自定义设置审核节点和审核人)后授予学生荣誉学士学位。

### 教职工服务

系统能为教职工提供所需的各种服务，包括：

通知公告：在微信平台或教务网首页查看各类教学通知公告信息。

个人设置：在线修改个人密码、提供密码找回功能、可设置密码保护问题。

教师卡片：查看教师个人基本信息，可以根据个人情况变化，在线提交个人信息变更申请。

个人课表：在网页或微信平台中查询个人课表，提交调停课申请，查看调停课记录；打印成绩登分册；查看全校课表。

培养方案：查询培养方案总纲，查询本院系各专业的人才培养方案和教学计划，查询教学进程表。

公选课开课申请：教师能在网页或微信平台中提交每学期的公选课开课申请。

考试安排：在网页或微信平台中查询自己的监考信息。

教师工作量：在网页或微信平台中查询自己的工作量、薪酬信息。

网上评教：在网页或微信平台中查询学生对教师的评价结果信息，并可进行同行评教。

成绩录入：定期网上录入学期课程成绩，送审上级主管部门，审批通过后查询和打印成绩单，报相关部门存档。

提供课程章节考试或作业等子项目成绩录入或导入功能，各个子项目成绩能够按比例合并为平时成绩或者是期未考试成绩，并可开放子项目成绩供学生平时查询。

成绩修改申请：对于个别学生成绩录入有误的情况，由成绩录入教师网上提交成绩修改申请，审核通过后对学生成绩进行修正。

教材管理：申报教学用书计划；提交新增课程教材书目的申请。

教室借用：在网页或微信平台中提交教室借用申请，查看审核情况。

毕业课题申报：在线申报毕业设计课题，查看学生选题情况。

教学日程表(日程、周、月)：在网页或微信平台中日程表中查询个人上课安排、监考安排等内容，在日程表中可以精确查询每个日程事件的时间，精确到时、分秒。

其它：校历查看、消息通知、在线咨询、文档下载等。

工作量管理

提供教师教学工作量的汇总计算、复核等功能，为教师职称评定、年度考核等提供依据。

系统可自动、快速、准确的统计出各类教学工作量，如按学院、教研室，按职称，按教学环节等。汇总方式可完全自定义，如按教师+课程+承担类别、按教师+课程、按教师+课程+教学班、按教师、按职称、按学院等。

提供对教师教学工作量进行汇总统计，可单个增加、批量导入教学工作量，对工作量信息进行修改、维护、删除，查询工作量明细信息。

提供教学工作量确认复核功能，若任课教师对个人教学工作量有异议，可以提出复核申请。支持工作量信息在教师端的展示及教师申请复核，管理人员可以定义允许展示的字段、允许复核的字段信息。

提供教师用户自主填写变更后的工作量，并提交审核。经流程化审核审批后，工作量复核变更生效。

提供教师各项工作量的汇总统计功能，可以按学年学期、教师院系、教学职称、专业职称、教师编号、教师姓名在岗状态进行查询，按‘教师、职称、教职工类别、院系、教研室’进行汇报统计。

### 学生服务

系统能为学生提供各类教学相关的实时在线服务，主要包括以下内容：

公告通知：在微信平台或在教务网首页查最新公告留言信息。

学籍卡片：在线浏览学生个人学籍信息，可根据学校规定，定期对学籍信息进行核对和完善。

学籍信息变动申请：学生可提交学籍信息变改申请，能查看学籍信息审核结果信息。

学籍异动与预警：按照学校异动流程的规定，由学生本人选定某一异动类别(如：转专业、休学等)并在网页或微信平台中提交相应异动申请，能查看异动审核信息(含已申请/未批准/已批准)、异动结果信息。能接收并查看本人的学籍预警消息。

学生主、辅修计划及毕业预审功能：查询学生本专业人才培养方案，包括：理论课程、实践环节、毕业学分、模块选修课等要求，可以随时对自已的学习完成情况进行毕业预审，或是在转专业时比较新专业与原专业的课程进行对比，及时申请补修；用不同颜色标记已通过、未通过、未修读的课程。

课表查询：在线查询打印各个学期的课表信息。查询调停课情况，能在网页或微信平台中接收到调停课变更信息。

网上选课：学生在网页或微信平台中进行网上选课、退选的操作，包括预选、正选、补/退选等不同阶段的选课，可查看选课结果。

成绩查询：在线查询所有已修读课程的成绩，包括正常考试、补考、重修、毕业清考的成绩，能查看学分获得情况，如总学分、必修学分、选修学分(包含公共选修课及限选课)等。

考试安排：在网页或微信平台中查询学期考试课程安排情况，提供申请缓考、申请免考的功能。

补考重修报名：学生在网页或微信平台中进行补考报名、毕业清考报名、重修报名、重修选课。

等级考试报名：在网页或微信平台中提供等级考试报名、成绩查询的功能。

网上评教：学生在网页或微信平台中根据评价指标对任课教师进行评价，能保存与提交评价结果。

毕业设计选题：学生能进行毕业设计网上选题。

辅修报名管理：学生能网上进行辅修报名。

免修申请管理：学生可以在网页或微信平台中提交免修申请，同时上传各类证明材料，包括已修免修或未修免修。

缓考申请管理：学生可以在网页或微信平台中提交缓考申请，同时上传各类证明材料。

免听申请，学生可以在网页或微信平台中提交免听申请，供管理人员审核。

选订教材，学生可以在网页或微信平台中选订教师填报的教材。

学生在网页或微信平台中查询学习日程表，其中包括：个人课表、个人考试情况、选课开放时间等教学安排情况。

学生可通过网页或微信平台修改或找回个人密码、设置密码保护问题、在线问答等功能。

课堂评教功能：学生可以在网页或微信平台中针对当天上课的教师进行实时评价，提交意见。

学习日程表查询功能，可快速查询自已的上课任务、考试任务、见习实习安排任务等。

**收费管理**

* + - 1. **通用收费模块**：支持根据学校收费管理办法，通过与财务系统或支付平台集成对接，实现学生缴纳学费情况与选课等系统使用资格联动（根据学费收费标准自动生成缴费订单，缴费完成后，返回订单缴费状态，方可具有系统的使用资格）。
			2. **学分收费管理模块**：支持基于学生选课，实现选课学分学费的结算、统计、查询，完成缴费状态的刷新。
			3. **自定义功能**：支持根据不同年级、不同专业、不同课程设置学费收费标准，对特殊课程可单独设置缴费标准。
			4. **查询功能**：可按不同维度查询和统计学生需要缴费的课程学分学费情况，学生可查询本人在各个学期的缴费情况，可查询缴费详细信息。

### 系统管理

* + - 1. 系统维护管理为系统管理员提供实时监控系统运行的有效手段，涉及到数据字典、流程管理、用户管理、权限管理、参数设置与系统日志等。
			2. 在系统初始数据字典(依据《国家教育管理信息化标准》)的基础上，允许用户根据需要自定义扩展数据字典。
			3. 管理系统用户，分配操作权限，支持按照角色对权限进行管理，能按照校区、院系、年级、专业等条件设置用户的数据权限范围。
			4. 为系统管理员提供模拟登录功能，可以模拟学生或教师登陆，检验教师或学生反馈的数据问题或功能问题。
			5. 可以设置未缴费、未完成评教等的学生或教师用户，不允许登录操作。
			6. 提供详细的用户操作日志查询功能。
			7. 系统要能支持多级授权管理，能设置授权的起始时间和失效时间，实现精确到按钮级别的多级授权。
			8. 系统能支持工作流引擎，实现管理流程的动态配置。支持系统内各项审批流程的自定义，包括：教材填报流程、调停课流程、成绩录入流程、教室借用流程、学籍异动处理流程、缓考申请流程、培养方案审核流程、创新学分申请流程、学籍信息变动审核流程等。
			9. 发布通知公告：可自定义通知公告的类别，可建立多个发送通知公告的群组，可指定每个通知公告的接收对象，提供通知公告的弹出提示功能。
			10. 提供教务文档分类管理的功能：可自定义文档下载范围，可指定每个文档的下载对象。
			11. 系统运行安全可靠，允许系统管理人员对服务器进行全面监控及针对恶意用户的黑名单管理功能；提供自我监控模块：系统能够对运行情况进行实时监控(包括WEB服务器CPU负载、内存波动、session连接情况、用户访问页面及响应情况、数据库服务器的SQL执行情况、SQL防火墙等各项运行数据)，以便系统管理员优化和安全审计。提供黑名单管理功能: 系统能够自动识别恶意用户，并自动放入黑名单，同时进行警告并给予禁止访问期限。
			12. 标签管理：要求提供学籍标签、教师标签、课程标签、教室标签的自定义功能，如：针对学生可设置拔尖人才、留学生、民族生、交流生、港澳台生、体育特长生等学生标签。支持用户自定义增加、修改标签，设置标签对象。方便各级用户按相关条件进行查询和统计，或是对相关成绩进行处理。
			13. 提供更改院系名称和班级名称的功能或方案，便于学校在进行部门名称或专业归属调整后能够将院系、专业、班级、培养方案、课程等信息进行关联，不影响排课或其他功能的使用。
			14. 提供在线用户及强制用户下线功能。
			15. 提供对学籍信息、上课信息、教学计划信息、学生成绩等数据的归档管理功能。

