【西安交通大学统一授权与认证中心】采购需求

一、采购标的需实现的功能或者目标，以及为落实政府采购政策需满足的要求：

（一）采购标的需实现的功能或者目标

本项目建设一套稳定、高效、安全、智能、开放兼容的统一授权和认证平台，建设内容主要包括统一认证中心、统一用户中心、统一应用中心、统一接口开放中心等。通过本次项目可以实现对用户、组织架构、账号、认证、应用、权限等进行全面集中式管理。

（二）为落实政府采购政策需满足的要求

1.根据《政府采购促进中小企业发展管理办法》（财库【2020】46 号）规定，本项目采购标的为中小型企业制造、承建或承接的，投标人应提供办法规定的《中小企业声明函》，否则不得享受相关中小企业扶持政策。投标人应对提交的中小企业声明函的真实性负责，提交的中小企业声明函不真实的，应承担相应的法律责任。

本项目采购标的对应的《中小企业划型标准规定》所属行业为：软件和信息技术服务业。

2. □**本采购项目允许进口产品参加。**

（说明：请项目单位根据采购实际情况在“□”中打勾（☑）。未进行勾选的，视为只接受本国产品参加）

二、采购标的需执行的国家相关标准、行业标准、地方标准或者其他标准、规范：

采购项目中所含的投标产品及制造商应符合国家有关部门规定的相应技术、计量、节能、安全和环保法规及标准，如国家有关部门对投标产品或其制造商有强制性规定或要求的，投标产品或其制造商必须符合相应规定或要求，投标人须提供相关证明文件的复印件。

采购项目中所含的投标产品需满足以下标准或规范：

1）《信息安全等级保护管理办法》(公通字[2007]43 号)

2）《信息安全技术-信息系统安全等级保护基本要求》(GB/T 22239—2008)6.1.4 应用安全

3）《西安交通大学网络安全管理办法（暂行）》

4）《西安交通大学统一信息门户与应用系统集成规范》

5）《西安交通大学浏览器兼容性规定（试行）》要求的系统浏览器兼容性

6）《西安交通大学信息化项目应用兼容性要求（2019.6 版）》

7）《西安交通大学信息化项目技术选型要求（2019.6 版）》

三、采购标的概况

（一）采购项目名称：统一授权与认证中心

（二）采购数量及计量单位：1 套

（三）最高限价：150 万元

（四）交付时间：合同签订后 60 天内

（五）交付地点：西安交通大学

（六）付款进度安排：项目验收合格后支付合同金额的 70%，验收合格满 1 年后且无质量问题支付合同金额的 30%

四、采购标的需满足的质量、安全、技术规格、物理特性等要求：

以下标注★的指标为实质性指标，负偏离或不响应为无效投标。标▲项必须提供有效佐证材料。本项目属于交钥匙工程，需要实现本标书的全部功能需求，投标人负责完成所有软件的开发、测试等工作，与其他系统的对接产生的费用等包含在招标总体费用中，采购人将不再另外支付任何与其他系统的对接费用。

（一） 功能需求

1. 统一用户中心

“统一用户中心”作为学校用户管理的核心枢纽，致力于整合全校各类型用户资源，实现用户数据的集中化、标准化管理。它全面涵盖学校人员的基本信息与安全信息，为校内所有应用服务提供统一、精准的用户数据支持。通过开放用户服务接口，该中心将用户管理功能进行统一输出，使各应用系统无需再单独构建用户管理模块，有效避免数据冗余与管理分散问题。其建设内容聚焦人员管理、组织架构管理、身份角色管理、授权管理四大核心板块，通过系统化的管理体系，保障用户数据的一致性、安全性和可用性，为学校数字化建设筑牢用户管理基础。

1.1 用户数据管理

用户数据治理是通过构建统一、规范的管理体系，对校内师生、校友、离退休人员等全域人员身份进行全生命周期管理的过程，通过数据治理实现用户数据的标准化与统一化；支持基本信息、安全信息管理及人员身份类别动态实时转换，并通过 API 接口实现与校内各应用系统的数据共享与交互，打破信息孤岛，为学校业务提供精准、高效的用户数据支撑，提升校园数字化治理水平与服务效能，推动智慧校园建设。

1.1.1 用户数据整合

针对不同源头基础数据进行梳理并整合，支持手动和自动同步。具体要求如下：

(1) ▲要求对校内师生、校友、离退休人员等全域人员身份进行全生命周期管理的过程。

(2) 梳理学校现有各类人员管理方式，确定有源数据的同步机制和更新逻辑，无源数据的维护功能等。

(3) 要求实时获取自动更新人员数据相关信息，自动同步的人员数据不允许人工修改、维护。

(4) 支持多级管理员按照分级权限手工新增用户信息，人员数据入库流程可配置。

(5) 支持单个/批量导入、导出操作，支持提供导入模板，方便历史数据的维护。并支持通过前台新增用户信息，须按照要求进行数据完整性、唯一性、准确性等校验，保证数据的一致性、完整性。

(6) 支持此类用户的新增必须有明确的标记或分类，用以和自动同步的用户进行明确区分。

1.1.2 用户数据标准化治理

人员身份与信息管理的标准化建设，是用户中心实现精准管理的关键。通过对多源头数据进行深度剖析，系统梳理人员身份与信息管理字段的标准化内容。其中，人员身份作为用户核心属性，直接关系到用户身份的精准识别与分类管理；而信息管理字段的设计，则决定了用户中心所涵盖的数据维度与管理范畴。

(1) 制定学校统一的身份管理标准体系，明确人员身份字段，统筹编制字段模型规范。

(2) 人员身份标准化工作梳理，应全面分析学校用户数据，以学生、教职工、校外用户为基

础分类，进一步细化身份类型。学生群体细分为在校生（含本科生、研究生）、交换生等；教职工涵盖在校在编、在校不在编人员；校外用户则包括来访专家、临时访客、运维人员等；同时覆盖校友、离退休人员等特殊群体。

(3) 针对每类身份，系统梳理其对应的数据来源，明确数据同步与维护的范围、权限，确保数据的完整性、准确性与可追溯性，为用户中心的高效运转提供坚实的数据支撑。

(4) 支持人员身份类型扩展、支持用户数据更新规则设置、支持提供身份类型变化规则设置。

(5) 支持包括但不限于以下用户信息，主要包含主身份信息和子身份信息，主身份信息包含用户姓名、唯一 ID、学工号、证件类型、证件号、手机号、邮箱等；子身份信息体现了用户所拥有的不同身份，一个用户可以有多个子身份，每个子身份都有一个组织机构和身份，子身份信息包含用户基本信息、组织机构、身份类型、统一认证账号、账号有效期、账号状态等。支持用户信息字段自定义扩充，包括但不限于基本信息、业务信息、联系信息、身份信息、校园卡信息、其他各类账号信息。

1.1.3 数据管理

支持对存储数据进行日常维护、查询和加工，具体要求如下：

(1) 支持添加、编辑、搜索、查看和删除用户数据等功能。

(2) 支持查看用户信息时，身份证件号码、手机号等敏感隐私信息，默认隐藏部分位数显示，查看时需经过二次验证。

(3) 支持模糊匹配查询。对查询出的人员，展示灵活可配置的关键属性，方便快速确认相关信息。支持高级查询功能，根据复杂筛选条件精确匹配对应的用户。并且支持将当前用户管理筛选列表中筛选出的用户的非敏感信息字段进行导出。

(4) 支持向二级部门提供分级管理功能，提供数据管理维护服务。

(5) 支持向个人提供查询功能，并支持自助纠错。

(6) 支持单个/批量删除某个指定人员。注意删除操作为逻辑删除，不是物理删除。来源于数据自动同步的人员不可被删除。

(7) 对于来源为数据自动同步的用户，不允许进行修改用户从第三方同步过来的数据，只可修改用户通过个人自助中心维护的安全手机号、安全邮箱、紧急联系人、通信地址、家庭地址等信息；对于通过本用户中心新增和导入的用户，除了唯一 ID、人员工号、证件号等确定用户身份的数据不可修改外，其他信息均可修改。

1.1.4 用户数据标准化同步

采集后的用户数据经过标准化后，服务于校内业务应用建设和集成，具体要求如下：

(1) 标准化的用户数据，须为全校各系统提供统一的权威数据源头支撑。

(2) 支持用户数据同步接口，实现数据的实时交互与共享；

(3) 支持查询与管理类接口,满足其对用户数据的调用与管理需求,确保全校数据的一致性、规范性与可用性。

1.2 组织机构管理

组织机构治理是通过构建统一、规范的管理体系，整合多维度组织架构与用户信息，多视角多维度搭建组织架构树，通过数据治理实现用户数据、组织架构的标准化与统一化；并通过接口实现与校内各应用系统的数据共享与交互，打破信息孤岛，为学校业务提供精准、高效的组织架构数据支撑，提升校园数字化治理水平与服务效能，推动智慧校园建设。建设要求包括但不限于如下内容，具体以校方实际要求为准。

1.2.1 组织机构数据整合

针对不同源头基础组织机构数据进行梳理并整合,支持手动和自动同步。具体要求如下:

(1) 梳理学校现有多层的组织机构类型、编码。

(2) 梳理现有组织机构的管理方式，包括新增、合并、撤销等规则。

(3) 要求支持维护多套组织机构信息，实现并行独立管理。

(4) 支持实时获取自动更新有源头组织机构数据，自动同步的机构数据不允许人工修改、维护。

(5) 支持无源头特殊数据的不限层级的多级组织机构模型设计。

(6) 支持多级管理员按照分级权限手工新增组织机构信息。

(7) 支持单个/批量导入、导出操作，支持提供导入模板，方便历史数据的而维护。并支持通过前台新增组织机构信息，须按照要求进行数据完整性、唯一性、准确性等校验，保证数据的一致性、完整性。非行政机构同时支持从权威数据源同步机构信息。

