会议材料之四

“地质云”管理制度

2017 年 11 月 6 日

北 京

目　录

一、管理办法

（一）“地质云”地质数据共享服务管理办法（试行）

（二）“地质云”网络安全管理办法（试行）

（三）“地质云”运行维护管理办法（试行）

（四）“地质云”用户管理办法（试行）

二、管理规定

（一）“地质云”网络安全组织管理规定（试行）

（二）“地质云”网络安全等级保护管理规定（试行）

（三）“地质云”网络安全事件管理规定（试行）

（四）“地质云”信息系统账户与密码安全管理规定（试行）

（五）“地质云”机房安全管理规定（试行）

“地质云”地质数据共享服务管理办法（试行）

第一章　总　则

第一条 目的依据

为规范和促进中国地质调查局（以下简称“局”）地质数据共享使用和社会化服务，深入推进地质数据的互联互通和开发利用，充分发挥地质大数据价值，进一步提升地质数据支撑服务经济社会发展的水平，依据国务院印发的《促进大数据发展行动纲要》、国土资源部印发的《促进国土资源大数据应用发展实施意见》、局印发的《加快推进地质信息共享服务的指导意见》、《“地质云”建设总体方案》等文件精神，结合局“地质云”建设实际，制定本办法。

第二条 概念定义

本办法所称的地质数据，是指局各直属单位依托各类地质工作、以及非局直属单位承担局组织实施的地质调查项目，采集和获取的各类原始地质数据、阶段性成果数据、成果综合数据和衍生的产品数据等。包括原始记录、图表、报告、数据库、多媒体等。

第三条 适用范围

本办法适用于局直属单位之间地质数据的共享行为，和局为政府部门、企事业单位、社会公众等提供地质数据的社会化服务行为。

第四条 职责分工

在局网络安全和信息化领导小组（以下简称“局网信领导小组”）的领

导下，局网信领导小组办公室（以下简称“局网信办”）负责地质数据共享服务的统筹规划和本办法的组织实施。

局各直属单位是地质数据共享、服务的责任主体，应当在各自职责范围内，做好地质数据资源目录编制、数据准备、产品开发、数据提供、数据更新维护等工作，并按照法律、法规和有关规定，合理使用其他局直属单位采集或获取的地质数据；同时统筹做好本单位内部各部门的地质数据共享工作。单位主要负责人是本单位地质数据共享、服务工作第一责任人。

局各部室在各自职责范围内，为地质数据共享、服务提供保障。局发展研究中心牵头负责局地质数据共享服务平台（以下简称“共享服务平台”）的建设和运行维护，为地质数据共享、服务提供技术支撑。

第五条 总体要求

（一）全面共享。地质数据以共享为原则，不共享为例外。局各直属单位有义务向其他局直属单位提供可共享的地质数据，并有权利根据履职需要，提出地质数据共享需求。构建形成“共建共享”机制与环境，各单位既是地质数据的提供者，也是共享数据的使用者和受益者。

（二）强化服务。局各直属单位均有义务提供地质数据的社会化服务。面向政府、企事业单位和社会公众等多元需求，以提供全面、权威、及时、便捷的地质数据服务为目标，加大服务产品开发，加快构建以数字化、网络化、智能化为主要特征的现代服务体系。

（三）分布式共享服务。结合各单位职责，局构建主节点、区域节点、专业节点等分布式节点，按照地质数据“谁生产，谁提供，谁维护”的原则，各单位原有的地质数据管理权限、信息系统维护权限不变。通过统一的共享、服务门户和技术标准，按照“物理分布、逻辑集中”的工作机制提供“一站式”共享、服务。

（四）规范使用。按照“谁使用，谁负责”的原则，对共享服务的地质数据，进行合法合理使用，不得泄露国家秘密、商业秘密和其他敏感信息，不得转予第三方，切实维护地质数据提供者的合法权益。

（五）安全可控。依托信息系统安全保障体系，健全完善地质数据共享、服务的安全机制，确保地质数据安全。

第二章　地质数据分级与共享服务分类

第六条 地质数据分级

按照涉密性及敏感性，将地质数据分为Ⅰ级数据、Ⅱ级数据和Ⅲ级数据。

Ⅰ级数据为涉密数据。涉及国家秘密的地质数据。

Ⅱ级数据为内部数据。包括：内容敏感，即公开后会造成一定范围或一定程度社会较大影响的地质数据，以及涉及单位或个人利益等的地质数据。Ⅱ级数据可进一步细分为Ⅱ-1级数据和Ⅱ-2级数据。Ⅱ-1级数据为内部控制数据，是指内容敏感的地质数据；Ⅱ-2级数据为内部公开数据，是指涉及单位或个人利益等的地质数据。

Ⅲ级数据为公开数据。包括：除Ⅰ类、Ⅱ类以外的所有数据。不涉及密级和敏感性，数据精度符合国家公开的标准和规定。

第七条地质数据分级的确定

Ⅰ级数据由数据提供单位按照国家保密相关管理规定，进行保密审查和涉密定级。Ⅱ级、Ⅲ级数据由数据提供单位确定，报局网信办备案。

第八条共享服务分类

（一）局直属单位地质数据共享分为无条件和有条件两类。

Ⅰ级数据实行有条件共享：按照国家保密相关管理规定执行。

Ⅱ级数据分两种情况共享：Ⅱ-1 级数据实行有条件共享：需提供项目实施、完成上级交办有关任务等证明材料。Ⅱ-2 级数据实行无条件共享。

Ⅲ级数据实行无条件共享。

（二）地质数据社会化服务分为无条件和有条件两类。

Ⅰ级数据实行有条件服务。按照国家保密相关管理规定执行。

Ⅱ级数据分两种情况服务：Ⅱ-1 级数据实行有条件服务：需书面提出使用理由，并经局批准。Ⅱ-2 级数据实行有条件服务：需提供项目实施批件、单位职责证明等相关材料。

Ⅲ级数据实行无条件服务。

第三章　地质数据资源目录管理

第九条 资源目录编制

局各直属单位对所拥有的地质数据进行梳理，按照地质数据资源目录编制相关要求，基于元数据信息，并增加其分级分类等内容，编制形成地质数据资源目录（以下简称“资源目录”）。

