安徽信息工程学院文件

校信字〔2024〕3号

关于安徽信息工程学院计算机病毒防护管理规定印发的通知

各单位:

为了加强我校计算机信息系统的安全管理，保障计算机信息系统的正常运行，根据国家有关法律法规和学校的实际情况，特制定安徽信息工程学院计算机病毒防护管理规定。现予印发，请遵照执行。本办法自发布之日起执行。

特此通知

安徽信息工程学院

2024年1月20日

安徽信息工程学院
计算机病毒防护管理规定

为了确保安徽信息工程学院信息系统能够连续、高效的运行，保证网络和信息的安全，参照相关标准，结合工作实际，特制定本规定。

第一条 采用国家许可的正版防病毒软件，并设置相应的病毒防范策略，通过授权后，方能使用。

第二条 网络安全人员应具有较强的网络安全和病毒防范意识，严格执行本规定，定期进行网络病毒检测并保存检测记录，发现病毒或病毒预警，应立即采取有效措施，保障系统安全。

第三条 提高安徽信息工程学院所有用户的防病毒意识，应定期进行安全意识培训，及时告知防病毒软件版本，在读取移动存储设备上的数据以及网络上接收文件或邮件之前，先进行病毒检查，对外来计算机或存储设备接入网络系统之前也应进行病毒检查。

第四条 未经批准，不得在服务器系统上安装新软件，确因工作需要安装，安装前应进行病毒例行检测。

第五条 病毒防护人员必须定期做好服务器操作系统、业务数据库系统和应用系统的安全补丁、漏洞检测及修补、病毒防治等维护工作。

第六条 病毒防护人员必须定期自动或手动更新防病毒

软件版本及病毒码引擎。

第七条 计算机系统终端用户不得随意退出防病毒软件、实时监控系统，不得随意安装新软件。

第八条 严禁浏览和工作内容无关、含有恶意代码以及安全级别较低的网页，严禁阅读和下载来历不明的电子邮件和文件，严格控制并阻断计算机病毒的来源。

第九条 严禁在办公计算机上使用自带软盘、光盘、优盘等存储设备，防止病毒感染。

第十条 病毒防护人员应密切关注计算机病毒的最新信息和动态趋向，做到预防为主。

第十一条 网络安全人员应当严格设置防火墙管理策略，防止网络攻击。察觉到网络处于被攻击状态后，网络安全人员应确定其身份，对其发出警告，同时在保护系统安全的情况下封锁被攻击端口，并向主管领导汇报。

第十二条 病毒防护人员要每月检查信息系统内各种产品的恶意代码库的升级情况并进行记录，对主机防病毒产品、防病毒网关和邮件防病毒网关上截获的危险病毒或恶意代码进行及时分析处理，并形成书面报表和总结，提交给安全管理员。

第十三条 各部门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。

第十四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。

第十五条 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报告，如果确认从别的机器传播而来的，应及时通知该机器的使用者，以便采取相应的防治措施。

第十六条 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，在问题处理之前，应禁止使用感染该病毒的文件，同时断开网络连接。

第十七条 智慧校园建设办公室指定专人对网络和主机进行恶意代码检测并保存检测记录。

第十八条 计算机操作人员有义务接受信息安全工作小组组织的恶意代码防范、防治的教育和培训。

第十九条 本规定最终解释权归安徽信息工程学院智慧校园建设办公室。

第二十条 本规定即日起执行。