(8) 支持此类机构的新增必须有明确的标记或分类，用以和自动同步的机构进行明确区分。

1.2.2 组织机构数据标准化治理

梳理各类组织机构在学校各业务的使用需求，梳理组织机构的隶属关系，并行维护完善非行政组织架构的数据关系，统一实行标准化治理，形成学校官方权威的组织架构树。具体要求如下：

(1) 支持新增、合并或撤销机构，实现动态更新机制。

(2) 支持记录组织架构变更历史。

(3) 组织树支持按组织机构编码表以及预设的规则定时自动同步。其中，组织树中“一级部门（手动创建）”，如：“教职工、本科生、研究生”等；组织树中“子部门”为各源系统的组织架构（按组织架构编码表导入并清洗），对应校方各业务系统，如“教职工下人事（人事系统）、行政（干部管理系统）、教学（教师平台）、科研，本科生下学院、书院”等。

(4) 支持对组织架构进行管理，须包括新增、编辑、启用/停用部门或子部门等，新增子部门时，系统须支持与数据源对接同步；对于特殊的无源组织机构，支持管理员在前台页面进行增加和管理。

1.2.3 组织架构管理

支持树形结构管理，支持不限层级的多级组织机构模型，支持多层级树状展示，支持动态调整分支节点（如调整层级、新增部门）。

(1) 支持可视化编辑界面，支持通过拖拽调整层级关系。

(2) 支持基于业务关系对人员和机构进行关联，人员可通过导入或者添加的方式分配到不同

机构下的组织机构节点上，用户账号可同时关联多个机构，实现一人多岗位管理。

1.2.4 组织架构标准化同步

支持通过接口向外推送组织机构信息。通过基础能力接口，将组织机构信息实时同步至企业微信等常见第三方软件，确保用户多入口访问智慧校园时的数据一致性。

1.3 统一授权管理

统一授权管理通过搭建集中化的授权管理中心，实现对角色和应用的一体化管控，将业务权限与角色紧密关联，支持为角色分配用户或用户组，构建起权责清晰、体系完备的权限管理架构。用户管理与授权支持多维度操作，既可依据类别、机构、岗位、角色、标签等既定规则进行分类管理，也能根据业务发展动态调整扩展，确保授权体系的灵活性与适应性。同时以多维度、精细化的授权策略，从组织架构的角色、岗位、工作组、人员等层面出发，精准控制用户可信身份对资源、功能、数据的访问与操作权限，在保障系统安全的基础上，提升资源使用效能，为学校各类业务场景提供统一、规范且高效的授权管理服务，赋能校园数字化管理升级。 建设要求包括但不限于如下内容，具体以校方实际要求为准。

1.3.1 用户/用户组管理

支持以组为单位将相同属性的用户归集管理，并提供按用户授权和按组授权的功能，具体要求如下：

(1) 支持以用户为单位实现授权管理，通过用户与角色绑定获得角色赋予的权限，管理员能够为单个/批量用户授予多个应用角色或角色组权限，能够自定义授权有效期。并能查看用户当前授权情况。

(2) 支持将具有相同属性、类别或权限的用户归成同一用户组，进行统一管理、检索和批量授权，方便批量管理具有相似需求的用户。

(3) 支持对用户分组的管理与维护，包括手工创建、维护、删除用户组信息。

(4) 支持手动添加或调用 API 维护用户组人员，并支持手动或者调用 API 地址控制用户组下人员信息的动态变更，用户可以同时存在于多个用户组中。

(5) 支持对单个用户组或多个用户组的批量授权，可根据角色组或应用角色授权，可以自定

义授权有效期，并能查看用户组当前授权情况。

1.3.2 岗位管理

支持岗位管理功能，能够建立岗位、组织机构和人员三元关系，岗位要求带有数据权限的用户组形式存在，该用户组中的用户能够关联组织机构中的其它部门，解决我校一人多岗、双肩挑场景下事务审批、数据权限等常见问题。具体要求如下：

(1) 支持根据业务要求将岗位类型划分成基本岗、通用岗、专用岗；其中基本岗人员由人事系统或数据中心同步。

(2) 支持开放分级管理权限，提供服务页面将岗位人员维护开放至各部门管理人员处维护，通用岗、专用岗可由基本岗或部门管理员设置，可实现快速的岗位下人员调整。

(3) 支持提供岗位预警服务，对于不在本部门的用于提供预警提醒，为行政变动后岗位人员的及时调整提供便利。

1.3.3 角色/角色组管理

支持对接获取业务系统角色，在统一授权中心实现应用角色与用户、用户组的关联，从而实现快速授权，具体要求如下：

(1) 支持角色与用户的关联绑定，实现用户与角色关联的权限之间的关联。支持按角色设置权限，为角色绑定用户或用户组，并可设置角色权限的有效期。

(2) 支持查看应用角色当前授予的用户、用户组范围。

(3) 支持角色组管理，角色组不直接与应用或系统相关联，支持将跨应用的不同角色放入角色组中，以便于统一快速授权。

(4) 授权方式与角色相同，可关联用户或用户组。角色组中的用户会继承组内所有角色具有的权限。

(5) 支持查看用户组当前授予的角色、角色组范围。

1.3.4 授权方式配置

支持提供集中授权能力。集中管理学校所有用户、所有应用的访问入口权限。支持业务

系统与授权对接的配置功能，具体要求如下：

(1) 方便各个业务系统角色数据同步到授权管理中心，由权限中心集中授权和审计管理，可对应用添加、查询、编辑和删除。

(2) 支持多种授权方式。基于角色、用户属性、岗位策略授权机制，实现统一授权。支持应用、功能动态权限管理。应用通过多授权方式实现授权，功能权限实行集中管理；提供精细力度权限进行授权。集中管理应用访问的角色、属性、策略、任务、数据等权限粒度，解决权限冲突问题，有效保障授权的正确性。

1.3.5 分级授权管理

鉴于授权服务支持对全校所有应用的统一授权，随着对接的业务系统不断增加，可对授权服务提供分级管理功能，具体要求如下：

(1) 支持设置分级授权管理员和用户授权管理员,将授权工作分解给各业务负责部门的用户，降低系统相关用户的授权负担，实现授权体系的扁平化管理。

(2) 分级授权应包括对分级授权的人员管理、各人员的授权权限设置和管理权限设置等。

(3) 支持设置分级授权管理员，支持多层级的分级管理，可以将自身具备的权限分配给下级管理人员，各级分级管理员只能管理本人所创建的下级直属管理员。

(4) 支持管理员设置分级授权用户、可修改、替换用户，添加授权，设置权限有效期。

1.3.6 授权管理

支持精细颗粒度授权能力，包括授权时段、访问策略等，具体要求如下：

(1) 针对应用的权限进行授权，支持多维度包括部门、角色、用户组、用户、用户标签等用户关系进行权限分配，支持设置使用时间段。支持设置禁止访问策略。支持黑白名单授权能力。

(2) 支持授权访问策略管理。系统可以根据需求对用户的访问进行多维度的控制，多种访问策略可以组合，以实现不同的访问策略规则。

(3) 支持权限视图查询。支持按照用户、应用、资源维度进行授权组合查询。支持快速查询、

统计用户、应用的权限数据。

(4) 支持临时权限申请。通过流程审批后获得相应应用的临时时间段的申请。

1.3.7 授权服务标准化同步

支持通过接口向外实时共享岗位角色等信息。

2. 统一认证中心

“统一认证中心”作为校园数字身份验证的核心枢纽，深度整合全校各应用场景的认证需求，实现身份认证的集中化与标准化管理。它不仅覆盖传统账号密码登录等基础认证方式，还着重引入二次认证与多因子认证机制，综合运用动态验证码、扫码、生物特征识别（如指纹、人脸）等多样化验证手段，为校内师生及其他人员打造多层级、高安全的身份核验体系，有效规避各系统独立认证导致的重复登录与管理分散问题。通过构建标准化认证接口，该中心将认证功能统一输出，各应用系统无需单独搭建认证模块，显著提升系统间互操作性与用户体验。其建设内容聚焦账号管理、登录方式管理、认证策略配置、多因素认证集成、认证安全管控、应用集成管理、个人自助中心等七大核心板块，以系统化的认证体系，全方位保障用户身份验证的安全性、便捷性与一致性，为学校数字化建设筑牢坚实的身份认证防线。

2.1 账号管理

账号管理以全生命周期管理为核心，构建起从账号创建、激活、多账号关联到状态管控的完整闭环体系。在人员身份、岗位发生变动时，系统自动更新账号状态、权限等信息，实现账号全流程闭环管理；依托自动化策略与消息通知机制，实时监测账号异常行为并即时预警，有效防范安全风险。同时，支持灵活配置账号管理规则，可根据业务场景、人员类别动态调整账号权限、激活流程等设置，显著减少人工干预与管理疏漏，全方位保障账号安全合规，为校园数字化服务筑牢坚实的账号管理防线。建设要求包括但不限于如下内容，具体以校方实际要求为准。

2.1.1 账号信息管理

支持从用户中心实时获取人员基本信息，通过差异视图实现增量数据的自动实时更新，并关联用户账号，具体要求如下：

(1) 支持根据不同业务需求灵活配置同步策略、处理规则和处理频次，创建多样化的账号周期性同步任务，自动实现对账号状态、用户组、角色、角色组、组织机构、身份、有效期等变更操作，从而实现账号数据的自动化同步与处理，保障数据的及时性和准确性。

