ICS 35.040
CCS L70

# 团　　体　　标　　准

T/CHI XX-202X

# 智慧校园信息共享平台通用技术要求

Generaltechnical requirements for the smart campus information sharing platform

（征求意见稿）

提交反馈意见时，请将您知道的专利连同支持性文件一并附上。



202X-X-X 发布　　202X-X-X 实施

中国高技术产业发展促进会　发布

# 目　　次

# 前　言

本文件按照 GB/T 1.1-2020《标准化工作导则第 1 部分：标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利，本文件的发布机构不承担识别专利的责任。

本文件由黄河水利职业技术大学提出。

本文件由中国高技术产业发展促进会归口。

主要起草单位：黄河水利职业技术大学、洛阳理工学院、河南科技大学、华北水利水电大学、四川职业技术学院、河南经贸职业学院、南阳农业职业学院、河南群智信息技术有限公司、洛阳市极限电子科技有限公司、洛阳矩阵软件有限公司、河南纪往来科技有限公司。

本文件主要起草人：李响、耿会涛、王国勇、张明川、张森、孟先新、刘明锦、宋建涛、陈西川 。

本文件首次发布。

# 智慧校园信息共享平台通用技术要求

## 1 范围

本文件规定了智慧校园共享平台通用技术的术语和定义，包括数据管理、数据中心信息安全、平台管理以及用户权限。

本文件适用于智慧校园共享平台的通用技术。

## 2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 36342-2018 智慧校园 支撑平台

GB/T 36342-2018 智慧校园总体框架

GB/T 22240-2020 信息安全技术 网络安全等级保护定级指南

GB/T 40684-2021 信息共享和交换架构

GB/T 40684-2021 物联网 信息共享和交换平台通用要求

GB/Z 42885-2023 信息安全技术 网络安全信息共享指南

DB4403/T 573—2024 信息共享应用规范

DB5301/T 117-2024 数据资源库 数据共享

## 3 术语和定义

下列术语和定义适用于本文件。

3.1

**映射转换 mapping transformation**

通过格式转换规则调整非标准数据集结构布局，依据映射规则执行数据类型转换、格式标准化及关系整合以优化一致性。

3.2

**数据加载 data loading**

数据上传、下载统称为数据加载。

[HB 8520-2015(2017),定义 3.1.3]

3.3

**数据挖掘 data mining**

从大量的数据中通过算法搜索隐藏于其中信息的过程。

注：一般通过包括统计、在线分析处理、情报检索、机器学习、专家系统(依靠过去的经验法则)和模式识别等方法来实现。

[GB/T 33745-2017,定义 2.5.3]

3.4

规则引擎 Business Rule Management System

通过预定义的业务规则集自动执行逻辑推理的软件组件，支持平台管理中的自动化决策。

## 4 数据集成平台

### 4.1 总体概念

平台用于连接若干业务系统，实现业务系统间的信息交互，符合GB/T 36478.1-2018中5.1 b)中介模式。平台与业务系统的关系见图1。业务系统可通过注册或注销的方式，加入或退出平台。注册的业务系统可作为数据提供方或数据需求方。

