上海大学大安全智慧协同子系统建设服务项目

采购需求

1. 项目简介

本次项目主要为提升校园安全管理能力，通过整合视频监控、人员通行管理、网络安全等多种安全资源，建设一个智能协同的安全系统。该项目涉及到多个安全技术和设备的集成，应标单位须具有丰富的异构设备安全技术协同管理能力和多业务平台技术集成经验的积累，能够提供高质量的技防视频监控设备集成能力和信息安全管理系统集成能力。可以实现多种安全设备的高效协同，确保校园内所有安全资源能够统一调度和管理。保障系统的长期稳定运行，特别是对于异构设备的协同管理，能够提供全面的解决方案，确保不同品牌、不同类型的设备能够无缝集成。并通过本次大安全平台的建设，可以有机的整合各个子系统所产生的数据。视频融合赋能底座负责技防系统所产生的数据，网络安全综合业务平台负责采集统计分析网络安全数据，数据安放防护系统则负责保护数据库安全，对出现的数据泄漏等问题实现溯源。数据安全大脑则充分利用大数据技术，对数据进行综合分析，从而实现大安全平台的协同和联动。

本次项目预算：459.9 万元，最高限价：370 万元。

2. 建设内容目标

序号	服务名称	服务要求
1	安全应急指挥系统	以立体化、专业化、智能化为方向，全面落实校园安全建设各项工作措施，构建校园全域安全主动预警体系，完善跨部门安全预警联动处置模式，进一步提升校园安全管理水平，打造集安全守护、贴心服务为一体的校园安全新模式。
2	校园安全综合业务平台	手机端功能开发，根据角色赋权使用，如消防科可查看消防设备状态和火灾报警信息，交通科可查看车辆轨迹（文字版）和超速车辆预警信息，辅导员可查看关注学生预警信息；安全管理者可查看学校整体安全状况，可查看闸访人员进校预警和校内轨迹等等。异常行为智能识别和防范，包括聚众斗殴，醉酒滋事，行为不检（拍摄擦边视频，裸露下体等），张贴广告，深夜水边徘徊，高处攀爬、楼顶徘徊，倒地不起，偷拍偷窥，校内钓鱼、偷盗财物、私搭帐篷，校园遛狗，放无人机，落水等等。安全决策支持模块，一键生成安全总况、人员安全、交通安全、消防安全、

		安保管理等决策咨询报告，内容包括基本情况，问题和意见等，如安保管理报告，能提出优化巡逻路线，巡逻区域和巡更点设置，优化监控点位设置等，从而达到资源优化配置、减员增效等管理效果。
3	数据安全大脑平台	通过对数据、应用、API 等进行智能数据采集和自动化梳理，形成数据资产分布、敏感数据资产清单、敏感数据流转视图和数据权责清单，同时实时采集业务动态访问过程中的数据流量，对流量进行智能分析，生成涉敏数据集、涉敏应用集、数据流转视图等，做到对数据全景与流转。
5	数据安全防护系统	基于云原生架构的 API 安全管理、访问控制、动态脱敏、API 接口攻击检测、文件隐式水印于一体的网关系统，并能够基于 API 的敏感数据标签进行 API 的访问策略控制，通过配置脱敏策略可实现涉敏数据的动态脱敏等，保护基于 API 数据大规模泄露的安全事件。功能能够与数据安全平台深度集成，利用 AI 大模型推理能力赋能数据安全平台，包括数据分类分级、风险检测、运营分析等方面。
6	出口带宽服务	提供出口带宽容量不少于 3000M。上下行对称。
7	实施服务及常驻服务	项目执行期间相关软件提供驻场开发不少于 2 名符合要求的开发人员，相关人员需要通过校方面试。提供不少于 36 个月的驻场技术支持服务。