(2) 支持管理用户账号详情信息，主要包括工号、别名、姓名、性别、身份分类、身份状态、手机号、邮箱号、证件类型、证件号码、组织机构、岗位、专业、班级、入校年份/当前年级等，及密码强度评分、账号状态、激活状态、账号周期等，并支持账号信息批量导入导出。

(3) 支持模糊匹配搜索，对检索出的人员，展示关键属性，方便快速确认信息。并且支持高级查询功能，根据复杂筛选条件精确匹配单个账户。

(4) 支持对账户信息进行添加、修改、删除等批量操作，并提供详细操作日志审计。

(5) 支持账号状态休眠、锁定/解锁、冻结/解冻、注销/激活、变更有效期等账号状态变更批量操作，并提供详细操作日志审计。

(6) 支持把账号信息相关的变更结果通过消息发送到账号下的手机或邮箱。

2.1.2 多账号身份管理

学校用户在校内可能存在多个账号，应对同一用户账号进行关联管理，方便用户访问使用。

(1) ▲支持一人多账号管理，用户名下账号采用同一个密码，每个账号都可以具有不同的组织机构、身份、状态和有效期等属性。当账户信息新增、导入或数据同步时会自动检测，通过身份证/护照作为唯一 ID 能把多个账户自动合并在同一人名下。

(2) 主账号必须绑定手机号，手机号在平台中不同的主账号之间不可重复，作为登录凭据。

(3) 用户在使用非账号/密码（如短信验证码）登录时，可选择某个具体子账号进行登录。用户在使用某个子账号登录时，直接通过本子账号进行登录。

(4) 多个关联账号支持设置某个账号为常用账号，设置为常用账号后，所有的非账号/密码登录均自动登录该帐号。

2.1.3 密码管理

要求提供多种密码管理和设置策略，实现密码安全防护，具体要求如下：

(1) 支持提供关键信息加密策略配置管理能力。具备身份鉴别安全能力，实现口令密文存储、传输，静态口令输入使用特定符号替代，密码框需要安全输入控件，不能被截取密码。

(2) 支持灵活配置默认密码与密码激活两种模式，学校可根据新生、教职工、校外人员等不同群体的使用场景与安全需求，针对性启用对应发放方式，兼顾便捷性与安全性。

(3) 密码安全防护方面应严格遵循国际安全规范，支持国密算法对密码进行加密存储，确保密码以密文形式保存，实现明文密码不可逆转化，从源头杜绝密码泄露风险。

(4) 支持全方位的密码策略配置，包括密码重置功能，用户可通过安全手机、邮箱等多重验证渠道快速重置密码；密码复杂度策略设置，可对密码长度、特殊字符、大小写字母组合等规则进行自定义，强制提升密码强度；弱密码库检测功能，能够实时识别弱密码并禁止使用；支持设定密码有效期，定期强制更新机制，周期性要求用户更换密码，持续提升账号防护水平。

(5) 支持提供密码错误次数限制、异常登录密码锁定等功能，有效抵御暴力破解攻击。

2.1.4 账号激活

提供用户免初始密码自助激活流程服务，为各类用户提供符合需求的激活方式，具体要求如下：

(1) 新用户首次使用时，实现导航式账号激活指引，支持各类人员账号自助激活功能，激活过程包括信息校验、绑定手机号、安全邮箱、设置密码、密码保护问题、补充完善资料、绑定第三方账号联合登陆、绑定学校微信企业号、维护个人电子签名章等环节功能，其中信息校验根据姓名、证件号、工号做一致性校验。

(2) 支持添加排除人群，灵活设置激活操作步骤。

(3) 支持灵活配置是否启用实人认证，即结合公安部等人脸识别接口进行二次校验，承担质保期间相关接口费用；

(4) 支持激活过程中，提醒用户对个人完善信息内容（安全问题、手机号）进行二次确认。

(5) 针对港澳台、海外留学生等无国内身份证信息群体，支持人工审核账号激活服务。

(6) 支持配置用户激活成功后，可以根据不同阶段不同人群跳转指定地址。

(7) ▲支持语言切换。登录激活等个人使用相关界面均支持国际化设置，登录界面及管控中台的菜单、页面显示信息进行中英文切换显示。

(8) ▲支持被冻结账号的自助激活，主要是根据信息通过将证件号、工号、姓名中的至少两个作为激活验证条件，或通过实人认证作为激活验证条件，激活过程支持人工审核，灵活配置激活流程。

2.1.5 账号申诉

用户账号使用问题无法自助解决时，可通过申诉完成信息重置，具体要求包括：

(1) 支持账号申诉功能，申诉类型需覆盖账号解冻、安全手机不可用、安全邮箱不可用、重置密码业务，支持对每日申诉次数做限制。

(2) 支持自动审核“申诉材料”失败后转人工审核，能对申诉材料进行维护，包括联系手机、联系邮箱、最近一次登录终端信息及自定义其他材料。

(3) 支持手动关闭自动审核功能，人工审核时可通过对联系手机、联系邮箱的加密进行隐私保护。

(4) 支持账号申诉配置，包括上传凭证方式、结果通知方式等。

2.2 认证登录管理

认证登录以安全与便捷并重为原则，集成多样化登录方式管理、基础安全基线配置、动态策略控制、密码策略、二次认证及双因子认证等核心功能，构建起全方位、多层次的身份认证防护体系。系统既支持账号密码、动态码、扫码等多样化基础与创新登录方式，适配多终端生物识别技术并打通主流社交平台联合登录，满足用户多元需求；又通过灵活配置多因子与二次认证触发策略，结合弱密码检测、登录频率监测、账号锁定等动态安全策略，对非可信环境、异常登录行为进行实时拦截预警。同时，各项策略可根据用户群体、系统安全等

级自由组合并全局生效，在严格保障身份认证合规性与安全性的前提下，兼顾用户使用体验，为校园全场景业务提供稳定可靠的认证服务支撑。建设要求包括但不限于如下内容，具体以校方实际要求为准。

2.2.1 ▲登录方式配置

支持后续根据学校业务情况灵活调整开放的登录方式，支持由管理员配置用户登录的方式，具体要求如下：

(1) 支持登录界面功能配置，提供对账号、预留手机号、邮箱、证件号+密码等多种登录方式的管理。

(2) 支持管理员灵活配置是否启用其他登录方式，包括手机或者邮箱动态码登录、扫码登录、人脸登录、专属 APP 或微信小程序中一键获取运营商手机号登录；要求在包括但不限于各迭代更新的 iOS 系统、Android 系统、鸿蒙（包括纯血鸿蒙系统），完成指纹认证等所需生物功能的深度开发与集成。

(3) 支持登录端绑定配置，用于管理社交账号联合登录包括微信、QQ、支付宝、企业微信、钉钉等，并提供对接参数配置。

(4) 支持设置登录别名配置。

(5) 支持配置默认认证方式。支持认证方式切换。

(6) 支持登录跳转地址配置，未配置则登录后跳转地址为用户端个人中心。

(7) 支持语言切换。相关界面均支持国际化设置，中英文切换显示。

2.2.2 多因子认证

当用户存在登录访问安全风险时，支持通过双因子方式完成安全登录验证，具体要求如下：

(1) 支持多因子认证方式和触发策略的配置，可对 PC 端与 APP 端不同终端分别配置不同的认证方式和触发策略。

(2) 支持配置自动触发多因子认证策略，包括非可信客户端、非可信网络环境、校外登录、

长期休眠状态等。

(3) 支持启用多因子后设置执行人群或排除人群；若选择执行人群，可设置全部用户或者指定用户组；若选择排除人群，可添加排除用户组，不受多因子影响。

(4) 多因子认证支持排序展示、支持认证方式切换。

(5) 支持用户自行配置可信认证方式，用户通过可信方式登录时，不触发多因子认证策略。

2.2.3 二次认证

在统一认证登录成功后，对于重要业务应用的访问，需要进行二次认证，具体要求如下：

(1) 提供丰富认证源接入能力，支持按照不同系统、不同安全级别、不同使用终端等多维度，便捷灵活配置可启用的认证方式及使用顺序，提供灵活二次认证功能。

(2) 支持对指定应用或系统开启二次认证（即再认证一次），支持配置二次认证的方式与触发策略。

(3) 支持配置必选校验应用，访问此列表应用时，用户必须完成二次认证。

(4) 支持配置可选校验应用，访问此列表应用时，用户可在个人中心配置是否需二次认证。

(5) 支持启用二次认证后设置排除人群，添加的用户组成员不受二次认证配置影响。

(6) 支持二次认证方式排序展示。

2.2.4 安全策略配置

提供终端配置、验证码策略、账号锁定策略等安全策略配置功能，保障认证登录安全，具体要求如下：

(1) 支持登录终端灵活配置，用于配置是否允许用户在不同终端登录，管理员可强制用户配置单处登录，也支持让用户自主配置，并支持强制退出；支持会话配置。

(2) 支持验证码策略配置，用于配置用户输入密码错误一定次数后，出现验证码。

(3) 支持提供账号锁定设置功能，认证密码输入错误超过“账号锁定阈值”的情况下锁定账号。

(4) 支持提供登录频率检测和配置，对于同一账号或 IP 在短时间内尝试连续登录的次数做出限定,超过登录阈值则系统留有异常警示登录日志,根据警示记录选择自动锁定账号。

