HUAMUX 华慕智学

华慕智学数据安全、系统架构与私有化部署技术说明

覆盖完整产品数据流、身份权限、接口、部署、备份恢复、安全运维与项目退出

文档用途	用于学校内部立项、产品评估、技术论证、项目实施、采购谈判与验收准备。项目范围、参数、价格和服务承诺以双方最终签署文件为准。
适用对象	学校/集团信息化负责人、网络安全负责人、数据保护负责人、采购技术评审人员和项目负责人

文档编号：HMX-ZX-SEC-003
版本：V2.0 · 发布日期：2026年8月13日
出品：四川华慕科技有限公司 · 产品：华慕智学
官网：https://zhixue.huamux.com · 电话：400-855-0065

文档控制

项目	内容
文档编号	HMX-ZX-SEC-003
当前版本	V2.0（正式发布版）
文档负责人	华慕智学技术、运维与安全团队
适用范围	华慕智学公有云、混合云、私有化、本地系统整合及设备接入场景
使用目的	用于技术评估和安全尽调，明确产品安全控制、部署选项、私有化前置条件及双方责任。
受控原则	电子版以采购信任中心当前下载版本为准；项目采用时，应复制为项目受控文件并补充学校名称、项目编号、审批人与生效日期。

版本记录

版本	日期	变更说明	状态
V1.0	2026-08-13	网站首发版本	已归档
V2.0	2026-08-13	围绕完整产品、技术、实施与验收体系重构，增加可执行模板和证据编号	正式发布

重要说明

项目化填写	文中标注“项目填写”的容量、并发、RPO、RTO、SLA、上线范围和验收阈值，必须根据学校规模、部署方式和合同约定确认，不能把空白模板视为华慕的默认承诺。

目录

1. 说明范围与安全责任

安全不是一份证书或一个部署选项，而是从账号建立、教学数据使用、接口交换、运维访问到项目退出的持续管理。

模块编号	能力域	主要范围	核心使用者
P-01	组织、账号与权限	集团、校区、年级、班级、教师、学生组织；角色权限与数据范围	信息化、教务
P-02	课堂互动与即时练习	教师发起练习，学生作答，班级参与、正确率和共性问题反馈	教师、学生
P-03	作业与辅助批改	作业布置、提交、客观题处理、主观题辅助与教师复核、结果统计	教师、学生
P-04	测评与学情诊断	周测、月考、入学诊断；按学生、班级、知识点和题型形成线索	教师、教务
P-05	错题归集与复练	错题归集、知识点与错因分类、任务下发、结果回看与复验	教师、学生
P-06	分层任务与培优补弱	教师确认分层策略，不同学生组配置任务并跟踪完成和调整	教师、年级
P-07	校长驾驶舱	学校、年级、学科、班级趋势；异常、责任、动作和复验进度	校长、教务
P-08	教育集团多校区	分级组织、统一口径、校区比较、资源共享、总部与校区权限	集团、校区
P-09	学生平板与设备管控	账号设备绑定、应用与时段控制、设备状态和异常处理	信息化、班主任
P-10	数据交换与系统整合	统一身份、教务、阅卷、题库等系统的数据映射、同步、对账与异常补偿	信息化
P-11	部署、日志与运维	公有云、混合云、私有化评估；日志、备份、监控、升级与支持	信息化、华慕

1.1 责任模型

责任域	学校/集团	华慕科技	共同确认
合法使用	确定处理目的、校内制度、授权和告知	按约定范围提供产品与处理服务	数据范围、期限、角色和接收方
账号与权限	提供真实组织关系、审批高权限	提供角色和权限配置、日志能力	权限矩阵与抽查周期
基础设施	私有化时提供符合要求的机房、主机、网络和基础安全	提供约定范围的部署、配置和应用维护	容量、补丁、证书、备份和监控
终端与网络	管理校内网络、终端、物理安全和使用制度	提供约定的设备管控与应用能力	兼容范围、异常和支持
事件处置	校内决策、通知、业务应急和监管配合	技术排查、止损、修复和证据支持	分级、联系人、时限和复盘

