

内蒙古科技大学信息化建设与网络管理中心

内科大网络字〔2025〕4号

关于印发《内蒙古科技大学信息化项目建设标准规范》的通知

各单位、各部门：

现将《内蒙古科技大学信息化项目建设标准规范》予以印发，
请认真贯彻落实。

内蒙古科技大学信息化建设与网络管理中心

2025年3月21日

内蒙古科技大学信息化项目建设标准规范

第一章 总则

第一条 为规范学校网络安全和信息化建设管理，加强统筹规划，依据《内蒙古科技大学网络安全和信息化建设与管理办法（修订）》（内科大校发〔2024〕77号）等相关规章制度，确保“数智科大”校园平台与各单位、各部门信息化项目的无缝对接，有效消除信息孤岛，特制定本文件。

第二条 按照学校统一规范、统一数据标准、统一身份认证、统一数据资产管理等建设要求，本文件规定须在信息化项目招投标阶段向投标方公示，并作为招标参数列入信息化项目采购文件和合同中。各单位、各部门在开展信息化项目建设时，须根据本文件的集成要求，制定详细的集成对接方案并严格落实，符合本文件要求后方可进行项目验收及业务系统上线运行。

第二章 信息标准集成

第三条 业务系统必须遵循国家、行业、省部及学校的信息编码标准，通过数据接口实现与学校数据中台的同步更新，确保信息编码标准的一致性与唯一性。如果业务系统为信息标准的权威数据来源，在系统实施前必须协助使用部门制定出业务数据标准并配合学校信息化建设与网络管理中心完善学校信息标准库。

第三章 业务数据集成

第四条 业务系统应开放数据库，支持全量数据采集，并提供必要的技术支持，包括数据库连接方式、访问权限配置、数据采集频率，数据库结构说明（包括每张表的名称、字段列表、字段类型及其功能说明），确保数据的全面性和准确性。数据上传

需符合数据中台集成规范，支持数据订阅和下发，设置明确的回写标识，确保组织机构、人员及业务数据在系统间和数据中台之间的有序流转，避免数据冲突或重复。

第五条 业务系统的所有用户（后台管理员除外）数据由学校数据中台或身份中台集中管理，统一下发并同步更新本地用户数据，确保用户身份认证、权限管理和业务流程的一致性。业务系统不得绕过数据中台或身份中台直接新增或修改用户信息。

第四章 统一身份认证集成

第六条 业务系统应接入统一身份认证平台，关闭自身独立的认证页面，并按照学校认证规范实现认证方式对接。系统原有认证功能可作为应急预案保留，并根据学校需求随时启用或关闭。在统一身份认证的框架下，用户的个人信息（如查询、修改功能）需引导至学校统一的个人信息管理平台，具体的功能授权和操作权限仍由业务系统内部完成，确保身份认证统一性与业务灵活性。

第五章 单点登录集成

第七条 业务系统应提供符合学校规范的单点登录入口 URL 和具体功能入口 URL（如查询、申请、统计等）。用户登录融合门户后，可直接通过图标或链接访问具体业务功能，无需重复登录。为保障用户体验，系统登录超时后应重定向至统一的单点登录界面，并在重新登录成功后恢复到超时前的操作界面。

第六章 门户消息和待办集成

第八条 业务系统应将所有与用户相关的通知、待办事项、日程等消息统一接入学校融合门户，确保登录融合门户的用户能

在同一界面查看并处理个人相关事项，实现消息的“统一发布、统一提醒”。同时，业务系统应遵循学校提供的消息或待办事项接口规范，按统一接口要求推送各类提醒消息，确保消息传递准确、及时。

第七章 移动端集成

第九条 业务系统所涉及移动功能须按照内蒙古科技大学移动集成标准规范，向系统外部提供移动端功能对应的 URL，并且支持对接企业微信和学校移动校园 APP。

第八章 系统安全性要求

第十条 各单位、各部门须落实国家网络安全等级保护制度，信息系统定级、备案、测评、整改同步推进。未通过等级保护测评和存在安全隐患的系统不得上线运行。业务系统及涉及的主机整体须满足等保 2.0 标准，具体如下：

（一）主机安全

1. 入侵防范

- （1）遵循最小安装原则，仅安装必要的组件和应用程序。
- （2）关闭不需要的系统服务、默认共享和高危端口。
- （3）限制远程管理终端，所有主机应通过堡垒机远程管理。
- （4）及时安装最新的操作系统补丁，修复高危漏洞，确保系统安全性。