3. 建设内容

3.1 安全应急指挥系统

序号	功能名称	说明
1	应用基础功能模块	基础支撑模块，提供人员信息管理、角色管理、用户管理及应用流程、三维地图应用、报表、规则等引擎
2	应用基础应用引擎	应用引擎模块，提供数据流程引擎、三维地图应用引擎、报表引擎、规则库引擎等
3	全域态势展示安防管控看板	全域态势展示模块，提供安防光控、人车通行分布态势、消防安全设备统计，消控室视频，隐患趋势分析，各设备报警等
4	安全预警体系	安全预警中心模块，提供 "围绕人、车、地、物、事等基本管控要素，聚焦环境区域安全、物品管理安全（如实验室危化品）、设备设施安全、人员行为安全、消防安全隐患等重点维度，基于前端智能感知和中心端智能分析，构建从保卫处拓展至各业务部门、从校园公共区域深入到各重点楼栋的全域安全主动预警中心。安全预警事件包括人工登记类预警事件、智能感知类预警事件和数据分析类预警事件及统计

5	预警联动处置	预警联动处置模块，提供汇聚以上各类预警事件，有机结合地图空间与智感设备，逐级下钻展示不同层级与场景相关的预警情况，及时了解当前场景产生的预警详情（如预警视频预览、预警录像回放、预警关联人或事、预警图片、预警所属场所等）并实施快速处置。支持预警事件实时精准推送，按配置的预警规则通知相关对象，如学生长时间未归寝事件，推送后勤管理处宿管老师、学工处辅导员和保卫处治安科网格员，保卫处可结合全息轨迹寻找该人员踪迹，处理结果实时推送相关部门人员，如此形成跨部门联动机制，实现安全预警业务流程闭环、记录存档和过程追溯。同时，在移动端实现各类预警事件的实时推送功能，支持预警事件的详情查看、流转处置，以及设置为误报或转具体事件处置流程，方便用户随时随地利用手机进行处置。
6	网格展示	网格配置管理模块，提供基于三维地图，按业务划分凸显呈现各个网格区域位置信息，通过地图交互动作展示网格基本信息如网格管理员、网格预警分布、网格事件信息，按照业务属性对网格排行，对于重点网格在地图中高亮凸显，统计及网格化管理视图等
7	预警安消联动	安消一体联动模块，提供预警联动：当发生消防预警事件（如烟雾预警），可通过联动最近的视频监控远程复核， 快速判断警情真伪，同时联动显示一定半径范围内（可自定义设置）消防设施数量和人员数量，关联该区域网格员信息；设备智能联动：出现真实火情时，可联动逃生路线上门禁、电梯、视频等物联设备合理动作，辅助现场快速疏散。
8	线上隐患排查	安全督导防控模块，提供线上隐患排查包括隐患排查配置、巡检执行（移动端）、隐患问题整改（移动端）、隐患问题审核（移动端），问题上报（移动端）等功能。具体流程如下：保卫处提前制定针对业务部门和二级学院安全管理员的安全隐患排查计划，定人定岗按计划执行，巡查过程发现安全隐患及时记录并提交，整改人收到隐患后及时处理，验收人审核验收，实现隐患排查闭环线上管理。巡检台账统计包括隐患问题统计，保卫处用户可以查看业务部门和二级学院在安全督查、部门自查、日常巡检、问题上报四种检查方式下所发现的问题，并对问题在分类、上报来源、状态等维度进行统计。二级部门用户可查看自己部门的问题统计数据。巡检记录查询为业务部门和二级学院用户提供巡检记录查询功能，展示的数据为当前登录用户在日常巡检方式下巡检的记录数据。
9	全域安全风险体系	安全风险评估模块，提供构建学校全域安全风险评价体系，将安全预警分类和数量、处置成效、技防投入、隐患问题分类及数量等纳入指标评价体系，以平安指数的形式表征校园整体安全情况，定期执行校园安全整体评估。同时，基于对全域安全预警事件/隐患问题的种类、数量，以及处置流程与结果、技防建设投入等形成安全评估报告，实现安防建设-预警-处置-评价-安防建设的良性循环。