不替代法律意见

本资料说明产品与项目控制框架。学校和华慕应根据实际处理活动、部署地点、数据类型和适用监管要求，由有权人员确定最终合规方案。

2. 逻辑架构与全产品数据流

实际物理架构会随部署方式变化，但应保留身份、业务、数据、集成、审计和运维等逻辑安全边界。

逻辑层	主要组件/对象	主要安全控制
用户与终端层	学生平板、教师电脑/移动端、教务和校长浏览器	设备与账号绑定、会话、终端策略、传输保护
接入层	域名、证书、反向代理、网关、访问入口	TLS、访问控制、限流、请求校验、可用性防护
身份与权限层	组织、角色、用户、认证、授权和会话	最小权限、数据范围、密码/认证策略、高权限审批
业务应用层	课堂、作业、测评、诊断、复练、分层、驾驶舱、集团和设备管理	业务校验、教师复核、敏感操作控制、输入输出校验
数据与内容层	关系数据、文件、题库、日志、备份和缓存	分类分级、加密/访问控制、完整性、备份、期限和删除
集成层	教务、统一身份、阅卷、题库、消息和第三方服务	认证、签名/白名单、字段最小化、超时重试、对账与审计
运维与审计层	监控、告警、日志、工单、发布、远程运维和应急	分权、临时授权、操作留痕、变更审批、恢复演练

2.1 典型数据流

01 身份进入
学校主数据或人工授权建立用户、组织与角色，用户通过受控入口登录。

02 教学产生
课堂、作业、测评、批改、错题和复练产生业务记录，按角色与班级授权使用。

03 分析与复核
系统聚合数据形成学情和管理线索，教师或学校人员对重要结果复核。

04 管理与协同
教务、校长和集团在授权范围查看趋势、异常、责任和处理进度。

05 运维与审计
接口、访问、配置、异常和高权限操作形成日志，按约定期限保存与审计。

3. 数据分类分级与生命周期

数据类别	产品中的对象	主要风险	建议控制
身份与组织	姓名、手机号、学号、学校、班级、角色、任课关系	身份冒用、越权、错误关联	最小字段、唯一标识、变更同步、角色权限
教学与成绩	作答、作业、考试、得分、错题、诊断、分层和评价记录	泄露、误用、标签固化、不当评价	用途限制、教师复核、范围控制、导出审批
未成年人信息	学生身份、学习过程、设备和联系信息	超范围处理、公开或不当使用	必要性评估、监护/学校规则、最小展示和期限
设备与行为	设备标识、绑定、登录、应用策略、操作和异常	过度追踪、设备串用	限定目的、授权角色、保留期限、解绑
内容与题库	试题、解析、教材映射、课件和作业资源	版权、错误内容、未授权共享	来源授权、审核、版本、下架和范围
运维与安全	管理员、接口、访问、告警、工单、远程维护和备份记录	高权限滥用、日志泄露	分权、审批、脱敏、留痕、限制访问

3.1 生命周期控制

阶段	必须确认	产品/项目措施
收集	目的、字段、来源、合法性和必要性	字段清单、接口范围、表单和授权
存储	位置、介质、权限、备份和期限	数据库/文件访问、备份与环境隔离
使用	角色、范围、业务规则和复核	RBAC、数据范围、教师复核与操作日志
传输/提供	接收方、字段、频率、保护和再委托	TLS、接口认证、最小字段、第三方清单
导出	用途、审批、格式、脱敏和接收人	导出权限、审批/记录和水印策略（按项目）
更正/删除	触发条件、影响范围和下游同步	更正流程、重算、级联处理和记录
退出	返还、迁移、删除、账号关闭和证明	导出、访问关闭、密钥回收、删除/保留记录