(5) 支持个人中心校验，用于配置个人中心绑定、解绑重要信息时校验方式与顺序，校验方式包括：邮箱、账号密码，默认为账号密码且不可取消。

(6) 支持实名认证配置。依赖人脸识别技术，对用户进行自然人真实身份校验服务。可用于重要场景下的身份校验，如账号激活、找回密码、账号申诉等。

2.2.5 密码策略设置

提供完善的密码管理策略，管理员可定期更换修改策略，强制用户修改密码等，确保用户密码安全，具体要求如下：

(1) 支持登录认证时要求自动进行弱密码检测。

(2) 支持修改密码配置，包括常用设备登录校内 APP 中修改密码免校验和定期修改密码。

(3) 支持配置密码有效期、密码使用时间。

(4) 支持使用账号/密码登录认证时具有密码可见功能，密码即将到期时能够提醒用户。

(5) 支持对弱密码检测规则的配置，可配置检测规则包括密码安全分数、密码策略、密码有效期、密码使用时间以及是否弱密码库的密码。

(6) 支持密码规则的配置，包括新旧密码允许重复的间隔次数、密码长度、密码组合规则、密码有效期，能够在密码即将到达失效期的时候发出提醒。

(7) 支持统计弱密码账号数量及配置统计规则。

(8) 系统会根据密码复杂程度自动计算密码强度得分，低于密码得分「可配置」为弱密码，可限制字符种类数量或指定字符种类，根据密码长度+密码涉及的字符组成弱中强的密码规则。

(9) 支持配置密码黑名单，限制用户设置密码时包含的字符内容。可配置：用户账号、用户邮箱、用户手机号、居民身份证号码、自定义字符。其中自定义字符，支持手工新增和批量导入。支持添加自定义黑名单字符，如 sysadmin，同时系统提供黑名单字典，供

用户参考使用。

(10)不符合密码策略时，下次登录使用可支持配置用户是否需要强制修改密码。

(11)密码未达标账号列表，展示包括账号、姓名、上次修改密码时间、未达标原因、操作（支持冻结账号）、导出列表。

(12)支持用户自助找回密码，可根据提供证件号码、姓名简单验证。或者是通过安全手机或者安全邮箱通过获取验证码方式、回答密码保护问题等辅助验证。

2.2.6 异常行为检测

提供用户异常行为检测，主动防护避免疑似恶意访问或攻击，具体要求如下：

(1) 支持基于配置的安全策略，实时检测异常登录行为（如过频登录、跨域地址跳跃、陌生设备/IP 登录）。

(2) 支持对异常行为自动执行相应的操作（如触发多因子认证、账号锁定、冻结、账号下线等），并支持对异常操作结果进行管理操作（如查看详情、解除锁定）。

(3) 支持筛选异常行为查询与管理，支持按照时间、账号信息、异常类型等多维度查询异常记录，包括异常会话、异常登录账号、异常登录 IP、休眠账号、冻结管理。

(4) 支持统计恶意登录账号数量及配置统计规则，包括账号、姓名、登录成功次/天、登录失败次/天、并支持批量操作（冻结、锁定等）。

(5) 支持休眠账号设置。长时间未登录自动锁定开关、未登陆天数设定、长时间未登陆白名单。以及支持认证会话管理策略配置。提供会话管理策略，配置应用级会话管理策略。查询现有系统的会话，并可以强制结束会话，踢用户下线，用户下线后，系统可以直接退出系统，不能再进行任何操作。支持统计并导出长时间不登录休眠账号数量及配置统计规则。

(6) 支持配置冻结异常登录 IP 规则、查询已冻结的账户列表，包括账号/IP 地址、类型、冻结时间、预计解冻时间、冻结原因，并支持批量操作（解冻、添加到白名单）

(7) 支持统计（长时间未使用）异常账号及配置统计规则。

2.3 移动端对接集成

深度聚焦移动端应用生态，全面支持多样化身份认证方式，涵盖动态短信验证码、生物识别（指纹、人脸）、手势密码、第三方应用授权登录等，为用户带来便捷、安全的身份核验体验。通过身份漫游技术，无需重复输入账号密码，一次认证即可无缝访问所有授权应用，实现多端操作的一致性与连贯性。依托数据互通机制，各平台间的用户权限、组织架构、角色信息等数据实时同步更新，确保信息的准确性与时效性，全面赋能智慧校园移动化建设。建设要求包括但不限于如下内容，具体以校方实际要求为准。

2.3.1 移动端 APP 对接

统一认证中心要求与学校现有移动 APP 对接，具体要求如下：

(1) 支持必要的数据接口供移动端 APP 调用实现多种登录方式：账号/密码登录、短信验证码登录、本机号码一键登录（支持 3 大运营商）、设备生物识别、人脸登录、第三方联合账号登录。

(2) 需提供接口实现第三方应用（H5 页面）在移动端 APP 内免登。

2.3.2 企业微信等第三方平台对接

统一认证中心要求与学校现有企业微信等第三方平台对接，具体要求如下：

(1) 支持通讯录数据自动同步功能，支持全量同步和增量同步。

(2) 支持用户微信与企业微信绑定的功能。

(3) 实现现有已绑定人员的数据平滑迁移，无需重复绑定即可使用。

(4) 支持接口实现第三方应用（H5 页面）在企业微信等第三方平台免登。

2.4 个人自助中心

以用户需求为导向，打造 PC 端与移动端双平台一体化自助服务体系，中心提供多语言支持，满足师生及访客多样化使用场景。灵活调整账号安全策略，如设置登录设备管理、多因子认证偏好等，全面掌控账号安全。用户可一站式查询各类操作记录，异常登录行为将自动高亮预警，支持可视化呈现账号使用动态，帮助用户快速了解近期安全状态，助力及时发

现潜在风险。深度适配学校门户集成需求，无缝对接校内业务系统，实现单点登录与数据互通，为用户构建安全、自主、高效的个人账号管理空间。建设要求包括但不限于如下内容，具体以校方实际要求为准。

2.4.1 账号个人信息

提供个人账号信息的查看与管理功能，具体要求如下：

(1) 支持查看账号个人信息，查看信息包括姓名、工号、所属单位、账户名、身份、所属机构、失效期、账号周期信息等。能够列出与其关联账号，支持变更或设置常用登录账号。

(2) 支持设置别名，用作登陆账号。

(3) 支持绑定安全手机号或者安全邮箱的功能，当绑定新账户时，会自动默认此手机号/邮箱作为最后一个用户的安全手机/安全邮箱，并提醒先前用户的安全手机/安全邮箱自动失效，无需后台人工操作。

(4) 支持“修改安全手机”、“修改安全邮箱”和“修改密码”时需要额外身份验证功能。

(5) 支持对有问题的信息进行反馈（信息错误、应用访问等问题）。

2.4.2 账号登录服务

为全校用户提供统一登录服务，支持多种快速登录方式，具体要求如下：

(1) 支持多种主流的登录方式，包括账号密码登录，动态验证码登录、第三方账号联合登录、扫码登陆等。

(2) 支持自行配置账号、工号、证件号、手机号码、邮箱、别名等作为账号登录。

(3) 支持一人多账号，每个账号对应不同的身份、状态和有效期等属性，满足不同身份登录系统的使用场景。

(4) 支持语言切换。平台登录、激活等个人使用界面均支持国际化设置，登录界面及管控中台的菜单、页面显示信息进行中英文切换显示。

(5) 支持绑定可信常用设备，如手机、电脑，后续在已绑定设备登录时简化核验流程；若在陌生设备登录，则触发额外验证，如二次身份确认或设备认证，平衡安全与便捷性。

2.4.3 密码重置

支持用户自助重置密码，可根据提供证件号码、姓名简单验证。也可通过以下方式辅助验证，包括安全手机或者安全邮箱通过获取验证码方式验证、或者通过密码保护问题进行辅助身份验证。

2.4.4 ▲账号委托授权

授权业务应用给第三者使用， 指定他人代替自己使用某应用，可设置访问有效期设置、访问提醒设置。同时提供访问授权操作日志记录、代为处理日志等日志。

2.4.5 个人账号使用分析报告

针对用户个人账号安全、账号使用等信息提供个人账号使用分析报告，具体要求如下：

(1) 支持用户实时查询自身账号的风险评估报告。

(2) 报告内容需包含各维度风险评分、整体风险等级及具体异常项说明。

(3) 支持报告详情展开/折叠，用户可逐项查看风险原因及改进建议。

2.4.6 账号使用过程记录

支持记录用户账号使用记录，方便用户追溯，具体要求如下：

(1) 支持用户查询个人登录日志数据，包括登录时间、登录 IP 地址、参考地点和所使用的设备信息。

(2) 支持用户查询个人基于认证系统的操作修改日志，包括账号信息、密码修改记录、操作时间、操作内容、操作 IP 地址和设备信息等。

(3) 支持用户查询使用过的终端设备清单，包括设备 ID、设备信息、设备类型、首次登录时间、最近登录时间、使用次数等，并且支持用户屏蔽并下线不可信的终端 ID。

(4) 支持查看有权限登录的系统列表。

2.5 身份核验管理

深度融合多项核心技术，构建功能完备、安全可靠的多维度能力矩阵，全面覆盖校园各

类身份核验场景，打造更智能、安全的校园身份核验体系，具体要求如下：

(1) 支持基于生物识别技术，支撑身份核验。通过眨眼、摇头等动作检测，判断操作者是否为真人，防止照片、视频等伪造攻击，常用于远程身份核验场景。

(2) ▲支持依托第三方数据，支撑身份核验。与公安系统、教育部学籍学历数据库、运营商实名信息库等权威平台对接，实时核验用户身份信息，确保数据真实可靠。并承担质保期间学校此类相关接口的所有费用。

(3) 支持围绕人脸识别技术，支撑身份核验。支持按姓名、学号、证件号等多字段快速检索，提供人工审核、批量导入导出功能，兼容多种图片格式，确保数据管理灵活高效；支持统一配置、批量处理及个性化定制多维度证照管理，满足不同场景下的身份核验需求。采用先进加密算法与脱敏处理技术，将人脸照片加密存储并分散保存，从源头杜绝数据泄露风险；集成以图搜图、智能审核功能，实现异常照片快速定位与处理。支持多类型人脸识别算法并行运行，通过算法质量评估与动态优化机制，保障识别准确率与稳定性；具备照片溯源追踪能力，一旦发生数据异常，可快速定位泄露源头，所有核心技术均配备权威认证文件，确保合规可信。

