北京市工业技师学院

软件更新升级管理制度

**第1章 概述**

第1条  为保证全学院所有计算机系统（包括主机服务器、存储、网络设备、通信设备、个人计算机、系统软件、应用软件等）的正常运行，需要及时更新计算机系统的软件补丁，特制定本制度。

第2条  适用范围：适用于北京市工业技师学院所辖范围系统。

**第2章 跟进和更新**

第3条 系统管理员负责跟进各产品的安全漏洞信息和产品厂商发布的安全更新补丁信息。

第4条 安全补丁根据其对应漏洞的严重程度分为三个级别：紧急补丁、重要补丁和一般补丁；紧急补丁必须在15天内完成加载，重要补丁必须在30天内完成加载，一般补丁要求3个月内完整加载。

第5条 系统管理员分别经主管领导批准后采用公告和邮件形式向相关的业务系统管理员和分公司的信息系统管理部门通告安全补丁信息。

**第3章 获取**

第6条 系统管理员负责从正式渠道获取软件及安全补丁，正式渠道包括集团公司下发的、产品厂商提供的或从产品厂商网站下载的安全补丁。

第7条 系统管理员负责对安全补丁进行完整性校验，确保获取的安全补丁软件未被修改和可用。

**第4章 测试**

第8条 软件及补丁升级加载之前必须经过严格的测试，严禁未经测试直接在生产系统上加载。加载经上级信息系统管理部门测试后下发的补丁可以不做测试。

第9条 补丁测试的方式有两种：实验机测试和现网测试。实验机测试必须进行，实验机配置环境需要与现网环境尽可能一致，并考虑差异性带来的风险；条件允许的情况下（如有测试设备或备机）可以进行现网测试。

第10条 补丁测试的内容包括安装测试、功能性测试、兼容性测试和回退测试： (一) 安装测试主要测试补丁安装过程是否正确无误，补丁安装后系统是否正常运行。 (二) 功能性测试主要测试补丁是否对安全漏洞进行了修补。 (三) 兼容性测试主要测试补丁加载后是否对应用系统带来影响，业务是否可以正常运行。 (四) 回退测试主要包括补丁卸载测试、系统还原测试。

第11条 补丁测试的工作由系统集成商或系统管理员负责实施。必须对补丁的现场测试和现网测试限定时间，测试完成后需要编写详细的测试报告，给出明确的测试结论。

第12条 系统管理员需要把《补丁测试报告》提交部门主管领导进行审核，审核通过后可以进行补丁加载和发布。

第13条 为确保系统集成商及时配合补丁的测试和安装工作，需要通过合同的方式，明确集成商的安全补丁测试和安装责任，约束条款至少应包括：实验机测试环境的构建，在规定时间内完成补丁测试，补丁加载，补丁加载失败时的测试与分析，补丁与应用冲突时的系统改造和升级等工作。

**第5章 安装**

第14条 软件补丁安装前，系统管理员根据需要给出应急措施建议，例如通过加强访问控制、临时关闭服务、加强安全审计等应急措施来加强网络安全，各相关业务系统根据建议采取适当的防护措施，并加强对系统的监控，及时发现和报告安全事件。

第15条 补丁加载前，必须向主管领导提交《安全补丁测试报告》、《安全补丁安装计划和实施方案》、《安全补丁回退实施方案》，经审批通过后按计划执行，审批的周期应限制在2个工作日内，并尽量缩短。

第16条 在补丁安装前，必须做好数据备份工作，确保任何的操作都可回退，在到达回退时间补丁加载没有完成时，启动回退操作，保证业务的正常运行。

第17条 补丁加载必须安排在业务比较空闲的时间进行，对补丁加载的操作过程必须详细记录。同时必须维护已成功加载设备、未加载设备及加载失败的设备清单。

第18条 核心业务主机的补丁加载建议要求厂商工程师现场支持。

**第6章 验证**

第19条 补丁安装完成后，业务系统管理员必需查看系统信息，确保安全补丁已经成功加载。

第20条 必须对加载补丁后的系统按照计划和验证方案进行严格的测试验证，确保补丁加载后不影响系统的性能，确保各项业务操作正常。

第21条 补丁加载后的一周内，系统管理员必须加强对系统性能和事件进行密切的监控。