**漏洞和安全预警管理规定**

**第一章 总则**

1. 为保障北京大学信息系统安全、稳定运行，加强漏洞处置和安全通报预警管理，特制定本规定。
2. 本规定适用于北京大学所有单位。

**第二章 漏洞和补丁管理**

1. 安全管理员、信息系统管理员应关注信息系统及其相关组件（操作系统、数据库、中间件、第三方组件）可能存在的漏洞，及时接收来自外部、网信办、计算中心的安全漏洞预警。
2. 系统运维单位应及时采取措施修复安全漏洞，可采取补丁升级、系统环境配置更改、安全防护策略配置等策略，降低漏洞利用可能性。
3. 补丁管理原则：
4. 及时性原则：确保及时准确地安装必要的安全补丁，把安全漏洞对信息系统的潜在威胁降到最低；
5. 严密性原则：提前制定补丁测试和分发计划，在保障安全的同时不影响生产和应用系统的正常运行；
6. 持续性原则：补丁管理工作是长期持续的工作，安全管理人员应定期跟踪厂商的补丁公告和安全公司的安全公告；
7. 适应性原则：根据不同的场景执行安全补丁管理要求。
8. 各信息系统管理员、网络管理员应确保补丁程序来源可靠，建议从厂商官方网站下载。对于支持校验的补丁程序，必须先校验可靠性，防止下载被恶意篡改后的补丁程序。安全管理员应根据最新的补丁通告信息，指导和组织各信息系统的安全补丁安装工作。
9. 系统补丁须预先在测试环境运行，确保不影响应用系统正常运行后，方可在生产系统实施。严禁未经测试直接在生产系统加载补丁。重要系统补丁升级前，应制定升级方案和恢复方案，对系统重要文件进行备份。
10. 完成补丁测试后，经相关主机系统管理员、应用系统管理员确认未发现问题后，根据漏洞威胁的紧急程度，制定补丁分发计划，根据实际情况在生产系统中分批安装。补丁加载的操作过程应按照计划严格操作，并详细记录。
11. 对于一些不能解决的补丁安装问题，需采用应急方案，使用备份系统或者卸载补丁，同时需确定临时解决办法消除漏洞潜在威胁，并尽快向补丁厂商寻求技术支持。

**第三章 安全通报预警**

1. 网信办负责北京大学网络安全通报预警工作组织；计算中心负责安全通报预警技术支持。
2. 系统运维单位应关注本系统存在的漏洞和风险，接收来自学校相关单位通报的安全风险，3个工作日内处置并反馈处理结果。
3. 系统运维单位的安全管理员负责本单位所有系统安全漏洞的协调处置并反馈。网信办负责对接上级单位，接收安全问题并反馈整改情况。存在高危漏洞的信息系统必须在3个工作日内完成整改，否则将对系统暂停对外服务。
4. 信息系统管理员应及时关注本系统所使用的操作系统、数据库、中间件、第三方组件等爆发的新漏洞和威胁，对可能影响的安全漏洞、事件及时处置。

**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。

本规定自发布之日起施行。