|  |  |
| --- | --- |
| ICS | 35.080 |
| CCS | |  | | --- | | D:\000000部门项目\09标准化插件开发\程序源代码\StandardEditor_ShanDongKeXieYuan\团标首页面字母T.pngD:\000000部门项目\09标准化插件开发\程序源代码\StandardEditor_ShanDongKeXieYuan\团标首页面字母T后面的反斜杠.png CS |   L 70 |

团体标准

T/CS XXXX—2025

智慧校园管理服务系统

Intelligent campus management service system

XXXX - XX - XX发布

XXXX - XX - XX实施

中国商品学会  发布

目次

[前言 II](#_Toc206079766)

[1 范围 1](#_Toc206079767)

[2 规范性引用文件 1](#_Toc206079768)

[3 术语和定义 1](#_Toc206079769)

[4 系统架构 1](#_Toc206079770)

[5 系统性能 1](#_Toc206079771)

[6 系统功能 2](#_Toc206079772)

[7 部署与环境要求 3](#_Toc206079773)

[8 数据安全 4](#_Toc206079774)

1. 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。

本文件由贵州众和宏远科技有限公司提出。

本文件由中国商品学会归口。

本文件起草单位：贵州众和宏远科技有限公司。

本文件主要起草人：。

智慧校园管理服务系统

* 1. 范围

本文件规定了智慧校园管理服务系统的系统架构、系统性能、系统功能、部署与环境要求、数据安全。

本文件适用于智慧校园管理服务系统的设计与构建。

* 1. 规范性引用文件

本文件没有规范性引用文件。

* 1. 术语和定义

下列术语和定义适用于本文件。

半安全区 semi-secure zone

部署 WEB 应用服务的网络区域，用于处理用户前端请求。

安全区 secure zone

部署系统核心应用及数据库的网络区域，保障数据与业务逻辑安全。

* 1. 系统架构
     1. 总体架构

系统采用分层架构，分为用户端、服务端、数据层及基础设施层，具体如下：

1. 用户端：包括家长通过黔农云访问的 H5 页面（支持学生绑定、充值等）和管理员使用的 PC 端（支持系统管理、数据统计等）；
2. 服务端：由 WEB 应用（部署于半安全区）和系统应用（部署于安全区）组成，基于 Java 语言开发，集成 Spring、Spring Boot、MyBatis 等框架，实现业务逻辑处理；
3. 数据层：包含 APP 应用数据库（MySQL 5.7）和缓存数据库（Redis），存储人员信息、消费流水等数据；
4. 基础设施层：由服务器、网络设备、中间件（Nginx、JDK 1.8）等组成，支撑系统运行。
   * 1. 部署架构
        + 1. 半安全区

部署 2 台 WEB 应用服务器（WEB 应用 1、WEB 应用 2），均配置 Nginx，用于接收并转发用户请求。

* + - * 1. 安全区

部署 2 台系统应用服务器（系统应用 1、系统应用 2），配置 JDK 1.8，处理核心业务逻辑；部署 2 台数据库服务器（DB1、DB2），分别运行 MySQL 5.7（存储业务数据）和 Redis（缓存数据）。