4. 身份、认证、权限与教师复核

角色	默认可见范围	主要动作	高风险控制
学生	本人任务、作答、反馈和授权内容	作答、提交、查看个人结果	不能查看他人数据；设备解绑按流程
教师	所授班级、学科和任务	发布、批改、复核、诊断、分层和反馈	批量导出、跨班访问和更正按授权
班主任/年级	授权班级/年级及必要跨学科信息	跟进任务、查看风险、组织复盘	不自动替代学科判断
教务	授权校区、年级、学科和管理数据	组织、规则、分析、复盘和权限管理	跨范围、高权限和导出审批
校长/集团	汇总和授权下钻范围	趋势、异常、责任和动作跟进	不直接修改原始教学数据
系统管理员	系统配置和运维必要范围	账号、角色、配置、接口和维护	分权、双人复核、日志和定期审计
华慕运维	仅工单和故障处理必要范围	按批准窗口临时处理	限时授权、全程留痕、结束回收

4.1 权限治理要求

- 角色权限和数据范围分开设计：拥有某功能不等于能查看所有学校或学生数据。
- 人员转岗、离职、毕业、转班、兼课和临时代课应触发权限复核。
- 管理员、高权限、批量导出、远程运维和敏感配置变更应单独控制并留痕。
- 定期按样本验证“谁能看什么、谁能改什么”，不能只检查权限配置页面。
- AI分析、主观题辅助、学生分层和争议结果应保留教师复核、修正与记录。

5. 应用、接口、内容与终端安全

5.1 应用与接口控制

控制域	要求	项目核验
输入与文件	校验输入类型、长度、权限和文件类型；限制危险内容	异常输入和越权用例
会话与认证	按风险设置会话、失败处理、退出和凭证保护	会话失效、并发/异地登录策略
接口认证	明确密钥/令牌、签名、白名单、证书和轮换方式	错误认证、重放、过期和撤销测试
接口数据	最小字段、传输保护、幂等、版本和错误返回	字段核验、重复推送和数据越界测试
异常补偿	超时、重试、告警、对账、补发和人工处理	断网、第三方失败和恢复测试
安全更新	依赖识别、漏洞评估、修复、测试和发布流程	版本记录和重大漏洞处理记录

5.2 题库与内容

- 记录题目、解析、教材映射和资源的来源、授权范围、版本、审核人与下架状态。
- 题目或答案更正后，评估是否需要重算批改、学情、错题和管理报表，并保留说明。
- 集团资源共享应区分总部发布、校区自有、个人草稿和对外授权范围。

5.3 学生平板与终端

场景	控制建议	学校配套
账号与设备绑定	记录绑定、换机、借机、解绑和异常登录	设备领用与身份核验制度
应用与时段	按学校策略控制可用应用、网站和时间段	审批、临时开放和自动收回规则
丢失/维修	暂停账号或设备访问，处理本地数据与重新绑定	报失、维修、备用机和责任台账
版本兼容	确认系统版本、浏览器/客户端和升级窗口	设备资产、充电、网络和更新安排
退出学校	解绑、回收、清理和账号状态变更	毕业、转学、离职和资产交接流程

6. 部署方式与边界选择

维度	公有云	混合云	私有化/本地化
适用	快速试点、校内运维资源有限	部分数据或系统本地，云端协同	明确内网、本地留存或自主运维要求
基础设施	由服务方按约定提供	双方分别负责各自环境	学校提供或采购并承担基础安全
上线和升级	较快，统一维护	需协调两端兼容和窗口	受学校窗口、环境和变更流程影响
数据边界	按服务说明和合同	按数据域/处理环节划分	核心业务数据可在指定环境
运维	华慕为主，学校管理账号和使用	联合监控、接口和故障定位	学校承担基础设施，华慕承担约定应用范围
主要风险	网络和服务依赖	边界复杂、跨域排障	补丁、备份、容量和人员不足

6.1 选型决策问题

- 是否存在明确的内网、本地留存、监管或数据出域限制，而不是仅以“私有化更安全”作判断？
- 学校是否具备服务器、网络、存储、备份、安全、监控和数据库等长期运维能力？
- 版本升级、漏洞修复、远程支持和故障恢复能否获得必要窗口？
- 三至五年总成本是否包含基础设施、第三方许可、人员、备份、容灾和升级？
- 与教务、阅卷、统一身份、题库和消息系统的网络和责任边界是否清楚？

