吉林建筑大学网络信息中心

吉林建筑大学信息系统开发运维安全管理规范

第一章 总 则

第一条 为加强吉林建筑大学网络信息中心（以下简称"网络信息中心"）信息安全管理工作，规范软件安全开发全生命周期管理流程和技术标准，依据国家有关法律、法规和网络信息中心相关制度，制定本规范。

第二条 本规范所称全生命周期包括应用系统开发的需求分析、设计、开发、测试、发布及运维等阶段。

第三条 本规范适用于网络信息中心承担的所有信息系统开发及运维安全管理活动。

第二章 组织与职责

第四条 全生命周期安全管理涉及系统开发团队、系统运维团队及安全管理团队，相关职责划分如下：

（一）系统开发团队负责安全需求分析、安全设计、系统开发及测试验收阶段的安全问题修复与改进。

（二）安全管理团队负责安全需求评审、安全设计评审、开

发安全培训、安全检测及验收工作。

（三）系统运维团队负责系统上线后的安全运维工作。

第三章 需求阶段

第五条 安全需求是应用系统必须具备的安全属性。系统需求分析阶段应融入身份鉴别、访问控制、数据安全、软件容错及源代码保护等安全要素，明确系统安全需求。

第六条 需求分析阶段，系统开发团队应依据安全需求分析原则形成《安全需求方案》，并提交安全管理团队评审。未通过评审的，需修订后重新提交直至通过。

第七条 安全管理团队应结合系统实际风险，审核安全需求方案的全面性。若方案未覆盖实际风险点，应在评审意见中补充要求。

第四章 设计阶段

第八条 设计阶段应根据安全需求制定对应的安全措施，确保系统安全功能完备。

第九条 系统安全功能应包括身份鉴别、访问控制、安全审计、软件容错、资源控制、数据完整性、数据保密性、备份恢复、剩余信息保护及个人信息保护等 10 个方面。

第十条 自行研发项目由系统开发团队编制设计方案；外包项目由开发单位提供设计方案。

第十一条 设计方案须经安全管理团队评审，未通过评审的

需重新设计。

第五章 开发阶段

第十二条 自行研发系统开发实施阶段应落实安全措施，定期使用源代码安全分析工具扫描漏洞，并修订代码问题。同时需编写完整的开发文档及使用指南。

第十三条 安全管理团队应组织安全编码培训，确保开发人员遵循安全编码规范，使用最新版本编译器。

第十四条 开发环境须与运行环境物理隔离，确保独立性。

第十五条 测试数据的选择及测试结果管理应遵循开发测试管理办法，严格控制数据使用范围。

第十六条 应监督编译过程，确保生成代码的完整性和安全性。

第十七条 原则上不得修改厂商提供的软件包。确需修改时，应满足以下条件:

（一）评估修改对软件包控制措施及完整性的风险。

（二）需获得厂商书面同意，并通过其标准流程实施修改。

第十八条 外包开发需签订协议，明确代码所有权、知识产权及违约处理条款。

第十九条 协议中应明确代码质量标准及编程规范要求。

第二十条 需对外包开发过程实施全程监管，确保符合安全管理要求。

第六章 测试阶段

第二十一条 自行研发系统测试阶段应对安全功能进行全面验证，发现问题需修复后重新验收。

第二十二条 安全管理团队应使用工具进行代码安全验收，并提交验收报告。

第二十三条 外包开发系统交付前需对照设计文档审查功能实现情况及代码质量。

第二十四条 交付前应进行安全评估，检测恶意代码并验证安全功能有效性。

第七章 发布阶段

第二十五条 系统上线前需经开发团队与安全管理团队联合检测，确认无重大安全隐患。

第二十六条 应采用漏洞扫描、渗透测试等手段评估系统整体安全性，并形成《上线安全评估报告》。

第二十七条 发现的安全问题需经评审并修复后，方可允许系统上线。

第八章 运维阶段

第二十八条 运维团队应定期开展漏洞扫描、配置核查等安全检查，保障系统持续安全。

第二十九条 系统变更后需重新进行安全性检测。

第三十条 对检查发现的安全问题应及时预警并修复。

第三十一条 因编码缺陷引发的安全问题，由原开发团队负

责修复。

第九章 持续改进

第三十二条 网络信息中心应根据内外部环境变化，适时修订本规范以保持其有效性。

第十章 附 则

第三十三条 本规范由吉林建筑大学网络信息中心负责解释。

第三十四条 本规范自发布之日起施行。

吉林建筑大学网络信息中心

2024 年 11 月 15 日