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）网络安全方针和策略

1　适用范围

网络安全方针和策略文件是由网络安全和信息化工作领导小组批准、发布并传达给中国地质大学（北京）所有工作人员和外部相关方。本文件是依据业务需求和相关法律法规的规定和要求而制定。

本文件由网络安全和信息化工作领导小组定期对其合理性和适用性进行论证和评审，并根据内、外环境的变化，对存在不足或需要改进的地方，适当地予以修订，以符合新形势的安全需求。网络安全管理人员应通过适当程序落实本文件的要求。

2　安全目标

规范业务操作，保护信息资产，有效控制安全风险，防止发生安全事故，提高全校工作人员的网络安全意识及安全操作能力，全面提升中国地质大学（北京）网络安全建设及管理水平，保证业务连续性，促进中国地质大学（北京）信息化建设的全面发展。

3　安全方针

网络安全方针由网络安全领导组长批准发布，定期评审其适用性和充分性，必要时予以修订。

网络安全方针总结为“系统稳定，安全运行”，网络安全方针分为如下几个层面：

1.成立网络安全和信息化工作领导小组，领导全校网络安全工作，负责重大安全事件的决策，加强各类管理人员和组织内部机构之间的合作与沟通，与外部安全专家或组织保持紧密联系。

2.开展网络安全工作应以安全管理为指导，充分发挥现有网络安全技术手段作用，通过不断完善管理措施促进网络安全技术的更新运用，做到技术与管理有机结合，形成完善的网络安全保障体系。

3.网络安全主管部门制定清晰的网络安全方针，并通过网络运维部门颁发和维护网络安全方针的具体措施来表明对网络安全支持和承诺。所有外网安全控制措施（包括技术控制措施和管理控制措施）的选择、运营和维护均依据安全策略进行。

4.根据国家网络安全等级保护坚持自主定级、自主保护的原则，根据网络和应用系统在国家安全、经济建设、社会生活中的重要程度，以及遭到破坏后对国家安全、社会秩序、公共利益以及公民、法人和其他组织的合法权益的危害程度等因素确定网络安全的等级。

5.对安全管理工作的各类管理内容建立安全管理制度和操作规程，并要求管理人员或操作人员按照管理制度和操作规程进行日常管理操作，形成由安全策略、管理制度、操作规程等构成的全面的网络安全管理制度体系。

6.开展网络安全工作本着“预防为主”的原则，通过建立网络安全保障体系。完善网络安全管理制度，有效实施运维体系，全面提高系统的网络安全防护能力，降低网络安全风险。

7.做好网络安全工作需要全员参与，加强全体工作人员的网络安全教育和培训；应紧密围绕网络安全保障体系，明确各级人员在网络安全相关工作中的角色和责任，做到权责清晰。

8.开展网络安全工作本着“重点防护”的原则，将有限的资源投入到网络安全防护的关键环节，最大程度提高中国地质大学（北京）的网络安全防护能力。

9.开展网络安全工作本着“适度安全”的原则，管理与技术并重，全方位实施，全员参与；分权制衡，最小特权；尽量采用成熟的技术，实现资源投入和安全效益的平衡。

4 策略框架

建立一套关于安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心、建设和管理等六个方面的安全需求、控制措施及执行程序，并在关联制度文档中定义出相关的安全角色，并对其赋予管理职责，“以人为本”通过对网络安全工作人员的安全意识培训等方法不断加强系统分布的合理性和有效性。

4.1 安全物理环境方面

依据实际情况建立机房管理程序，明确机房的出入管理办法，机房介质存放方式，机房设备维护周期及维护方式，机房设备信息保密要求，机房温湿度控制方式等等环境要求。通过明确机房责任人、建立机房管理相关办法、对维护和出入等过程建立记录等方式对机房安全进行保护。

4.2 安全通信网络方面

从技术角度实现网络的合理分布、网络设备的实施监控、网络访问策略的统一规划、网络安全扫描以及对网络配置文件等必要信息进行定期备份。

从管理角度明确网络各个区域的安全责任人，建立网络维护方面相关操作办法并由某人或某部门监督执行看，确保各信息系统网络运行情况稳定、可靠、正常的运行。

4.3 安全区域边界方面

要求各类主机操作系统和数据库系统在满足各类业务系统的正常运行条件下，建立系统访问控制办法、划分系统使用权限、安装恶意代码防范软件并对恶意代码的检查过程进行记录。明确各类主机的责任人，对主机关键信息进行定期备份。

4.4 安全计算环境方面

从技术角度实现应用系统的操作可控、访问可控、通信可控。从管理角度实现各类控制办法的有效执行，建立完善的维护操作规程以及明确定期备份内容。

4.5 安全管理中心方面

对系统管理员、审计管理员及安全管理员进行身份鉴别，访问控制，对安全审计、入侵防范，主机的恶意代码防范，终端接入控制和重要服务器的监控等。

4.6 安全管理制度方面

网络安全策略、方针性文件，规定网络安全工作的总体目标、范围、原则和安全框架，是管理制度体系的灵魂和核心文件。

4.7 安全管理机构方面

通过构建和完善网络安全组织架构，明确不同安全组织、不同安全角色的定位、职责以及相互关系，强化网络安全的专业化管理，实现对安全风险的有效控制。

4.8 安全管理人员方面

对人员的录用、离岗、安全意识教育和培训、外部人员访问管理等方面应通过制度和操作程序进行明确。

4.9 安全建设管理方面

根据信息等级、系统重要性和安全策略将信息系统划分为不同的安全域，针对不同的安全域确定不同的网络安全保护等级，并进行相应的保护。网络安全等级的定级决定了系统方案的设计、实施、安全措施、运行维护等信息系统建设的各个环节。信息系统定级遵循“谁建设、谁定级”的原则。

4.10 安全运维管理方面

对环境、资产、介质、设备进行综合监控管理，对支撑重要信息系统的资源进行监控保护，确保密码防护、恶意代码防护和系统变更等事件要求按照定义好的安全管理策略措施。