### 数据挖掘服务

接口定制系统:系统提供接口和开发者管理模块，用户可以在系统中自定义各种接口给外部开发者，开发者提供访问凭据后才可获取对应接口提供的数据。

数据挖掘管理:为满足更高层次的数据挖掘应用，系统应为系统管理员提供数据挖掘功能，使系统管理员可以通过配置SQL语句直接从系统中查询或导出所需的各类型数据，如各类型的教学状态数据、高基报表数据以及临时性的数据分析统计等，如近几年课程及格率分析及未开课情况统计等各类临时统计。自定义数据挖掘功能，系统管理员可以在该模块通过自定义sql的方式从系统中提取所需的各类型数据，使用数据列表或图表(柱状图、折线图)形式展示；提供高基报表导出功能；提供教学状态数据表导出功能，专业基本情况、外聘教师、本科生、专业培养计划、开课情况、本科生辅修、双学位情况、分专业实验课情况等。

提供数据分析功能：如面向学生的年度异动人数、在校生人数、各学院、省市、民族学生人数；面向教学的承担学时数、调课数报表。

**教学监控：**提供教学运行情况统计功能，如教室每周、学期的使用率、学生挂科率、教师每周、每天承担学时数比较情况以及各学院学生每天、每周上课学时、教室每周承担学时数等各种自定义表格。

提供文档管理功能：支持照片、附件、文档等各种类型文档的上传管理，支持大文件分块上传、断点续传。

### 微信服务平台

学生和教师关注微信平台，绑定教务系统用户名和密码后，微信服务平台为全校师生提供教学信息服务功能，包括：

学生和教师查询个人每日课表功能，包括：时间、教室、上课班级、人数、授课内容、教学类型。

学生查询考试成绩功能，包括课程考试成绩、分项成绩，录成绩教师等信息。

教学评价功能，学生可以通过微信平台完成学期末的教学评价。

学生课堂评价，学生可通过微信平台对当天授课教师进行评价。

学生和教师空闲教室查询功能：通过微信服务平台查询全校所有教室的使用情况，从中可以查询教师上课(可查教室当天授课内容)，教室被借用，教室被考试占用等各种使用情况。

教师查授课任务功能，教师可以查询自已本学期的授课任务。

学生查上课任务功能，学生可查本学期自已的上课任务，并可设置是否课前提示上课时间地点。

教师和学生查询教务系统发布的公告通知。

管理人员可通过微信平台完成新生注册功能，通过扫描学生证上的条形码或二维码完成注册。

学生和教师查询考试安排功能。

学生查询自已的考级成绩功能。

学生和教师查询校历及全校课表功能。

学生查询自已的学习计划功能。

学生查看自已的学习完成情况功能，包括必修课完成情况，学分完成情况，与毕业学生的差距等。

微信服务平台可向学生和教师推送上课提醒、考试提醒、调、停、补课提醒功能。

系统支持学生在线进行创新学分申请，支持附件上传，由管理员进行审核，审核通过即可生效。创新学分申请流程支持在系统中自定义设置审核流程，包括审核的步骤层级、每级审核的人员，流程处理结果主动通知。系统支持用户自定义设置创新项目字典表。

提供微信审核功能模块：手机端微信端审核模块包括：成绩录入审核，调停补课审核，缓考审核，教学进度审核，免修审核。

为了简化新学期注册报到工作流程，在教务微信端增加学期扫码注册功能。各个班级由辅导员负责给学生扫码注册，最终可根据班级查看已注册人数、未注册人数并统计导出。具体操作流程如下： 教务微信端增加“我的二维码”菜单，点击查看个人二维码。 新学期开学后，辅导员打开学期报到功能，点击扫一扫对学生出示微信教务端的个人二维码进行扫码，确定注册。 辅导员可在手机微信端查看自己负责的班级，包括查看各个班级的已扫码报到人数、未注册人数及具体的学生。系统管理员界面增加学期注册模块，可查询统计全校的学期注册学生情况并导出。

增加微信自定义消息推送模块，管理员可以在系统设置推送消息内容，消息推送的对象可选择教师或学生，其中学生的推送范围可以按学院、按专业年级，按班级、按学生设定推送或不推送的条件，教师的推送范围可以按部门按教研室，按教师，按角色按部门，按教研室，按教师，按角色设定推送或不推送的条件。

消息点击推送以后标记推送状态为已推送，避免重复推送的误操作。

#  OA系统建设需求

## OA系统建设必要性

高校实行办公自动化有利于事务处理信息化、咨询决策的智能化和指挥调度的现代化。办公自动化系统的建设和应用对提高高校行政管理工作的效率和质量有着十分重要的影响。高校办公自动化系统的应用可以大大提高高校办公效率，也是适应未来办公发展的必然趋势。高校办公自动化系统的设计与建设必然会对学校的信息化和管理现代化起到巨大的推动作用。

##  OA系统功能要求

**1 门户管理**

入口统一：

支撑学校统一的信息化入口，包括PC门户和移动门户，用户通过一个入口访问学校各个应用系统

提供统一消息管理，可以将用户系统内的各个模块和异构系统的待办、待阅、通知等信息集成在一个模块界面内展示，并标注该消息来源；通过统一消息中心可以直接进入该消息来源的模块及系统进行处理

门户展现：

支持把系统中的各个模块的信息科学的、有机的展现在工作门户上，方便工作人员第一时间了解自己的待办、待阅的各种公文、会议、通知、公告、新闻、知识、档案等

可以根据业务导向展示业务地图，根据用户业务地图引导用户工作，指引用户自助查找相关材料和自助完成相关工作。且支持样式的场景地图。

门户配置：

支持根据用户的需要有业务人员通过拖拉拽的方式配置门户中的内容，根据登录人的信息需求显示对应的门户，实现门户千人千面展示，比如学校信息门户、各个部门门户、高管门户、新人门户、个人工作台等

提供常用部件，包括快捷方式、常用链接、多级树菜单、自定义页面等，方便用户从门户中快速导航到系统内或系统外的已有页面

提供系统弹窗功能，维护人员可以在系统中选择弹窗固定模板或者自定义模板新建弹窗。通过弹窗可以给用户呈现公司的重大事项，员工生日或者入职关怀内容

支持构建匿名门户，匿名门户和普通门户一样都可以通过配置完成搭建，且匿名门户上的组件也必须是有匿名权限的才可以访问使用

门户除了可以配置外，还支持源码模式，支持源码调整

可以实现一键将系统主题置为灰化，类似名人诞辰忌日、国家重大事件发生、客户有重大事件发生时可使用

门户权限：

根据按组织按角色按业务进行构建的不同维度门户，支持给予不同的权限人员维护和使用

统一搜索：

支持正文、附件搜索，用户自定义并组合多种文档查询条件外，还提供全文检索，支持用户输入关键字快速检索；支持查看快照，准确定位搜索字段在内容中的位置。同时能把相关知识智能推送给用户

**2 值班管理**

为学校排班提供便捷、直观的操作，通过管理区域组的排班、节假日、假期将管理员从繁复的工时计算中释放出来。员工还可查看假期额度、请假明细等，使工时的管理更加透明、有据可依。

**3 公文管理**

支持公文起草、审核、会签、编号、套红、盖章、分发、签收、归档全周期管理，支持稿纸格式、公文流程自定义配置，分颜色区分公文紧急程度

支持将审批操作按钮放在稿纸指定位置，方便领导直观操作

支持公文正文在线编辑、附件上传两种模式，支持痕迹保留

支持公文归档至档案管理模块，支持归档路径设置，归档字段自动从公文稿纸中获取

支持公文发起督办，建立督办事项，发起的督办自动关联原公文

支持移动端发起公文、在线编辑、在线批注等

多人同时阅签公文时，可以由公文秘书根据实际情况手动变更处理顺序

**4 督办管理**

支持监督督办事项的立项、执行、沟通、反馈等操作过程；

支持督办立项、任务分派、督办结项、督办反馈、督办考评；

支持用百分比展示督办进度；支持督办统计；

支持从流程管理，会议管理，公文管理等模块中关联新增督办；

支持以日历的形式对所有督办进行统一展现，可以按督办状态、不同时间维度展现

能根据督办进展情况进行提前和延期两种方式预警。通知方式有待办、邮件、短信。

**5 会议管理**

支持日历式可视化的会议室管理，显示预定情况；

支持自动会议室资源冲突检测提醒，检测冲突后支持移动端一键电话沟通。有删除权限的角色可以删除会议室预约，释放当前时段会议室资源

支持会议纪要上传；

支持会议关联生成工作任务；

支持会议的各个阶段启动督办分派，实现会前的工作安排以及会后的工作落实。并实时进行督办反馈和评价等

提供与印象笔记、移动终端、365日历、MAXHUB会议平台等的互相同步功能

会议签到支持动态二维码实时刷新、GPS定位等多种方式签到

**6 流程管理**

提供遵循国际标准BPMN2.0规范的流程引擎，可独部署供业务系统调用；

免插件，流程引擎支持主流浏览器，提供可视化的流程引擎，支持拖拽式配置流程，提供流程泳道图，便于流程梳理；

支持超时自动催办、提醒发起人、自动处理，时间精确到分钟；

可以在流程节点可设置关键条款，需审批人查看了关键条款进行勾选确认后进行下一步审批处理；审批人可以查看每个流程节点的审批时间，可以根据审批时间设置预警提示，系统自带的流程分析工具可对组织效率和流程效率进行深度分析，为流程优化提供数据支撑；

