吉林建筑大学网络安全病毒检测与漏洞扫描管理制度

第一章 总 则

第一条 为确保校园网络与信息系统安全，防范病毒攻击与漏洞风险，保障教学、科研及行政管理活动正常开展，落实《网络安全法》《数据安全法》等法规要求，特制定本制度。

第二条 适用范围。覆盖校内所有网络基础设施（含无线网络）、服务器、终端设备、信息系统（教务、科研、财务等）及接入校园网的第三方系统。主要包含：恶意 IP 地址、恶意电子邮件及程序、应用服务器高危漏洞和弱密码等网络安全隐患。

第二章 管理职责

第三条 由分管校领导牵头，网络信息中心、各部门/单位网络安全工作负责人构成三级管理架构。分管校领导负责统筹安全策略与资源调配。

第四条 网络信息中心负责部署病毒检测与漏洞扫描技术工具，定期执行安全检测，并协调漏洞修复。

第五条 各部门/单位负责配合网络信息中心落实终端设备安全管理，及时上报异常事件。

第六条 全体师生应严格遵守网络安全规范，安装指定防护软件，禁止擅自关闭安全服务。

第三章 病毒检测管理

第七条 检测机制

（一）定期检查信息系统和网站是否存在异常情况。

（二）加强账号及密码管理，杜绝弱密码，重要业务系统管理账号需定期更换密码。

（三）定期对服务器重要数据进行备份。

（四）信息系统发生变更时，需及时更新备案信息，并对新变更部分进行跟踪监测。

（五）确保信息发布前履行审核程序。

（六）定期对服务器操作系统及杀毒软件进行升级。

（七）实时防护：全网部署统一杀毒软件（如 EDR），支持病毒库自动更新与行为分析。

（八）定期扫描：每周对服务器、终端设备执行全盘扫描，重点区域（如数据中心）每日进行增量扫描。

第八条 处置流程。发现病毒后自动隔离，网络信息中心需在 2 小时内定位感染源并通报责任单位；重大病毒事件（如勒索软件）应立即断网，启动应急预案，并于 48 小时内提交溯源报告。

第四章 漏洞扫描管理

第九条 扫描规范。频率：核心系统每月进行一次全面扫描，普通系统每季度一次；重大活动（如招生、考试）前需开展专项扫描。采用合规扫描工具（如 Nessus、OpenVAS），避免对业务系统造成干扰。

第十条 漏洞分级与修复。高危漏洞（CVSS 评分≥7.0）需在 24 小时内制定修复方案，72 小时内完成闭环处理；中低危漏洞需在 15 日内修复，暂无法修复的需采取临时防护措施（如防火墙隔离策略）。

第十一条 第三方系统监管。外包系统需在合同中明确安全责任，上线前需通过渗透测试并提交修复证明。

第五章 预防与应急

第十二条 常态化防护。强制使用复杂密码策略（长度≥8 位，含大小写字母、数字及特殊符号），关键系统启用双因素认证；定期开展师生网络安全培训，组织模拟钓鱼邮件演练。

第十三条 数据备份。核心业务系统每日进行增量备份、每周进行全量备份，离线备份数据保留周期不少于 90 天。

第十四条 应急预案。依据《吉林建筑大学网络安全监测预警通报制度（试行）》，明确病毒爆发、漏洞被利用等场景的处置步骤，每年至少组织 1 次应急演练。

第六章 监督与问责

第十五条 检查机制。随机抽查10%的终端安全状态，检查结果纳入部门年终考核；聘请第三方机构每年开展1次渗透测试与合规审计。

第十六条 责任追究。因未及时修复漏洞导致数据泄露的部门，将予以通报批评并限期整改；故意关闭防护软件或传播病毒者，按校纪校规及相关法律法规追究责任。

第七章 附 则

第十七条 技术层面：构建校园网络安全态势感知平台，联动防火墙、入侵检测系统（IDS）、日志分析系统，实现自动化威胁响应。

第十八条 协同机制：与属地公安网安部门、中国教育和科研计算机网（CERNET）建立情报共享与事件通报渠道。通过本制度，学校可系统性降低网络风险，平衡开放性与安全性，为数字化校园建设提供坚实保障。

第十九条 本制度自发布之日起执行。

吉林建筑大学网络信息中心

2024年11月15日