资源目录是局各直属单位地质数据共享、服务的依据，并将作为规划和安排各单位信息化建设项目与运行维护项目的重要依据。

第十条 资源目录管理

局各直属单位应当建立本单位资源目录管理制度，并加强对本单位资源目录编制、审核和更新等的管理。

局各直属单位应当建立本单位资源目录更新机制，因资源目录实体数据发生调整或可共享服务的地质数据出现变化时，应当在 15 个工作日内，在地质数据共享服务平台对资源目录进行更新操作；并每年至少进行一次单位资源目录的全面更新维护。资源目录更新应采用在线方式（资源目录

涉密的除外）。

第四章　共享服务方式与流程

第十一条 共享服务方式

地质数据共享、服务包括在线和离线两种方式，具备在线条件的，原则上都应采用在线方式。通过统一的局地质数据共享服务平台，提供地质数据共享和社会化服务。

涉密数据通过涉密网在线提供；内部数据通过业务网、涉密网在线提供；公开数据通过互联网、业务网、涉密网在线提供。不具备相应网络条件的，应采用离线方式提供。对于尚未接入共享服务平台的，或数据量大，不适合在线传输的，可采用离线方式。地质数据资源目录通过互联网、业务网、涉密网提供全部在线查询检索（资源目录涉密的除外）。

申请使用有条件共享、服务地质数据的，数据需求方应当通过共享服务平台提出申请，说明使用范围、用途（附相关证明材料等）和申请的地质数据项内容等。数据提供方在收到申请后 5 个工作日内，按照本办法第六条、第八条规定，提出处理意见及理由，向需求方提供在线或离线共享服务。

涉及国家秘密、单位或个人利益的地质数据，应当签订地质数据使用安全保密协议，按照约定方式使用地质数据。

地质数据提供方应提供机器可读取的数据集，确保所提供数据的完整性和可用性。

局各直属单位应加强对地质数据的深度加工和整合，设计、开发具有广泛社会影响的服务产品，加强地质科普产品制作和推广。鼓励根据用户特定需求，提供定制处理和专题服务。

第十二条 共享服务的协调

如数据需求方、提供方持有异议的，可以申请协调处理，由局网信办会同相关部门对该事项进行研究并作出结论，必要时报请局网信领导小组决定。

设立局地质数据共享、服务信箱和热线电话，及时协调监督共享、服务工作。

第十三条 共享服务的反馈

共享服务平台应提供接收用户使用反馈，记录用户点击、使用及下载情况，共享、服务统计等功能，不断提高共享、服务的针对性。

局网信办应定期对地质数据共享、服务情况进行统计分析，及时将分析结果反馈给数据提供方，不断提高共享、服务质量。

第十四条 地质数据更新维护

局各直属单位应建立地质数据的更新维护业务团队，对其提供的地质数据进行动态管理，在数据产生或者变更后15个工作日内完成更新。地质数据库按照统一的分工，由指定的局直属单位更新维护。

局各直属单位应加强项目实施过程中形成的阶段性成果数据（项目任务书中规定的年度成果、经阶段性评审验收认定的成果等）的共享、服务工作，缩短成果共享、服务周期。

第十五条 工作流程

地质数据共享、服务包括以下六个主要步骤:

1.共享服务资源目录更新：局各直属单位在线编制或更新本单位地质数据资源目录；局发展研究中心汇总更新局地质数据资源目录。

2.地质数据整理准备：局各直属单位按照相关技术要求，进行地质数据整理和准备，研制服务产品，并上传更新到共享服务平台中。

3.地质数据使用申请：数据需求方在共享服务平台上提出使用申请。

4.地质数据审核授权：地质数据提供方进行使用审核，同意的，由提供方在共享服务平台上为需求方授权或离线提供数据。

5.地质数据使用及反馈：地质数据使用方按规定使用数据，并将使用情况在共享服务平台上进行反馈。

6.共享服务评价：局网信办对局各直属单位共享、服务工作定期进行评价。

第十六条 共享服务的用户注册

地质数据共享实行用户实名认证。

地质数据服务实行用户分级注册管理：仅查询浏览地质数据的，无需注册；下载Ⅲ级地质数据的，仅需简单注册；申请使用Ⅰ级、Ⅱ级地质数据的，需实名认证并提供相关证明材料。

第十七条 共享服务费用

地质数据共享均为无偿提供。地质数据对社会提供简单服务的，不应收取费用。需要对数据加工处理或利用多种资料进行编研才能满足用户需求的，可以项目委托方式收取数据处理分析与综合研究费用。

第五章　知识产权保护

第十八条知识产权标注

地质数据使用者在发表论著、申报奖励、发布成果等时，应注明地质数据来源和提供方。

通过用户注册管理、实名认证、数字水印、地质数据出版等技术，加强对地质数据的知识产权保护。

地质数据需求方在申请本单位生产的有条件类地质数据时，原则上应提供其使用。

第十九条 共享服务数据使用限制

地质数据使用单位应按照相关法律规定和单位职责合理使用有条件类地质数据，不得提供给第三方；并加强地质数据使用全过程管理，对数据的非授权使用、未经许可的扩散以及泄露等行为负责。

