防灾科技学院信息化管理中心

信息中心〔2021〕15 号

关于印发《防灾科技学院信息系统恶意代码防范管理》的通知

学校各部门、各单位：

为加强学校信息系统安全保护，避免遭受恶意代码攻击和病毒感染，特制定《防灾科技学院信息系统恶意代码防范管理》，现予印发，请遵照执行。

防灾科技学院信息化管理中心

2021 年 10 月 7 日

防灾科技学院信息系统恶意代码防范管理规定

第一章　总则

第一条　为加强防灾科技学院（以下简称“学院”）信息系统安全保护，避免遭受恶意代码攻击和病毒感染，特制定本规定。

第二条　本规定适用于学院所有单位及个人。

第二章　恶意代码防范措施

第三条　禁止以任何名义制造、传播、复制、收集恶意代码。

第四条　每台计算机必须安装信息化管理中心指定的防病毒软件。未经许可，不得随意下载使用标准规定之外的防病毒软件或病毒监控程序。

第五条　在发布最新版本杀毒软件后，必须在一周内对杀毒软件进行升级。

第六条　防病毒网关以及杀毒软件需启用实时更新功能，保证恶意代码库实时更新。

第七条　新购置的、借入的或维修返回的服务器，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。

第八条　软盘、光盘以及其它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。

第九条计算机软件以及从其它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。

第十条　必须遵守软件使用许可，禁止使用未授权的软件。

第十一条 对员工进行恶意代码防范意识教育培训，提高所有用户的防病毒意识，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，先进行病毒检测，对外来计算机或存储设备接入网络系统之前也进行病毒检查。

第三章 工作职责

第十二条 安全管理员的职责：

（一）定期每月查看一次防病毒网关日志文件；

（二）及时跟踪解决发现的病毒问题；

（三）及时跟踪恶意代码库的升级情况；

（四）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；

（五）对病毒的发作时间、发作现象、清除等信息的进行维护、备案、并制作案例；

（六）日常病毒信息的公告和发布。

第三章 工作要求

第十三条 向外发布文件或软件时，应该用规定的防病毒软件进行检查，如有病毒应及时清除，之后才能向外发布。

第十四条 如发现服务器感染病毒，应及时采取相应的防治措施。

第十五条 升级杀毒软件的病毒库。启用杀毒软件的自动升级病毒库功能，并设定自动升级的时间，可设置自动更新病毒库的时间为每天、每周或每月，原则上每周应该升级一次病毒库；保证防病毒服务器能连接

到杀毒软件厂商的升级网站，进行病毒库更新；安装网络版杀毒软件客户端接受防病毒服务器的统一管理，及时从防病毒服务器下载最新病毒库进行更新。

第十六条 应定期每周对网络和主机进行恶意代码检测并保存检测记录。

第十七条 用于远程管理信息系统服务器的计算机应安装防病毒软件，并升级至最新的恶意代码库。

第十八条 对系统增加的软件包应先进行恶意代码检测。

第五章 附则

第十九条 本规定由信息化管理中心负责解释。

第二十条 本规定自发布之日起生效。

防灾科技学院信息化管理中心 2021 年 10 月 7 日印发