**网络环境安全管理规定**

**第一章 总则**

1. 为提高北京大学信息系统所在网络环境的安全性，降低信息系统安全风险，确保信息系统在可靠环境下运行，特制定本规定。
2. 本规定适用于北京大学所有单位。

**第二章 网络运维管理**

1. 计算中心指定专人负责校级网络和信息系统安全运维和监控，为二级单位相关工作提供技术支持。二级单位负责本单位网络的安全运维和监控。运维单位应通过网管系统对通信线路、网络设备、主机系统和应用软件的运行状况进行实时监测，形成监测记录，保障各项业务的正常运行。
2. 网络运维单位应定期分析监测记录，对设备状态、网络流量、恶意代码、补丁升级等安全事项进行评测，发现可疑行为和安全隐患，主动采取必要措施。
3. 网络运维单位应制定运维工作计划，根据运维执行情况形成安全运维报告，包含但不限于：设备维护、安全监控、操作日志、日志审核、故障管理、系统升级、应急处置等内容。

**第三章 网络及安全设备管理**

1. 应按照分层设计、区域划分的原则规划网络拓扑结构，保证核心网络稳定可靠，接入网络安全运行。网络拓扑结构应便于扩充和管理、易于问题排查和故障隔离。网络管理员应定期分析网络性能，了解系统资源使用情况及通信效率，提出网络优化方案。
2. 应合理配置边界访问控制设备，通过访问控制技术保护重要网段，实现与其它网段的访问隔离，仅开放必要的端口和服务。
3. 网络拓扑结构、IP地址等信息属于系统运行相关关键信息，应在一定范围内予以保密。
4. 严格按照流程执行网络和安全设备的安装、配置、变更、撤销等操作。
5. 按照最小服务原则为每台网络和安全设备进行配置。

**第四章 用户账号管理**

1. 遵循最小授权原则，设置网络设备登录账号的权限级别。
2. 保证用户身份标志的唯一性，即不同的个人用户必须采用不同的用户名和口令登录设备，拥有不同的权限级别。在设备日志上记录用户登录操作，便于问题追查。
3. 网络管理员拥有网络设备的超级用户权限，不得私自为其他人开通管理权限。
4. 网络管理员口令应遵循《口令管理规定》中对基础设施管理员口令的要求。

**第五章 配置文件及日志管理**

1. 修改网络和安全设备配置信息需经相关运维部门集体讨论，获得批准后方可实施，并详细备份修改前及修改后配置信息文档。
2. 需定期备份网络和安全设备配置文件，并以电子文档形式保存。
3. 网络管理员须定期查看设备日志文件，及时发现异常情况，尽早消除安全隐患。
4. 网络管理员应定期备份网络设备日志文件，至少保存6个月日志记录。

**第六章 设备软件及登录管理**

1. 根据设备厂商稳定版本的发布情况，统筹安排网络和安全设备软件版本升级，降低安全隐患。
2. 网络和安全设备开启远程登录时需采用加密通信信道，并限定可远程登录主机，拒绝潜在攻击者，保证网络安全。

**第七章 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。