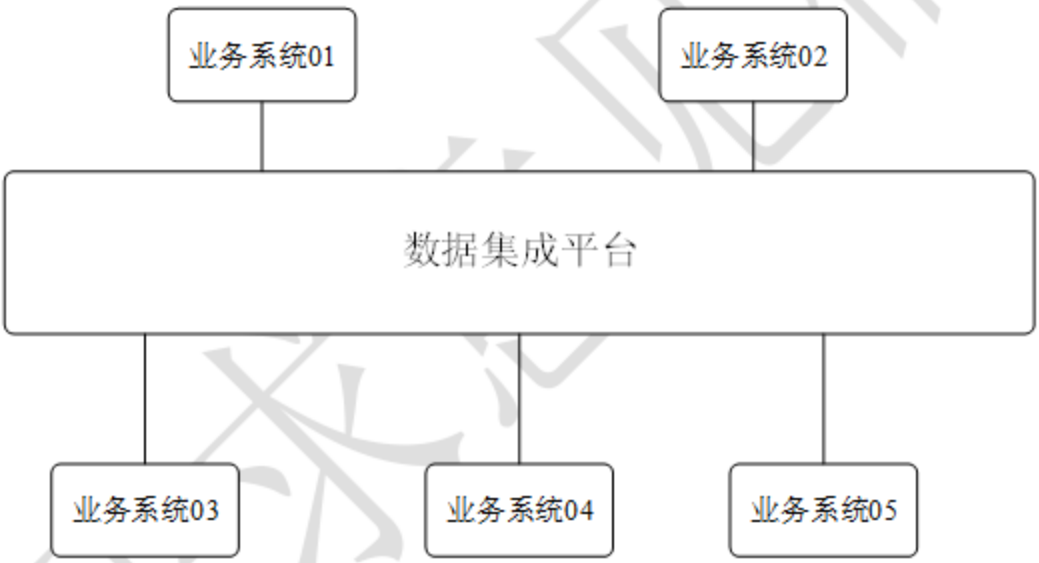


图 1 平台与业务系统的关系

平台与平台之间可采用不同连接方式进行部署，例如分布式、级联式。本文件不规定平台之间的具体部署实现。

### 4.2 平台的功能架构

平台的功能模块组成见图2。

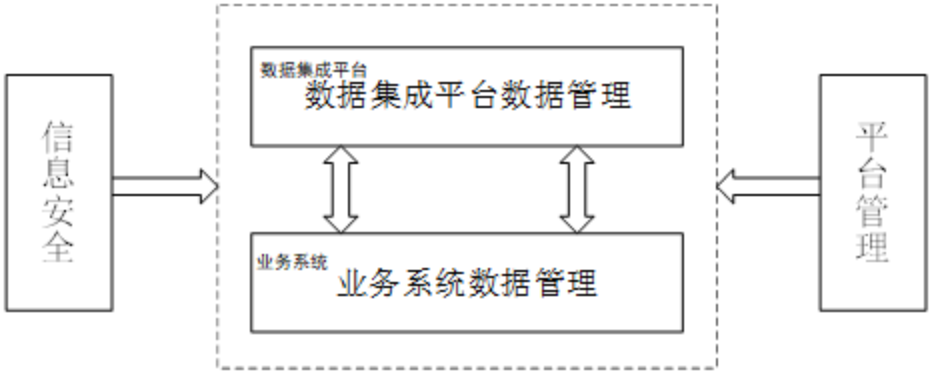


图 2　平台的功能架构

a）平台主要由数据集成平台数据管理、业务系统数据管理、平台管理和信息安全功能模块组成。
b）数据集成平台提供数据提取、映射转换、数据加载、数据共享等功能，对汇聚到平台上的数据进行管理。
c）业务系统提供业务系统数据来源管理、数据存储、数据处理、数据可视化等功能，对业务系统进行管理。
d）平台管理提供平台配置管理、平台日志管理、用户权限管理、平台菜单管理等功能，对平台进行管理。
e）信息安全提供数据安全、数据传输安全、数据使用限制、共享权限安全管理、共享过程监控、外网的防护功能、VPN访问控制、攻击和入侵防范要求、访问安全等功能，保障数据的安全传输与访问控制。

