**7 主机系统安全管理规定**

**第一章 总则**

1. 为加强北京大学信息系统安全管理，明确岗位职责，规范操作流程，维护系统正常运行，确保主机系统的安全，特制定本规定。
2. 本规定中所述人员职责参见《北京大学网络安全管理办法·网络安全工作人员管理规定》；本规定中所述信息系统定义参见《北京大学网络安全管理办法·信息系统建设安全管理规定》。
3. 本规定适用于北京大学所有单位。

**第二章 安全策略与配置**

1. 由信息系统管理员根据业务需求和系统安全分析制定主机系统的访问控制策略，控制分配信息系统、文件及服务的访问权限。
2. 由安全管理员组织定期对系统进行漏洞扫描，并形成漏洞扫描报告，内容包含系统存在的漏洞、严重级别等方面。安全管理员及时通知系统管理员修补发现的安全漏洞，并通报处理结果。
3. 系统安全配置由系统管理员负责，在安全管理员指导下完成，其余任何人不得随意更改配置。
4. 系统管理员应对服务器安装防火墙或杀毒软件，定期对服务器系统、杀毒软件等进行升级和更新，并进行病毒清查，禁止下载和使用未经测试和来历不明的软件，禁止随意使用U盘等移动存储介质。
5. 应保留安全配置更改记录，由安全审计员负责审计。
6. 任何人员不得制造或故意输入、传播计算机病毒和其他有害数据，不得利用非法手段复制、截收、篡改计算机信息系统中数据。

**第三章 补丁管理**

1. 应根据《漏洞和安全管理规定》中对漏洞和补丁管理的相关要求，开展漏洞修复、补丁升级测试、数据备份、补丁更新操作。
2. 主机系统批量补丁升级，应先完成补丁测试；经信息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。
3. 安全管理员应督促本单位办公环境计算机安装安全补丁。

**第四章 账号安全**

1. 主机系统管理员负责该主机操作系统用户账号的申请、删除、禁用、口令重置以及权限复审等操作，并在系统中保存操作记录。
2. 系统管理员每半年对操作系统用户账号使用情况进行一次检查，及时禁用、删除系统中的空账号、临时账号等存在安全隐患的账号。
3. 系统管理员每年对操作系统用户账号权限进行一次检查，根据用户的安全责任和工作要求对其身份以及相应的权限进行变更。
4. 做好对特殊用户和用户组的管理，包括超级用户、访客用户、匿名用户以及缺省帐户的安全管理。

**第五章 日志管理**

1. 系统管理员对系统进行维护，详细记录操作日志，包括重要的日常操作、运行维护记录、参数的设置和修改等内容，严禁进行未经授权的操作。
2. 安全审计员定期对运行日志和审计结果进行分析，并形成分析报告，报告内容包括帐户的连续多次登录失败、访问受限系统或文件的失败尝试、系统错误异常事件。

**第六章 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。