(4) 支持围绕校园二维码技术，支撑身份核验。支持用户信息自动同步推送与手工维护双模式，无缝对接教务、人事等第三方系统，灵活实现数据新增、查询与更新。二维码模板管理支持自定义配置携带信息，如身份标识、权限范围等，可快速生成、调整或删除模板，适配不同业务场景需求。支持第三方应用根据开放标准接口快速接入，提供安全可靠的申码、解码服务，通过密钥分配与权限管理保障数据传输安全，并配备测试功能与完整日志记录，便于调试与审计追溯。运维监控模块实时记录在线用户状态、异常强退事件，提供操作日志查询功能，同时对服务资源使用情况进行动态监测，确保系统稳定运行。

2.6 风险审计中心

提供日志管理、统计分析、风险管理及审计管理功能，实现智能化风险管控，建设内容包括但不限于以下内容，具体以学校实际要求为准。

2.6.1 日志管理

支持平台所有人所有权限、所有操作都需要有详细规范的记录日志，具体要求如下：

(1) 支持多级授权查看管理。系统管理员可查看所有系统中的所有日志，普通管理员只能查看自己的操作日志，日志的查看以列表形式展示。其中管理员日志是指所有管理员在系统中（包含系统管理、用户管理、接口管理、权限管理、组织机构管理等）的所有操作日志；接口调用日志是指系统对外授权的接口访问日志，包含接口被调用的次数、返回数据等。

(2) 支持提供登录日志的记录查询和在线记录的查看，存储登录结果及异常登录的 IP，能查询并导出账号的在线时长。

(3) 支持用户登录及应用访问的操作日志查询与导出。

2.6.2 统计分析

解决用户数据外流、权限混乱等安全风险，通过建设数据安全审计、权限审计、信息完善配置及评估监测用户授权分析等功能，实现从用户管理到权限操作的全流程风险可控，有效防范内部误操作导致的安全风险。数据统计分析模块包含用户基本信息统计、接口信息统计、登陆统计、授权统计等。建设要求包括但不限于如下内容，具体以校方实际要求为准。

2.6.2.1 用户统计分析

提供用户信息统计，包括用户数据概览、组织机构、及特定人群统计，具体要求如下：

(1) 基本信息统计是指按基本信息、用户类别信息、组织机构、组织树、部门人数、总人数等信息统计系统中各类人员信息，同时也包含各类权限信息统计等。

(2) 支持按时间段进行统计，统计结果可按照表格、曲线图、饼图等多种方式进行展示。

(3) 支持用户数据概览，包括总人数、无账号人数、男/女性人数及占比、总账号数、任意三类身份账号数及各自占比、年度新增账号数和新增人数。

(4) 支持图形化展示账号状态、激活状态、锁定状态、组织机构、身份、失效期等六个指标维度的分布情况，能够呈现账号明细并支持下载。

(5) 支持对于特定人群（如新生）的激活状态统计。

2.6.2.2 授权统计分析

提供应用授权、角色授权等信息的统计分析，具体要求如下：

(1) 支持统计已授权角色数、未授权角色数、已授权账号数、未授权账号数。

(2) 支持按照业务或应用系统统计授权的角色数和未授权的角色数。

(3) 支持按角色/所属业务域/所属应用系统，统计各维度下已授权账号数量。按应用系统/所属业务域统计各维度近 30 天内每天的账号授权变更次数。按角色/用户，统计各维度下账号授权变更次数。列表形式呈现明细数据并支持导出。

(4) 支持在线浏览授权统计分析报告，可以将授权统计分析内容下载到本地。

2.6.2.3 登录统计分析

提供登录分析概览、各终端登录、各身份登录等信息的统计分析及趋势，具体要求如下：

(1) 提供身份认证数据分析看板，包括认证登录分析、应用认证分析、使用用户分析、账号变动分析，帮助用户发现认证使用价值及使用中的问题。

(2) 支持统计当天登陆人数、当前用户上线率、登录成功率、当前在线人数和在线率、当天 PC 端和 APP 端登录人数以及近三天异常登录人数。支持以 PDF 格式生成认证统计分析报告。

(3) 支持统计用户正常登录情况，以曲线图对趋势进行统计，包括日环比、周同比的对比统计，统计维度支持按账号、次数。以环形图或柱形图分终端、组织机构、身份类型统计占比情况，包括日环比、周同比的对比统计，统计维度需按账号、次数分别展示。

(4) 支持通过趋势统计呈现历史登录异常人数在不同时间范围内的数据波动，通过占比统计从终端类型、异常类型两个维度呈现历史登录异常人数占比分布。

(5) 支持按账号或访问次数通过柱状图呈现应用访问统计，维度分终端类型与组织机构统计。

(6) 支持所有的系统操作统计，包含管理员操作统计（如人员管理、授权等）、以及登录系统统计等，支持按时间段进行统计。

2.6.2.4 接口调用统计

支持统计接口被调用的次数分布以及接口异常调用、失败调用（含非法用户、非法 IP 等）等统计。

2.6.3 风险管理

建设统一的风险建模、识别、处置管理中心。建设要求包括但不限于如下内容，具体以校方实际要求为准。

(1) 支持建设全维度风险评估体系。通过用户行为、访问设备、访问环境、访问时间、访问威胁情报、访问异常信息，建立用户可信等级，进行分权安全访问。

(2) 支持风险事前检测。提供常规风险检测服务，包括多行为类型、多维度的风险检测，提供实时风险检测接口、非侵入式的实时离线检测风险服务。

(3) 支持多种风险评级方式，不同检测点，可设定不同的评分方式。支持风险检测模型扩展，不断更新检测方法。

(4) 支持千人千面的识别模型。基于用户数据实现用户画像，支持基于画像的风险识别机制，具备自动学习、管理用户特征的能力。

(5) 支持动态为不同用户群体关联不同风险检测策略。实时在线分析用户多维度异常行为，对异常进行监控、预警，实现事前风险识别；通过用户行为特征、习惯等进行身份鉴别，根据鉴别结果进行认证、权限访问等风险处置；匹配每个用户的行为形成每个用户的行为画像，智能匹配安全风险规则，建立千人千面的风险安全防范体系。

(6) 支持提供完备的风险处置能力。针对不同级别的风险，提供自动风险处置能力，可人工干预相关风险处置结果。

(7) 支持提供多视角风险报表能力。提供用户风险分析报表、认证记录分析报表、历史风险分析报告能力。实现基于用户、角色、身份、权限的风险分析报表，支持导出到 pdf 格式。

(8) 支持提供风险大屏。提供用户全维度身份访问情况、异常情况、访问高峰分布等信息，提供识别的风险展示。

(9) 支持建立用户密码风险中心。以密码特征库维度，对用户密码进行评分，密码不应为弱密码库中列举的密码，提高密码的安全杜、复杂度。

(10) 支持建立用户安全风险评分机制。针对用户的安全设置、认证方式、访问风险、用户行为等进行分析，得出用户安全评分，提出改进建议。

(11) 支持建立认证安全风险评估中心。提供安全策略设置、审核功能,对于异常频繁登录的用户、IP 可实现冻结功能、踢用户下线等操作。异常频繁登录用户特征、频繁登录 IP 特征、异常会话特征可进行相关策略设定。

2.6.4 审计管理

审计是系统安全防范措施不可缺少的功能，建立全面、有效的回溯、准差机制，实时检测用户对应用的访问情况、系统运行状态进行追踪。建设要求包括但不限于如下内容，具体以校方实际要求为准。

(1) 支持审计用户敏感数据的分级分类是否符合国家安全要求，是否加密、脱敏。

(2) 支持账号审计功能。支持对近 3 个月从未登录过、锁定账号、未分配角色或工作组的账号进行审计，可以一键查询、导出等操作。

(3) 支持权限合规审计。定期基于最小化权限原则进行合规检查。

(4) 权限合规策略实现用户属性与应用访问权限、账号权限分配关系等。权限合规策略属于正向授权动作，权限互斥是反向的、事后审计策略。支持根据角色和角色组名称查询授撤权的情况，可区分手动和自动的操作类型，方便对角色的授权撤权记录进行准确的审查追溯。

(5) 支持授权统计。对授权结果进行监控和统计，包括当前授权接入的应用数、角色数、用户数，未授权的角色数、应用数、用户数，应用授权情况、角色授权情况、进期的授权操作信息等信息。支持权限溯源。授权历史、授权时间、取消授权等信息记录过程，重要权限提供审核后赋权。

(6) 支持个人认证全量分析报告，统计、分析系统用户个人行为，形成分析报告，支持前台用户自行下载。

(7) 支持提供用户行为分析，实现用户画像、应用画像，实现知识图谱，进行关联分析。用户画像包括用户身份特征、认证特征、访问应用最频繁、访问应用时间段等特征。

(8) 支持提供全量日志审计管理。提供管理员日志、用户认证日志、用户应用日志、用户操作日志等日志查询、导出功能。管理员日志提供管理员登录客户端类型、登录时间、操作类型、登录账号、失败原因、客户端地址等信息；用户认证日志包括工号、姓名、认证方式、证件、认证时间、认证 ip、备注等细腻；用户应用日志信息包括用户登录应用、登出应用时间、设备、访问客户端地址等信息；用户操作日志信息包括操作人工号、操作人姓名操作日志、操作类型、操作模块、操作摘要、操作方式、访问客户端地址等信息。