地质数据使用方在利用数据完成申请的工作任务后，应按电子文件销毁相关要求销毁地质数据。

第六章　共享服务的安全保障

第二十条 平台安全保障

局网信办会同发展研究中心负责局地质数据共享服务平台的安全体系规划和建设。局发展研究中心负责主节点的平台安全，其他局直属单位负责所建节点的平台安全。

第二十一条 地质数据安全保障

局各直属单位按照“谁生产，谁提供，谁维护；谁使用，谁负责”的原则，在各自的职责范围内，做好地质数据安全工作。

第七章　条件保障

第二十二条 工作保障

局各直属单位应将地质数据共享、服务工作纳入单位发展规划和年度工作计划，在各自承担的地质调查项目中统筹安排相关预算，并在项目任务、预期成果中明确应提交的数据与服务产品。

第二十三条 机构与人员保障

局各直属单位应明确专门机构和专人负责地质数据共享、服务工作，

设置服务场所。局网信办将不定期组织开展地质数据共享、服务工作业务培训。

第二十四条 单位共享服务制度建立

局各直属单位应制定本单位地质数据共享、服务方式，流程，收费等细则，公布服务咨询电话。

第八章　监督检查

第二十五条 评价考核

局网信办会同有关部门督促检查地质数据共享、服务落实情况，提出地质数据共享、服务评价指标体系，对各单位共享、服务情况进行定期评价，并将评价结果进行通报。

第二十六条 监督

（一）局直属单位违反本办法规定，有下列情形之一的，由局网信办会同相关部门根据实际情况予以书面通报，并责令其限期改正。对于违反以下第4、5条的当事人，还将纳入诚信记录档案，暂停或取消其共享服务平台账号。

1.未按要求编制或更新地质数据资源目录;

2.未向共享服务平台及时提供地质数据的;

3.提供的地质数据和本单位所拥有的数据不一致，未及时更新数据或提供的数据不符合有关规范、无法使用的;

4.将有条件类地质数据用于履行本单位职责需要以外的目的;

5.未按要求进行地质数据使用标注的;

6.违反本办法规定的其他行为。

（二）社会用户的地质数据使用者违反本规定，有下列情形之一的，

由局网信办会同相关部门根据实际情况予以书面通知或通报，纳入诚信记录档案，暂停或取消共享服务平台账号。

1.将有条件类地质数据用于申请用途以外的目的;

2.未按要求进行地质数据使用标注的;

3.其他违反本办法应当给予处分的行为。

第九章　附　则

第二十七条解释单位

本办法由中国地质调查局网信办负责解释。

第二十八条 实施日期、有效期

本办法自发布之日起试行。

“地质云”网络安全管理办法（试行）

第一章　总　则

第一条 为推进“地质云”建设与运行，保障中国地质调查局（以下简称“局”）地质调查网络安全、信息系统稳定运行，维护地质数据和地质信息产品共享服务环境，依据国家网络安全法、国土资源部网络安全管理等有关规定，结合地质调查网络建设运行实际，制定本办法。

第二条 本办法适用于“地质云”所涵盖的非涉密网络和信息系统，包括地质调查网络基础设施和机房环境，以及所承载的信息系统和相关的数据、产品。

第三条 网络安全管理的目的是保障地质调查网络的完整性、可靠性、可用性、真实性、不可抵赖性，保证网络系统持续稳定运行、网络服务不中断，使信息系统和数据免受偶然或恶意的破坏篡改及泄漏，避免网络安全事故。网络安全管理的任务是指按照国家信息系统安全等级保护制度，确定信息系统安全保护等级，构建相应的安全防护能力和策略。

第二章　管理职责分工

第四条 地质调查网络安全实行“统筹协调、分级负责”的原则。在局网络安全和信息化领导小组（以下简称“局网信领导小组”）的领导下，局网信领导小组办公室（以下简称“局网信办”）负责局网络安全的统筹

协调和组织实施。

各节点单位按照局信息化建设总体规划和网络安全的有关要求，负责本单位的网络安全工作，制定本单位的网络安全工作细则和安全策略。各节点单位主要负责人是第一责任人，主管网络安全的领导是直接责任人。

第五条 以节点单位边界路由器为界，边界路由器（含）之内的分节点网络系统，由所在单位负责该节点网络安全工作；主节点网络系统以及各分节点路由器之外的网络系统由局发展研究中心负责。

第六条 各节点单位应设立网络管理岗位，包括系统管理员、网络管理员、网络安全员等，并明确岗位职责。

其中网络安全员主要负责本单位网络安全等级保护和安全评估工作、组织开展本单位网络安全检查和整改，协调网络安全重大事件的处理。

网络安全员不得兼任系统管理员、网络管理员。各单位的网络安全员应报局网信办备案，人员发生变更后及时报备。

第七条 网络管理岗位人员的聘用和离岗应有严格审批手续，上岗时签订安全责任书，离岗时签订离岗协议等。各单位应制定岗位上岗资质相关要求。

第三章　机房及设备安全环境要求

第八条 机房是地质调查信息系统集中部署和运行服务的重要场所和基础环境。机房建设应当确保具有支持业务稳定、持续运行的能力，并保证安全技术措施同步规划、同步建设、同步使用。

第九条 机房物理位置、物理访问控制、物理环境应达到相关国家标准和基本要求，消防、配电、电磁防护安全等应符合国家相关标准规范。

第十条 网络安全产品和设备应当符合相关国家标准的强制性要求，

采购和使用由具备资格的机构安全认证合格或者安全检测合格的产品。应加大国产自主可控产品的使用。

第十一条 每季度应进行至少一次机房核心设备、重要网络设备和安全设备的安全风险检测评估，每年应组织至少一次网络安全应急演练，提高网络安全事件的应急处置与网络功能恢复能力。