流程仿真测试，管理员在流程配置界面可以发起仿真，输入必要字段，可以自动测试流程的审批路径，系统自动计算并显示各个节点实际处理人，支持保存测试实例，进行批量测试，异常节点通过红色预警；

流程中支持关联学校相关管理制度、关联事项等，且支持自定义配置；流程结束后可将流程归档至档案模块，或知识库，并自动将流程中的关键信息记录下来；

满足嵌入性子流程的设置，即总部设置主流程，分部则可以自由灵活的设置主流程中分部的内容；

流程中产生通知待办消息可让用户根据场景对节点进行自定义设置，流程中的审批意见可以自定义常用审批语；

流程跟踪可以按照节点进行自定义选择，跟踪细化到自己关注的节点，当该节点审批人处理时，通知到自己。

**7 表单管理**

表单使用：

支持表单数据的导入，明细表数据的导入、导出

支持附件的批量上传、下载，支持附件顺序调整，以及附件重命名

提单人可以设置表单中的阅读权限、附件权限，附件权限可以管理到是否可拷贝、可下载、可打印等这种细化程度

审批意见可以显示在表单上，且打印表单时可以打印出审批意见

关键流程执行情况可以在表单上呈现，投票结果也可以在表单上以图表呈现

表单配置：

支持可视化表单配置，提供丰富的表单控件，包括但不限于常规表单元素（单行输入、多行输入、单选按钮、多选按钮、下拉菜单、日期选择、附件上传、值计算、大小写转换等）、集成表单控件、地图控件、大数据控件、二维码控件、投票结果控件、审批意见控件、OCR图文识别控件（身份证、营业执照、驾驶证、行驶证等）等，配置效果即真实效果，所见即所得

支持多种方式生成表单，包括直接使用通用表单、引入通用表单再调整、Execl导入生成表单等多种方式

可实现权限区段控制，不同节点不同审批人有表单字段权限

支持多表单，不同流程审批节点可展现不同的表单

表单中的敏感字段支持安全加密，同时数据库中该字段也加密

PC端表单配置与移动端表单自适应，移动端表单自动生成无需二次设计，如需调整也可以拖拉拽调整

**8 知识文档**

支持建立不限层级的知识目录，并可设置目录访问权限

支持知识版本管理；支持知识发布流程审核，支持知识在线点评、评分、推荐

支持知识的统一搜索，支持正文、附件搜索，支持查看快照，准确定位搜索字段在内容中的位置，搜索结果能呈现相关问答、热词、其他用户搜索推荐

支持文档在线阅读，无需下载到本地，无需安装插件，且可加载动态水印。此功能要求移动端也必须满足。

**9 车辆管理**

实现对公司内部公用车辆的统一管理，包括车辆信息登记、车辆保养/保险/违章信息维护、车辆状态跟进、历史用车情况查询、车辆保险日期提醒等功能

根据用车申请统一进行车辆调度，合理的安排出车资源，以避免造成不必要的浪费。车辆调度时，填写车辆的出车时间、用车人、具体行驶路线等信息

用车完成后，由回车登记员进行回车登记，记录回车时间、出车时产生的费用等资料

**10 规范制度**

规范制度实现学校制度流程的起草、审批、校对、发布、完善、新版本的全生命周期管理。支持按照学校特点，对制度流程进行不同类别的划分，例如建立“法律法规标准、学校标准及制度、资料和指引”等。

**11 工作沟通**

提供一对一、一对多的沟通过程管理，方便日常工作沟通、督办、协调等工作。适合解决跨部门、多任务的协作难题，通过发起某一协作主题，将参与人添加到该协作主题中，组成一个虚拟团队共同完成一个工作事项，让每一个参与人都能及时准确的了解事情的进展情况并进行相关交流。常见的应用场景如信息的传达知会或就某一主题的讨论协商，强调的是参与交流和事项跟踪。

**12 工作总结**

支持按年、季、月、周设置总结模版，新建总结可自动关联上一周期总结内容及计划，与本阶段进行对比；

工作总结可与流程功能关联，实现部门领导审核，支持优秀总结推荐到新闻公告；

**13 网上调查**

支持设置不同类型得调查题型，包括单选、多选、评分、问答、矩阵等；

可设置问卷有效期、调查对象，支持统计调查结果，支持结果导出Excel,支持匿名调查；

支持组织架构外部人员扫码参与调查

**14 投票管理**

提供面向学校内部投票活动的管理功能，实现从发起投票、参与投票、查看投票、终止投票、催办投票的全周期管理，可用于快捷的学校调查、市场调查、项目调查、活动组织、个人抉择等。当学校员工有一些新的想法或建议，也可以通过投票方式来采集这些新的想法、建议或者解决方案的受欢迎程度。

**15 员工活动**

通过员工活动模块面向企业员工组织各类员工活动。企业可以创建活动计划、发布员工活动通知，员工可对活动做出响应，方便活动组织部门对实际的活动安排做出调整。历次活动的发布及报名信息将分类保存在系统中作为企业知识沉淀下来。

**16 用品管理**

支持办公用品库存管理，入库、领用自动增加、扣减库存；

支持按部门、人员统计领用情况

**17 移动办公**

系统提供移动端H5页面，支持手机、平板等移动端，包括不限于钉钉、企业微信、自研APP等

可以将移动门户在移动端上展示；可以实现移动端工作消息提醒；可以在移动端发起流程、审批流程、查阅资料(不限于word、PDF、PPT等)等

流程审批与即时通讯功能无缝连接，可以通过流程直接发起群聊，拉取相关人员进群，针对当前流程进行沟通交流，所有沟通记录与流程关联，后续通过流程可查看群聊信息，通过群聊信息可查看流程情况。保证沟通与流程很好的挂钩并留痕

**18 WPS在线预览**

提供基于OA系统内的Office文档的在线预览能力

支持PDF文件在线阅读，免安装插件

提供预览文件时动态页面水印能力和页面防复制功能

可在safari、firefox、chrome等常用浏览器和移动端（ios、Android）正常使用，免安装插件

# 学工一体化系统建设需求

## 学工一体化系统建设必要性

开展学工一体化工作是实现院校人才培养模式变革、提升技能人才培养质量的重要突破口，是实现从知识灌输向能力培养转变、从课堂教学向生产教学转变、从书本教学向实践教学转变的重要举措。学工一体化培养模式将工作过程和学习过程融为一体，培育德技并修、技艺精湛的技能劳动者和能工巧匠，是院校新形势下的必由之路，因此学工一体化系统建设势在必行。

## 学工管理系统

### 学工管理[PC端]

#### 学生基本信息管理

学校提供学生基础信息，进行数据初始化。

学生数据导入监测：系统可以对一键导入的学生数据进行匹配监测，自动显示导入数据总条数，错误数据条数以及成功执行条数。可对错误数据进行导出并可查看错误数据情况，再次导入数据时可以选择是否覆盖原有数据。

###### 平台集成

与学校数据平台对接，每天定时同步学生数据。

##### 学生信息采集

学生首次登录系统需要对学生身份合法性进行实名认证，并采集学生基础信息（民族、宗教信仰、家庭信息、健康状况、照片、户口所在地、籍贯、出生地、政治面貌、入党日期、入团日期、联系方式等），认证后学生不能修改数据，如需修改只能在学校开启的可修改字段范围修改。

##### 基础信息管理

###### 学院信息管理

展示全校学院信息，包括：代码、名称、简称等信息，校级管理层可对数据进行新增、修改、删除操作。

###### 专业信息管理

展示全校专业信息，包括：代码、名称、层次、所属学院、学科门类等信息，校级管理层可对数据进行新增、修改、删除操作。

###### 班级信息管理

展示全校班级信息，并统计出班级党员人数、男女人数、在校人数等信息，根据不同权限范围用户，可以管理自己负责范围内的班级数据并可对班级数据新增、修改、导出统计操作。

###### 学生信息管理

展示学生基础信息和各项业务综合办理数据，除展示学生基础信息外还将展示：评奖评优信息、家庭困难生认定信息、违纪、勤工助学、学籍异动、资助等。根据不同权限范围用户，可以管理自己负责范围内的学生数据可根据查询条件精准定位群体或个体学生并可对学生数据新增、修改、删除、导出统计操作。

##### 学生其它信息管理

学生可提交自己的其它信息，提交后需辅导员审批。其它信息包括：任职信息、技能证书信息、科研项目信息、学术论文信息、发明专利信息、学科竞赛参与及获奖情况、活动参与及获奖情况。