(9) 支持提供风险行为审计。依赖规则引擎，内置风险规则，实时风险检测、预警、处置。异地登录、异常事件登录等风险发现后，可以通过邮件、短信、微信消息进行用户预警。访问场景信息包括访问时间、访问账户、访问行为、访问关系、访问习惯、访问位置等信息。

(10) 支持提供审计统计。提供审计各类统计汇总信息，包括用户、账号、应用、服务、认证、访问、授权、风险等多维度信息。提供异常行为实时检测与自动处置、多维认证统计分析、全量日志审计及账号风险画像，通过自动化规则引擎、实时监控与权限管控，实现风险识别、审计分析、安全处置闭环。

3. 统一应用中心

作为校内服务应用的管控备案中心，需构建完善的应用管理体系，实现应用的接入到废弃全周期管理，包括增加、排序、编辑、查询、导出、生成报告、启停应用、统计等功能。在功能层面，为校内应用提供应用注册、信息维护、授权使用等核心服务；在应用集成方面，支持 CAS、SAML2、Oauth2 等多种认证接入协议，满足不同应用的对接需求。同时，提供精细化的应用访问授权配置功能，管理人员可依据指定人员、时段、网段等条件，灵活设置访问权限，实现对应用访问的精准管控，便于管理人员在应用上线时集中配置各项关联能力，达成“一处授权，各处畅通”的高效管理目标，确保校内应用的有序运行与便捷使用。建设要求包括但不限于如下内容，具体以校方实际要求为准。

3.1 应用管理

3.1.1 应用基本信息管理

构建全量应用标准化档案库，支持智能分析与动态扩展，具体要求如下：

(1) 应用基础属性字段应至少包括应用名称、接入状态、业务域、适用终端、有效期、开发商信息，字段校验规则以学校要求为准。

(2) 扩展属性管理：支持自定义字段类型，字段可设置为“必填”或“可选”；提供字段级权限控制。

(3) 支持多维度统计：按业务域、部门、终端类型生成实时统计图表，支持数据下钻至单应用详情。提供交叉分析功能。

(4) 支持自动生成应用使用报告：支持按日/周/月/年周期生成报告，内容包含应用名称、管理部门、调用总量、平均响应时间、异常率。

(5) 导出与分享：支持 PDF/Word/Excel 格式导出，分享时需二次身份验证。

3.1.2 权限管理

构建精细化权限体系，实现多角色、多层级协同管理，角色定义与权限配置具体要求如下：

(1) 超级管理员：具备全局权限，包括业务域管理、资源目录分配、参数策略配置、系统级审计及平台数据备份/恢复功能；支持配置部门管理员与应用管理员的权限边界。

(2) 部门管理员：按部门维度管理所属应用信息，包括应用注册审核、属性维护、资源授权审批；可查看本部门应用统计报表，无权跨部门操作。

(3) 应用管理员：业务部门管理员负责应用基本信息维护、资源服务申请、使用报告生成与导出。技术部门管理员负责技术参数配置、接口权限管理、生命周期状态监控。支持权限回收的级联操作。

3.2 应用生命周期管理

覆盖应用注册、维护、停用全流程，支持自动化审批与策略联动。具体要求如下：

(1) 应用注册支持由管理员直接创建并录入应用信息，支持批量导入，导入时自动去重并校验格式。

(2) 支持开发者或部门管理员在线提交申请注册，并填写应用名称、业务域、责任人、用途说明等信息；

(3) 应用注册审批流程支持多级审批，审批意见需记录并通知申请人。

(4) 支持管理员修改维护应用信息，系统应具备各级管理员修改的不同权限。

(5) 自动记录每次修改的版本号，支持查看历史版本差异。

(6) 支持应用停用与清理，支持自动停用：有效期到期前 30 天发送预警通知，到期后自动停用并禁止 API 调用。

(7) 支持手动停用：需填写停用原因，停用操作需记录审计日志。

(8) 数据清理支持配置数据保留策略，清理时需二次确认。

(9) 清理过程生成操作日志，包括删除的数据量、关联文件列表。

3.3 操作日志管理

实现操作日志的审计管理，具体要求如下：

(1) 日志记录范围：覆盖权限变更、应用属性修改、资源申请审批、密钥刷新等所有管理操作。

(2) 日志查询功能：支持按操作类型（增/删/改）、操作人、时间范围（精确到秒）、IP 地址多维度筛选。提供操作详情查看，包括修改前后的字段对比。

(3) 审计合规性：日志存储周期≥3 年，提供标准化日志接口。

3.4 信息化资源管理

实现资源服务的统一申请、授权与监控，具体要求如下：

(1) 提供资源服务的管理、维护功能，包括基础信息、描述，启用、停用资源服务，设置资源服务相关的首页地址、对接文档地址、接口文档地址，配置资源服务的对接配置参数

等。核心服务及扩展服务的服务能力由三方应用提供。

(2) 在线申请流程：开发者选择目标服务（如成绩查询 API），填写用途说明并关联应用。

(3) 审批自动化：支持按服务类型配置审批规则（如消息推送需部门管理员审批，API 调用需技术管理员审批）。审批通过后，系统自动分配资源权限（如 API 密钥）并通知申请人。

(4) 提供实时监控看板：展示各服务调用量、成功率、响应时间，支持按应用/服务类型筛选。

(5) 提供异常告警功能（如 API 调用失败率≥10%触发短信通知）。

(6) 支持配额管理，特定应用支持按应用配置每日/月度调用限额，超限时自动阻断并生成违规报告。提供临时配额调整功能，需管理员审批并记录操作日志。

3.5 应用治理

实现应用资产全生命周期管理、容器化应用管理平台与开放 API 服务生态建设，具体要求如下：

(1) 建设校级统一应用资产库，支持新建系统以及对接原统一身份认证平台、消息中心、数据交换平台等系统，采集应用系统名称、开发厂商、接口类型等基础信息。

(2) 建立三级分类管理体系，按业务域、安全等级、服务类型等多维度进行分类标识，支持自定义标签扩展功能。

(3) 构建应用全生命周期看板，实现从立项评审、开发测试、上线运行到下线退役的全流程可视化跟踪。

(4) 构建符合 OpenAPI 3.0 规范的接口管理平台，要求支持可视化文档生成、在线调试沙箱环境，提供 API 版本管理、流量监控、熔断降级等治理功能。

(5) 建立 API 全生命周期管理机制，包含接口注册审核、服务编排、调用鉴权、服务质量监控等模块，日均承载十万级 API 调用请求。

(6) 集成 SDK 生成、在线文档查阅、要求支持第三方开发者自助式服务接入，提供 OpenAPI

合规性检测工具。

(7) 搭建基于 Kubernetes 的容器云平台，支持多集群管理、自动弹性伸缩、要求单集群支撑 50+节点规模。

(8) 支持第三方应用容器化交付部署，包含 Docker 镜像构建、Helm Chart 打包，兼容主流技术栈。

(9) 实现容器级资源监控，具备 CPU/内存使用率热力图展示、日志聚合分析、安全漏洞扫描等功能，支持国产化芯片适配。

3.6 系统管理

3.6.1 业务域管理

根据应用类型划分业务域，便于为管理人员按域授权，实现业务权限独立管理。

(1) 支持业务域树形结构创建，节点支持拖拽排序与层级调整。

(2) 提供业务域与部门管理功能（如“教务处”关联“教务管理”域）。

(3) 业务域管理员仅能管理所属域的应用，无权查看其他域数据。

3.6.2 文档中心

(1) 支持 html 等格式的文档发布，支持代码块、流程图、表格等元素。

(2) 提供文档版本控制，支持差异对比与历史版本恢复。

(3) 按角色分配文档访问权限（如开发者仅可查看 API 文档，管理员可见审核指南）。

3.7 应用监控

3.7.1 应用接入分析

提供应用接入的统计分析及增长分析等，具体要求如下：

(1) 统计维度支持按部门、业务域、服务类型统计应用接入数量及环比增长率。

(2) 支持导出原始数据及可视化图表。

3.7.2 资源使用分析

提供应用对接口等资源的使用情况分析，具体要求如下：

(1) 服务 TOP 榜：提供服务 API 调用量排名榜。

(2) 针对异常调用关联日志生成分析报告（如“服务器负载过高”）。

3.7.3 无侵入式健康监测

实现对应用的无侵入式健康监测，具体要求如下：

(1) 监测配置：支持通过 URL 配置第三方系统健康检查端点（如/health），无需嵌入 SDK 或修改代码。

(2) 检查频率可配置（默认 5 分钟/次），支持 HTTP/HTTPS 协议及自定义请求头。

(3) 监控指标展示：服务可用率、网络层指标、安全指标

4. 统一接口开放中心

4.1 接口规范与标准化接入

实现 API 标准化发布及规范管理，具体要求如下：

(1) OAS 3.0 规范要求：应用系统须基于 OpenAPI Specification 3.0 标准发布 API 文档，支持 Swagger UI 在线可视化展示。提供 API 文档自动生成模版。

(2) 合规性检查：必填信息检查如接口名称、版本号、请求方法（GET/POST 等）、鉴权方式（OAuth2 Scope）为必填项，缺失时禁止发布。

(3) 参数风格检查：请求参数与响应参数命名统一采用小驼峰风格（如 userName）；路径参数采用大括号包裹（如/api/v1/users/{userId}）；Scope 授权检查：接口需声明所需权限 Scope（如 user:read），未声明或 Scope 冲突时禁止发布。

