## 风险评估与识别-风险清单更新

### 1.风险数据采集

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **任务** | **操作方法** | **工具/资源** | **责任人** | **交付物** |
| **系统日志分析** | 1.提取近6个月系统错误日志（error级别） 2. 统计高频错误类型model\_timeout、db\_crash） 3.按模块（AI对话、知识库、访问控制）分类汇总 | 日志分析工具（ELK） | 技术组-运维 | 《系统故障热力图与频率报告》 |
| **用户反馈聚类** | 1.收集200条用户反馈如客服工单、AppStore评论 2.分词提取高频问题如“AI回答错误”、“登录慢” 3.标注用户画像如年级、使用场景 | NLP分词工具（Jieba） | 运营组-客服 | 《用户反馈问题聚类表》 |

### 2.风险框架构建

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **任务** | **操作方法** | **工具/资源** | **责任人** | **交付物** |
| **风险分类标准制定** | 1.定义4大风险类型： -系统风险（性能、稳定性） -数据风险（存储、传输、访问） -用户体验风险（交互、响应） -合规风险（隐私、政策） 2.每类下细分3-4个子项如数据风险→未加密存储、越权访问 | 思维导图工具（XMind） | 产品组+安全组 | 《风险分类标准V1.0》（含子项与场景示例） |
| **风险描述模板设计** | 模板字段：风险ID、名称、场景、影响范围、等级、责任人、解决期限 | Word模板 | 产品组-文档 | 《风险描述模板V1.0》（含填充示例） |

### 3.风险等级评定

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **任务** | **操作方法** | **工具/资源** | **责任人** | **交付物** |
| **矩阵法风险赋值** | 1.定义概率等级：高（>70%）、中（30-70%）、低（<30%） 2.定义影响等级：高（数据泄露/系统宕机）、中（功能异常/用户投诉）、低（界面错误） 3.对15条风险打分如“知识库越权访问”：高概率×高影响→高风险 | 风险矩阵表（Excel） | 安全组+产品组 | 《风险等级矩阵表V1.0》 |
| **跨部门评审会** | 1.组织技术、运营、法务部门评审 2.确定优先级： -高风险（3天内修复） -中风险（30天内修复） -低风险（季度迭代） | 会议记录模板 | 项目组全体 | 《风险优先级清单V1.0》 |

### 4.风险清单文档与合规

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **任务** | **操作方法** | **工具/资源** | **责任人** | **交付物** |
| **清单条目化撰写** | 按模板撰写15条风险条目，关联检测报告与解决方案 | Word+Excel | 产品组+技术组 | 《风险清单V1.0》（初稿） |
| **法务合规审查** | 1.审核隐私相关风险如数据收集合法性 2.修订合规性描述如引用《个人信息保护法》第28条 | 法务审查清单 | 法务组+安全组 | 《合规审查意见V1.0》 |
| **最终归档** | 1.整合报告与审查意见，生成正式版清单 2.上传至校园OA系统，抄送信息中心、教务处 | 电子归档系统 | 产品组-文档 | 《风险清单（最终版）》（PDF+在线文档） |

## 风险应对措施文档

### 风险应对策略

|  |  |  |  |
| --- | --- | --- | --- |
| **风险等级** | **策略** | **执行原则** | **响应时间** |
| **高风险** | 立即修复 | 优先处理核心安全漏洞如数据未加密、身份认证绕过等，阻断风险源头。 | 风险识别后≤7 天内 |
| **中风险** | 限期优化 | 优化系统性能与功能体验如高并发延迟、知识库更新滞后，提升用户体验。 | 风险识别后≤30 天内 |
| **低风险** | 迭代改进 | 基于用户反馈持续优化细节如界面交互、合规文案，纳入季度迭代计划。 | 风险识别后≤90 天内 |

### 具体风险应对措施

高风险

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **风险名称** | **风险描述** | **应对措施** | **责任人** | **时间节点** | **交付物** |
| 知识库敏感文档未加密访问 | 未认证用户可查看敏感知识库 | 1.存储端采用 AES-256 加密，传输使用 HTTPS 2.访问增加 “学号 + 时间戳” 二次验证 3.开发加密日志监控系统 | 技术组-架构师 | 2025-06-09 至 06-15 | 《加密模块验收报告》 |
| 高并发场景服务器宕机 | 并发量≥3000时CPU持续100%导致崩溃 | 1.新增2台ECS服务器，配置Nginx负载均衡 2启用自动扩容策略 | 技术组-运维 | 2025-06-09 至 06-16 | 《负载均衡配置报告》 |

中风险

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **风险名称** | **风险描述** | **应对措施** | **责任人** | **时间节点** | **交付物** |
| AI对话高并发响应超时 | 5000并发时20%请求延迟>5秒 | 1.优化Rasa对话流程，减少数据库查询 2.引入Redis缓存热门问题（命中率≥70%） | 技术组-算法工程师 | 2025-06-16至06-30 | 《性能优化对比报告》 |
| 知识库更新延迟>24小时 | 教务系统数据变更后知识库未及时同步 | 1.开发定时同步任务（每日凌晨1点） 2.失败自动重试+邮件报警 | 技术组-后端 | 2025-06-16至06-25 | 《数据同步测试报告》 |
| 多设备登录未触发安全预警 | 同一账号在手机/电脑同时登录无提醒 | 1.开发设备登录监控看板 2.异地登录触发短信预警 | 技术组-前端 | 2025-06-16至06-22 | 《安全预警功能截图》 |

低风险

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **风险名称** | **风险描述** | **应对措施** | **责任人** | **时间节点** | **交付物** |
| 收藏按钮点击率低 | 用户反馈“找不到收藏入口” | 1.按钮尺寸从24px扩大至32px，增加红色角标提示 2.优化交互逻辑：长按快速收藏 | UI组+前端 | 2025-07-01至07-15 | 《高保真交互原型图》 |
| 隐私政策合规性不足 | 未明确说明数据存储期限 | 1.法务审核修订隐私政策，补充数据使用条款 2.新增用户首次使用合规声明弹窗 | 法务组+产品组 | 2025-07-01至07-10 | 《隐私政策修订稿V1.0》 |