##### 学生信息可编辑设置

学校可设置学生信息可编辑操作范围，可灵活设置学生处、学院、辅导员、学生可以修改的学生信息字段。

##### 班级配置管理老师

灵活设置辅导员所带班级，支持辅导员只带一个班级或多个班，支持一个班配多个辅导员。辅导员可管理自己所带班级学生信息及业务审核查询。

##### 班干部、评议小组设置

辅导员设置所带班级班干部包括：班长、心理委员、团支书等。

辅导员设置困难生认定、评奖评优、综合测评评议小组包括：一名组长负责最终的审核操作和多名小组成员负责核查数据留言。

##### 设置及还原毕业生

可根据毕业届次将学生设置为毕业生，也可将毕业生还原为在校生。如与数据平台集成可按照数据平台数据自动认定毕业生。

##### 学生数据备份

###### 备份时间设置

备份库由学生处进行管理，学生处设置备份时间点，按照学期进行备份，设置每学期备份时间点，学生处也可直接进行手动备份。

###### 备份学生库

学生处、学院可导入、新增、调整、删除备份库的权限范围内学生信息，可自定义导出和统计数据。学院可查看本学院学生的备份库学生信息，辅导员可查看所带班级的备份库学生信息。

#### 学生异动信息管理

##### 班级异动

1、可同步数据中心学生降级或调班信息并形成记录。

2、可支持手动调整，院系可以在本院系内调整、学校可以跨院系调整。

3、支持院系、学校不同层次范围的批量调班。

##### 学籍异动

1、可同步数据中心学籍异动数据并形成记录。

2、可按照学籍异动流程完成异动业务：由学院发起申请，学生处审批，如休学、退学、转学等学籍异动类型。

##### 异动数据还原

学生处、学院可查看学生异动记录，学院可还原本学院调整的异动记录，学生处可还原全部的异动记录。

#### 入学教育考试

##### 业务设定

###### 考试类型管理

可设置考试类型名称及所属层次，如专科、本科等。

###### 考试题库管理

可设置题目所属类型、题干、试题类型，试题类型支持单选题、多选题、填空题。

###### 批次设置

设置考试批次，包括批次名称、所属层次、所属学年、所属年级、所属学院、试题类型、考试类型（是否重复考试）等，并可设置单选题数、多选题数、填空题数及对应的分值，设置学生合格总分，设置考试时长及考试时间段。

##### 业务流程

###### 学生考试

学生点击开始考试，系统根据考试批次设置的条件自动从题库提取试题随机生成试卷，学生在规定的时间内进行考试。考试结束后，若该批次考试类型为重复考试，未达到合格总分的学生不计成绩，学生可重新生成试卷重新考试。

###### 考试进度监控

在考试时间段内可实时监控各二级学院的考试情况，包括：所属学院、应参考人数、已参考人数、未参考人数、参考率、平均得分等。可查看各学院学生考试详细情况，并可按照学号、姓名查询学生考试详情，支持导出数据。

##### 数据查询统计

学生处、学院、辅导员可查询自己权限范围内学生的考试情况，包括：参考人数、比例、通过率等，可对学生考试数据进行自定义统计和导出。

#### 学生资助管理

##### 家庭经济困难生认定

###### 数据导入

根据四川省资助系统家庭经济困难生数据模板，学校可一键导入四川省资助系统家庭经济困难生数据数据到学工系统。

###### 认定结果查询

学生处、学院、辅导员可查询权限范围内学生的家庭经济困难生认定结果。

###### 认定结果统计

学生处可根据学年、层次、年级统计各学院总人数、各困难等级人数、家庭经济困难生比例。

##### 生源地助学贷款

###### 批次设置

学生处设置生源地贷款批次，包括：批次名称、年度、登记开始时间、登记结束时间。

###### 学生登记

学生在登记时间段内进行登记，登记内容包括：贷款银行类别、是否已回执、回执码、合同号、贷款总金额、每年放款金额、贷款年限、附件等。

###### 数据管理

学生处、学院、辅导员可查询权限范围内学生的生源地助学贷款记录。

##### 校园地助学贷款数据管理

可对校园地助学贷款数据维护管理，提供批量导入贷款记录。包括：应缴学费、实缴学费、当年贷款金额、贷款年限、贷款总额、贷款时间等。

##### 临时困难补助

###### 学生申请

学生随时可提交临时困难补助申请，包括：申请理由、家庭情况、佐证材料等。

###### 各级审核

辅导员、学院、学生处审核学生申请信息，学院审核时填写补助金额。

###### 数据管理

学生处、学院、辅导员可查询权限范围内学生的临时困难补助记录，学生处统计年度各学院临时补助情况。

##### 绿色通道数据管理

可对绿色通道数据维护管理，支持批量导入贷款记录。绿色通道类型包括：助学贷款、建档立卡精准扶贫、服兵役、其他等类型。

如类型是助学贷款，需要填写合同号、回执码、贷款金额、放款金额。

如类型是建档立卡精准扶贫，需要填写地址（精确到门牌号）、上传佐证材料（学生身份证复印件、扶贫手册复印件、户主身份复印件、户口本复印件）。

如是服兵役，需要选择退役复学或退役入学并上传退伍证。

如是其他类型，填写原因即可。

##### 助学金管理

###### 助学金项目设置

助学金类型管理：国家助学金、学校助学金、社会助学金；助学金信息包括：助学金名称、颁奖单位、金额、适用对象、申请条件、申请字段选择（主要包括：家庭经济情况、家庭成员、学习情况、获奖励或荣誉情况、申请理由、附件等）。

###### 项目不可兼得设置

通过设置项目不可兼得，避免学生重复多次获得同类助学金。

###### 批次设置

学生处开启评定批次，主要包括：批次名称、适用学生、申请时间段、学年、成绩调用年、说明等，学生处开启批次后各学院在时间范围内开启各学院的申请批次。

###### 申请名额设置

学生处设置各学院助学金名额，学院审核时将只能审核通过小于或等于该名额。

###### 学生申请

学生按照学生处设置的助学金申请表，填写并提交助学金申请，不满足申请条件的学生将提示不符合原因。

###### 各级审核

辅导员、学院、学生处审核学生申请信息，国家助学金审核时可选择助学金等级。

###### 名单公示

学院审核通过后，可开启院内公示；公示期间可以调整获奖信息。学生处审核通过后可开启校内公示。

###### 获奖名单查询

辅导员、学院、学生处可查询权限范围内的获奖名单信息。

###### 打印申请表

按国家助学金统一模板或校内模板打印学生助学金申请表，可以单个打印或批量打印。

###### 生成电子发放表

学生处公示结束后，可一键生成电子发放表并设置发放比例。

##### 数据上报

###### 上报资助中心

按照资助中心上报要求，形成上报数据，支持一键导出。如：家庭经济困难生数据上报、建档立卡困难学生数据上报。

###### 上报教育部

按照教育部上报要求，形成上报数据，支持一键导出。如：在校学生信息上报、家庭经济困难生上报、各类国家奖助学金上报等。

#### 勤工助学管理

##### 业务设定

###### 用人单位管理

资助中心维护需要勤工助学单位的基础信息，并设置用人单位的负责人。

###### 岗位申请设置

资助中心设置当前勤工助学的学年，可同步上一学年的岗位信息和学生在岗信息到当前学年。

资助中心设置岗位最高金额，岗位最高金额将作为单位申报工资时的限制条件，申报的工资不得超过最高工资限制。

##### 用人单位岗位申报流程

###### 用人单位岗位申报

用人单位负责人申报本单位需要的岗位，岗位分为：固定岗位和临时岗位。

申请信息包括：岗位名称、类型、预计月工资、需求人数、工作开始时间、持续时间、岗位描述，可设置岗位申请条件，如：是否为家庭经济困难生、是否限制性别、年级、专业等信息。

###### 各级岗位审核

资助中心审核用人单位申报的岗位，可修改用人单位岗位需求人数和详细信息。

###### 岗位发布

资助中心岗位审批通过后，系统将按照岗位设置的发布时间段自动发布到岗位公示区，学生可查阅、申请岗位。

##### 学生岗位申请流程

###### 学生申请岗位

学生提交岗位申请，如不满足岗位申请条件，系统将提示不满足项。

申请岗位时需填写家庭情况、受资助情况、特长优势、是否服从安排、是否参与过其他勤工助学、是否为家庭经济困难生，以及空闲时间段等。

学生可同时提交多个岗位申请，最终只能在一个固定岗位入职，临时岗位无限制要求。

###### 岗位申请审核

用人单位审核学生岗位申请，用人单位确认意向学生后可以联系线下面试，面试通过后再进行审核通过操作。

###### 学生上岗

用人单位审核通过后，设置学生到岗时间和开启学生在岗状态。用人单位可手动添加学生。

##### 用人单位工资申报流程

###### 工资申报

用人单位每月提交在岗学生工资，根据工作时长可调整工资金额。

系统自动判定所设置金额不能超过设置的岗位最高金额限制。

###### 工资审核

资助中心审核用人单位工资申报，资助中心可修改工资金额。

###### 工资汇总

用人单位工资申报通过后，形成全校工资汇总表，用于各级用户查询。

##### 工资发放流程

###### 设置发放批次

资助中心审核工资后，按月生成发放批次，每月支持多个发放批次。

###### 生成工资发放表

资助中心设置发放批次后系统自动生成学生工资发放表，确认后资助中心将发放名单提交至财务进行工资打款。

###### 工资发放记录

财务打款后将打款成功的学生名单反馈到资助中心，资助中心设置学生工资发放状态（已发放、未发放）

##### 数据查询统计

###### 用人单位岗位情况统计

按年度统计各用人单位年度岗位数量和需求人数与预计需求人数的使用比例。

###### 学生岗位情况统计

按年度统计学生岗位数量、用工时长及工资总额汇总排行。

#### 评奖评优管理

##### 业务设定

###### 奖项设置

奖项类型管理：国家奖学金、学校奖学金、社会奖学金、常规评优、优秀毕业生，奖项内容包括：奖项名称、颁奖单位、金额、适用对象、申请条件、申请字段选择（主要包括：学习情况、获奖励或荣誉情况、申请理由、附件等）。