第四章　信息系统开发建设及上线运行要求

第十二条 信息系统开发应符合代码编写相关安全要求，开发活动应受到控制、监视和审查，开发人员和安全测试人员应分开。

信息系统开发建设外包的，应选择具有相应专业资质单位，签订安全保密协议，确保开发建设、功能和安全测试、成果验收、交付发布等环节都在控制和监视下完成，应有完善的审批流程。

第十三条 信息系统应实行开发环境和实际运行环境物理分开。全局性信息系统应部署到地质调查网络环境，非全局性的信息系统应部署到本单位网络环境或地质调查网络环境。

第十四条 网络和信息系统应按照国家等级保护相关要求，进行定级、备案、整改、测评。

（一）依照信息系统安全保护等级要求实行保护，采取数据分类、重要数据备份和加密等措施。采用网络安全防护技术措施，监控并记录网络运行状态和安全事件，落实网络安全保护责任。

（二）针对系统变更、重要操作、物理访问和系统接入等事项建立审批程序，按照程序进行审批，对重要活动建立逐级审批制度。

（三）全局性信息系统的运行使用以及接入全局性信息系统都必须报局网信办审批（含设备地址、应用系统发布地址、应用系统域名等），仅

在局属单位内部运行使用的信息系统由本单位审批。

第五章　网络安全管理要求

第十五条 网络安全应根据业务的实际情况及安全需求从网络结构上划分安全区域，实行边界防护，按等保级别分区域保护。

（一）地质调查网络系统主节点划分为内网、业务网、互联网接入服务区。

（二）按照信息系统安全等级保护制度规范要求，采取主机和系统安全防范措施，进行应用系统和数据安全管理，采用身份鉴别技术，实现有效访问控制。

第十六条 安全审计和集中管控。

（一）对网络边界、安全区域、主机设备、应用系统等进行安全审计，并对审计进程进行保护。

（二）划分出特定的管理区域，建立集中管控中心，对分布在网络中的安全设备或安全组件进行管控；对安全策略、恶意代码、补丁升级等安全相关事项进行集中管理；对网络链路、安全设备、网络设备和服务器等的运行状况进行集中监测；对网络中发生的各类安全事件进行识别、报警和分析。

第十七条 定期进行全面安全检查。检查内容包括现有安全技术措施的有效性、安全配置与安全策略的一致性、安全管理制度的执行情况等。检查结果应形成记录，汇总安全检查数据，形成安全检查报告。

第十八条 网络和信息系统应仅采集和保存业务必需的用户个人信息，需要个人提供的应保证真实有效；禁止未授权访问和使用用户个人信息。应当对收集的用户信息严格保密，不得泄露、篡改、毁损收集的个人

信息。

第六章　地质数据和地质信息产品安全管控要求

第十九条 地质数据和地质信息产品应从源头控制，进行分级分类管理和全过程监控，实行发布审批。

第二十条　地质数据和地质信息产品安全控制及管理。

（一）支撑地质数据和地质信息产品运行的应用、管理、服务系统应保证代码安全。结构化数据设置记录级访问权限，非结构化文档设置文件级访问权限。

（二）地质数据和地质信息产品下载服务应设置权限管控措施，实现访问控制。

（三）应采用校验码技术或加解密技术保证重要地质数据在传输、存储过程中的完整性。

第二十一条 地质数据和地质信息产品安全备份管理。

（一）根据数据的重要性和数据对系统运行的影响，制定数据的备份策略和恢复策略、备份流程和恢复流程等。

（二）应提供地质数据和地质信息产品的本地、异地数据备份与恢复功能；规定备份信息的备份方式、备份频度、存储介质、保存期等。提供重要地质数据和地质信息产品处理系统的在线冗余，保证可用性。

第七章　安全运行维护和应急处置

第二十二条 对地质调查网络安全和信息系统管理活动中的各类管理内容建立安全管理制度；对日常管理操作建立操作规程；对管理过程中形成的安全策略、管理制度、操作规程、记录表单等信息归档留存。其中信息安全管理应参照 GB/T 22080/ISO27001 标准执行，运维服务管理应参照 GB/T 24405/ISO20000 标准执行，质量管理应参照 GB/T19001/ISO9001 标准执行。

第二十三条 合理部署和配置网络及信息系统安全防护体系，维护网络拓扑结构，管理资产信息。开展网络攻击和入侵防范日常工作，进行网络运行状态监控与记录，及时完成系统补丁升级管理。

（一）运维过程中应严格管控变更性调整，经过审批后才可改变链接、安装系统组件或调整配置参数；严格控制运维工具的使用，经过审批后才可接入进行操作；严格控制远程运维的开通，经过审批后才可开通远程运维接口或通道；保证所有与外部的链接均得到授权和批准。全局性系统变更由局网信办审批，非全局性系统由本单位网信办审批。

（二）定期验证防范恶意代码攻击技术措施的有效性。对外来计算机或存储设备接入系统前进行恶意代码检查，防范恶意代码软件的授权使用、恶意代码库升级、恶意代码的定期查杀等。

第二十四条 建立健全网络安全风险评估和应急工作机制，将网络安全事件分为有害程序事件、网络攻击事件、信息破坏事件、信息内容安全事件、设备设施故障、灾害性事件等类别，划分为特别重大事件、重大事件、较大事件、一般事件等级别，分类分级制定网络安全事件应急预案。发生网络安全事件，应当立即启动网络安全事件应急预案，对网络安全事件进行调查和评估。定期对应急预案进行评估和完善。