(4) 兼容性检查：新版本 API 必须保留旧版本所有必填字段，向下兼容。不兼容的升级，需要支持不同版本的基线管理。

4.2 敏感数据防护

实现敏感数据脱敏配置，包括脱敏规则管理与脱敏验证，具体要求如下：

(1) 脱敏规则管理：支持字段级脱敏规则配置，如身份认证号、手机号、邮箱号等：

(2) 脱敏验证要求：第三方调用 API 时，若未申请敏感字段权限，响应结果中相关字段自动替换为****或 null。提供脱敏测试，支持模拟调用并验证脱敏效果。

4.3 API 流量管控

实现限流策略配置，包括阈值设置、限流响应，具体要求如下：

(1) 阈值设置：支持按应用配置调用频率阈值（如单个应用≤10 次/分钟）。

(2) 限流响应：触发限流时返回标准化错误信息，如请求过于频繁，请稍后重试。

4.4 字段级动态授权

通过权限申请与验证实现对重要数据的字段级动态授权，具体要求如下：

(1) 字段权限声明：API 发布时需标注敏感字段，并关联独立 Scope，未声明字段默认对所有调用方开放。

(2) 权限申请流程：第三方申请 API 时需勾选所需字段权限，审批通过后第三方应用请求才会返回对应字段信息。否则接口不返回。

4.5 接口能力清单

要求开放接口清单包括但不限于以下内容，通过开放的接口能力实现学校现有 PC 服务门户、移动 APP、预约中心的无用户化管理，接口能力包括但不限于用户接口、用户批量接口、组织机构接口、用户组接口、用户标签接口、用户组（岗位）管理、字典数据同步接口、身份数据同步接口、组织机构数据同步接口、账号数据同步接口、认证接口、角色接口等相关各类接口。具体以学校实际要求为准。

5. 系统管理功能

提供登录页面、多语言设置、多终端设置、消息配置等系统基础信息维护管理功能，具

体要求如下：

5.1 登录页面配置

提供用户登录页的配置能力，方便管理员定期更换页面，提升用户新鲜感，具体要求如下：

(1) 支持对 PC/H5、APP 等不同服务端登录页面的配置，在 PC 端提供至少 5 种以上登录页样式可供选择。

(2) 支持 PC 端登录页 logo 图片、背景图片的上传，多张背景图支持幻灯片形式切换。

(3) 支持配置和切换登录主题，个性化定制身份认证登录页面样式。

(4) 支持提供网址标题、版权信息、专属 APP 下载地址、忘记密码地址、账号激活地址、自定义链接的维护。

(5) 支持个性化配置背景图。支持一定时间内保持账号免登录，免登录周期可配置。

(6) 支持校内 APP 端上自定义链接、登录公告内容的维护。

5.2 多语言支持

为方便留学生、外教等外籍用户使用，应提供多语种支持，具体要求如下：

(1) 支持语言切换。个人使用相关界面均支持国际化设置。

(2) 支持系统自动记忆用户最近使用的语言偏好。

(3) 支持根据不同角色配置自动识别需要的语言版本。

5.3 ▲多终端支持

支持与学校现有 PC 办事服务门户、移动 APP 多终端对接，实现多端的登录功能，具体要求如下：

(1) 根据学校要求，前端相关功能均支持 PC 端和移动端。

(2) 基于更好的用户体验，支持与学校一网通办门户、移动 APP 进行多项功能深度集成，打造一体化服务入口，提升操作便捷性与服务连贯性。

5.4 通知消息配置

支持提供认证相关的所有消息模板内容的配置，通过对接学校消息平台进行消息推送，包括查询账号、完善信息、激活账号、找回密码、绑定/修改安全邮箱、修改安全手机、修改安全问题、绑定/解绑社交账号等操作时的消息推送，具体要求如下：

(1) 支持自定义对应错误类型的提示语，包括信息格式提示、动态码登录、可信设备登录、完善资料-密码符合规则、账号异常、账号登录、找回密码-输入账号、激活页-信息校验。

(2) 用户在使用忘记密码、账号激活、密码检测信息完善流程的页面中需支持按照需求提供“帮助指南”引导完成。

5.5 版本管理

支持系统版本、镜像版本管理，记录版本更新记录。建立功能、安全、系统、镜像持续升级机制。升级日志信息包括：编号、补丁包序号、名称、补丁包内容、补丁包详情、更新日期、升级文件信息、补丁包检验功能。镜像信息包括：编号、英文镜像名称、中文镜像名称、更新内容简述、更新文件信息、更新日期。

5.6 字典管理

支持提供系统级字典管理能力。为提高系统的可维护性、扩展性，提供系统级字典集中管理能力。字段管理由系统管理员在后台进行维护。字典管理，提供字典名、字典值信息设置，字典信息包括代码、名称、启用状态、数据来源、父级名称、备注、更新日期等信息。。其中，通用字典即用户基本信息所对应的字典（如：学生类别、性别、专业、学籍状态、证件类型、人员状态等）在数据同步时从第三方业务系统一起同步并不可修改。私有字典随着系统中角色、组的管理可自动进行更新。

5.7 运维监控

支持提供运维监控平台，做好各服务健康监控服务，提供视图化监控、按钮启停服务。平台、服务器等的健康状态检查。提供预警能力。针对时间策略的相关服务，提供系统预警、用户提前告知服务能力。

5.8 其他功能

(1) 支持认证平台可信授权功能。授权信息不限交大环境用户数、并发数、应用数，实现各微服务时间可信授权能力，非授权微服务不能对外提供服务。

(2) 支持系统关键功能配置、安全配置文件的在线备份恢复能力。提供前端门户集成能力，并提供“我的”相关账号安全设置等服务能力。前端门户可以看到分配给自己的应用（可以 API 方式获取），并且可以申请新应用的权限；“我的”页面提供用户认证与安全服务能力，包括密码重置、手机号变更、邮箱变更、解除第三方绑定、我的委托及委托日志记录等功能。

(3) 支持通过定时计划任务完成指定的工作，完成计划任务的配置管理、执行日志查询等功能。计划任务信息包括计划任务标识、计划任务类、定时时间、任务描述、任务状态、下次执行时间、任务参数设置。定时时间支持 cron 表达式生成器，秒、分钟、小时、日、月、星期、年多维度配置。

6. ★现有平台无感知迁移

6.1 已对接应用迁移

针对学校现已对接原认证平台的业务系统，提供迁移服务，具体要求如下：

(1) 全面覆盖历史数据迁移需求。不仅完整迁移原有日志审计数据，确保系统操作记录的完整性和可追溯性，还实现了 Appid、appsecret 等关键配置信息的精准导入，保障第三方应用接口的正常调用和系统间的无缝对接。

(2) 为最大程度降低对现有业务的影响，应保障学校现有认证平台已对接所有校内业务系统的迁移工作，须确保已对接系统无需进行任何代码改动或配置调整，均能在不中断服务的前提下，即可无缝完成升级切换，实现用户使用的无感知过渡。

6.2 用户数据迁移

现有统一认证体系和企业微信内的用户数据完整迁移对接，确保用户无感知登录新认证平台，企业微信登录校园应用不受影响，具体要求如下：

(1) 针对现有统一认证体系内的用户，实现历史账号密码的完整迁移与无缝对接，确保用户

无需重新注册或修改密码，即可无感知地完成系统升级切换，业务操作不受任何影响，充分保障用户体验的连续性与稳定性。

(2) 对于已绑定学校官方企业微信的用户，无需用户重新绑定操作，升级后仍能保持原有使用方式，真正实现零门槛、无感知的系统升级体验。

6.3 其他要求

(1) ▲深度整合校园数字化生态，实现与学校 VPN 无缝对接，确保用户可畅通访问各平台；

(2) 支持结合人工智能技术，通过智能分析用户行为与使用习惯，提供个性化的智能认证服务，并支持与学校人工智能平台深度集成，实现数据与能力共享，为师生带来更加智能、高效、安全的认证体验。

（二） 非功能性要求

非功能性要求包含安全要求、运行环境与技术要求、性能要求等。

1. 安全要求

(1) 平台开发与测试阶段，测试数据和测试结果需受到控制，不得出现在互联网；

(2) 平台的关键结构化数据需采用商用密码技术加密处理，如证件号、手机号、邮箱等重要字段，在质保期内按照学校要求加密指定字段，实现数据保密性、数据完整性和不可否认性；针对加密数据，提供离线解密工具，可实现数据离线解密操作；

(3) 平台需针对重要数据具备本地数据备份与恢复能力，制定备份策略并执行，备份结果使用商用密码技术开展机密性、完整性、不可否认性；

(4) 平台需采用 SSL 等技术保证数据的加密传输，并建立数据完整性检验机制，保证收发双方数据的一致性；具有一定的容错能力、数据安全备份和恢复能力，并能保持系统故障情况下的快速恢复运行。

(5) 平台需遵循最小安装原则，仅安装需要的组件，仅开放必要的端口，关闭不需要的系统服务、默认共享和高危端口；

(6) 平台需能发现可能存在的漏洞，及时修补漏洞，从接到漏洞、修补完成到升级成功，不得超过 48 小时；

(7) 供应商须无偿配合学校实施本平台的信息系统安全等级保护相关工作，本平台达到信息

安全等级保护二级标准，符合国标《信息安全技术-信息系统安全等级保护基本要求》（GB/T 22239-2019）7.1.4 安全计算环境要求。供应商须根据学校要求签订保密和数据安全协议。

(8) ★信息建设完成后应按照学校信息系统安全审查流程完成安全审查，确认系统建设与运维符合《西安交通大学信息系统安全基线技术规范》要求后方可提交验收。

(9) 平台需安装学校要求的恶意代码防护软件，定期查看防护结果并采取对应措施；

(10) 平台应定期进行安全检查，定期形成安全报告，及时发现安全问题，并进行安全修复等工作；

(11) 平台必须提供安全手段防止非授权用户的非法侵入、攻击，防止信息的非法、非授权的泄漏，必须避免平台操作人员的越级操作；

2. 运行环境与技术要求

(1) 要求系统校内本地化部署，支持容器化部署，并支持用户中心、统一认证的独立部署；系统采用分布式架构，处理节点支持水平多点扩展；系统必须采用负载均衡，支持动态监测负载状况，自动对可用资源进行并发检测，调整和分配等功能；支持 Linux、Windows 多种平台，完全支持跨平台的部署；