###### 奖项不可兼得设置

通过设置奖项不可兼得，避免学生重复多次获得同类奖项。

###### 批次设置

学生处开启评定批次，主要包括：批次名称、适用学生、申请时间段、学年、成绩调用年、说明，学生处开启批次后各学院在时间范围内开启各学院的申请批次。

###### 申请名额设置

学生处设置各学奖项名额，学院审核时将只能审核通小于或等于该名额。

##### 业务流程

###### 学生申请

学生按照学生处设置的奖项申请表，填写并提交奖项申请。不满足申请条件的学生将提示不满足原因。

###### 各级审核

辅导员、学院、学生处审核学生申请信息，如奖项名额不足，可将学生调整到同批次不可兼得的奖项。

###### 名单公示

学院审核通过后，可开启院内公示。公示期间可以调整奖项信息。学生处审核通过后可开启校内公示。

##### 数据查询统计

###### 获奖名单查询

辅导员、学院、学生处可查询权限范围内的获奖名单。

###### 打印申请表

按国家奖学金统一模板或校内模板打印学生获奖申请表，可以单个打印或批量打印。

###### 生成电子发放表

学生处公示结束后，自动生成电子发放表并可设置发放比例。

###### 学生综合名单生成

评奖评优完成以后，可以按照学年、学院以及奖项自动生成获奖学生的详细名单，点击下载后可查看评奖评优综合名单，名单包含学院、专业年级、学号、姓名、班级、各获奖项目金额明细及获奖总额。

##### 其他奖项数据管理

未经过系统审批的奖项可由学生处按照学年导入系统，导入的字段包括：学号、姓名、奖项名称、奖项金额等。

#### 学生综合素质测评

##### 业务设定

###### 测评指标设置

1、预置加分规则表:由学生处或学院预置加分项目，包括测评类型（德育、智育、体育、美育、劳育）、测评项目、限制类型（无限制、次数限制、分数限制、在校期总次数限制）、限制值、分值类型（固定分值、分值范围、子项分值）。

2、预置减分规则表:由学生处或学院预置减分项目，包括测评类型（德育、智育、体育、美育、劳育）、测评项目、限制类型（无限制、次数限制、分数限制、在校期总次数限制）、限制值、分值类型（固定分值、分值范围、子项分值）。

###### 考试成绩管理

集成数据平台或导入学生各科基础成绩(考试成绩和其他基础成绩，其他基础成绩为预置的测评类型数据)：由学生处或学院统一进行导入；

检测学生学年内是否存在重修的成绩，然后根据情况作删除处理；

###### 批次设置

学生处开启测评批次，设置学年、批次名称、参评届次、批次时间段、学生数据备份库等。

##### 业务流程

###### 学生申报加分

学生提交加分申请，加分项限于本学年或学期参与的活动、获得的奖项。

###### 班长/辅导员申报本班减分

由班长/辅导员录入学生的减分项；

###### 各级审核

流程:学生提交数据、班长提交数据→辅导员审核→学院审核→学生处审核。

###### 测评进度监控

辅导员、学院、学生处可实时查看权限范围内学生提交综合测评的加减分情况，学生处可查看各学院学生提交时间、辅导员审批时间、学院审批时间、当前状态等，可按学院查看学生确认情况，包括学院人数、已确认人数、未确认人数，并可查看具体未确认学生名单。

###### 成绩计算

学院和学生处根据各测评项权重计算学生综合测评成绩，自动计算出班级排名和专业年级排名。

##### 学生综合测评一览表

系统自动为每个学生生成综合测评成绩一览表，该表支持导出和打印。

##### 综合素质测评数据查询统计

辅导员、学院、学生处可对权限范围内学生综合测评数据进行查询、统计。

#### 学生违纪管理

##### 违纪申报

辅导员上报本班违纪学生，主要包括：处理部门、违纪情况描述、认定结果、违纪时间、处分结果、处分时间、处分截止时间。由学生处最终审核通过后打印违纪送达书。

##### 学生申诉

学生收到违纪送达书后7天内可提起申诉，提交申诉申请。

##### 违纪解除申请

当学生违纪达到处分截止时间，系统将在待办提醒中提醒学生申请违纪解除。申请内容包括：符合解除条件（处分期满、处分期间表现突出、处分期间无违纪）、申请理由、附件等。

##### 各级审核

由辅导员、学院、学生处审核通过后即可解除违纪。

##### 违纪数据查询统计

辅导员、学院、学生处可查询权限范围内的学生违纪信息。

#### 学生请销假管理

##### 请假流程配置

可灵活配置辅导员、学院、学生处相应审核请假的天数，学生申请的请假天数不同则审核的流程不同，若更改请假流程，更改前提交的请假申请沿用原审核流程，更改后提交的请假申请遵循最新请假流程。

##### 学生申请

学生可提交请假申请，内容包括：请假时间段、请假事由、请假原因、外出地点、外出联系人信息、往返交通工具等。

##### 各级审核

根据学生处配置的请假流程，在审核人员权限范围内的天数可直接准假，例如3天以内辅导员审核即准假、6天以内学院审核即准假、6天以上需学生处审核方可准假。

##### 请假数据管理

辅导员、学院、学生处可查询权限范围内的请假名单信息并可打印请假单。

##### 学生销假

学生请假结束返校后，需要到辅导员处进行销假，只有销假成功的学生请假流程才最终结束，未销假学生不可再次请假。请假时间到期后如果学生未进行销假，系统会自动提醒学生本人及辅导员。

##### 学生请假数据统计

可以按照学期、学院、年级查询学生的请假汇总情况，汇总情况表包含学院、年级、请假情况、请假原因、请假天数等。

#### 节假日去向管理

##### 节假日设置

学生处进行节假日去向登记设置，包括：节假日名称、节假日开始结束时间、学生登记开始结束时间、是否开启、年纪范围、层次范围及注意事项等。

##### 学生去向登记

学生在批次时间段内进行去向登记，包括：类型（留校、外出）留校无需填写其他内容，外出需要登记：外出时间段、外出类型（求职、实习等）、外出原因、外出地点、外出联系人、同行人数等信息。

##### 学生去向登记监控

可按照学历、学院、年级、专业、班级、性别、学号、等级状态等查询学生去向登记情况，并可对查询数据进行数据导出。

##### 学生返校登记

节假日结束后所有学生都需要到辅导员处进行返校登记，辅导员标记已返校或未返校，未返校需要选择未返校原因。

##### 返校情况统计

统计各学院返校情况，包括返校应到、实到、未到及未返校原因，点击未返校人数可查询未返校人数名单，并可进行查询数据导出。

#### 寒暑假留校管理

##### 寒暑假留校批次设置

设置假期名称、放假开始日期、放假结束日期、留校申请开始日期、留校申请结束日期、留校须知、留校承诺、留校材料等。

##### 学生申请

学生在线登记寒暑假留校信息，如：留校住宿时间、留校住宿事由、上传本人签字安全责任书、上传家长签字留校知情书及上传其他附件。

##### 审批及留校宿舍安排

学生申请后，经辅导员→学院→宿管中心或学生处各层级审批完成后安排宿舍。

##### 寒暑假留校数据查询与统计

可查询学生寒暑假留校登记详细情况，并可按照学历、学院、年级、专业、班级、性别等查询寒暑假留校详细信息，可对寒暑假留校数据进行统计与导出。

#### 网络问卷调查

可灵活设置问卷调查主题、设置主题名称、性别限制、困难等级限制、政治面貌限制、学历限制、学院限制、年级限制及填写说明等。

主题设置完成后，可对该问卷调查主题添加题目，题目类型包括：单选、多选、填空等，设置问卷调查题目名称是否为必填项，题目设置完成后可开启问卷调查预览，可对问卷调查结果进行监控。

学生实名在线完成调查并提交，可监控已经提交问卷调查学生及未提交问卷调查学生，调查结果可以自动生成并下载存档，根据需要可对调查结果进行统计、分析。如：调查新生思想状况及学生关注的热点问题。

#### 网络评选投票

设置网络投票评选批次、批次名称、评选开始时间、评选结束时间、是否进行投票限制、候选人排名、限选人数及规则介绍等。

批次设置完成后可预览、设置参选人员等。学生在线实名投票评选候选人，并可与候选人网上留言互动，投票结果实时查询、统计。

#### 政工队伍建设

##### 教职工信息管理

学生处维护所有需要参与学生工作的教职工，或与数据平台集成后该数据可自动同步。

##### 教职工其他信息管理

教职工可填报自己的其他信息、学生处可维护所有教职工的其他信息，包括：教育背景信息、任职情况信息、工作经历信息、继续教育信息、行政职务信息、专业职务信息、职业培训信息、项目学习信息、职业证书信息、奖励情况信息、科研情况信息等。

