8.信息系统安全运维管理规定

第一章　总则

第一条　为保障北京大学信息系统运维过程中的安全，确保系统业务连续性和数据安全，特制定本规定。

第二条　涉及校务信息数据的采集编目、共享应用，按照《北京大学校务数据管理办法》执行。

第二章 日常维护

第三条　信息系统运维应遵照以下安全原则：

（一）最小权限原则：指在保证信息系统运行正常的前提下，只能授予管理员和用户必要的权限；

（二）最少服务原则：指在保证信息系统运行正常的前提下，关闭其它无关的系统服务和网络服务。

第四条　对信息系统的后台访问，应通过堡垒机认证后方可进行。

第五条　系统运维原则上应避免从校外远程访问，如因工作需要必须远程运维，须经信息系统管理员同意，并在访问结束后及时关闭远程访问通路，并记录访问结束时间。

第六条　信息系统管理员口令管理应遵循《口令管理规定》中相关要求。

第七条　信息系统管理员应定期对配置文件、应用程序文件进行备份。

第八条　信息系统管理员定期填写《信息系统安全巡检记录》（见附件一），对系统运行状况，如系统可用性，操作系统/数据库的CPU、内存、磁盘空间，系统用户账号，可疑进程等进行监控和分析，及时

上报安全隐患。

第九条　信息系统管理员应启用系统安全审计功能，以日志的形式记录用户登录系统、访问操作、账户修改等行为的过程和结果信息，做到发生可疑事件时有据可查。

第十条　信息系统管理员应确保审计记录集中存储在日志审计系统或日志服务器中，至少保存六个月。审计记录包括信息系统操作日志、WEB 系统中间件访问日志、操作系统日志、数据库日志等。

第十一条　信息系统管理员应关注系统主机、数据库、应用层面存在的安全漏洞、隐患，按照《漏洞和安全预警管理规定》中对漏洞发现、补丁升级和安全预警通报机制的要求，对安全漏洞及时整改。

第十二条　信息系统发生安全事件时，信息系统管理员应根据《安全事件处置管理规定》中相关要求，以及应急预案开展安全事件应急响应。

第三章 运维外包

第十三条　信息系统主管单位在实施日常运维外包前，应对服务提供商资质进行审查，应与服务提供商明确签订服务合同，根据服务需求、风险评估和资质审查结果确定实施重点和细节，确保实施质量。

第十四条　信息系统主管单位应当在合同或协议中明确服务提供商在网络安全和保密方面的责任，相关措施包括但不限于：

(一) 服务提供商具备运维安全相关资质；

(二) 禁止服务提供商在合同范围内使用或披露信息系统内数据和信息，防止数据和信息被非授权使用；

(三) 在合同或协议中约定服务提供商不得以本单位名义开展活

动；

(四) 当信息系统发生安全事件时，服务提供商应第一时间向本单位报告事件发生和整改方案，并在事件处置结束后报告处置措施。

第十五条 信息系统主管单位应制定和落实网络安全管控措施，防范因外包活动引起的信息泄露、信息篡改、信息不可用、非法入侵、物理环境或设施遭受破坏风险，定期对服务提供商进行安全检查、获取服务提供商自评估或第三方评估报告。

第十六条 信息系统主管单位应根据合同或协议建立明确的服务监控指标，对外包服务进行持续监控，及时发现和纠正服务过程中存在的异常情况。

第十七条 信息系统主管单位每年对服务提供商的工作完成情况、服务水平、服务质量、用户满意度、是否符合合同或协议的质量标准等各方面进行考核和评估。

第十八条 如外包服务无法满足要求或发生重大事件，信息系统主管单位应在充分评估其影响及制定退出计划的前提下，考虑主动要求服务提供商终止服务。

第十九条 信息系统主管单位应针对外包服务中断的场景，拟定相应的应急计划，并定期进行演练。

第三章 重要变更

第二十条 信息系统发生应用层面变更时，如功能模块调整、版本升级等，应由系统管理员和系统运维单位讨论实施。

第二十一条 信息系统发生基础设施层面变更时，如需调整网络策略、变更对外开放端口和服务、变更访问控制策略、系统迁移等，

应参考《变更管理规定》执行，并填写《变更申请审批表》。

第二十二条 系统变更可能影响学校师生服务和管理活动时，应提前通知可能涉及的学校各二级单位、教师和学生。重要变更应事先制定变更方案，做好系统和数据备份，明确回退程序。

第二十三条 系统变更对服务造成影响的，应立即采取措施解决问题或采用恢复、回退等方式，降低影响、恢复服务。

第四章 系统停用

第二十四条 停用告知。信息系统主管单位在系统停用前，应向信息系统的用户做好解释与说明工作，确保所有用户都知晓。

第二十五条 停止服务。信息系统主管单位指导信息系统运维单位停止系统的日常服务与运维，关停信息系统的互联网访问服务。合理处置信息系统所用的 IP 地址、计算、存储等资源。

第二十六条 注销备案。信息系统主管单位应在系统关停后一个月内，登录备案系统进行系统注销操作同时注销域名。等保定级为二级及以上系统，由网信办统筹向公安机关申请办理撤销系统的网络安全等级保护备案。

第五章 附则

第二十七条 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）。

第二十八条 其他校区参考本规定制定相应管理规定。

第二十九条 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。

第三十条 本规定自发布之日起施行。

附件一 《信息系统安全巡检记录》

系统名称	
巡检日期	
网络信息	
可用性	☐ 未发生中断 □发生中断 中断时间_____
IP 地址	
端口开放	互联网开放服务端口_____
存在漏洞情况	☐ 未发现高危漏洞 ☐ 高危漏洞，尚未整改 漏洞名称_____ ☐ 高危漏洞，已整改 漏洞名称_____
存在安全事件情况	☐ 未发现安全事件 ☐ 发现安全事件—挂马 ☐ 发现安全事件—植入暗链 ☐ 发现安全事件—页面篡改 ☐ 发现安全事件—数据泄露 ☐ 其他安全事件_____ 安全事件处置情况_____