10	单位消防安全评估	单位消防安全评估模块，提供围绕试点单位楼栋维度，通过建筑防火、消防设施和器材数量、消防相关预警数据和趋势、消防预警处理率等维度，对单位楼栋消防安全进行评估，输出消防评估结果，包括消防安全码、各维度得分和整改意见，定期输出该楼栋消防安全分析报告。
11	三维应用引擎	三维数字驾驶舱模块，提供基于**延长、嘉定校区**校园三维地图，宝山延长嘉定三校区道路建模。提供基础通用的三维模型地图构成、三维动态功能交互、三维动画效果、应用功能框架构建等能力和三维云渲染，并**与宝山校区现有三维数字孪生平台无缝对接。**
12	三维云渲染	▲三维云渲染模块，提供基于后端云渲染和视频串流技术，在后端实现分布式渲染，采用视频串流技术将极致的 3D 渲染画面实时传送给用户，并支持终端用户和后端应用的实时交互，超低延迟的可靠传输及用户免插件即点即用的体验

3.2 校园安全综合业务平台

序号	功能模块	说明
1	统一身份与角色权限管理模块	与上海大学现有统一身份认证对接集成,基于角色-权限模型控制访问，支持多校区、楼栋、部门级粒度权限，提供多因素登录认证和临时授权管理。
2	数据接入与对接模块	对接我校综合安防平台、消控平台、技防多业务平台、公共数据平台，建立实时数据总线实现事件联动，进行数据标准化和安全传输。▲与公共数据平台和企业微信对接
3	消防管理手机端功能	查看消防设备状态、火灾报警信息、接收报警推送、巡检任务提醒与记录上传、调取应急预案。
4	交通管理手机端功能	查看车辆轨迹（文字版）、接收超速、逆行、违停预警、车牌查询、黑名单车辆管理。
5	辅导员手机端功能	▲接收重点关注学生异常行为预警（夜间外出、高危区域）、查看安全历史、快速联系学生或家属。与上海大学学工管理平台对接集成。
6	安全管理者手机端功能	查看校园整体安全态势，接收 AI 异常行为警情推送，查看闹访人员进校预警和校内轨迹，生成安全周报/月报。
7	异常行为智能识别与预警模块	AI 识别聚众斗殴、醉酒滋事、擦边视频、偷拍、高处攀爬、水边徘徊、倒地不起、遛狗、放无人机、盗窃、钓鱼等异常行为，并联动推送到相关部门。
8	交通安全与车辆管理模块	车辆出入登记、轨迹追踪、超速检测、违停抓拍、黑名单车辆布控及校车调度管理。
9	访客与重点人员管理模块	对接访客系统，识别闹访及重点关注人员，实时进校预警，轨迹追踪，临时访客二维码管理。
10	消防安全管理模块	消防设备台账管理，报警联动视频、疏散路线，消防演练管理，

		巡更路线优化。
11	安全决策支持与报告模块	自动生成安全总况报告、人员安全、交通安全、消防安全、安保管理报告，提供问题分析及优化建议。
12	安保管理与巡逻优化模块	巡逻任务管理、排班、任务下发、轨迹记录，AI 推荐巡逻路线、巡更点优化，巡逻完成率统计。
13	综合报警与应急联动模块	整合消防、技防、交通、AI 识别报警，按事件分流到相关部门，支持一键应急响应及闭环管理。
14	视频监控与取证模块	对接监控平台，支持移动端实时查看，报警后自动回溯视频，AI 智能检索人脸、车牌、行为、时间段。
15	跨校区联动与分级管理模块	统一管理宝山、延长、嘉定校区安全数据，支持分校区切换与合并，跨校区应急联动与预案执行。
16	统计分析与大数据研判模块	安全事件按时间、区域、人员、类型统计，趋势分析，安全指数评估，热点区域与安全盲区可视化。
17	系统运维与安全保障模块	日志管理、系统运行状态监控、数据安全与隐私保护、高可用与备份方案，支持断网模式本地运行。
18	AI+安全综合管理集成	▲按照上海大学 AI 大模型应用的标准匹配构建大模型与校园安全综合业务平台的集成，构建对话模式的安全管理应用。供应商需要在本次项目中包含不少于 FP16 （1.9P）的算力，并且完成相关算力在我校的部署，GPU 显存不少于 140G，带宽 4.8TB/S，以便于部署相关的推理模型。