（5）安装主机防护软件。

（6）安装主机监控软件。

2. 身份鉴别

- （1）禁止使用弱口令，配置口令复杂度要求：至少 8 位，

且包括大小写字母、数字和特殊字符。

(2) 配置口令有效期策略，有效期不得超过 90 天。口令过期后，强制更改口令，且禁止重复使用最近的 5 个口令。

(3) 配置无操作超时时间为 15 分钟，超过时限自动注销用户会话。

(4) 配置非法登录锁定策略：连续登录失败 5 次，锁定 10 分钟。

(5) 禁用明文传输服务（如 Telnet、HTTP 等），必须使用 SSH、HTTPS 进行远程管理。

(6) 及时更改默认初始口令。

3. 访问控制

(1) 限制或禁用默认用户的访问权限，确保默认账户不具有过高的权限。

(2) 实行最小权限原则，严格划分用户权限，仅授予用户执行其任务所必需的权限。

(3) 制定主机资源访问策略，并配置访问控制列表进行权限控制，防止未经授权的访问。

4. 日志审计

(1) 启用日志功能，日志数据应包括事件的日期和时间、用户标识、事件类型、事件是否成功及其他相关的信息。

(2) 对日志数据进行保护，确保其机密性和完整性，并定期备份。日志保存时间不少于 6 个月。

(3) 对日志访问进行严格的访问控制，防止未授权用户篡改日志。

5. 数据备份恢复

- (1) 具有重要数据的本地备份和恢复功能。
- (2) 具有异地数据备份功能。

(二) 应用安全

1. 入侵防范

(1) 配置 Web 应用防火墙，对应用层流量进行过滤，防止常见的 Web 攻击。

(2) 应使用国家密码算法，通过国家《商用密码应用安全性评估》（GM/T 0054），对数据进行加密，确保数据传输和存储的机密性。

(3) 建立数据完整性验证机制，确保数据在传输和存储过程中未被篡改。

(4) 对用户的输入进行严格过滤和校验，防止恶意输入导致的攻击。

(5) 定期进行补丁更新，及时修复高危漏洞。

(6) 建议启用人机交互验证（如滑动验证码），防止自动化攻击。

2. 身份鉴别

(1) 对登录的用户进行身份标识，确保身份标识应具有唯一性。

(2) 禁止使用弱口令，配置口令复杂度要求：至少 8 位，包括大小写字母、数字和特殊字符。

(3) 配置口令有效期策略，有效期不得超过 90 天。口令过期后，强制更改口令，且禁止重复使用最近的 5 个口令。

(4)配置无操作超时时间为 10-15 分钟,敏感应用建议 5-10 分钟。

(5) 配置非法登录锁定策略：连续登录失败 5 次，锁定 10 分钟。

(6) 建议启用多因素登录，增加登录过程的安全性，特别对于管理员和敏感操作用户。

(7) 使用加密的会话令牌，确保会话数据的安全性。

(8) 检测并阻止同一账户同时多地点登录，防止账户被滥用。

3. 访问控制

(1) 实行最小权限原则，严格划分用户权限，普通用户只能访问与自身业务相关的数据。

(2) 对敏感资源（如配置文件、日志、数据库）设置访问白名单，限制未经授权的操作。

(3) 定期审查权限分配，确保权限合理并及时撤销不再使用的权限。

4. 日志审计

(1) 启用日志功能，日志数据应包括事件的日期和时间、用户标识、事件类型、事件是否成功及其他相关的信息。

(2) 对日志数据进行保护，确保其机密性和完整性，并定期备份。日志保存时间不少于 6 个月。

(3) 对日志访问进行严格的访问控制，防止未授权用户篡改日志。

5. 数据备份恢复

(1) 具有重要数据的本地备份和恢复功能。

(2) 具有异地数据备份功能。

(三) 数据库备份

1. 根据业务重要性和数据更新频率，制定并执行定期备份计划。备份数据应保留多个备份点。

2. 备份数据应存储在异地，避免自然灾害或其他突发事件导致本地备份丢失。

3. 定期进行数据备份的恢复演练，确保在发生灾难时能够迅速恢复业务。

4. 备份数据的存储介质应采用冗余设计，防止硬件故障导致数据丢失。

(四) 资产统计

1. 对所有信息化资产进行详细统计、登记、分类和编号，确保对硬件资产和软件资产进行有效管理。

2. 定期对资产进行清点和审计，确保资产管理的准确性和完整性。

3. 对资产的部署、变更进行审批、记录并管理，确保资产的变更过程符合规范和安全要求。

第九章 验收阶段要求

第十一条 按照本文件集成规范，对项目完成情况进行检查验收，验收合格后项目方可上线运营。项目验收材料包括：（一）部署信息系统所需硬件环境或公有云部署的相关说明；（二）数据标准执行情况和数据质量情况的相关说明；（三）与学校数据中台、融合门户、统一身份认证平台、消息中心、任务中心、统

一卡码脸平台、公共应用支撑平台等对接情况说明；（四）网络安全测试报告或证明材料；（五）性能测试报告。

第十章 上线运行阶段要求

第十二条 业务系统部署应使用学校数据中心要求的国产虚拟机模板，部署在学校数据中心，虚拟机部署不得使用硬件加密形式进行授权，如 U 盾等，软件授权方式在虚拟机漂移时不需要重新授权。如自有集成系统需按照学校操作系统安全基线规范进行加固，符合项目验收相关要求后可正式上线。

第十三条 业务系统上线前须进行安全测试，包括服务器安全扫描、代码安全扫描、Web 安全扫描等，进行针对性渗透测试，确保系统不存在重大安全漏洞。各单位、各部门须指定专人进行管理和日常维护。

第十一章 下线停服阶段要求

第十四条 信息化项目因故发生合同终止，各单位、各部门应及时总结项目执行情况，清理资产，编制项目终止报告，并呈请各单位、各部门主要负责人审核。审核通过后，可按照相关规定终止项目，具体包括下线前需将系统中的数据迁移到新的系统或安全的存储设备中。迁移方式和存储位置由信息化建设与网络管理中心配合完成。取消该系统的所有外部链接，防止下线后仍有访问请求。回收服务器软硬件资源、IP 地址、域名等，并撤销相关的网络安全设备防护策略。停用或删除该系统的所有账户，包括 VPN、堡垒机等远程通道账户。

第十二章 附则

第十五条 本规范自发布之日起施行。此前学校相关规定与

本规范不一致的，以本规范为准。

第十六条 本规范发布后，新建及在建信息化项目均须严格遵循；已建成系统须在过渡期内逐步完成整改并达到本规范要求。

第十七条 本规范由信息化建设与网络管理中心负责解释与修订。