吉林建筑大学恶意代码防范安全管理规定

第一章 概　述

为加强学校信息系统安全防护，避免遭受恶意代码攻击和病毒感染，特制定本规定。

第二章 工作职责

第一条 网络信息中心统一规划、统一部署具有国家许可的正版计算机防病毒系统软件。所有服务器和终端必须安装学校配发的计算机防病毒软件，否则不允许连入学校网络和处理工作。

第二条 安全管理员的职责

（一）对于尚未进行安全域管理的系统，要定期从相关技术支撑单位获得升级支持。要在第一时间以邮件、书面或短信等方式通知所有负责用户进行升级，收到通知的用户在登录局域网的当天要按照要求进行病毒代码升级，完成后以邮件、书面或短信方式回复安全管理员，安全管理员根据实际情况进行抽查。

（二）及时跟踪解决单位内部员工反映的病毒问题。

（三）及时跟踪防病毒软件的升级情况，并及时将升级的版本及相关措施公布。

（四）对内部员工上报的病毒追踪其根源，查找病毒传播者。

（五）对于不能立即解决的病毒问题，应及时组织协同相关的技术和业务人员进行跟踪解决，在问题解决前尽快采取相应措施阻止事件进一步扩大。

（六）对病毒的爆发时间、爆发现象、清除等信息进行维护、备案，并制作案例。

（七）日常病毒信息的公告和发布。

（八）对本部门员工进行病毒防治的教育和培训。

第三章 恶意代码防范工作原则

第三条 禁止任何员工以任何名义制造、传播、复制、收集恶意代码。

第四条 在发布最新版本杀毒软件后，必须在规定期限内，将个人计算机的杀毒软件升级。

第五条 新购置的、借入的或维修返回的计算机，在使用前应当对硬盘认真进行恶意代码检查，确保无恶意代码之后才能投入正式使用。

第六条 软盘、光盘以及其他移动存储介质在使用前应进行病毒检测，严禁使用任何未经防病毒软件检测过的存储介质。

第七条 计算机软件以及从其他渠道获得的电脑文件，在安装或使用前应进行病毒检测，禁止安装或使用未经检测过的软件或带毒软件。

第八条 安全管理员负责对防病毒软件系统进行监控，并记录病毒查杀情况。安全管理员负责定期对防病毒系统的病毒库进行升级，升级完成后进行记录。

第九条 安全管理员应定期检查信息系统内各种产品的恶意代码库的升级情况。

第四章 工作要求

第十条 网络信息中心向外发布文件或软件时，应该用规定的防病毒软件检查这些文件或软件，有病毒应及时清除，之后才能向外发布。

第十一条 对邮件中的附件在使用之前应该进行病毒检测，收到来历不明的邮件不要打开并及时通知安全管理员处理。

第十二条 如果发现本机感染了病毒，不管病毒从何处传播而来，都应该向安全管理员进行汇报，如果确认从别的机器传播而来的，还应该及时通知该机器的使用者，以便采取相应的防治措施。

第十三条 任何个人不得私自发布计算机病毒疫情。如果发现防病毒软件不能清除的病毒，在病毒得到处理之前，还应禁止使用感染该病毒的文件，同时断开网络连接。

吉林建筑大学网络信息中心

2023 年 10 月 26 日