

附件 2

学校实验室设备及管理系统采购其他要求

一、总体目标

确保实验室终端设备、网关、服务器管理平台形成闭环可控的接入体系，通过标准化协议、可控开放的 SDK 及分层架构设计，保障系统扩展性与安全性，同时满足学校授权的第三方再次扩容、整改、维修等需求的顺利（如技术维护方、二期建设方、合作科研团队）介入。

二、接入网关设备要求

1、南向兼容性

- (1) 接入通道的物理接口（接口参数（引脚定义、电气特性）需提供详细标准化文档（仅限授权方获取）；
- (2) 通信协议需（兼容）开放网关南向协议（如 Modbus RTU/TCP、OPC UA、国标通信规约等），禁止仅支持私有协议（若有私有协议，需随设备提供协议转换插件，且插件仅对授权方开放）；
- (3) 提供免费提供技术咨询支持，对第三方物联设备满足第三方通用传感器、控制器、仪表等接入网关的兼容性 & 接入可控性；

2、北向兼容要求

- (1) 支持标准化北向协议（如 MQTT over TLS、Coap、RESTful API 等），若网关设备使用私有协议，网关需完成协议转换（转换规则需对学校透明，并提供详尽描述文档资料）；
- (2) 与服务器平台的通信必须采用加密，保证敏感控制器不受外界侵入攻击；
- (3) 并提供完备详细描述文档，原则上禁止使用私有协议与服务器通信；

3、离线处理与安全

- (1) 对终端上传的敏感数据（如实验数据）进行本地加密后再传输至服务器。
- (2) 建议具备物理端口锁定功能：非授权人员插拔网线 / USB 设备时，自动触发报警并阻断该端口通信。
- (3) 建议网关侧有离线存储功能，保证掉线后可保留最低区域内采集、控制闭环要求。

四、服务器管理软件（平台）要求

1、架构与接入策略

- (1) 采用微服务架构，需包含独立的“接入授权模块”，所有设备（终端、网关）及第三方系统接入前必须通过该模块审核（审核流程：设备 / 第三方申请→学校管理员审批→生成临时授权令牌）。
- (2) 支持设备自动发现（基于 DHCP/mDNS），但发现后需手动确认授权方可注册，未授权设备仅显示“待审核”状态，无法获取平台功能接口。
- (3) 建议要求平台支持通用组态化中间件（如 Node-RED、Apache Kafka），实现设备数据与业务系统的解耦。中间件最好提供可视化流程编排工具，降低设备接入门槛。

2、协议与开放控制

- (1) 提供标准化 API 接口（RESTful API），但 API 调用需携带学校签发的令牌（令牌有效期可配置），未授权第三方调用时返回 403 错误并记录日志。
- (2) 禁止向未授权第三方开放核心协议文档（如平台与网关的通信规约），授权第三方需签署保密协议后，由学校提供加密版文档（含时间限制）。

3、数据与日志管理

- (1) 平台需存储所有接入行为日志（包括终端、网关、第三方的接入时间、操作内容、IP 地址），日志保存时长不低于 1 年，且仅学校管理员可导出。
- (2) 支持数据接口权限细分：对授权第三方仅开放其所需的特定数据字段（如仅允许查询某类设备状态，禁止修改配置）。

五、数据交互规范（终端 - 网关 - 服务器全链路）

1、格式标准

- (1) 终端→网关：支持 JSON/XML 格式，字段需包含设备 ID、时间戳（基于 NTP 同步，误差≤1 秒）、数据类型标识。
- (2) 网关→服务器：统一采用 JSON 格式，附加网关签名（基于设备 ID + 时间戳的哈希值），服务器需验证签名有效性，无效数据直接丢弃。

2、双向通信控制

- (1) 终端接收指令（如参数修改）必须经过“网关转发 + 服务器授权”双重校验：服务器指令需携带网关 ID，网关验证指令匹配自身 ID 后才转发至终端，防止指令被非法拦截篡改。

六、数据仓储

- (1) 物联网化数据仓储作为智慧实验室设备数据的核心存储与管理中枢，需紧密衔接设备兼容性、数据交互规范、安全机制等核心要求，确保新设备数据无缝接入、历史数据可追溯且支持平台迁移
- (2) 支持水平扩展以适配新增设备的海量数据（如实验仪器高频测量值、设备状态日志），且需兼容文件中要求的各类协议数据接入（如 MQTT 上报的实时数据、OPC UA 传输的设备参数）。
- (3) 跨平台数据兼容：数据仓储需支持多种数据格式的原生存储与转换，包括文件中强制要求的 JSON/XML 标准格式，以及设备可能产生的二进制流、CSV 等格式，同时提供格式转换接口（符合 RESTful API 规范），确保平台更换时历史数据可无损迁移至新平台。
- (4) 时序数据特性适配：针对实验室设备的时序数据（如温度、压力随时间的变化曲线），设计专门的时序数据分区策略（如按设备类型、时间窗口分区），并满足文件中“时序数据循环存储时长”要求（建议可配置存储周期，默认不低于 1 年，重要实验数据支持长期归档，视频、图像数据可酌情放低存储要求）。

七、安全与授权机制（阻断未授权第三方核心措施）

1、接入认证流程

- (1) 终端设备：MAC 地址 + 序列号白名单→网关认证→服务器注册。
- (2) 第三方（如技术维护公司）：提交接入申请（含用途、期限）→学校审核→签署保密协议→获取临时 SDK/API 令牌→定期复核（每 3 个月）。

2、加密与防泄露

- (1) 所有协议文档、SDK 仅通过学校内部系统发放，且需绑定接收方设备 MAC 地址，禁止复制传播。
- (2) 服务器与网关、网关与终端的通信禁止明文传输，强制采用 TLS 1.2 + 或国密 SM4 加密，密钥由学校定期（每 90 天）更新。

3、白名单管理

- (1) 服务器平台需支持基于 MAC 地址、IP 段、设备型号的多层白名单，未在白名单内的设备 / 第三方，即使获取协议文档也无法建立连接。

八、测试与验证要求

1、兼容性测试

- (1) 成交供应商需提供自动化测试工具，覆盖“终端→网关→服务器”全链路接入测试，重点验证：未授权终端的接入阻断效果、第三方无令牌调用 API 的失败场景。
- (2) 测试用例需包含“模拟未授权第三方破解 SDK”场景，确保 SDK 内置的授权验证机制有效。

2、开放可控性测试

- (1) 验证授权第三方接入流程：提交申请→审核通过→正常接入；未提交申请→无法获取 SDK / 协议→接入失败。
- (2) 测试 SDK 时效性：授权到期后，第三方是否无法继续调用接口（需提供测试报告）。

3、长期支持承诺

- (1) 成交供应商需承诺至少 5 年的固件 / 软件更新支持，更新内容需包含“未授权接入防护强化”模块，且更新前需经学校测试确认。

九、实施保障条款

- (1) 若发现成交供应商未按要求开放 SDK / 协议（导致授权第三方无法接入），或存在“后门”允许未授权接入，学校有权退货并要求合同金额合同约定的违约金。

十、参考标准

建议符合 IEC 62443（工业网络安全）、ISO/IEC 27001（信息安全管理）及教育部《教育行业网络安全防护指南》相关要求。