3.3 数据安全大脑平台

序号	功能名称	说明
1	产品形态	采用软硬一体机方式部署，硬件数量不少于 3 节点。
2	单台硬件要求	规格：2U，内存≥8*32GB DDR4 3200，系统盘≥480GB SATA SSD，数据盘≥12*4T，标配盘位数≥12，电源：白金，冗余电源，接口：千兆电口≥4、万兆光口≥2。
3	单台性能要求	日志接入量≥2 亿条/天。
4	数据采集	采用旁路镜像对接流量探针形式获取业务流量，对网络流量内容进行解析，实现动态数据采集。
5		为保障对数据采集的广泛适用性，支持接入数据源类型至少应包含 MySQL，Oracle，SQL Server，Hive，Sybase，PostgreSQL，DB2,GreenPlum，DM，Kingbase。
6		支持连接数据源自动获取并生成数据目录，数据目录以树状结构展示层级关系，包括数据源、数据库。

7	API 资产发现	▲支持流量解析方式来发现 API 资产，分析 API 个数及涉敏 API 个数，通过敏感数据类型关联分析是否涉敏，并通过列表模式展示：API、所属应用、访问用户组、API 名称、请求类型、敏感数据类型、发现时间、最近一次访问时间、是否涉敏、接口状态、日志详情（需提供产品相关功能截图证明）
8	资产管理	为了便于对应用和 API 资产的可视化管理，应提供应用资产管理列表，展示应用的信息，包括名称、HOST、应用地址、访问量等，支持筛选和排序。
9		为了能够快速统计应用和 API 资产情况，应支持统计应用总数、以及涉敏应用数量、失活应用数量、复活应用数量，增量统计近七天或者近 30 天的应用增量、涉敏引用增量、风险应用增量。
10		▲支持以动态数据为中心的应用/API 资产梳理，基于敏感数据类型进行关联分析，数据类型包括但不限于个人信息数据如身份证、电话号码、银行卡、邮件地址、姓名以及客户信息、产品信息等多种类型，支持自定义数据类型，匹配不同业务场景的敏感数据规则（需提供产品相关功能截图证明）
11		支持配置数据源名称，组织架构，数据源类型（MySQL，Oracle，SQL Server，Hive，Sybase，PostgreSQL，DB2,GreenPlum，DM），连接地址，数据源用户名，数据源密码，描述。
12		支持配置数据源扫描任务，可配置扫描范围，排除数据表。
13		支持配置扫描网段，扫描协议，扫描端口，以 NMAP 方式进行扫描，在配置的条件下扫描出数据源信息，支持过滤不同类型的数据源，支持对 IP 地址进行搜索。
14	数据分类分级	为便于用户的不同场景需求，支持新增自定义分类分级模板，支持新增数据类型，可配置数据类型名称、描述、所属分类、关联的字段标签和数据分级。
15		支持修改所属行业信息，可从内置的 8 个行业中选择，也可以自定义填入行业名称。
16		支持编辑字段标签，支持修改名称，描述和配置正则表达式，支持新增字段标签，所有新增标签默认打开 AI 识别且不允许关闭。
17		支持增加或删除数据级别，支持修改数据级别的命名和描述，支持修改敏感数据的阈值。
18		支持数据多层级数据类型定义，并支持以树状结构展示数据分类分级情况，支持五层以上级数据类别定义。数据类型需要支持可添加类别描述。
19		支持对数据库字段列表进行清单梳理，包括字段名称、字段类型、长度、样例数据、字段描述信息、分类分级标签。支持过滤已打标签的字段、待打标签字段、无需打标、待确认推荐打标。
20	数据访问可视	支持展示用户最近一周通过应用访问的方式进行访问敏感数据的情况，直观展示应用被哪些用户访问，用户获取了哪些敏感数据，可下钻看具体某个应用访问情况，可以看到应用的某个 API 被用户访问情况，访问了哪些敏感数据。