(2) 系统设计的数据表结构、数据字段、数据字典、范式设计必须符合学校数据标准，提供符合该标准的数据库设计文档，数据库采用国产数据库、MySQL、Oracle 等主流数据库；

(3) 平台系统应是一个开放的且符合业界主流技术标准的系统平台；系统架构中各层应采用成熟并符合技术标准的服务器、中间件、数据库产品，并保证基础平台的独立性，不依赖于某固定商家产品；

(4) 支持多种缓存管理工具（如 Ehcache、Redis），提高应用程序的性能和可伸缩性；

(5) 要求开放与其它系统的接口，并按学校要求，与其它应用系统进行对接，提供部分预留的其他应用系统接口或提供健全的二次开发接口，便于学校未来进行二次开发，本系统提供的应用程序接口不能影响其他系统的稳定性。支持开放数据库接口，开放数据库表结构等。系统在版本升级中保证接口协议、功能不发生变化；

(6) 国产化适配支持：要求系统可以基于国产化技术路线部署（芯片：鲲鹏、飞腾等主流国产 CPU，操作系统：麒麟、统信等主流国产操作系统，数据库：达梦、人大金仓、海

量数据等主流国产数据库，中间件：金蝶天燕、东方通等主流国产中间件）；按照学校要求进度完成信创适配改造的工作，技术路线以学校最终选择为准；

(7) 支持 IPv6。

3. ▲性能要求

基于微服务+容器部署架构，提供自动、快速扩展支持高并发场景的横向扩充能力。通过微服务的限流等措施，高并发熔断机制，满足高并发要求。系统满足在高负载、高并发环境下提供稳定、持续的服务。在满足用户安全策略的要求下，性能满足至少 10000 人同时登录；5000 以上用户并发，页面响应时间<3 秒，检索响应<3 秒，7×24 小时不间断运行。

4. 扩展性要求

(1) 系统应采用先进的技术架构和框架，以便在未来能够轻松升级和扩展。要求使用微服务架构、容器化等技术，提高系统的可维护性和可扩展性。

(2) 系统应支持新功能的快速开发和部署，而不影响现有功能的稳定性和性能。应提供灵活的配置和扩展机制，以便根据业务需求快速调整系统功能和结构。

(3) 系统应支持易使用要求。支持通过管理中心的策略配置功能，前台界面、功能点、授权动态变化，不影响使用界面，界面提供 PC 端、移动端友好的交互响应效果。

(4) 最大限度地满足本单位的个性化管理要求，能根据学校要求进行个性化设置和二次开发。

5. 其他要求

(1) 投标要求。供应商须在投标方案里用固定章节说明以上功能的详细技术方案。以上是本次项目建设的基本功能，系统的可扩展性要支持学校的实际建设需求。

(2) 知识产权要求。本项目交付的所有成果、文档资料、应学校要求定制开发的源程序代码的知识产权归学校所有。

(3) 项目管理与实施要求：项目组应包含实施本项目所必须的各类技术和管理人员，供应商选派参加本项目管理的项目经理应具有同类同规模项目的实施管理经验，选派的项目组主要成员应参加过同类同规模项目的实施。本项目要求驻场开发实施，现场技术人员不得少于 3 人。在项目建设期间、系统正式上线期间及学校要求重点保障期间保证至少 2 位技术人员驻场，保障系统稳定、业务正常办理。供应商的项目实施方案中应包含对项目组织机构及项目实施人员的详细描述，并附项目组织机构示意图和项目实施人员简历。

供应商还应对学校的项目实施组织模式给出相应建议。为了保证项目实施的连续性，在项目实施过程中，至少保证 1 名以上核心技术人员不能更换。

五、采购标的需满足的服务标准、期限、效率等要求

1. 质保期

质保期不少于五年。质保期内，根据学校要求，免费做好合理的需求开发保障。供应商免费提供原厂免费维护、升级服务，若有升级版本须及时通知用户，是否升级由学校决定；免费服务期结束后，供应商应提出升级、维护服务方案，并对服务内容、费用、方式、范围（产品、技术、模块）等方面进行承诺，另行签订服务合同。

2. 服务响应时间

要求提供 7*24 小时技术支持服务，提供应用系统各业务模块日常维护，保证各业务模块功能正常使用，数据准确无误。保障平台和各系统接口数据正常交互；紧急问题，如：系统崩溃导致业务停止、数据丢失等。1 小时内提交故障处理方案，4 小时内解决故障；严重问题，如：出现系统报错或警告，但业务系统能继续运行且性能不受影响。1 小时内提交故障处理方案，24 小时内解决故障；普通问题，如：系统技术功能、安装或配置咨询，或其他不影响业务的预约服务。1 小时内提交故障处理方案，48 小时内解决故障；

3. 培训要求

各标段供应商负责对学校人员提供技术培训，包括多种形式的系统使用指南及系统操作现场培训会，积极协助推进新系统。须按照不同的角色提供《用户使用手册》，方便学校用户掌握系统的所有功能；根据学校需求提供定期或不定期的技术交流与使用培训，包括操作人员培训和管理维护人员培训，便于学校掌握系统的使用和维护。供应商应在投标文件中提出培训计划，计划包括培训类别、培训项目、人数、时间、地点及培训方式等详细内容，达到使相关人员熟练使用系统的目的。

4. 服务标准及效率

(1) 标准化实施流程，应至少每季度进行一次系统巡检，并提交巡检报告，内容包括：磁盘空间、内存、CPU 使用率；网络环境检查；查看应用程序日志，查找系统异常日志等。对用户使用的系统部署实施的应用服务器、数据库服务器等的运行环境进行性能调优、

系统诊断、系统各模块日常维护等工作； 提供至少每年一次安全漏洞扫描和加固服务；操作系统、数据库、中间件及系统本身及相关组件出现安全漏洞时，免费升级服务，修复漏洞。供应商应无偿配合学校实施本平台的信息系统安全等级保护相关工作。

(2) 系统质保期内，能够安排技术人员提供技术和业务支持，关键时间段提供现场技术保障和维护服务。 整个项目全流程服务过程均需有完善的文档记录，便于跟踪、分析问题；对各项服务提供详细的书面报告，包括故障处理报告、健康巡检报告、维护总表报告、服务年度报告等。对运行过程中师生用户及业务部门的问题提供解答和问题解决跟踪。

(3) 在质保期内，对于学校自身业务规则的变化导致的非模块级功能需求变更、性能要求提升导致的部署结构变化等，提供配套的支持服务，响应需求，优化升级现有功能设置。针对本次建设的系统中存在的 bug、缺陷，不论在质保期内、外，均应持续免费提供修正与消缺服务。

5. 项目验收要求

各标段建设需满足招标文件中所列举的所有功能模块的实现要求。

交付的成果和文档资料包括但不限于：

(1) 可长期有效运行的系统。

(2) 交付文档包括不限于：

项目执行阶段：软件相关设计文档、项目过程资料（如《项目简报》、《会议纪要》、《阶段交付报告》、《需求确认单》等）、其他需要存档的资料。

项目验收阶段：《需求设计说明书》、《详细设计说明书》、《数据库设计说明书》、《用户操作手册》、《功能测试报告》、《性能测试报告》、应用系统及文档电子版光盘、其他需要存档的资料（如执行代码和源代码、需求说明书、设计说明书、数据字典、使用说明书、配置安装说明、系统维护说明、系统培训资料等）。还须提交第三方安全公司出具的渗透测试报告。

六、采购标的的履约验收标准

现场的检验指标及方法		
序号	功能或指标	验收或测试方法
项目建设单位验收要求：		

1	货物外包装与外观无损伤	现场核查
2	货物配置、包括备品备件、耗品耗材等提供齐全，货物实物品牌、规格、型号、配置数量与采购结果、合同约定相符。	依据《合同》及其附件（包括但不限于《采购需求》《供应商投标（响应）文件》《投标澄清函》《技术协议》等）约定，现场核查。
3	所有功能和指标参数（包括边界极限值）达到采购结果合同约定要求。	依据《合同》及其附件（包括但不限于《采购需求》《供应商投标（响应）文件》《投标澄清函》《技术协议》等）约定，现场测试。
4	提供《培训视频》影像资料	现场核查
5	验证测试设备的运行稳定性	试运行验证测试设备运行稳定达标
6	《供应商货物类项目完工报告》《项目建设单位货物类项目完工自验收报告》《项目建设单位货物类项目完工自验收报告》《第三方检测报告》等与验收相关的材料由项目建设单位妥善保管存档。	
学校验收复核要求：		
1	项目建设单位填写《学校采购货物类项目验收复核申请表》	
2	提供《供应商货物类项目完工报告》	
3	提供《项目建设单位货物类项目完工自验收报告》	
4	学校组织验收专家组现场复核供应商与项目建设单位货物到货完工验收完成情况	
验收时是否需要供应商提供样品	是□	否☑
验收时是否需供应商提供必要的其他设备	是□	否☑
除现场验收外，需提供的其他验收要求		
除现场验收外，是□否☑需提供第三方检测报告	对于检测机构的要求：国家正规检测机构，出具的检测报告由验收复核专家认可之后作为验收复核通过的主要依据。 对于检测执行标准的要求：各项检测项目标准以检测机构按照行业相关要求最新适用并执行的标准为准。	