

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）系统安全管理制度

第一章 总则

第一条 为了明确中国地质大学（北京）所管署信息系统的维护内容，使信息系统运行维护工作制度化、规范化和科学化，确保系统安全可靠运行，特制定本制度。

第二条 本制度适用于中国地质大学（北京）信息系统的日常运行与维护。

第二章 信息系统维护基本要求

第三条 信息系统的维护应满足以下基本要求：

1. 系统应具有可维护性：具体包括系统应具备故障恢复的能力，必须制定合理的应急方案与措施以便在发生系统故障时，可以有效的恢复关键业务、应用及数据；具备对重要数据进行备份及恢复的能力；具备业务的可维护性，性能的可测试性，结果的可统计性，突发事件的可控制性，业务发展的可预测性等能力。
2. 系统的维护必须规范化、制度化：系统的各项维护工作如日检查、故障处理、账号管理、数据配置等工作要有明确的工作流程和考核标准，以规范维护工作，明确职责，奖优罚劣，确保系统安全可靠运行。

3. 定期进行安全漏洞扫描，并对发现的安全漏洞和隐患及时进行修补，或者对漏洞或隐患评估可能的影响后进行修补。

第三章 例行检查

第四条 定期对信息系统进行例行检查，相关人员的职责如下：

1. 信息系统负责人职责：

- 与运维人员共同制定例行检查作业计划，对检查执行情况进行监督和考核。

2. 维护人员职责：

- 制定检查作业计划，定期检查以下内容：
 - 物理层检查：检查门户网站系统设备相关物理环境，设备板卡、设备相关线缆等是否工作正常。
 - 系统层检查：检查各个设备主机的操作系统、CPU、磁盘、内存、日志、备份等是否工作正常。
 - 网络层检查：检查网络设备的CPU、内存、磁盘、日志、备份等运行情况，对网络设备的时延、丢包率进行检测，对系统内网的联通性进行检测。
 - 应用层检查：检查业务进程运行状况，业务功能运行状况，业务软件的日志、备份情况。
- 执行预防性维护工作，具体包括：
 - 应及时清理磁盘文件，删除过时或无用的系统数据文件和程序。应保证磁盘空闲空间 $\geq 20\%$ 。
 - 每日日志的备份与整理。
 - 每周对整个系统进行一次病毒检查与治理。
 - 每周对所有网络设备的配置进行备份。
- 对信息系统主机进行预防性维护：
 - 每天对所有主机进行系统日志的备份。

- 每周对硬盘参数、计算机引导区参数、系统文件及其他数据进行数据备份，以便发生大故障时恢复计算机正常工作。
- 每半月对系统的服务器数据进行整理，清除无用的数据，修复错误的数据，维护系统的稳定性。
- 每半年对系统中的硬件进行清洗，保持各硬件清洁干净，有效保护硬盘等易损硬件，延长硬件的工作寿命。
- 每半年整理在线的网线、电缆编号，对网线、电缆进行性能测试。
- 定期向信息系统负责人提交检查作业记录。

第四章 日常管理

第五条 加强系统安全管理，具体内容包括：

1. 信息系统负责人职责：
 - 对系统安全管理及实施情况进行监督。
2. 运维人员职责：负责保障系统安全、可靠地运行，具体要求包括：
 - 对设备的账号口令的管理应遵循最小适用原则。必须仅仅限于分配给必须需要这些权限工作的人，并仅分配需要的最小权限。各个系统设置不同的密码，密码的设置及修改应遵循《账号管理制度》和《密码管理制度》。
 - 网络设备和主机的操作系统及重要应用程序等安装最新的安全补丁，无严重安全漏洞，并提供系统漏洞及相应补丁跟踪办法。
 - 安装防病毒软件，定制合理的病毒查杀策略和病毒库升级策略，并有补救和修复措施，确保感染病毒后可修复受影响的系统。
 - 删除不必要的网络协议和服务，无用途不明的端口开放，关闭远程服务端口。仅开放保证系统正常运行的最少的端口和服务，减少系统的安全隐患。
 - 利用防火墙的访问控制策略、主机系统访问控制机制和路由器的

