**13 恶意代码防范管理规定**

**第一章 总则**

1. 为提升北京大学网络安全防护能力，避免遭受恶意代码攻击，特制定本规定。
2. 本规定适用于北京大学所有单位及个人。

**第二章 恶意代码防范措施**

1. 禁止以任何名义制造、传播、复制、收集恶意代码。
2. 计算机应安装正版防病毒软件。在发布最新版本杀毒软件后，应及时对杀毒软件进行升级。
3. 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方可投入正式使用。
4. 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。
5. 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。
6. 必须遵守软件使用许可，禁止使用未授权的软件。

**第三章**  **工作要求**

1. 通过网站、邮件等途径向外发布文件或软件时，应先开展防病毒检测。
2. 对系统增加的软件包应先进行恶意代码检测。
3. 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。
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. 服务器应根据业务需要，采取恶意代码防范措施。如发现服务器感染了病毒、木马，应及时治理。

**第四章 附则**

1. 本规定是《北京大学网络安全管理办法》（试行）配套系列制度之一，从属于《北京大学网络安全管理办法》（试行）。
2. 其他校区参考本规定制定相应管理规定。
3. 本规定由北京大学网络安全和信息化委员会办公室及北京大学计算中心负责解释。
4. 本规定自发布之日起施行。