

中国地质大学（北京）

信息网络中心文件

信息网络中心

2021. 11. 9

中国地质大学（北京）人员安全管理规定

第一章 总则

第一条 为适时对中国地质大学（北京）信息系统建设及维护工作人员进行安全管理，提高工作人员网络安全方面的业务水平、操作技能和协同能力，提升管理水平，特制定本规定。

第二条 本规定适用于中国地质大学（北京）内部工作人员及外部第三方人员的安全管理。

第三条 信息网络中心负责所管署信息系统人员安全管理和第三方人员的安全管理。

第二章 人员入职管理

第四条 由中国地质大学（北京）人事部门负责人员的录用，录用的过程中国地质大学（北京）人事部门规定执行。

第五条 信息网络中心对本校工作人员进行职责分工，设置网络管理员、系统管理员、安全管理员。清楚定义每位人员的安全职责，并填写《岗位网络安全职责说明书》。

第六条 关键岗位人员在试用期满后，信息网络中心安排专人对其进

行专业知识、动手能力等全面的考核。

第三章 培训管理

第七条 信息网络中心应定期对全体工作人员进行安全教育和培训，针对不同岗位制定不同的培训计划，对网络安全基础知识、岗位操作规程等进行培训。

第八条 信息网络中心负责制定网络安全的年度培训计划，在识别各岗位的培训、考核要求以及所需的频次后，制定年度培训计划，并保证计划的合理性，培训计划中应明确培训时间、地点、培训内容、授课教师、培训对象等。

第九条 信息网络中心对关键岗位人员定期进行相关培训：

- （一）对关键岗位人员进行专业理论与操作的培训。
- （二）对新入职关键岗位人员应注重其工作态度、学习能力、接受能力、动手能力、组织能力、沟通及协调能力、团队精神等方面的考察，全面了解人员的能力、潜力及试用动态。

第十条 信息网络中心对关键岗位人员定期进行相关考核：

- （一）对所有网络安全管理人员进行全面、严格的安全审查（安全知识、安全技能、操作行为、社会关系、社交活动等）。
- （二）定期对网络安全管理各个岗位的人员进行安全技能及安全认知的考核，对考核结果进行记录并保存。
- （三）对于培训考核成绩不符合要求的人员进行全校通报批评，对于安全培训后安全意识仍然薄弱且日常工作中违反安全策略的人员进行警告处分。

第四章 人员离岗管理

第十一条 信息网络中心对信息系统安全管理人员离岗应做好以下事项：

1. 立即终止即将离岗人员的所有资源访问权限。
2. 及时收回各种身份证件、密钥等以及单位提供的软硬件设备。

第十二条 信息系统安全管理离岗人员在被批准离岗后，信息网络中心应指派交接人员履行交接手续；离岗人员交回各种身份证件（门禁卡等）、保密文件、钥匙、徽章、软硬件设备等，并签署保密承诺协议。

第十三条 人事部门通知系统管理员撤销离岗人员的访问权限。

第五章 第三方人员管理

第十四条 第三方人员（如向系统提供服务的系统软、硬件维护人员，业务合作伙伴、评估人员等）在访问信息系统资源前，须签署安全责任合同书或保密协议。

第十五条 第三方人员对重要区域（如访问主机房、重要服务器或设备、保密文档等）的访问，须提出书面申请，经批准后由专人全程陪同或监督，并记录备案（记录第三方人员访问重要区域的进入时间、离开时间、访问区域、访问设备或信息及陪同人等信息）。

第六章 附则

第十六条 本规定由中国地质大学（北京）信息网络中心负责解释。

第十七条 本规定自发布之日起执行。附件：

1. 人员名册
2. 岗位网络安全职责说明书
3. 人员培训及考核记录

人员名册

序号	姓名	性别	出生年月	岗位	学历/资质	办公地点	办公电话	手机	状态	备注
1										
2										
3										
4										
5										
6										
7										
8										
9										
10										

岗位网络安全职责说明书

序号	姓名	岗位	岗位职责	要注意的安全问题	备注
1		安全管理员	负责贯彻执行网络安全和信息化领导小组的各项决议； 负责及时向信息网络中心主任汇报各信息系统安全状况及重大安全事件。 负责汇报本年度系统安全运维总体情况及年度安全规划； 负责对安全设备和系统（包括入侵检测系统、防病毒网关、防火墙、服务器、路由器、交换机、终端审计软件、业务系统等）所产生的日志进行审查分析； 负责定期进行安全检查，检查内容包括系统日常运行、系统漏洞和数据备份等情况； 负责监控网络的运行情况，从中检测出攻击的行为并给予响应和处理，遇到重大黑客事件应及时向网络安全和信息化领导小组汇报； 负责网络防病毒管理。防止网络资源被非法使用，防止网络资源由于入侵攻击而遭到破坏，防止病毒入侵等。 负责机房安全管理。		
2		系统管理员	负责服务器与操作系统的日常运行与维护； 负责数据存储与备份管理。 负责SQL Server、Oracle等数据库的管理与维护。		
3		网络管理员	负责网络运行与维护工作； 负责路由器、交换机、防火墙等网络设备和安全设备的配置调整。		
4		安全审计员	负责网络、系统、应用安全等操作的安全审计； 负责定期提交信息系统安全审计报告。		
注：1. 对违反网络安全管理规定的部门和个人，评估其造成的损害程度，根据相关规定给予必要的批评教育、通报批评、行政处分等处罚。2. 利用网络从事侵犯他人知识产权、危害国家安全、泄露国家秘密等违反国家法律活动的，依法交由相关国家机关，依照有关法律法规予以处罚。					