##### 工作提醒

具备全面的工作提醒机制，教职工登录系统后，及时准确提醒当前待办事宜。

##### 辅导员工作日志

辅导员在线填报工作日志，包括：工作类型、指导班级、对象、时间、地点、工作内容，并上传工作图片等，可查看辅导员工作日志填报情况，并按照学院、填报起止时间统计辅导员工作日志情况。

##### 个人工作代理

设置个人工作代理给其他工作人员，工作代理完成后自动退出系统，再次登录系统时可取消代理，取消代理完成后，可正常登录系统处理工作。系统将自动记录被代理人和代理人的代理记录。

#### 辅导员考核

##### 业务设定

###### 考核部门设置

设置参与辅导员考核的相关部门，包括：部门名称、部门用户、联系人、联系电话等。

###### 考核规则设置

设置学生、学院、职能部门对辅导员考核的考核指标。

指标包括：考核项目、考核内容、考核要求、分值，评分指标设置后各评分人员在进行评分操作时系统将根据设置的评分指标自动生成辅导员考核评分表。

###### 批次设置

学生处开启考核批次，设置批次名称、学生评分时间段、学院评分时间段、职能部门评分时间段，设置学生、学院、职能部门评分权重比例，设置分值系数，如：优秀分值、良好分值、合格分值等。可设置班级有效评分人数比例，如：每个班评分人数必须达到60%该班考核评分才纳入到辅导员考核公式中进行计算。

###### 设置参评辅导员

根据批次设置参评辅导员名单，按查询条件精准定位到需要参与考评的辅导员信息，可批量选择确认操作。

##### 业务流程

###### 学生评分

学生为本班辅导员进行考核评分，按辅导员考核学生评分指标表填报。

班级评分人数必须满足批次中设置的人数比例，本班的评分结果才纳入计算。

###### 学院评分

学院评分人员为本学院参与考核的辅导员进行考核评分，按辅导员考核学院评分指标表填报。

###### 职能部门评分

职能部门为全校参与考核的辅导员进行考核评分，按辅导员考核职能部门评分指标表填报。

###### 进度监控

学生处、学院可实时监控各评分人员的评分情况。

辅导员可监控所带班级评分情况，查看评分人数是否满足学生有效评分比例。

###### 考核结果自动计算

考核评分结束后，根据各项考核指标的占比自动计算得出辅导员考核最终得分。

###### 考核结果手动调整

辅导员考核结束后，学院、学生处可对考核结果等级手动调整。

##### 数据查询统计

辅导员可查询自己考核最终得分和考核等级，但不可查询评分明细。学生处可查询全校辅导员考核得分和明细，可对辅导员考核结果数据进行统计、导出。

#### 学生证补办管理

##### 乘车区间设置

设置全国乘车区间。

##### 学生申请

学生提交证件补办申请，包括：遗失情况说明、遗失时间等。

##### 各级审核

辅导员、学院、学生处审核学生申请信息。

##### 数据查询统计

辅导员、学院、学生处可查询权限范围内的证件补办信息。

#### 学生签到管理

1. 发布签到任务，如查寝、晚自习、早操等，发布信息包括签到名称、类型、涉及年级、涉及学院、签到方式（拍照签到、定位签到、二维码签到）、签到开始时间和签到结束时间等。
2. 可对签到的定位进行设置，设置签到位置、位置维度、位置经度及覆盖范围。
3. 可查看学生的签到情况：包括学院名称、年级、学院总人数、已签到人数、未签到人数、已签到人数比例和未签到人数比例。点击未签到人数可以查看具体未签到学生信息。

#### 学生登记表

##### 批次设置

批次信息包括：批次名称、年级、开始时间、结束时间、说明等。

##### 学生填报

学生在规定时间内填写学生登记表内容。

##### 辅导员审批

辅导员可批量/单个审批学生填报数据，审批通过后可批量下载打印学生登记表，学生也可直接打印预览本人登记表。

##### 数据查询与统计

学生处、学院、辅导员可查询、导出、统计权限范围内的学生登记表信息。

#### 毕业生登记表

##### 批次设置

批次信息包括：批次名称、年级、开始时间、结束时间、说明等。

##### 学生填报

学生在规定时间内填写毕业生登记表内容。

##### 辅导员审批

辅导员可批量/单个审批学生填报数据，审批通过后可批量下载打印毕业生登记表，学生也可直接打印预览本人毕业生登记表。

##### 数据查询与统计

学生处、学院、辅导员可查询、导出、统计权限范围内的毕业生登记表信息。

#### 自动生成学生成长档案

通过学生在校期间各项业务数据自动生成学生成长档案，展示学生在校期间所有学习、生活、活动和社会实践过程，反应出学生态度、思想品德、专业技能、特长爱好、创新意识、身心健康情况，学生毕业后成长档案能够让用人单位全方面的了解学生在校期间的表现。

#### 学生学生综合画像

根据学生基本信息、通过收集与分析学生基础信息、学习情况、奖励信息、处分信息、学习行为等、以及业务流程模块以及各系统对接，自动生成学生综合画像，学生的综合画像为可视化图表。

学生的综合画像包含学生基本信息、综合测评、评奖评优、各类资助信息（形成年度受资助总额）、入伍相关信息、处分信息、包括住宿信息、教务信息（成绩单，是否学业警示、休学等）。

学习情况展示内容：展示学生各学年学期总的已修课程门数/总学分，不及格门数/总学分，对上述内容进行各学期的表格展示，支持筛选和查看明细表，明细包括：课程编号、课程名称、课程类型、学年、学期、考试成绩、获得学分，并支持导出。

奖励信息展示内容：展示学生获得的奖学金名称、次数、金额，获得荣誉情况，竞赛获奖情况，对上述内容进行学期表格展示，并支持查看明细记录，明细包括：学年、学期、奖学金名称、设奖单位、类型、金额、获奖时间，并支持导出；荣誉明细包括学年、学期、荣誉名称、设奖单位、获得时间，并支持导出。

展示处分信息内容：展示学生受处罚次数、处分原因，可进行整体的表格展示，并支持查看明细和导出。

展示资助情况内容：展示学生贫困等级认定情况，以及受资助的总次数、金额，助学贷款、助学金、勤工助学、困难补助、补偿代偿等总次数和总金额，并支持各学期详细数据展示。助学贷款明细包括学年、学期、类型、银行、贷款时间、贷款金额；助学金明细包括学年、学期、助学金名称、资金来源、等级、金额；勤工助学明细包括学年、学期、岗位、用人单位、工作性质、月发放金额、发放日期；困难补助明细包括学年、学期、补助名称、发放单位、发放金额、发放日期；补偿代偿明细包括学年、学期、补偿代偿名称、发放金额、发放日期。支持明细数据导出。