## 5　数据集成平台数据管理

### 5.1　数据提取

#### 5.1.1　收集原始数据

从教务、图书馆及宿舍管理系统中提取学生课程成绩、借书记录和宿舍分配等数据，主要通过各业务子系统的采集界面实现，或以文件形式存储于 PC 端。

#### 5.1.2　提取规则

通过预定义的抽取规则，从原始数据中提取数据模式信息和字段数据信息，确保准确解析数据的逻辑关系和内容特性。

### 5.2　映射转换

#### 5.2.1　格式转换

通过预定义的格式转换规则，将抽取的非标准数据集调整为新的数据组织结构和布局格式。此过程保持原始数据内容不变，仅改变其表现形式以适应目标需求。

#### 5.2.2　导入数据库

将转换后的中间数据集加载至关系型数据库中，确保数据顺利迁移。

#### 5.2.3 映射规则处理

依据数据映射规则，对中间数据集执行数据类型转换、格式标准化及关系整合操作，优化数据一致性以满足目标要求。

### 5.3 数据加载

#### 5.3.1 数据连接

识别教学管理系统、科研平台、校园一卡通等各类数据源，通过 API 接口、文件传输、数据库直连等方式建立数据连接。

#### 5.3.2 数据清洗

剔除重复值、处理缺失值、纠正错误格式，确保数据完整性与准确性。

#### 5.3.3 数据转换

按照平台统一数据标准，对数据类型、编码规则（如学籍号、部门编码）进行标准化转换。

#### 5.3.4 数据加载执行

将处理后的数据按既定规则写入目标存储，记录加载时间、数据量等元信息。

#### 5.3.5 异常处理

加载过程中若遇异常，触发重试机制，对多次失败的任务，生成异常报告并推送至管理员，人工介入排查数据源、转换规则等问题，确保数据加载流程的可靠性。

### 5.4 数据共享

#### 5.4.1 共享原则

数据共享应遵循以下原则：

a) 围绕智慧校园整体建设目标，统一规划数据共享架构，避免重复建设；
b) 建立数据共享安全体系，确保数据在传输、存储、使用过程中的保密性、完整性与可用性；
c) 严格遵守国家法律法规及教育行业规范，明确数据共享边界；
d) 以教学、科研、管理、服务等实际需求为驱动，按需开放共享数据。

#### 5.4.2 共享范围

覆盖学校教学部门、管理部门、科研机构、图书馆等，共享教学数据、科研数据、资产数据、师生基础信息等。

#### 5.4.3 权限管理

根据用户角色分配不同权限，建立数据访问申请、审核、授权的标准化流程，记录操作日志，确保权限分配可追溯。

#### 5.4.4 隐私保护

对涉及师生个人信息的数据进行敏感等级标注，实施差异化保护策略，制定隐私泄露应急预案，对外共享数据时，采用加密、脱敏、匿名化等技术手段，确保共享数据不可识别特定个人。