7. 私有化部署技术基线

以下为方案设计检查项，不是未经调研即可套用的固定配置。正式方案应形成架构图、资源清单、端口清单、数据流和责任矩阵。

编号	核验事项	责任方	状态	证据/备注
PRI-01	生产、测试、备份与管理边界已确定	双方	☐	架构图
PRI-02	服务器/虚拟化、CPU、内存、存储、IO和扩容方式已按容量估算	学校	☐	资源清单
PRI-03	操作系统、数据库、中间件、运行时和第三方组件版本已确认	双方	☐	软件清单
PRI-04	网络区域、域名证书、DNS、NTP、代理、防火墙、端口和白名单已确认	学校	☐	网络清单
PRI-05	账号、系统管理员、数据库管理员、运维和远程访问分权已确认	双方	☐	权限矩阵
PRI-06	监控、日志、告警、备份、恢复、容量和证书到期监测已配置	双方	☐	运维验证
PRI-07	安装、初始化、数据导入、上线、升级、回退和应急流程已演练	双方	☐	演练报告
PRI-08	离线/受限网络条件下的依赖、许可、补丁和技术支持方式已确认	双方	☐	依赖清单

7.1 容量估算输入

输入项	项目填写	说明
学校/校区、注册及活跃用户	_____	区分账号总量和日/月活跃
课堂/考试高峰并发	_____	按班级、时间表和操作类型建立并发模型
作答、图片、附件、题库和日志增长	_____	估算月/年增长和保留期限
接口数量、频率与批量大小	_____	包含高峰、补发和历史回灌
可用性与维护窗口	_____	明确业务时段和可维护时间
RPO/RTO与备份保留	_____	结合业务影响和恢复成本确定
预留与扩容触发阈值	_____	约定监测、告警和扩容责任

8. 日志、监控、备份与业务连续性

8.1 日志与监控范围

类别	建议记录	核验用途
身份与权限	登录、失败、退出、角色、数据范围和高权限变更	账号异常与越权调查
业务关键操作	发布、批改/更正、导出、分层、配置和数据处理	结果追溯与争议处理
接口	调用方、时间、结果、错误、重试和对账标识	同步失败与数据一致性
运维	发布、配置、数据库、远程访问、备份和恢复操作	变更和故障调查
运行监控	可用性、响应、资源、队列、错误率、容量和证书	预警、容量和SLA

8.2 备份恢复设计

控制项	项目需要确认	验证证据
备份对象	数据库、文件、配置、密钥/证书（按安全方式）、日志和部署资料	备份清单
频率和保留	全量/增量、保留周期、覆盖和清理方式	任务与保留记录
副本与隔离	是否跨存储/区域、访问权限、勒索和误删防护	副本位置与权限
恢复目标	业务级RPO/RTO、优先级和依赖恢复顺序	合同/运维方案
恢复演练	范围、频率、环境、校验、耗时、问题和整改	演练报告

9. 安全运维、变更与事件响应

活动	控制要求	项目证据
变更发布	申请、评估、审批、测试、窗口、验证、回退和记录	变更单/发布记录
漏洞与补丁	获取、评估、分级、修复、测试、发布和暂缓风险接受	漏洞/版本记录
远程运维	学校审批、指定人员、限时访问、最小权限、全程记录和结束回收	工单/访问日志
管理员操作	实名账号、分权、关键操作复核、日志保护和定期审计	账号/审计记录
第三方依赖	清单、来源、许可、版本、风险、升级和退出替代	组件/供应商清单
安全事件	发现、分级、隔离、取证、通知、恢复、复盘和整改	事件报告