（一）应规定统一的应急预案框架，并在此框架下制定不同事件的应急预案，包括启动预案的条件、应急处理流程、系统恢复流程、事后教育和培训等内容。

（二）从人力、设备、技术和财务等方面确保应急预案的执行。

（三）应在安全事件报告和响应处理过程中，分析和鉴定事件产生的原因，收集证据，记录处理过程，总结经验教训。

（四）对造成系统中断和造成信息泄漏的重大安全事件应按照应急预案操作处理并及时逐级上报。

第二十五条 各单位应当建立健全网络安全监测预警和信息通报制度，加强网络安全信息收集、分析和通报工作，并向局网信办报送网络安全监测预警信息。

第二十六条 针对发现的系统漏洞、安全威胁、网络攻击等行为应及时采取有效措施，进行风险防控和整改加固，消除隐患。因网络和信息安全防范及处置不当，发生突发事件或者生产安全事故的，应当依照国家有关法律、行政法规的规定处置。

第八章　网络用户使用安全要求

第二十七条 用户使用网络系统必须自觉遵守国家有关安全、保密法律法规。不得从事危害网络安全的活动，严禁上网传输、处理、复制、储存、发布反动言论、扰乱社会秩序、封建迷信、淫秽色情、恐怖暴力等法律法规规定的各类有害信息。

第二十八条 局内部用户登录使用地质调查网络系统，应实行实名注册登记制度，服从账号使用登记和操作权限管理，保证接入网络设备的系统安全，自觉做好客户端设备的安全防护工作。

第二十九条 局内部用户应接受并配合国家相关部门以及局组织的监督检查、安全评估，并完成网络终端安全加固和系统整改工作；安装杀毒软件和防护系统，及时升级病毒库和安装漏洞补丁。

第九章　网络安全教育及培训

第三十条 各单位应有计划地组织开展网络安全基础知识、岗位操作规程、安全防护意识、保密责任等教育和培训。

（一）各节点单位主要负责人和主管网络安全的领导每年应至少参加1次网络安全形势教育培训，提高网络安全规划和宏观决策能力。

（二）各节点单位每年至少组织召开1次全员参加的网络安全教育培训，提高网络安全防护意识、安全责任意识和法律意识。

（三）网络管理岗位人员每年至少参加1次网络安全技术培训，加强业务交流，提高网络安全防护技能和水平。

第三十一条 各节点单位每年底应制订下一年度网络安全教育培训计划，应保障网络安全教育培训经费和培训时间；同时将本年度网络安全培训情况报局网信办备案。

第三十二条 局网信办负责组织全局网络安全教育培训工作。

第十章　监督及处罚

第三十三条 局网信办负责对网络安全管理工作进行监督检查。对违反规定的行为提出处置建议，视情况对当事人予以批评教育、通报等。对产生严重后果的网络安全事件，按照国家网络安全法的相关要求处置。

第十一章　附　则

第三十四条 涉密网络安全和“地质云”用户管理办法另行制定。

第三十五条 本办法由中国地质调查局网信办负责解释。

第三十六条 本办法自颁布之日起试行。

“地质云”运行维护管理办法（试行）

第一章　总 则

第一条 为规范和促进中国地质调查局（以下简称“地调局”）“地质云”的日常管理和运行维护，保障“地质云”的有序高效、安全稳定、常态化运行，推进地质调查、业务管理、数据共享和地质信息服务工作，根据国家的有关法律、技术标准，国土资源部和地调局的有关规定，结合“地质云”实际情况，制定本办法。

第二条 本办法适用于“地质云”日常管理与运行维护行为，涵盖地质数据、地质信息产品、应用系统、地质云平台等方面的运行维护管理。

第三条 本办法相关术语含义：

（一）“地质云平台”：是指“地质云”的核心部分，由地质云基础设施平台、地质云管理系统和地质云门户等组成。地质云基础设施平台包括地质云基本的硬件设备和虚拟化的管理系统；地质云管理系统是指以服务方式管理各类地质云资源的信息系统；地质云门户是“地质云”的统一对外服务网站。

（二）“地质数据”：是指地调局直属各单位依托各类地质工作、以及非地调局直属单位承担局组织实施的地质调查项目，采集和获取的各类原始地质数据、阶段性成果数据、成果综合数据等。本办法所称“地质数据”是指集成到地质云平台业务网区的实体数据、浏览数据、元数据以及其他数据服务。

（三）“地质信息产品”：是指基于“地质数据”整理、加工、开发形成的各类衍生品。本办法所称“地质信息产品”是指集成到地质云平台国

际互联网区的产品实体数据、浏览数据、元数据以及其他数据服务。

（四）“应用系统”: 是指集成到地质云平台的以应用为目的的各类计算机网络信息系统。

（五）“地质云资源”: 统称集成到地质云平台的地质数据、地质信息产品、应用系统和软硬件设施等。

（六）“地质云节点”、“地质云节点单位”: 地质云节点是指地质云的实体组成单元，分为主节点、分节点和备份节点三种类型。主节点是地质云的主中心；分节点是地质云的分中心，可通过物理集成或逻辑存在的方式接入到主节点。备份节点是地质云的同城、异地备份数据中心。地质云节点单位是指地质云节点的建设和运行维护单位。

（七）“上云”: 是指地质数据、地质信息产品、应用系统、软硬件设备集成到地质云平台的行为和过程。

（八）“下云”: 是指地质数据、地质信息产品、应用系统和软硬件设备从地质云平台退出、删除的行为和过程。

第四条 总体要求:

（一）统筹规划、分工负责。

根据“地质云”的总体规划，按照统一的管理要求及技术规范，地质云主节点、分节点、备份节点单位应在各自职责范围内，做好本节点的运行维护工作。把好“地质云”入口关，数据、产品、信息系统、软硬件设备等资源上云均应符合有关要求；地质云资源的分配使用要合理规划，确保资源利用效率。