#### 5.4.5 数据要求

统一数据存储与交换格式，确保共享数据准确、完整、一致，建立数据校验机制，剔除错误、重复、无效数据。

#### 5.4.6 监督系统

建立数据共享平台的监督系统，定期对数据共享平台进行评估，监督各部门数据共享执行情况，确保标准有效落地。

## 6 服务支撑

校园数据服务系统通过多种功能模块，为用户提供个性化和高效的数据支持：

a) 系统根据来访用户(学生、教师、管理员、游客)的身份分配相应的数据访问权限及功能使用权限，例如，学生查看课程表、成绩等相关数据。

b) 用户可按需订阅数据推送，如活动通知、放假提醒或课程更新等，确保及时获取最新信息，同时也支持管理订阅，包括查看、取消、更新推送频率等。

c) 根据学生的学习习惯、兴趣爱好等历史信息，精准推荐符合其需求的学习资源，例如，优质的在线课程和学习资料。

d) 系统内置学习社区模块，为学生提供在线交流、分享学习经验的平台，鼓励学生之间互助合作，共同进步。

e) 系统通过收集教师的教学评价和学生学习反馈数据，对教学效果进行量化评估，为教师提供具体的教学改进方向和建议。

## 7 业务系统数据管理

### 7.1 业务系统数据来源管理

#### 7.1.1 学生信息

涵盖学生从入学到离校的全过程数据，包括基础身份信息、学业记录、行为表现等。

#### 7.1.2 教职工信息

涵盖教职工入职、在职、离职全流程信息，包括基础身份信息、职务变动及工作成果等。

#### 7.1.3 图书馆信息

涵盖图书档案查询、电子与纸质资源管理、座位预约等全流程服务数据，包括资源借阅记录、访问统计及调度信息等。

#### 7.1.4 物联信息

涵盖校园设施设备运行监测与智能管控全场景数据，包括环境监测、能耗管理、设备状态等物联感知等信息。

#### 7.1.5 教务管理信息

涵盖教学计划制定、课程实施到考核评估全流程数据，包括课程安排、成绩管理、教学评价等核心信息。

#### 7.1.6 财务管理信息

涵盖资金收支、预算执行到核算审计全周期数据，包括经费流动、成本核算、财务审计等基础信息，保障管理透明规范。

### 7.2 数据存储

#### 7.2.1 存储架构

需支持结构化、半结构化及非结构化数据的分类存储，采用分层策略并具备弹性扩展能力，平衡性能、成本及数据动态增长需求。

#### 7.2.2 对应存储数据库

需涵盖关系型数据库、非关系型数据库、时序数据库等数据库，实现数据服务的稳定性与快速存取。

#### 7.2.3 灾备机制

##### 7.2.3.1 数据备份

对核心业务数据进行定期自动备份，保留多份历史版本，避免因硬件损坏或操作失误导致数据丢失。

##### 7.2.3.2 冗余容灾

将关键数据同步备份至不同的服务器或云端存储，确保单一设备或机房故障时，其他备份能自动接管服务。

##### 7.2.3.3 恢复验证

通过模拟灾难场景，验证关键业务在指定时间内恢复运行，确保恢复策略有效性。

### 7.3 数据处理

#### 7.3.1 数据清洗

采用噪声消除、冗余剔除及结构化处理等方法，将原始数据转化为规范化数据。

#### 7.3.2 数据标准化

采用归一化等方法将数据映射到一个共同的数值范围内，以满足后续数据分析任务的要求。

#### 7.3.3 数据分析

采用机器学习、数据挖掘等方法从校园多源数据中学习有价值的信息，获取其中的潜在规律。

### 7.4 数据可视化

#### 7.4.1 数据可视化方式

根据校园数据的特点使用折线图、直方图、环形图等不同的可视化方式来展示其状态变化情况，如表 1 所示。

表 1 不同校园数据统计结果可视化方式

| | |
|---|---|
| 学生成绩变化趋势 | 折线图 |
| 学生行为分布 | 热力图/柱状图 |
| 教职工部门分布 | 树形图 |
| 图书馆热门书籍排行 | 条形图 |
| 座位预约时段高峰分布 | 折线图 |
| 物联设备运行状态统计 | 饼图 |
| 校园环境监测 | 动态折线图 |

#### 7.4.2 业务部门视图集成

各业务部门的可视化图表需适配部门职责定制，并直接嵌入其业务平台界面，支持在本部门系统内直接查看与交互，避免跨平台跳转。

#### 7.4.3 数据动态更新

图表数据需实时更新，确保业务状态变化、突发事件响应等场景下可视化结果与最新数据一致。

## 8 平台管理

### 8.1 平台配置管理

#### 8.1.1 系统参数配置管理

支持内存大小、日志路径等核心参数的集中化配置，提供界面化操作与版本管理功能，确保参数调整的灵活性与可追溯性。

#### 8.1.2 资源配置管理

实现存储、计算资源的分类配置与使用策略定义，支持业务应用的资源分配规则、权限控制及配额动态调整机制。

#### 8.1.3 资源分配管理

基于业务需求优先级动态分配存储与计算资源，支持自动化调度、配额实时监控及闲置资源回收机制，确保资源利用效率与业务连续性。

### 8.2 平台日志管理

#### 8.2.1 日志数据来源管理

应全面收集平台及相关设备的运行日志，包括系统日志、操作日志、错误日志等。

#### 8.2.2 日志分析与异常检测

基于规则引擎实现异常日志识别与告警提示，提供查询、监控、导出等一体化管理功能以及简单可视化反馈与告警提示。

### 8.3 用户权限管理

用户权限管理要求如下：

a）用户角色分类，不同角色具备不同的权限。
b）支持角色组设置功能,实现对角色的分类授权。
c）最小权限原则，根据用户角色分配最低必要权限，确保仅能访问与其职责相关的数据和功能。
d）权限随用户角色变更（如转岗、毕业）实时更新，无效权限需在24小时内撤销。
e）支持多角色设置,使得同一用户可获得多种权限。
f）用户具备对角色的添加、分配、授权、修改、删除、自定义变量授权等功能。

