# 技术更新管理政策

版本: 2.0 | 生效日期: 2024年8月20日 | 审批人: CTO

## 1. 政策目标

确保所有技术系统保持最新状态，及时发现和替换过时系统，保障信息安全和业务连续性。

## 2. 适用范围

* 生产环境系统
* 开发测试环境
* 第三方应用服务
* 基础设施组件

## 3. 更新分类与时限

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 类型 | 定义 | 响应时限 | 部署时限 | 审批人 |
| 紧急安全更新 | 严重安全漏洞修复 | 2小时 | 24小时 | 安全总监 |
| 重要安全更新 | 一般安全漏洞修复 | 4小时 | 72小时 | 安全总监 |
| 功能更新 | 新功能或性能改进 | 1周 | 1个月 | 技术总监 |
| 系统替换 | 停止支持的系统 | 提前6个月 | 提前3个月 | CTO |

## 4. 更新流程

### 4.1 发现与监控

* 自动化监控: 漏洞扫描工具、官方安全公告订阅
* 定期审查: 月度技术栈审查、季度架构评估

### 4.2 评估与决策

* 风险评估: 业务影响 × 技术风险 × 攻击可能性
* 优先级: P0(紧急) > P1(重要) > P2(一般) > P3(可选)

### 4.3 测试与部署

* 测试环境: 开发环境 → 预生产环境 → 生产环境
* 部署策略: 分批部署、实时监控、快速回滚

## 5. 责任分工

|  |  |
| --- | --- |
| 角色 | 主要职责 |
| CTO | 技术更新战略制定、重大系统替换审批 |
| 安全总监 | 安全漏洞评估、安全更新优先级制定 |
| 技术总监 | 功能更新审批、技术架构评估 |
| IT运维部 | 日常更新执行、系统监控、应急响应 |
| 开发团队 | 应用层更新、代码依赖管理 |

## 6. 关键指标

### 6.1 及时性指标

* 安全补丁平均部署时间 ≤ 72小时
* 系统更新覆盖率 ≥ 95%
* 过时系统识别率 = 100%

### 6.2 质量指标

* 更新成功率 ≥ 98%
* 计划外回滚次数 ≤ 2次/月
* 业务中断时间 ≤ 4小时/月

## 7. 应急响应

### 7.1 零日漏洞

* 2小时内启动应急响应
* 4小时内完成影响评估
* 24小时内部署防护措施

### 7.2 更新失败

* 立即启动回滚程序
* 30分钟内恢复服务
* 24小时内完成根因分析

## 8. 文档要求

* 更新申请表与审批记录
* 影响评估与测试报告
* 部署日志与监控数据
* 问题处理与经验总结

## 9. 政策维护

* 每年审查一次政策有效性
* 重大技术变更时及时修订
* 定期开展培训和演练

文档控制: 创建 2024-01-01 | 修订 2024-08-20 | 审查 2025-08-20