ACL 等各种网络层面的手段共同达到阻挡非授权访问的目的，加强主机安全性。

- 不安装无关软件，无垃圾数据。
- 系统中使用的软件都必需是合法授权的，都必须有高的安全标准和兼容性。不安装与所提供业务无关的软件。
- 采用自检及专业安全评估工具相结合的方法，对应用程序及数据库的配置、业务逻辑进行检测，减少系统应用层安全隐患。
- 建立渠道保证及时，准确地收集安全预警信息，包括最新的安全漏洞，病毒，安全补丁，最新的入侵手法，例如通过系统供应商，重要的安全信息网站等。
- 按照脆弱性评估或安全测评结果，对系统进行安全整改。

第六条 对系统配置数据进行管理，主要工作内容包括：

1. 信息系统负责人职责：

- 对系统配置数据的变更进行审批。

2. 运维人员职责：

- 网络、系统方面的配置，例如网络设备、主机等硬件设备策略和端口的配置，网络时钟同步，IP 地址的分配和管理等。
- 业务应用层面的配置，如系统运行库、源程序、脚本、页面文件等的配置。

第七条 对软件版本的升级管理，主要工作包括对主机、数据库、网络设备、应用软件等进行版本更新和补丁加载、向主管人员提交软件版本更新和补丁加载的升级申请、升级具体实施、相关文档保存等，应依照《系统变更操作规程》执行。

第八条 加强对维护档案和技术资料的管理。技术档案、资料和原始记录是进行质量管理、统计分析、做好经常性维护工作的重要依据。必须

做到记录和统计及时、准确，技术档案和资料应完整，并妥善保管。

1. 信息系统负责人职责：负责系统维护档案和技术资料的保存管理工作。系统维护档案和资料项目如下：

- 系统设备的说明书，图纸，维护手册；
- 系统数据和用户数据及系统软件和应用软件；
- 机房内布线系统图，包括通信系统、信号电源、电力及照明等布线系统图；
- 机房平面图，包括数据通信机房分布平面位置，机房内机架及设备所在位置图；
- 工程技术设计、施工、竣工资料和验收记录等；
- 网络系统拓扑结构图，IP 地址的分配情况；
- 电源，配线设备的接线记录；
- 应急处理方案；
- 系统重大故障报告及原始记录；
- 系统操作权限及口令字；
- 软件版本升级报告等相关文档；
- 各项测试记录；
- 新功能上线测试报告；
- 各种有关规章制度：有关专业的技术维护规程和维护技术指标，业务规程，各种责任制度及技术文件等。

2. 维护人员职责：负责维护档案和技术资料的搜集、整理及更新工作。并将更新的系统数据资料内容及时提交给项目负责人，由信息系统负责人统一归档保存。

第九条 提供技术支持，主要工作内容包括：

1. 信息系统负责人职责：

- 审核维护人员关于系统优化的建议，并监督具体实施。

- 向维护人员提出投诉处理、业务数据统计分析及其它相关配合工作需求，并监督完成。

2. 维护人员职责：

- 系统优化：定期对信息系统主机设备、操作系统、数据库、应用相关产品的性能、指标、运行状态进行评估和分析，调整系统配置，提高系统运行质量和稳定性。
- 投诉处理：对用户投诉进行原因分析，并给出合理的解释。如果属于故障，则进行故障处理。
- 系统升级改造：根据用户的要求，结合业务统计分析数据，对系统进行升级。
- 其它配合工作：包括配合安全测评，与系统相关的其它系统或网元调整、割接的配合支持等。

第五章 附则

第十条 本制度由中国地质大学（北京）信息网络中心负责解释。

第十一条 本制度自发布之日起执行。