ICS 35.080
CCS L 70

T/CS

团 体 标 准

T/CS 235—2026

智慧校园管理服务系统

Intelligent campus management service system

2026－01－13 发布 2026－01－13 实施

中国商品学会 发 布

目　　次

前言 II
1　范围 1
2　规范性引用文件 1
3　术语和定义 1
4　缩略语 1
5　系统架构 1
6　系统性能 2
7　系统功能 2
8　部署与环境要求 3
9　安全性要求 5

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、江苏开放大学、南京艺术学院、贵州鼎一企服科技有限公司。

本文件主要起草人：李建锋、刘高璐、何永军、陈广超。

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（以下简称“系统”）的设计、研发与应用。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；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 22080 网络安全技术 信息安全管理体系 要求

GB/T 22239 信息安全技术 网络安全等级保护基本要求

3 术语和定义

下列术语和定义适用于本文件。

3.1

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。

3.2

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。

4 缩略语

下列缩略语适用于本文件。

WEB：互联网（World Wide Web）

APP：应用程序（Application）

DB：数据库（Database）

CPU：中央处理器（Central Processing Unit）

AES：高级加密标准（Advanced Encryption Standard）

IP：网络之间互连的协议（InternetProtocol）

SSL：安全套接层（Secure Sockets Layer）

TLS：传输层安全（Transport Layer Security）

5 系统架构

5.1 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：

a) 用户端：包括家长通过系统访问的 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）；

b) 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；

c) 数据层：包含 APP 应用数据库（MySQL）和缓存数据库（Redis），存储人员信息、消费流水等数据；
d) 基础设施层：由服务器、网络设备、中间件（Nginx、JDK）等组成，支撑系统运行。

5.2 部署架构

5.2.1 半安全区

宜部署 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。

5.2.2 安全区

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

6 系统性能

6.1 开发环境

6.1.1 操作系统

开发端系统宜使用 Windows 10（简体中文）；服务器端宜使用 Linux Redhat 7.4。

6.1.2 开发工具

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

6.1.3 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。

6.2 性能要求

6.2.1 数据库

MySQL 最大连接数不低于 1 024，Redis 支持高并发缓存；关键操作（如充值、消费）响应时间不超过 3 s。

6.2.2 服务器

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

6.2.3 稳定性

支持 7 d×24 h 运行，单月故障时间≤1 h。

6.3 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。

6.4 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）。

6.5 防干扰

系统运行不受电磁干扰，适应校园复杂网络环境。

7 系统功能

7.1 学校与人员管理

7.1.1 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）。

7.1.2 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。

7.1.3 班级及人员绑定

将班主任与班级绑定，家长与学生绑定。

7.2 消费与缴费管理

7.2.1 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。

7.2.2 余额管理

查看学生、教职工账户余额，处理退款申请。

7.3 月账单统计

财务人员可查看包括但不限于充值、消费、退款流水的账单统计，每月进行对账。

7.4 学杂费缴纳管理

7.4.1 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。

7.4.2 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；对接系统实现家长线上缴费。

7.5 考勤管理

7.5.1 门禁记录

记录学生门禁出入信息（家长可查看）。

7.5.2 请假管理

家长在黔农端申请请假，老师在系统批复后下发门禁。

7.5.3 打卡配置

支持教师出勤打卡识别。

8 部署与环境要求

8.1 部署架构图

如图 1 所示。

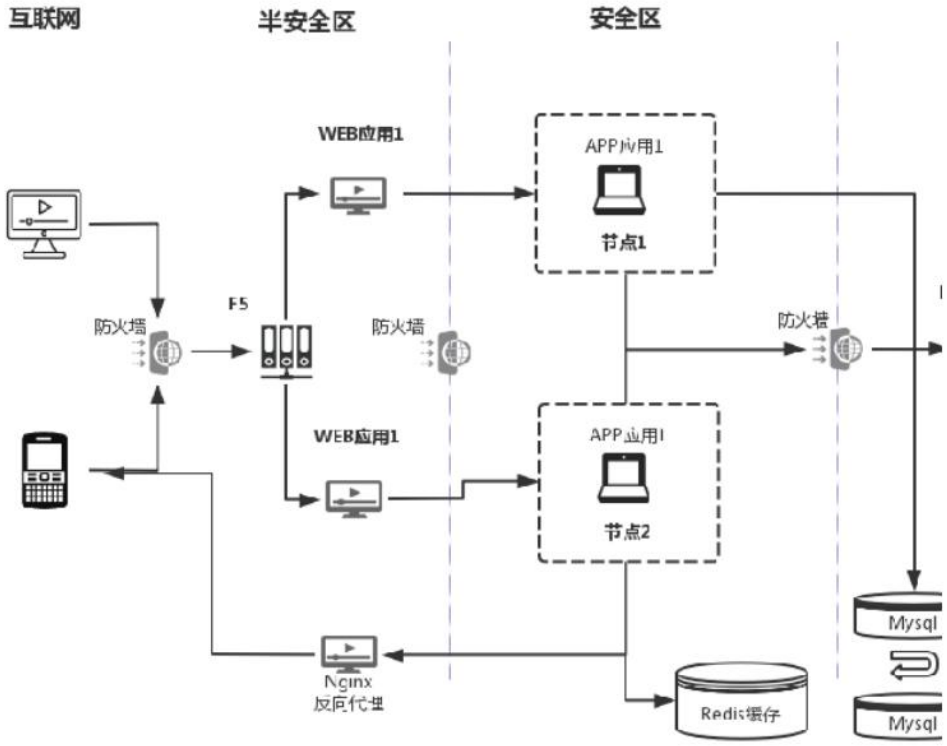


图 1　部署架构图

8.2　服务器及中间件需求

如表 1 所示。

表 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

8.3　数据库需求

如表 2 所示。

表 2　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

8.4　网络环境

8.4.1　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）。

8.4.2　支持与系统、校园一卡通系统等外部系统对接，网络带宽≥100 Mbps。

9 安全性要求

9.1 网络安全

按 GB/T 22239 的要求划分网络安全区域，半安全区与安全区、内部网络与外部网络（如互联网、黔农云平台）之间应部署防火墙、入侵防御系统等安全设备，实现逻辑隔离；仅开放业务必需的端口和协议，关闭不必要的网络服务，定期审计网络访问策略。

9.2 信息安全管理体系

按 GB/T 22080 的要求，建立健全信息安全管理制度体系，包括安全管理总则、网络安全管理、数据安全管理、设备安全管理、人员安全管理、应急管理等制度。

9.3 数据分类与敏感等级

9.3.1 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，应采取最高级保护措施。
9.3.2 重要数据：包括充值流水、消费记录、账户余额等，应确保完整性和不可篡改性。
9.3.3 一般数据：包括学校名称、班级信息等公开信息，应保障可用性。

9.4 数据存储安全

9.4.1 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）。
9.4.2 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。
9.4.3 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。

注：强密码策略是指长度不低于 12 位，含大小写字母、数字及特殊符号的密码设置。

9.5 数据传输安全

9.5.1 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。
9.5.2 接口安全：系统对外接口（如与系统的对接）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。

9.6 数据使用安全

9.6.1 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。
9.6.2 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。
9.6.3 数据脱敏：在不影响业务正常开展的前提下，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”）。

9.7 数据销毁安全

9.7.1 过期数据处理：学生毕业或离校后，其敏感数据（如人脸图片）应在 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）。
9.7.2 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，应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。