21		▲支持将以应用为中心查看访问 IP、访问 API、访问账号的趋势分析图，支持查看该应用包含的 API 资产列表，并且支持下钻 API 资产内包含的参数名称、字段标签、样例数据、样例日志、关联分类等（需提供产品相关功能截图证明）
22		▲为了能对不同数据类型的流动情况进行分析，应支持以数据类型为中心扩展查看用户访问情况及详细访问员工列表，看到组织架构、角色、用户、访问时间等（需提供产品相关功能截图证明）
23		▲为了能够对数据流动情况进行追溯分析，应支持对访问数据类型进行趋势分析并列出 TOP5 用户、TOP5 应用，能够按访问部门、访问角色进行分布可视（需提供产品相关功能截图证明）
24		支持以泡状图直观展示数据资产大类的总量及占比情况，支持下钻查看数据资产大类分布的关联应用、关联 API，支持下钻二级子类型、三级子类型，并且可以逐级查看数据资产在 API 和应用上的分布情况。
25		支持切换数据分布可视的统计维度，如静态数据库表数据和流动数据，支持自定义时间段切换。
26	数据风险监测	支持风险告警，包括风险等级占比统计、风险事件 TOP10、风险主体排行 TOP5 展示；支持选择过滤最近 24 小时、7 天、30 天或自定义指定风险天数；产品具备风险事件的聚合分析，包括支持对不同时间点发生的同一风险事件进行合并，生成高级风险。支持风险列表分析及风险举证包括但不限于：风险主体、主体类型、访问应用、风险、风险等级、处理状态、首次发生时间、最后发生时间、发生次数、查看风险告警详情。
27		▲为了对数据访问行为的异常进行分析，应支持自定义风险规则，选择指定风险等级，设置风险过滤条件，包括：基于应用、API 分组设置访问 API、检测周期、告警条件、排除账号的设置。应支持行为分析能力如去重、稀有度等维度（需提供产品相关功能截图证明）
28		为了对数据访问行为的异常进行分析，产品应具备 UEBA 行为 DNA 分析中枢，支持至少 20+风险探针，结合动态基线学习引擎识别可疑行为，包括但不限于：数据操作异动、业务模式偏离、攻击行为特征、自定义规则。
29		内置多种数据风险模型： 偏离基线规则不少于十条：获取敏感数据量超过历史基线、单个 IP 访问同一涉敏 API 次数超过历史基线、单个账号访问同一涉敏 API 次数超过历史基线、单用户访问同一涉敏 API 次数超过历史基线等； 过量操作规则不少于十条：单个 IP 短时间内访问大量敏感数据、境外 IP 访问大量敏感数据、请求参数遍历等； 权限滥用规则：敏感数据被大量账号突发访问、单 IP 使用多个账号疑似账号泄露、账号共享、垂直越权访问等
30		支持启用、禁用脆弱性规则，并支持编辑脆弱性等级、指定脆弱性识别的应用范围，支持配置指定排除 API 列表。

31		▲为保障数据安全脆弱性监测能力完整可用，脆弱性类型应不低于200条，且应涵盖了OWASP Top 10类型。支持至少10项失效用户身份认证类脆弱性问题，包括鉴权信息在URL中、开发环境涉敏API在公网暴露、凭证长期生效、K8S面板认证绕过等；支持30+授权脆弱性问题，应包含未授权获取密码信息、敏感接口未鉴权、未授权获取明文密码信息等。支持5+安全配置错误脆弱性问题，比如CORS配置不当、ssh secret key信息泄露等（需提供产品相关功能截图证明）
32	运维管理	▲用户可以在页面配置应用的账号提取策略，包含basic场景——业务报文自身直接携带账号，token登录场景——用户使用账号登录，成功之后业务请求携带登录接口返回的token，单点登录业务场景——使用从认证服务器交换得到的业务token访问（需提供产品相关功能截图证明）
33		支持对http报文符合页面对应配置的策略时会在报文中富化出账号相关的字段信息，标识这条流量日志的账号身份。
34		▲支持将同步用户信息关联日志的日志身份富化功能，以便于后续审计和分析，实现在风险日志分析中将风险行为对应到用户（需提供产品相关功能截图证明）
35		支持定义平台个性化内容，比如平台背景图、登录页、简介等。
36	资质要求	所投产品需具备公安部颁发的含有“数据安全平台”字样的《网络安全专用产品安全检测证书》，需提供相关证书复印件。
37		所投产品需具备国家版权局颁发的含有“数据安全平台”字样的《计算机软件著作权登记证书》，需提供相关证书复印件。
38	服务要求	至少提供3年售后服务，包括硬件质保、软件升级、规则库等