（二）谁建设，谁维护。

各节点单位做好所提供地质数据、地质信息产品、应用系统（含软件工具）等资源的质量、保密等的审核把关和更新维护工作。

（三）安全可靠、稳定运行。

健全网络安全保障体系，构建有效运行机制，建实有关机构和岗位，

确保“地质云”运行安全可靠、稳定流畅。

第二章　职责分工

第五条 在局网络安全和信息化领导小组（以下简称“局网信领导小组”）的领导下，局网信领导小组办公室（以下简称“局网信办”）负责本办法的组织实施。地调局负责“地质云”的建设和运行维护工作；局发展研究中心负责主节点、备份节点的运行维护，以及地质云建设运行的技术支撑；备份节点单位负责备份节点的物理环境和网络维护；各分节点单位负责所建节点的运行维护。

第六条 局网信办的运行维护职责与任务：

（一）　负责“地质云”运行维护的统筹规划；

（二）　负责制定“地质云”建设运行的制度与技术标准；

（三）　负责地质云门户的规划和管理；

（四）　负责“地质云”运行维护的监督管理；

（五）　组织开展“地质云”建设运行维护和推广应用的培训。

第七条 主节点单位的运行维护职责与任务：

（一）研究起草“地质云”建设运行维护的管理与技术要求。负责各节点地质数据、地质信息产品、应用系统、软硬件设备等上云、变更、下云的技术审核；

（二）承担“地质云”运行监控和技术保障，以及运行使用情况的统计分析；

（三）负责主节点物理环境维护，以及软硬件设备增加、退出和维护；

（四）负责主节点地质数据的准备、上云、使用审批与提供服务、变更和下云；

（五）负责主节点地质信息产品的开发、上云、使用审批与提供服务、

变更和下云;

（六）负责主节点部署的应用系统的日常管理;

（七）承担“地质云”骨干网络系统的日常运行维护;

（八）承担地质云门户的运行维护，以及用户的日常管理;

（九）承担地质云资源的配置和网络安全管理。

第八条 分节点单位的运行维护职责与任务:

（一）参与“地质云”建设运行维护管理与技术要求的研制;

（二）配合主节点做好测试调试、安全防护、漏洞检测等安全管理方面工作;

（三）负责本节点物理环境和网络维护，以及软硬件设备增加、退出和维护;

（四）负责本节点地质数据的准备、上云、使用审批与提供服务、变更和下云;

（五）负责本节点地质信息产品的开发、上云、使用审批与提供服务、变更和下云;

（六）负责本节点部署的应用系统日常管理，支撑“地质云”应用系统运行的相关工作;

（七）负责本节点的网络安全;

（八）承担本节点用户管理的相关工作;

（九）负责本节点地质云资源的配置和相关技术培训。

第九条 备份节点单位的运行维护职责与任务:

（一）承担备份节点的物理环境和网络维护;

（二）配合主节点单位做好备份节点系统运行维护的相关工作。

第三章　地质数据管理

第十条 数据上云

（一）地质数据基于“地质云”业务网区进行管理。上云前，节点单位应做好数据的分级分类、数据资源目录编制；完成数据的组织与整理、数据包制作、数据接口封装以及元数据采集等；履行数据涉密审查程序。经本单位同意后，将数据接口、相关信息、或实体数据和申请表（附件 1）同时上传。

（二）地质云主节点单位审核数据资源目录、元数据、审请表等，核实数据内容及数据接口等。审核合格，分配资源编号，纳入地质云数据资源进行管理。

第十一条 数据变更

（一）云上数据发生变更时，节点单位应按照附件 2 格式，填写资源编号、资源名称、变更内容、变更理由等内容，更新元数据相关内容，并经过本单位同意后，将相关数据和申请表同时上传。

（二）地质云主节点单位审核申请表和提供的相关数据等。审核通过后，更新相关内容。

（三）对于重要地质数据的变更，需报局网信办审批。批准后，在地质云门户公告一个月方可变更。

第十二条 数据下云

（一）数据下云时，节点单位应按照附件 3 格式，填写资源编号、资源名称、下云理由等内容，并经过本单位同意后，将申请表上传。

（二）地质云主节点单位审核申请表等是否按要求提交，然后报局网信办审批。审批同意后，在地质云门户上公告一个月方可下云。并对该地质数据的运行维护和共享服务的相关记录进行归档存储。

第十三条 数据使用申请与授权

（一）依据数据的分类分级属性和管理规定，各节点单位审核或审批用户申请，并提供在线或离线服务。

（二）当用户申请的是II_1级地质数据需进行有条件共享服务时，应通过主节点报局网信办审批。

第十四条 数据日常维护

（一）节点单位负责本节点提供数据的更新与维护，保障本节点数据的网络地图服务、数据接口、数据包及元数据等正常运行。

（二）主节点单位负责各节点数据共享状态、数据接口、地质云门户展示等的运行和监控。其中，“地质云”数据管理部门负责地质数据接口的稳定运行和各节点数据共享状态监控，地质云平台运行部门负责数据在地质云门户上的集成展示。

第四章　地质信息产品管理

第十五条 产品上云

（一）地质信息产品基于“地质云”国际互联网区进行管理。上线前，节点单位应按照相关要求，采集元数据信息、制作产品缩略图，做好产品的分级分类、资源目录编制，履行产品涉密审查程序。经本单位同意后，将产品相关数据和申请表（附件 4）同时上传。