9.1 事件响应流程

01
发现与登记
记录时间、来源、现象、影响范围、数据类型和当前状态。

02
分级与升级
依据可用性、数据、用户、传播和合规影响确定级别与负责人。

03
控制与保全
阻断风险、保护业务、保留日志与证据，避免未经授权的破坏性操作。

04
修复与恢复
修复原因，按批准顺序恢复服务和数据并完成业务验证。

05
通知与复盘
按合同和适用要求沟通，形成时间线、根因、影响和预防措施。

10. 第三方、委托处理与合规映射

10.1 第三方与委托处理清单

字段	要求
主体与服务	名称、服务内容、部署地点、联系方式和替代方案
数据	数据类别、字段、主体范围、数量级、敏感程度和传输方向
目的与期限	处理目的、方式、频率、保留期限和删除方式
安全	访问、加密、日志、备份、事件、人员和再委托控制
退出	数据返还/删除、账号关闭、证明材料和业务连续性

10.2 现行法规控制主题映射

法规/制度主题	本资料对应控制	项目落地文件
《网络安全法》及网络安全等级保护	网络运行、身份权限、日志、监测、事件、产品和服务安全	安全方案、等级保护相关材料、运维制度
《数据安全法》	分类分级、风险管理、全生命周期、事件和组织责任	数据清单、分类分级、风险评估和应急
《个人信息保护法》	目的、必要性、告知、权限、委托、个人权利、删除和未成年人保护	处理规则、委托处理、权限与期限清单
《网络数据安全管理条例》	制度、访问控制、认证、加密/备份、风险与事件、第三方产品服务	网络数据安全制度、技术措施和事件流程
学校/教育主管制度与合同	校内审批、教学使用边界、人员职责、档案和服务承诺	学校制度、合同附件和项目方案

参考来源（访问日期：2026年8月13日）：中国人大网《数据安全法》、国家法律法规数据库《网络数据安全管理条例》、国家密码管理局/中国人大网《网络安全法》、工业和信息化主管部门转载的《个人信息保护法》。

11. 项目退出、数据迁移与销毁

编号	核验事项	责任方	状态	证据/备注
EXIT-01	数据导出范围、格式、关联关系、校验值和交付介质已确认	双方	☐	导出清单
EXIT-02	接口、定时任务、账号、远程访问、密钥和证书已停止或回收	双方	☐	关闭记录
EXIT-03	学校需保留、返还、迁移、归档和删除的数据已分类处理	双方	☐	处理记录
EXIT-04	题库、定制代码、配置、文档、第三方许可和知识产权已按合同移交	双方	☐	移交清单
EXIT-05	备份、副本、日志和依法/依约需保留数据的后续规则已确认	双方	☐	保留/删除说明
EXIT-06	未结事件、漏洞、变更、工单和业务连续性风险已移交	双方	☐	未结清单

附录A：安全尽调与验收模板

A.1 安全尽调问题

编号	核验事项	责任方	状态	证据/备注
SEC-Q01	数据存放在哪里，哪些人员、系统和第三方可能接触	供应商	☐	数据流/第三方清单
SEC-Q02	角色、数据范围、高权限、导出和远程访问如何控制	供应商	☐	权限矩阵/日志
SEC-Q03	关键日志记录什么、保存多久、谁能查看和防篡改	供应商	☐	日志策略
SEC-Q04	备份对象、频率、副本、RPO/RTO和最近恢复演练结果	双方	☐	备份/演练
SEC-Q05	漏洞、补丁、第三方组件和重大安全更新如何处理	供应商	☐	安全运维记录
SEC-Q06	发生泄露、不可用、越权或数据错误时如何分级、通知和补救	双方	☐	应急流程
SEC-Q07	合作结束后怎样导出、删除、关闭访问并提供处理记录	双方	☐	退出方案

A.2 恢复演练记录

字段	填写内容
演练范围	系统/数据：_____ 环境：_____ 时间：_____
目标	RPO：_____ RTO：_____ 完整性验证：_____
步骤与人员	备份选择、恢复顺序、依赖、负责人和业务验证人
结果	实际数据点：_____ 实际耗时：_____ 业务验证：通过/不通过
问题与整改	问题、影响、责任人、完成时间和复验
批准	技术负责人：_____ 业务负责人：_____ 日期：_____