

中国地质大学（北京）

信息网络中心文件

信息网络中心

2020. 9. 21

中国地质大学（北京）病毒防范管理制度

第一章 总则

第一条 为了预防病毒与各种恶意软件的入侵，提高中国地质大学（北京）服务器及终端对病毒的抵抗能力，保障中国地质大学（北京）的业务系统和日常工作的正常进行，特制定本制度。

第二条 本制度适用于中国地质大学（北京）所管署信息系统的所有可能被病毒危害的资产。

第三条 安全管理员负责信息系统防病毒工作，监督防病毒软件的安装、病毒库的更新管理和定期排查，以及提供其它相关技术性支持。各处室负责本处室的防病毒及相关预防措施的实施。

第二章 防病毒控制措施

第四条 每台计算机必须安装指定的防病毒软件。

第五条 必须遵守软件使用许可，禁止使用未授权的软件。

第六条 对于从外部获得数据（光盘、磁盘、U 盘等媒体，以及电子邮件等）必须经过病毒检查才能在处室内部使用。

第七条 安全管理员负责计算机病毒防范,负责防毒软件的升级、维护,病毒信息获取与提前防护,以及对病毒事件的处理。

第八条 每周检查信息系统内各种产品的恶意代码库的升级情况,并填写《杀毒软件升级记录》,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,并形成书面的报表和总结汇报。

第九条 安全管理员负责对系统所出现的病毒作记录,并纠察其原因。

第十条 各处室应及时报告病毒攻击事件,安全管理员负责协助对受攻击的计算机系统进行恢复。

第三章 防病毒操作程序

第十一条 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,原则上每三天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;安装了网络版杀毒软件客户端的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。如果软件不能自动升级,到杀毒软件厂商的网站手工下载升级包并手工升级病毒库。

第十二条 使用杀毒软件扫描所有的硬盘分区,以发现硬盘中可能存在的病毒或异常情况;对外来的软盘、光盘和其它介质、电子邮件和从互联网下载的文件做病毒检查;定期或不定期地进行磁盘文件备份工作,重要的数据应当定期备份,备份前先要进行查病毒工作;对新购置的计算机软件在使用前也要进行病毒检测。注意扫描出来的新病毒。

第十三条 记录杀毒日志。将杀毒日志记录人信息处理设施中导出来，并作保存。如果不能从计算机中导出杀毒日志记录，则管理员手工填写《杀毒日志记录》。

第十四条 信息化建设处定期组织对所有计算机进行扫描；用户发现不可清除的病毒和异常情况时，及时报告给安全管理员，安全管理员及时对用户报告的病毒事件进行响应，并记录病毒检测和处理的情况，填写《病毒事件响应记录》。病毒异常情况包括：

1. 系统运行速度比平时明显变慢。
2. 有打印、显示异常现象。
3. 文件夹下有不明的文件自动生成。
4. 磁盘空间自动产生坏簇或磁盘空间无故减少。
5. 系统文件无故丢失。
6. 系统异常死机的次数增加。

第四章 附则

第十五条 本制度由中国地质大学（北京）信息网络中心负责解释。

第十六条 本制度自发布之日起施行。

附件：

病毒事件响应记录

杀毒日志记录

病毒事件响应记录

编号：

病毒名称		病毒类型	
报告阶段			
事件简要描述：			
报告人		报告时间	
部门		电话	
响应阶段			
病毒检测和处理情况：			
操作人		操作时间	
部门		电话	
备注：			