* 1. 系统性能
     1. 开发环境
        1. 操作系统

开发端使用 Windows 10（简体中文）；服务器端使用 Linux Redhat 7.4。

* + - 1. 开发工具

JDK 1.8、IDEA（英文）、MySQL（版本适配）、Nginx/Tomcat。

* + - 1. 技术框架

集成 Spring、Spring Boot、MyBatis；采用 Security（安全控制）、Redis（缓存）、FastJSON（数据解析）等技术。

* + 1. 性能要求
       1. 数据库

MySQL 最大连接数≥1024，Redis 支持高并发缓存；关键操作（如充值、消费）响应时间≤3 秒。

* + - 1. 服务器

WEB 应用服务器 CPU≥2 核、内存≥4G；系统应用服务器 CPU≥4 核、内存≥8 G；数据库服务器磁盘≥200 G。

* + - 1. 稳定性

支持 7×24 h 运行，单月故障时间≤1 h。

* + 1. 安全要求
       1. 数据传输

用户端与服务端通信采用加密协议，防止信息泄露。

* + - 1. 权限控制

基于角色分配权限（如家长仅可查看本人绑定学生信息，管理员可管理全量数据）。

* + - 1. 防干扰

系统运行不受电磁干扰，适应校园复杂网络环境。

* 1. 系统功能
     1. 学校与人员管理
        1. 学校信息管理

对学校基础信息（名称、编码等）进行增删改查；管理学校组织机构（班级、部门）。

* + - 1. 人员信息管理

手动添加或通过模板导入学生、教师信息（含姓名、身份证号、家长联系方式等）；支持人员信息修改与同步。

* + - 1. 班级及人员绑定

将班主任与班级绑定，家长与学生绑定。

* + 1. 消费与缴费管理
       1. 流水管理

查询充值流水（含订单号、金额、时间、支付方式）和消费流水（含设备编号、消费金额、余额变化），支持流水导出。

* + - 1. 余额管理

查看学生、教职工账户余额，处理退款申请（需学校审核后打款）。

* + 1. 月账单统计

可查看对充值、消费、退款流水的账单统计，方便财务人员进行每月的对账。

* + 1. 学杂缴费管理
       1. 对账管理

支持每天下载对账文件与系统实际金额进行对账。

* + - 1. 账单管理

导入学费、住宿费等账单，支持按学校、班级生成缴费报表；对接黔农云实现家长线上缴费。

* + 1. 考勤管理
       1. 门禁记录

记录学生门禁出入信息（家长可查看）。

* + - 1. 请假管理

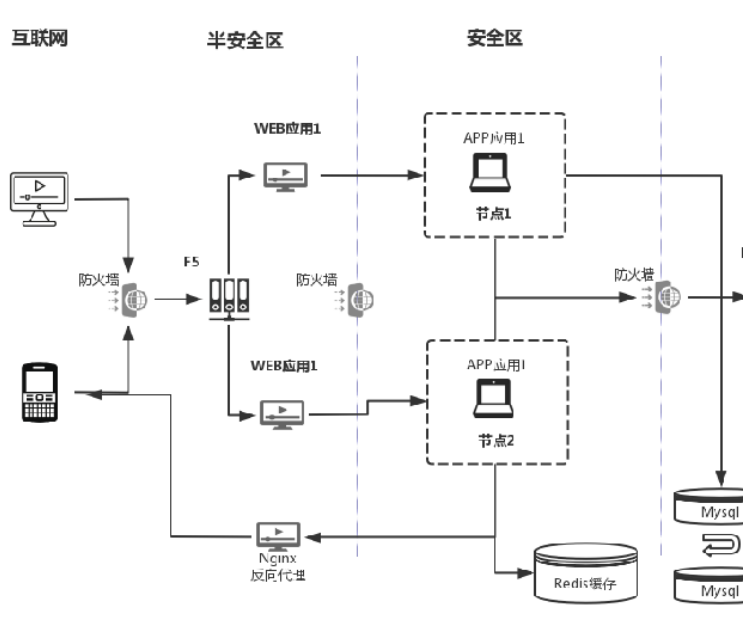
家长在黔农端申请请假，老师在黔农云批复后下发门禁。

* + - 1. 打卡配置

老师进出最早，最后一次识别打卡。

* 1. 部署与环境要求
     1. 部署架构图

如图 1 所示。



1. 部署架构图
   * 1. 服务器及中间件需求

如表 1 所示。

1. 服务器及中间件需求

| 服务器名称 | 部署位置 | 操作系统 | CPU | 内存 | 磁盘 | 软件安装需求 |
| --- | --- | --- | --- | --- | --- | --- |
| WEB应用1 | 半安全区 | linux Redhat7.4 | 2 | 4 | 50G | Nginx |
| WEB应用2 | 半安全区 | linux Redhat7.4 | 2 | 4 | 50G | Nginx |
| 系统应用1 | 安全区 | linux Redhat7.4 | 4 | 8 | 100G | jdk1.8 |
| 系统应用2 | 安全区 | linux Redhat7.4 | 4 | 8 | 100G | jdk1.8 |
| DB1 | 系统数据库应用 | linux Redhat7.4 | 4 | 8 | 200G | Mysql\_5.7 |
| DB2 | 缓存数据库应用 | linux Redhat7.4 | 4 | 8 | 200G | redis |

* + 1. 数据库需求

如表 2 所示。

1. 数据库需求

| 项目 | 配置 |
| --- | --- |
| 数据库用户名 | qn\_shop |
| 数据库编码 | utf-8 |
| 数据库最大连接数 | 1024 |

* + 1. 网络环境

半安全区与安全区之间通过防火墙隔离，仅开放必要端口（如 80、443）。

支持与黔农云平台、校园一卡通系统等外部系统对接，网络带宽≥100Mbps。

* 1. 数据安全
     1. 数据分类与敏感等级

敏感数据：包括学生及家长身份证号、银行卡信息、人脸图片、手机号码等，需采取最高级保护措施。

重要数据：包括充值流水、消费记录、账户余额等，需确保完整性和不可篡改性。

一般数据：包括学校名称、班级信息等公开信息，需保障可用性。

* + 1. 数据存储安全

加密存储：敏感数据（如身份证号、银行卡号）在数据库中采用 AES 加密算法存储，密钥定期更换（周期≤90 d）。

人脸数据保护：学生人脸图片存储路径加密，仅授权用户（如班主任、系统管理员）可访问，且操作日志全程留痕。

访问控制：数据库采用强密码策略（长度≥12 位，含大小写字母、数字及特殊符号），并启用双因素认证；仅允许安全区服务器通过指定 IP 访问数据库。

* + 1. 数据传输安全

传输加密：用户端与服务端、服务端与数据库之间的所有数据传输均通过 SSL/TLS 协议加密，防止中间人攻击。

接口安全：系统对外接口（如与黔农云的对接）采用 Token 认证机制，Token 有效期≤2 h，且包含时间戳防止重放攻击。

* + 1. 数据使用安全

权限最小化：按照“按需分配”原则授予用户权限，例如：家长仅能查看本人绑定学生的信息，行社管理员不可直接获取人脸原始图片。

操作日志：记录所有敏感数据的访问、修改、删除操作，包括操作人、时间、IP 地址及具体内容，日志保留至少 1 年。

数据脱敏：在非必要场景下，对敏感数据进行脱敏展示（如身份证号显示为 “123\*\*\*\*\*\*\*\*\*\*1234”，手机号码显示为“123\*\*6789”）。

* + 1. 数据销毁安全

过期数据处理：学生毕业或离校后，其敏感数据（如人脸图片）需在 30 d 内删除，历史消费记录可匿名化后留存（去除姓名、身份证号等标识信息）。

设备报废处理：存储过敏感数据的服务器、硬盘等设备报废前，需通过专业工具进行数据擦除（至少 3 次覆写），确保数据无法恢复。