（二）地质云主节点单位审核产品目录、元数据、申请表等，核实产品内容及产品接口等。审核合格后，分配资源编号，纳入“地质云”地质信息产品资源进行管理。

第十六条 产品变更

（一）云上产品发生变更时，节点单位应按照附件 2 格式，填写资源编号、资源名称、变更内容、变更理由等内容，经本单位同意后，将相关数据和申请表同时上传。

（二）地质云主节点单位审核产品变更后的资源目录、元数据和申请表等。审核通过后，更新相关内容。

（三）对于重要地质信息产品的变更，需报局网信办审批。批准后，在地质云门户公告一个月方可变更。

第十七条 产品下云

（一）地质云节点单位应按照附件 3 格式，填写资源编号、资源名称、下云理由等内容，经本单位同意后，将申请表上传。

（二）地质云主节点单位审核申请表等内容，然后报局网信办审批。批准后，在地质云门户公告一个月方可下云。并对该地质数据的运行维护和共享服务的相关记录进行归档存储。

第十八条 产品使用申请与授权

（一）依据产品的分类分级属性和管理规定，各节点审核、审批用户申请，并提供在线或离线服务。

（二）当用户申请的是 II_1 级地质信息产品需进行有条件服务时，应通过主节点报局网信办审批。

第十九条 产品日常维护

（一）节点单位负责本节点提供产品的更新与维护，保障本节点产品的网络地图服务、产品接口、产品数据包及元数据等的正常运行。

（二）主节点单位负责各节点产品服务状态、地质信息产品接口、地质云门户展示等的运行监控。其中，“地质云”地质信息服务部门负责地质信息产品接口的稳定运行和各节点产品服务状态监控，地质云平台运行部门负责产品在地质云门户上的集成展示。

第五章　应用系统管理

第二十条 应用系统上云

（一）应用系统上云的基本要求：可调用地质云基础设施、平台软件和数据资源等，数据库接口应对地质云平台开放，用户管理符合“地质云”

用户体系架构，安全防护符合“地质云”网络安全保护要求。

（二）应用系统上云时，申请单位应填写申请表（附件 5 或附件 6），提供系统基本情况，提出对地质云基础设施资源的需求，并提供应用系统相关材料（系统开发报告、系统测试报告、专家评审意见、安全等级定级报告、系统接口参数等）。未完成开发或未通过自测的系统，禁止上云。

（三）地质云平台运行部门负责核实申请材料的完整性和基础设施云资源需求的合理性，应当在 3 个工作日内作出受理或不予受理意见。不予受理的，应当提出不予受理意见；受理的，应当在 2 个工作日内提供试用环境，试用时间一般为 15—30 天，确有必要的经审批可以延长试用时间。

（四）申请单位在试用环境中部署应用系统，并对应用系统进行功能、性能及安全测试；信息系统安全等级保护三级以上的重要应用系统，须提供由国家认可的第三方测评机构出具的软件性能及信息系统安全测试报告。应用系统通过测试的，正式启用，临时试用环境转为正式环境。

（五）专业软件、常用办公软件等软件工具可申请作为桌面云资源提供共享服务。

（六）地质云平台运行部门应提供地质云技术咨询和方案优化，配合申请单位完成应用系统、软件工具上线和迁移工作。

第二十一条 应用系统变更

（一）正式运行过程中，应用系统运行单位要求更新应用系统版本，或调整地质云资源配置的，须提交变更申请（附件 2）。涉及重大变更的，须重新提交本办法第二十条中的有关材料，还应通过性能和安全测试。

（二） 主节点地质云平台运行部门应当在 3 个工作日内完成变更审批。审批通过的，在 2 个工作日内完成变更。

（三）应用系统升级可能产生较大影响的，主节点单位还应报局网信办审批，批准后，在地质云门户公告 1 个月方可变更。

第二十二条 应用系统下云

（一）应用系统下云时，须做好系统下线和数据迁移备份工作，并提交终止申请（附件 3）。

（二）主节点单位应当在 3 个工作日内完成终止审核，并报局网信办审批。批准后，在地质云门户公告 1 个月，然后在 2 个工作日内回收相应的地质云资源，终止有关服务。

第二十三条 应用系统日常维护

（一）各应用系统负责单位设立系统管理员，组建相应的技术支撑团队，承担应用系统的运行维护工作。

（二）集成到地质云平台的应用系统运行于业务网或互联网区，地质云平台要按照相关的权限规定对应用系统的用户、数据等作为服务资源进行管理，应用系统的网络服务端口和共享服务接受地质云门户的统一监管。

（三）局网信办组织制定重要应用系统的运行管理规定，建立健全值班值守、运行维护、备份恢复及应急处置演练等制度。应用系统单位负责系统应用层的日常运维和监控，包括自有应用软件、数据、文档等。主节点单位负责系统基础设施层的运行监控，并定期（每月不少于 1 次）向应用系统单位提供地质云资源利用情况表和优化建议。

（四）应用系统一旦在地质云平台上部署运行，不得随意对系统进行重启、重新安装、临时暂停服务等操作。

第六章　地质云平台运行管理

第二十四条 地质云存储、计算、网络等基础设施的使用管理。

（一）“地质云”基础设施资源面向局系统用户使用。用户创建时，默认实时分配适当的存储空间、计算等资源；当对基础设施资源的需求超

过默认值时，实行申请审批制。

（二）基础设施资源使用包含申请、受理、审批、测试、开通、变更和终止等环节。申请基础设施资源应通过地质云门户实现。

（三）申请基础设施资源的，应提交申请表，包括使用理由、资源需求等。申请将应用系统（含软件工具）上云提供服务时，应按本办法第十八条执行。

（四）主节点负责核实申请、变更材料的完整性和对基础设施资源需求的合理性，应当在1个工作日内作出受理或不予受理意见。不予受理的，应当提出不予受理意见；受理的，应当在1个工作日内提供地质云资源或提供试用环境。

