恶意代码防范管理规定

（V2.1，2021年10月16日修订）

## 第一章 总则

1. 为加强北京工商大学信息系统安全保护，避免遭受恶意代码攻击和病毒感染，特制定本规定。
2. 本规定适用于北京工商大学所有单位及个人。

## 第二章 恶意代码防范措施

1. 防恶意代码指导方针：构建以预防为主、防杀结合的计算机恶意代码管理与应急处理机制，全面落实“早发现、早报告、早隔离、早防杀”的防恶意代码工作原则，提高快速反应和应急处理能力，将防治工作纳入科学化和规范化的轨道，保障信息系统的安全性和稳定性。
2. 禁止以任何名义制造、传播、复制、收集恶意代码。
3. 每台计算机必须安装具有计算机信息系统安全专用产品销售许可证的计算机防恶意代码产品，不得下载使用其他防病毒软件或病毒监控程序。
4. 定期检查信息系统内各种产品的恶意代码库的升级情况。
5. 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。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。
6. 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。
7. 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。
8. 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。
9. 必须遵守软件使用许可，禁止使用未授权的软件。

## 第三章 工作职责

1. 安全管理员的职责：

（一）每月定期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。

## 第四章  工作要求

1. 向外发布文件或软件时，应该用具有计算机信息系统安全专用产品销售许可证的计算机防恶意代码产品进行检查，如有病毒应及时清除，之后才能向外发布。
2. 如发现服务器感染了病毒，应及时采取相应的防治措施。
3. 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。
4. 应定期对网络和主机进行恶意代码检测并保存检测记录。
5. 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。
6. 对系统增加的软件包应先进行恶意代码检测。

## 第五章 附则

1. 本规定的解释权归北京工商大学信息网络中心。
2. 本规定自发布之日起生效。