### 8.4 平台菜单管理

#### 8.4.1 菜单设计原则

菜单按功能模块分类，便于用户快速定位，层级不超过三级，名称简洁清晰，避免专业术语或模糊表述。根据用户角色动态显示，仅展现相关功能，隐藏无关选项。

#### 8.4.2 菜单权限分配

菜单项与用户角色权限挂钩，仅显示用户有权访问的功能选项。高级菜单仅对管理员可见，普通用户仅能访问基础功能菜单。

#### 8.4.3 菜单访问管理

点击敏感菜单（如数据导出、权限设置）前需二次验证身份。禁止通过URL绕过访问未授权功能，系统返回权限不足提示。菜单需适配PC和手机，移动端自动优化布局。

#### 8.4.4 菜单使用监控

操作日志记录菜单点击详情，保存至少6个月。异常检测监控高频点击敏感菜单等行为，触发警报并通知管理员。使用统计每月生成频率报告，优化菜单布局。

#### 8.4.5 菜单维护与更新

定期审查菜单结构与功能，确保符合最新需求。新建或调整菜单需经技术与安全团队审核后上线，不影响系统运行。变更后通过弹窗或消息通知用户并提供指引。

## 9 信息安全

### 9.1 数据安全

#### 9.1.1 数据加密

敏感数据在存储和传输时必须采用符合行业标准的加密技术。确保数据在静态存储和动态传输时均处于加密状态，加密密钥需定期轮换。

#### 9.1.2 访问控制

实施基于角色的访问控制，根据用户身份和职责分配权限，确保只有授权用户可访问特定数据。

#### 9.1.3 日志审计

所有数据访问和共享行为需详细记录日志，日志需加密存储，保存期限不少于 12 个月，以支持安全审计和事件追溯。系统应提供日志查询功能，确保在发生安全事件时可快速定位问题来源。

#### 9.1.4 安全备份

定期对关键数据进行异地备份，确保数据在意外丢失或损坏时能够快速恢复。

#### 9.1.5 漏洞管理

信息系统需定期进行全面安全评估，包括漏洞扫描和渗透测试，识别并修补已知的安全漏洞。

#### 9.1.6 储存安全

对敏感数据采用加密存储技术，防止未经授权访问。存储设备部署在安全的物理环境中，配备访问控制和监控设施。严格限制存储权限，仅授权人员可操作，保留访问日志，以支持审计和异常追溯。

### 9.2 数据传输安全

#### 9.2.1 加密保护

所有通过网络传输的数据必须使用端到端加密技术，防止数据在传输过程中被拦截或篡改。

#### 9.2.2 通道隔离

敏感数据传输需通过专用安全通道，避免与公开数据混用，降低泄露风险。

#### 9.2.3 传输验证

接收端需验证数据完整性，确保数据未被恶意修改。

### 9.3 数据使用限制

#### 9.3.1 使用范围约束

接收方只能在授权范围内使用共享数据，禁止二次共享或用于非授权目的。

#### 9.3.2 数据生命周期管理

系统应支持自动标记数据有效期，到期后自动限制访问或删除临时数据。

#### 9.3.3 使用行为规范

禁止通过截屏、复制或其他方式私自留存敏感数据副本。

### 9.4 共享权限安全管理

#### 9.4.1 动态授权

信息共享前，系统需根据请求者的身份和需求动态分配权限，权限有效期不得超过任务所需时间。

#### 9.4.2 多级审批

涉及敏感数据（如学生成绩、健康记录）的共享，必须经过至少两级授权审批。

#### 9.4.3 最小权限原则

共享时仅提供任务所需的最小数据集，禁止一次性开放全部数据访问权限。

### 9.5 共享过程监控

#### 9.5.1 实时日志

记录所有信息共享行为，包括共享发起者、接收者、数据类型、时间戳和共享目的，日志需加密存储。

#### 9.5.2 异常检测

部署自动化监控系统，识别异常共享行为（如批量下载敏感数据），并立即报警。

#### 9.5.3 事后追溯

确保共享记录可追溯，任何安全事件发生时可通过日志快速定位责任人和问题源。

### 9.6 外网的防护功能

对于外网的安全防御，需在外网与核心交换设备之间部署相应的防火墙设备，并部署相关策略。包括结构安全、访问安全、安全审计、入侵防范、恶意代码防护等。

### 9.7 VPN 访问控制

对于通过公共网络访问智能校园内部系统的内网用户，应启用 VPN 功能，以确保数据的机密性和完整性，防止数据在传输过程中被窃取或遭到未经授权的篡改。

### 9.8 攻击和入侵防范要求

提供基于应用的入侵防范，在实现对攻击行为的深度检测同时，通过应用识别来锁定真实的应用，并以此为基础进行深度的攻击分析，准确、快捷地定位攻击的类型。

### 9.9 访问安全

#### 9.9.1 用户身份认证

所有访问信息系统的用户必须通过至少两种身份验证方式，以确认身份合法性。

#### 9.9.2 访问限制

禁止从未经授权的设备或非安全网络（如公共 Wi-Fi）访问敏感数据。

#### 9.9.3 访问地点限制

对于高度敏感数据（财务系统），仅允许从校园内指定区域或设备访问。

#### 9.9.4 权限回收

用户离职、毕业或角色变更时，需在 24 小时内撤销其访问权限。