手机端应用：支持不同用户手机端查询查看权限范围内学生综合画像信息。

#### 数据管理功能

##### 自定义数据统计

1、提供强大的数据自定义统计功能，实现多表关联的三维统计报表；

2、用户可以根据需要定义不同的统计项，定义不同的统计方式，定义不同的统计条件。

3、可以自主定制统计模板。

##### 自定义数据导出

1、提供强大的自定义数据导出功能，可实现多表数据自动关联；

2、用户根据自身需要可以导出基本信息库里任意字段的数据；

3、可以自主定制导出模板。

### 学工管理[移动端]

#### 学生用户

##### 信息激活

学生第一次登录系统，按学校采集要求完善个人信息。

##### 待办事宜提醒

学生可以通过手机端查看当前待办事宜。

##### 通讯录

学生可以通过手机端查看班级同学联系方式。

##### 辅导员信息

学生可以通过手机端查看辅导员个人信息，包括姓名、联系电话等。

##### 学生日常请假申请

学生可以在手机端完成请假操作，未销假会提示学生销假，学生必须先销假再请假。

##### 节假日去向登记

学生可在手机端完成节假日去向登记，可查看历史记录。

##### 寒暑假留校登记

学生可在手机端完成寒暑假留校登记，可查看历史记录。

##### 签到管理

学生可通过手机端进行签到，如返校、归寝、晚自习、早操等，签到方式为拍照签到、定位签到、二维码签到等。

##### 违纪申诉及解除申请

学生可通过手机端提交违纪申诉及解除申请，并可查询结果。

##### 家庭经济困难生认定情况查看

学生可以通过手机端查看家庭经济困难学生认定情况，还可查看结果及历史认定情况。

##### 临时补助申请

学生可以通过手机端申请临时补助，并可查看结果及历史补助情况。

##### 生源地贷款信息查看

学生可在手机端查看自己的生源地贷款信息。

##### 助学金查看

学生可以通过手机端查看各类助学金，还可查看结果及历史获得助学金情况。

##### 评奖评优信息查看

学生可通过手机端查看本人评奖评优获奖情况。

##### 勤工助学

###### 勤工助学申请

学生可以通过手机端申请当前已经发布的工作岗位。

###### 勤工助学工资查看

学生可通过手机端查看自己勤工助学工作岗位的工资发放情况。

##### 辅导员考核评分

学生可以在手机端对辅导员进行考核评分。

##### 入学教育在线考试

学生可以通过手机端完成入学教育考试。

##### 在线投票

学生可以通过手机端完成投票。

##### 问卷调查

学生可以通过手机端提交问卷调查。

##### 综合素质测评加分提交

学生可以通过手机端提交综合素质测评加分申请，班长可提交本班学生减分申请；综合素质测评结束后，学生可查看本人综合素质测评总分及排名情况。

##### 处长信箱

学生通过手机端给学生处处长留言，回复后学生可以查看本人的留言及回复情况。

##### 站内公示

学生可在手机端查看相关的公示信息。

##### 站内公告（站内信息）

学生可在手机端查看相关站内公告。

#### 辅导员用户

##### 本人信息维护

辅导员修改完善本人信息。

##### 我的工作委托

辅导员可以通过手机端将业务委托给其他老师代理，也可通过移动端结束代理委托。

##### 我的带班信息

辅导员查看本人的带班信息。

##### 我的学生信息

辅导员查询当前所带的班级学生，可查看学生职务、联系方式等信息。

##### 日常请假审批

辅导员可以通过手机端审批学生的请假信息及完成学生销假。

##### 去向登记查看及返校标记

辅导员可通过手机端查看学生的去向登记信息，可通过手机端标记学生是否返校。

##### 违纪申诉及解除审核

辅导员可通过手机端审核学生提交的违纪申诉及解除申请。

##### 业务信息查看

###### 综合测评

辅导员可以通过手机端查询班级学生综合测评总分及排名情况。

###### 家庭经济困难生

辅导员可通过手机端查询所带班级学生家庭经济困难认定情况。

###### 助学金

辅导员可通过手机端查询所带班级学生助学金情况。

###### 评奖评优

辅导员可通过手机端查询所带班级学生奖、优获得情况。

###### 勤工助学

辅导员可通过手机端查询所带班级学生勤工助学情况。

##### 工作日志

辅导员可通过手机端填写工作日志，可拍照上传。

##### 待办事宜提醒

可以通过手机端查看当前待办事宜。

#### 学院用户

##### 学生信息查询

按班级、学生姓名等查询学生信息。

##### 在校学生统计

按年级、学生层次统计本学院在校学生情况。

##### 性别分布

按年级、层次、性别统计本学院在校学生情况。

##### 民族分布

按年级、层次统计本学院在校学生民族分布。

##### 生源地分布

根据学生生源地地区，统计本学院在校学生生源地地区分布情况。

##### 学生请假审核

学院用户可通过手机端审核辅导员通过后的学生的请假申请，并可查询本学院学生请销假情况。

##### 学生违纪解除及申诉审核

学院用户可通过手机端审核学生提交的违纪解除及申诉申请，并可查询本学院学生违纪情况。

##### 政工队伍信息查询

学院用户可通过手机端查询本学院政工队伍中教职工名单，查询内容包括：工号、姓名、性别、联系电话等。

##### 辅导员带班情况

学院用户可通过手机端查看辅导员带班情况及学生激活完成情况。

##### 查看辅导员日志

学院用户可通过手机端查看本学院辅导员日志信息。

##### 业务信息查询

###### 综合测评

学院可以通过手机端查询本学院学生综合测评总分及排名情况。

###### 家庭经济困难生

学院可通过手机端查询本学院学生家庭经济困难认定情况。

###### 助学金

学院可通过手机端查询本学院学生助学金获得情况。

###### 评奖评优

学院可通过手机端查询本学院学生奖、优获得情况。

###### 勤工助学

学院可通过手机端查询本学院学生勤工助学情况。

##### 学院待办事宜提醒

学院用户可以通过手机端查看当前待办事宜。

#### 学生处用户

##### 学生信息查询

按学院、班级、学号、姓名查询学生信息。

##### 在校学生统计

按年级、学生层次统计当前在校各学院学生人数及其激活率。

##### 性别分布

按年级、层次、性别统计各学院在校学生情况。

##### 民族分布

按年级、层次统计各学院在校学生民族分布情况。

##### 学生请假审核

学生处用户可通过手机端审核学院通过的学生请假信息，并可查询全校学生请假情况。

##### 违纪申诉及解除审核

学生处用户可通过手机端审核学院通过后的学生违纪申诉及解除信息。

##### 政工队伍信息查询

学生处用户可通过手机端查询政工队伍中教职工名单，查询内容包括：工号、姓名、性别、联系电话、所在学院等。

##### 处长信箱

学生处用户可通过手机端对学生在处长信箱中反馈的问题进行回复，回复时可选择该问题是否公开。

##### 业务信息查询

###### 综合测评

学生处用户可以通过手机端查询全校学生综合测评总分及排名情况。

###### 家庭经济困难生

学生处用户可通过手机端查询全校学生家庭经济困难生认定情况。

###### 助学金

学生处用户可通过手机端查询全校学生助学金获得情况。

###### 评奖评优

学生处用户可通过手机端查询全校学生奖、优获得情况。

###### 勤工助学

学生处用户可通过手机端查询全校学生勤工助学情况。

##### 待办事宜提醒

学生处用户可以通过手机端查看当前待办事宜。

## 宿舍管理系统

### 宿舍管理[PC端]

#### 校区管理

 设置校区编号、校区名称、校区管理员、校区电话及校区地址等。

#### 园区管理

 设置园区所属校区、园区编号、园区名称、园区管理员、园区电话等。

#### 楼栋管理

 设置楼栋所属校区、园区、楼栋编号、楼栋名称、楼栋管理员及楼栋电话等。

#### 单元管理

 根据所属楼栋设置单元编号、单元名称、联系电话、设置单元管理员等。

#### 房间管理

1.维护房间所属校区、所属楼栋、所属楼层、房间功能（可将房间分类设置：如学生宿舍、办公房、配电室、值班室等）、房间标准（4人间或6人间）、房间号、房间名称等。

2.可对房间信息进行新建、删除、修改、查询，并导入、导出房间信息；可按查询或按勾选条件进行批量删除宿舍。

3.按照查询条件查出满足条件的房间后，点击生成床位，按照指定规则一键自动生成床位号。

4.查询宿舍入住人员，可统计空宿舍数据及未住满宿舍数据。

5.勾选满足条件的宿舍一键批量修改宿舍的性质及入住人数等。

#### 床位管理

1.设置床位所属校区、所属楼栋、房间号、床位编号、床位名称、床位类型、是否预留床位等。

2.对床位信息进行新建、删除、修改、查询，可导入、导出床位信息。

3.床位信息可以按房间属性初始化床位信息，如：4人间，自动初始化为1/2/3/4号床位。

4.按用户查询条件查询后或用户自己勾选一键批量删除床位。

5.勾选满足条件的床位，批量将满足条件的床位一键设置为闲置或回收。

6.清空不在校的学生床位。

#### 宿舍分配管理

##### 新生宿舍分配

1、设置新生年级。

2、设置推送数据至迎新系统，设置开始推送日期、结束推送日期。

3、设置接收迎新系统数据，设置开始接收日期、结束接收日期。

4、一键批量或单个设置空闲床位为预分配迎新床位，可锁定预分配迎新床位。

5、一键收回全部预分配迎新床位。

##### 在校生宿舍分配

1、设置在校生宿舍分配开始时间及结束时间。

2、为学院分配宿舍，可选择分配女生床位或男生床位，可按宿舍或床位进行分配，并查看各学院未分配床位男生数、空闲男生床位数、未分配床位女生数、空闲女生床位，可对学院空闲床位进行一键收回。

#### 学生入住信息管理

 可按校区、园区、楼栋、单元、楼层、宿舍号、学历、学院、年级、专业、班级、性别等查询学生宿舍信息，并可对学生入住信息进行自定义统计、导出。

#### 学生历史入住信息管理

 可按学院、年级、班级、学号、姓名、入住类型、退宿原因等条件查询学生历史入住信息，并支持数据导出。

#### 宿舍入住情况总览

 可按校区、园区、楼栋、单元等条件查询宿舍入住情况，自动生成楼栋或单元入住总体情况，如楼栋总体入住数、入住女生人数、入住男生人数、空闲女生床位数、空闲男生床位数，点击详情可查看该栋楼入住平面图，查看满员、未满员、空宿舍等信息；点击具体平面图房间，可查看该房间详细入住人员情况。

#### 宿舍调换管理

1.学生可提交宿舍调换申请、申请内容为申请时间、申请原因、以及是否有无意向宿舍及意向宿舍房间号等。

2.宿舍调整审批：学生提交宿舍调换申请，经辅导员、学院、学生处/宿管中心审批。

3.宿舍调整记录：学生处/宿管中心审批通过后进入记录库，可以查询相关调换记录。

4.学生处/宿管中心可手动调换寝室或床位。

#### 床位清空管理

 可单个或批量办理退宿，可按照查询条件进行批量或单个清空退宿，清空宿舍信息时需填写床位清空的原因。可还原最后一次清空的数据。

#### 宿舍违纪管理

1、可新建学生违纪信息，设置学生违纪类型、违纪时间、违纪理由、附件上传等，或从线下导入宿舍学生违纪信息，如：不归、晚归或其它违纪信息等，可以查询、统计违纪数据，并可按学历、学院、年级、专业、班级等查询条件一键导出查询违纪数据。