3.4 数据安全防护系统

序号	功能名称	说明
1	产品形态	产品采用软硬一体的部署方式，产品功能能够与数据安全平台深度集成，利用AI大模型推理能力赋能数据安全平台，包括数据分类分级、风险检测、运营分析等方面。
2	硬件要求	规格：4U，内存≥16*32GB DDR5 4800，系统盘≥2*480GB SATA SSD，缓存盘：无缓存盘，数据盘≥8*4TB，标配盘位数≥12，电源：白金，2+2冗余电源，显卡≥2*RTX 4090D；显存≥24G；接口：千兆电口≥4、万兆光口≥4。
3	性能要求	支持不少于3亿日志量接入；支持不少于40W字段处理能力；
4	数据分类分级	▲为了对动态数据字段进行识别，支持采用GPT技术自动化进行API名称和用途推理，并对API内的关联数据参数通过GPT进行智能分类分级，应体现GPT完整分类分级推理依据和思考过程，体现明确的数据参数分类与分级结果，可选择应用的分类分级模板（需提供产品相关功能截图证明）

5		为了解决对动态数据所分布的应用资产与 API 资产的识别，应支持通过 GPT 智能进行应用名称和 API 名称识别，在无需人工录入的情况下自动化对 API 和应用进行推理，给出 API 描述和应用名称。
6	异常分析	▲为了提高数据安全分析效率，应支持通过 GPT 机器人开展针对数据类型异常事件的根因分析，通过对话框方式自由输入任意数据类型，GPT 机器人能够自动进行针对数据类型图表开展分析，发现异常图表，并针对异常图标一键点击实现根因分析，分析结论包含载体因素分析、用户因素分析等，并给出推理结论（需提供产品相关功能截图证明）
7	风险监测	▲支持通过 GPT 关联分析和推理举证实现如口令认证类、安全规范类、访问权限类、数据暴露类、接口未授权访问、敏感信息泄漏等类型的 API 脆弱性检测，API 脆弱性模型包括：url 中存在密码信息、响应数据存在密码信息、cookie 中存在密码信息、敏感接口未鉴权、单次访问数据量过大等。应明确具备敏感数据判定维度，作为推理真实风险事件依据（需提供产品相关功能截图证明）
8		为充分保证数据安全事件可运营可解读，应支持告警的下钻事件的解读、触发事件过程详情、GPT 的思考过程、研判结果、历史的事件关联、多报文的举证、基本用户信息、访问资产信息的举证展示。
9		为了提升数据安全事件可运营性，应支持针对业务访问波动导致的告警通过 GPT 进行智能削减，智能消减引擎在覆盖传统规则、统计消减的能力基础上，结合大模型的语义能力，实现对告警的智能消减，界面需明确体现误报、真实告警标签。
10		▲支持基于 GPT 推理大模型对平台规则引擎检出的脆弱性规则告警或 UEBA（用户和实体行为分析）规则告警进行研判，基于上游告警举证信息（包括 API 报文、授权分析、数据识别）与真实客户运营真实数据安全事件的蒸馏知识，对风险进行定性评估、得到真实风险/误报等研判结论（需提供产品相关功能截图证明）
11		▲支持基于 GPT 推理大模型对平台规则引擎检出的脆弱性规则告警或 UEBA 规则告警进行分析，给出解读内容，帮助运营人员提升对数据安全业务理解、降低运营门槛、提升运营效率，包括例如 API 报文解读（基于平台提供的数据报文，对请求报文与响应报文进行数据安全业务分析），保证解读内容与规则的逻辑一致性（需提供产品相关功能截图证明）
12	资质要求	所投产品需具备国家版权局颁发的含有“GPT 数据安全”字样的《计算机软件著作权登记证书》，需提供相关证书复印件。
13	服务要求	至少提供 3 年售后服务，包括硬件质保、软件升级、规则库等

3.5 出口不低于 3000M 带宽服务（补充技术要求）

根据项目采购需求负责安装、部署、调试、测试、上线、优化，供应商负责协同学校相关负责老师完成整个项目的安装实施部署工作；需要提供原厂服

务进行网络的总体设计以及安装调试部署，项目执行期间，原厂服务工程师需要驻场服务。网络部分需要根据学校的管理部门要求进行整体调试优化，与现有校园网络能够有效衔接融合。纳入学校网络的统一管理。

