中国地质大学（北京）

信息网络中心文件

信息网络中心　　2020.9.21

中国地质大学（北京）漏洞和风险管理制度

第一章　总则

第一条　为保障中国地质大学（北京）信息系统安全、稳定运行，加强漏洞处置和风险管理，特制定本规定。

第二条　本规定适用于所有处室。

第三条　信息网络中心对此规定在中国地质大学（北京）的落实情况进行监督检查。

第二章　漏洞与补丁管理

第四条　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，及时接收来自外的安全漏洞预警。

第五条　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。

第六条　补丁管理原则：

1. 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；

2. 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；

3. 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；

4. 适应性原则：根据不同的场景执行安全补丁管理要求。

第七条 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。

第八条 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。

第九条 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。

第十条 对于一些不能解决的补丁安装问题，需采用应急方案，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　服务供应商选择管理措施

第十一条　风险管理是指导和控制组织风险的过程。风险管理遵循管理的一般循环模式—计划、执行、检查、行动的持续改进模式。

第十二条　针对风险评估的范围，开展详细的风险分析，包括业务影响分析。

第十三条　定期聘请第三方单位开展安全测评工作，针对报告发现的安全问题采取相应的措施进行整改。

第四章　附则

第十四条　本规定由信息网络中心负责解释。

第十五条　本制度自发布之日起施行。