2、可对违纪数据进行自定义统计导出。

#### 宿舍卫生管理

##### 宿舍检查标准设置

 按学期设置宿舍卫生达标分数线及优秀分数线。

##### 卫生检查数据管理

1、录入：相关人员录入卫生检查数据，可选择按寝室、床位录入卫生检查的分数，可支持导入数据。

2、可按校区、园区、楼栋、单元、楼层、宿舍号、检查时间段等查询宿舍卫生成绩，可对卫生检查成绩进行自定义统计与导出。

##### 卫生成绩自动计算

 可按学校规则自动计算宿舍卫生成绩。

#### 宿舍卫生结果统计

 可查看宿舍卫生总体检查次数、未达标的次数、达到优秀的次数等。

#### 学生校外住宿管理

1、学生校外住宿，可线上提交申请，申请信息包括学校要求的各类佐证材料，可打印申请表。

2、经辅导员、学院、宿管中心审核通过后进入校外住宿库。

3、学生处可批量或单个打印申请表并对各学院的校外住宿学生信息进行统计与导出等。

#### 入住学生信息统计

 可按学院、在校学生人数、男生总人数、女生总人数、总床位数、男生总床位数、女生总床位数、使用中床位数、使用中男生床位数、使用中女生床位数、闲置床位数、闲置男生床位数、闲置女生床位数、床位使用率、学生入住率等条件查询统计，并可按查询条件导出。

### 宿舍管理[移动端]

#### 学生用户

##### 公寓制度

 查看公寓住宿的相关学生制度。

##### 服务指南

 查看后勤服务相关指南。

##### 我的宿舍

 查看同宿舍成员及联系方式。

##### 违纪管理

 查看本人的宿舍违纪信息。

##### 宿舍调换申请

 在线申请宿舍调换。

##### 校外住宿管理

 在线申请校外住宿，查看相关信息。

#### 辅导员用户用户

##### 学生住宿

 查询权限范围内学生的住宿信息。

##### 违纪信息录入

 录入学生的宿舍违纪信息，查看相关信息。

##### 宿舍调换申请

 审批学生宿舍调换申请，查看相关信息。

##### 校外住宿管理

 审批学生校外住宿申请，查看相关信息。

#### 学院用户

##### 学生住宿

 查询本学院学生的住宿信息。

##### 违纪信息查看

 查看本学院学生的违纪信息。

##### 宿舍调换申请

 审批本学院学生宿舍调换申请，查看相关信息。

##### 校外住宿管理

 审批本学院学生校外住宿申请，查看相关信息。

#### 学生处用户

##### 学生住宿

 查询全校学生的住宿信息。

##### 违纪信息查看

 查看全校学生的违纪信息。

##### 宿舍调换申请

 查看全校学生宿舍调换申请及相关信息。

##### 校外住宿管理

 查看全校学生校外住宿及相关信息。

## 健康管理平台

### 健康填报管理（日常填报）

#### 采集信息

学生处开启采集信息批次；可灵活设置本次采集信息的内容、主题名称、采集时间段、学生每天登记时间段、采集对象等。

#### 批次设置

学生处可灵活设置主题批次。

#### 上报情况率统计

查看各学院及各班级总人数、应报人数、实报人数、未报人数、填报百分比、未填报学生填报次数、联系方式等，支持自定义的导出和统计学生信息。

#### 学生填报情况

查看学生填报状态：主题、填报日期、填报情况、学历、院系、年级、学号、手机号、辅导员、当前所在地等；可查看具体某学生基本信息、采集信息情况。

#### 填报学生管理

可调整学生填报状态，查看学生基础信息，支持导入学生信息。

#### 学生情况查看

查看学生填报状态：主题、填报日期、当前所在地、目前所在风险区情况、目前身体健康情况、14天内是否在学校所在地、近14天有无中高风险地区旅居史或居住史、近14天是否有接触过确诊病例、无症状感染者、疑似病例、中高风险地区人员等异常接触史等；可查看具体某学生基本信息、填报情况。

#### 重点关注

可查看各批次重点关注项学生情况。预警情况查询

可查看预警学生信息：学号、姓名、辅导员、学院、连续日期段、预警项、连续天数。

#### 学生情况总览

可查看各学院填报情况。

### 返校监控管理

#### 承诺书管理

学生返校承诺书、学生到校承诺书、教职工及家属返校承诺书、教职工及家属返校信息确认中的显示、教职工及家属返校信息确认不同意返校的显示等。

#### 部门信息管理

可维护参与疫情管理部门的信息。

#### 采集信息设置

学生处开启返校采集信息批次；可灵活设置本次采集信息的内容、主题名称、采集时间段、体温信息展示、异常体温设置、学生日常采集信息展示、学历、学院、年级、学生返校申请状态、核酸检测附件上传等。

#### 学生返校信息确认

业务流程：学生处开启返校批次设置，学生在限定时间内申请返校，辅导员、学院审核学生返校申请，学生处可审批、查看返校学生信息状态。具体可查看学生基本信息、情况采集信息、近14天内体温纪录、近14天内日常采集信息等。

#### 学生返校信息查询

学生处可查询、返校学生状态：学号、姓名、学院、联系电话、返校时间、现居地址、返校住宿地址、返校状态、确认状态、是否撤销等。

#### 学生行程查询

学生处可查看学生形成信息：学号、姓名、学院、形成时间段、交通工具、航班/车次、座位、是否有效等。

### 体温监控管理

#### 体温监控设置

此业务为日常体温监控。学生处可灵活设置主题、填报对象、学生采集范围（已到校、未到校）、启用状态、每次填报次数、每次填报间隔时间、每次填报时间段、其他说明等。

#### 体温情况查询

学生处可查询学生体温填报情况：学号、姓名、辅导员、学院、班级、填报日期、填报状态、体温情况、当日填报次数等。

### 体温填报监控

学生处可监控学生体温填报情况：学院、应报人数、上报次数、体温大于37.3℃人数、填报日期；可具体该学院具体专业、班级、学生填报情况、填报百分比。

### 到校生管理

#### 到校学生管理

学生处可查询到校学生信息：学籍状态、学历、院系、年级、专业、班级、学号、姓名、返校申请状态、在校状态、现居地址、预计到校日期、实际到校日期、进入校门、进校方式等。

#### 到校学生统计

可统计各学院、各班级在籍在校人数、到校人数情况（到校总人数、正常人数、异常人数）、未到校人数、剩余到校人数等。

#### 学生异常上报

可管理异常学生数据：异常类型、上报时间、处理状态，查看具体学生信息。

### 疫苗接种管理

#### 学生填报

学生填报疫苗接种信息，包括：是否接种疫苗、疫苗总剂量、是否接种完成、接种时间、接种地点、接种批次等；可上传疫苗接种附件、凭证；系统支持查询、修改及导入。

#### 教师填报

教师填报疫苗接种信息，包括：是否接种疫苗、疫苗总剂量、是否接种完成、接种时间、接种地点、接种批次等；可上传疫苗接种附件、凭证；系统支持查询、修改及导入。

## 系统管理

### 学院管理

学生处可查看学院信息，可对数据进行新增、修改、删除操作。

### 专业管理

学生处可查看全校专业信息，可对数据进行新增、修改、删除操作。

### 年级管理

学生处可查看年级信息，可进行新增、修改和删除。

### 学期设置

学生处可进行系统学期信息设置，可维护学期的开始时间和结束时间。

### 火车站点维护

学生处可维护火车站点信息，可新增和导入。

### 重置密码

辅导员、学院、学生处可重置权限范围内用户的密码。

### 预制数据管理

可对民族、违纪类型、政治面貌等类型数据进行预制管理。

### 权限管理

根据需要设置不同层级的角色，给角色赋予不同的权限，给用户匹配相应角色权限。学院、学生处具有权限范围内功能管理权限。

### 系统日志

#### 登录日志

学生处可进行登陆日志查询，同时可导出相应的数据。

#### 操作日志

学生处可进行用户操作日志查询，同时可导出相应的数据。

## 数据集成

按学校要求，配合完成本系统与学校数据中心平台的集成：包含单点登录、数据共享、数据同步等。

# 教务管理系统、OA系统、学工一体化系统等硬件需求

## 教务管理系统、OA系统硬件需求

应用服务器 2台

1.CPU：≥1颗，核心≥12核，主频:≥2.1GHz

2.内存：≥128G

3.硬盘：≥4 \* 480GB SSD,

4.缓存：≥2G

5.网卡：≥2\*10GE,≥4\*1GE

6.配置双电源

数据库服务器2台

1.CPU：≥2颗，核心≥24核，主频:≥2.1GHz

2.内存：≥128G

3.硬盘：≥2 \* 480GB SSD,≥4 \* 1.2T SAS

4.缓存：≥2G

5.网卡：≥2\*10GE,≥4\*1GE

6.配置双电源

## 学工一体化平台硬件需求

应用服务器1台

1.CPU：≥2颗，核心≥20核，主频:≥2.3GHz

2.内存：≥128G

3.硬盘：≥4 \* 480GB SSD,

4.缓存：≥2G

5.网卡：≥2\*10GE,≥4\*1GE

6.配置双电源

数据库服务器1台

1.CPU：≥2颗，核心≥24核，主频:≥2.1GHz

2.内存：≥256G

3.硬盘：≥2 \* 480GB SSD,≥4 \* 1.92T SSD

4.缓存：≥2G

5.网卡：≥2\*10GE,≥4\*1GE

6.配置双电源