3.6 实施服务及常驻服务

由于本次项目涉及到的功能需求较多，后期项目交付后还有跟多的技术支持工作和二次开发工作需要提供可持续的服务，因此要求中标单位提供36个月的技术支持服务工作。要求项目期间提供不少于2名熟悉java以及信创软件开发的软件开发工程师驻场提供开发服务。

3.7 技术要求

本次招标中的定制开发的业务系统或者在招标要求中的需要用到学生、教师以及其他业务系统数据的平台，该系统将接入上海大学SSO统一身份认证，符合上海大学的主数据管理要求。

3.7.1 对接要求

- 与上海大学企业微信实现对接
- 与上海大学统一身份认证平台实现对接
- 与上海大学公共数据平台实现对接
- 提供开放的接口，允许新业务系统将来与其它系统的对接
- 软件系统部分要具有全信 创 适 配
- 要求支持国密环境

3.7.2 系统性能要求

系统完成后达到以下性能要求：

1.易于理解和使用

没有任何多余的复杂选项，界面友好简单，容易上手，省时高效。

2.系统可拓展性强

考虑到系统将来有功能拓展的可能，对目前功能设计时做好可拓展性预留。

3.良好的性能和速度

做好页面加载及网络设置，保证系统访问时的良好性能和速度。

4.安全性

本项目按照行政事业单位以及高校信息化的安全标准进行建设。

本项目在验收前需要提供学校指定入围机构的信息安全监测报告,安全监测费用包含在项目费用中。

5.注重网络标准

遵循网络标准进行开发，保证系统良好兼容性。

3.8 项目实施的要求

3.8.1 项目管理要求

项目组需由专人担任项目负责人直接对项目中的各项事务负责,需提供《项目实施方案》、《项目实施计划》、《项目跟踪记录》关键性项目节点文件。

3.8.2 项目进度要求

自合同签订之日起 60 天内完成本项目建设内容并通过验收（含 30 天试运行）。

3.8.3 人员培训要求

由供应商为系统操作相关的各部门业务人员提供培训,培训材料由供应商提供。将来校内其他应用系统接入时，需向第三方系统供应商提供对接技术支持。

3.8.4 项目负责人基本要求

项目组负责人具备 10 年以上相关软件研发或实施经验，具有信息系统项目管理师（高级）证书。

3.8.5 项目实施组织基本要求

项目组负责人具备 10 年以上相关软件研发或实施经验。

项目组实施人员不少于 2 人常驻现场，该 2 名团队成员需具备计算机类专业本科或以上学历、且具有 3 年或以上工作经验。

项目开发与实施人员中要求有参与过高校相关业务管理软件开发与实施经验的工程师，并提供简历、社保、参与项目的合同证明。

投标人需具有 ISO/IEC27001 信息安全管理体系认证证书、ISO/IEC20000 信息技术服务管理体系认证证书

3.9 项目质量和服务保障要求

项目验收通过后提供 36 个月的免费质保维护服务。项目完成交付后，项目团队成员中有不少于 1 人常驻业主方现场提供长期技术支持服务工作。

要求建立一套规范的技术支持服务运作系统和流程，服务期内服务响应时间为 1 小时，如需到达现场，则要求在 4 小时内到达现场，1 个工作日内给出解决方案。除现场支持外，还需提供通过电话、网络、邮件等多种通讯手段向用户提供服务。

中标人应详细说明维护期（3 年）满后服务的方式、内容与相应的价格，此费用不计入总价。

3.10 知识产权承诺

供应商应针对以下内容作出以下承诺：

本项目为二次定制开发信息系统，二次开发产生的系统知识产权（包括软件、源程序、数据文件、文档、记录、工作日志、或其它和该合同有关的资料的）归采购人所有，如果供应商向采购人交付使用的信息系统已享有知识产权的（需提供证明文件），采购人可在合同文件明确的范围内自主使用。

提供相关系统源代码及数据库设计文件，提供对应的承诺书，后期验收时需要提供最新相应的代码以及设计文件、第三方测试报告等。