按照用户正常运行所需要的合理值来分配计算、存储、网络等基础设施资源；业务量变化幅度较大的应用系统，可以根据实时需要动态弹性调整所需云资源。操作系统、GIS软件等支撑软件在构建虚拟主机时，可选择自动构建。

（五）通过申请方式获得地质云资源的用户不再使用时，须做好系统下线和数据迁移备份工作，并提交终止申请，主节点应当在3个工作日内完成终止审核；审核通过后，应当在2个工作日内回收相应的云资源，终止有关服务。

（六）用户应当在职责范围内合理使用基础设施资源，监控运行状况，及时发现问题并向主节点地质云平台运行部门反映。主节点不定期将系统基础设施层资源利用情况表和优化建议提交给用户。

第二十五条 地质云平台的日常维护。

（一）主节点单位负责地质云平台的运行监控，并定期（每3个月不少于1次）向局网信办和各节点单位提供各节点运行维护情况、基础设施资源利用情况及优化建议。

（二）各节点单位负责节点基础设施资源的日常运行维护工作，定期

开展巡检，形成书面记录，及时解决地质云故障。

（三）各节点的软硬件设备添加、退出，节点单位应填写审批表（附件 7、附件 3），并报主节点单位备案。主节点重要设备的添加、退出需报局网信办审批，并根据需要通报有关节点单位。

（四）在基础设施云资源剩余 30%以下，应启动动态扩容机制，开展地质云平台扩容升级工作。

（五）地质云门户栏目设置的调整和相关内容的变更，应事前征得局网信办同意。

第二十六条 地质云基础设施平台、各应用系统、地质云门户、地质云管理系统应分别制定割接、升级、调整等操作规程，尽量降低对其他层的影响；对于可能产生较大影响的操作，应事前进行评估，并告知相关方，在征得相关方同意后方可实施操作。

第二十七条 应用系统进行关闭维护、各节点设备进行停电检修，应事前征得局网信办同意，并提前 1 周在地质云门户公告和其他方式告知用户。

第七章　保障措施

第二十八条 “地质云”各节点单位应设立并建实“地质云”运行维护相关责任部门和岗位。

第二十九条 “地质云”各节点单位应将“地质云”运行维护纳入单位日常性工作，构建常态化运行机制，与单位业务发展同步规划、同步推进。

第三十条 “地质云”运行维护相关部门和岗位人员应积极参加云技术和应用培训。

第三十一条 “地质云”主节点单位负责地质云资源和运行记录的备

份。每天在同城备份中心、异地备份中心分别备份。各应用系统实时备份动态数据；至少每周备份一次本系统增量数据。地质云平台和各应用系统应每 3 个月将所拥有的资源和运行记录做 1 次数据归档。

各分节点单位负责本节点地质云资源和运行记录的备份和相关数据归档。

第八章　监督检查

第三十二条 局网信办建立“地质云”节点运行评估指标体系，每年对节点单位的地质数据上云和实体数据下载量、地质信息产品上云和实体数据下载量、应用系统云化比例、云平台使用效率、网络安全状况等进行综合评估，并通报评估结果。

第三十三条 局网信办不定期对各节点运行维护情况进行检查，及时通报检查结果，并组织开展“地质云”运行维护的考核和奖惩。

第九章　附 则

第三十四条 “地质云”用户管理、网络安全管理办法另行制定。

第三十五条 本办法由中国地质调查局网络安全和信息化领导小组办公室负责解释。

第条 本办法自发布之日起试行。

附件:

1. 地质数据上云申请表

2. 地质数据、地质信息产品、应用系统、软件工具变更申请表

3.地质数据、地质信息产品、应用系统、软件工具、设备下云申请表

4.地质信息产品上云申请表

5.应用系统上云申请表

6.软件工具上云申请表

7.新增软硬件设备申请表

附件 1

地质数据上云申请表

单位：

序号	数据集（库）名称	数据摘要	数据分级	用户获取途径	共享服务对象	数据容量	数据类型	备注

我单位承诺以上地质数据采集了元数据信息，编制了数据资源目录，明确了共享服务的分级分类属性，进行了涉密审查和定级，符合有关要求。申请上云。

单位（盖章）：

年　月　日

附件 2

地质数据、地质信息产品、应用系统、软件工具
变更申请表

单位：

类　别	资源编号	资源名称	变更内容	变更理由	备注
1.地质数据					
2.地质信息产品					
3.应用系统					
4.软件工具					

我单位承诺以上地质数据和产品更新了元数据信息、资源目录，明确了共享服务的分级分类属性，进行了涉密审查和定级；开展了以上列表中应用系统、软件工具功能、性能及安全测试。符合有关要求。特申请变更。

单位（盖章）：

年　月　日

附件 3

地质数据、地质信息产品、应用系统、软件工具、设备下云申请表

单位：

类　别	资源编号	资源名称	下云理由	备注
1.地质数据				
2.地质信息产品				
3.应用系统				
4.软件工具				
5.软硬件设备				

我单位承诺以上信息符合实际情况。特申请下云。

单位（盖章）：

年　月　日

附件 4

地质信息产品上云申请表

序号	产品名称	产品摘要	一级类别	二级类别	共享服务类别	用户获取途径	共享服务对象	数据容量	数据类型	备注

我单位承诺以上地质信息产品采集了元数据信息，编制了产品缩略图，编制了产品资源目录，明确了共享服务的分级分类属性，进行了涉密审查和定级，符合有关要求。特申请上云。

单位（盖章）：

年　　月　　日

附件 5

应用系统上云申请表

单位：

一、应用系统详细信息表			
系统名称			
系统简述			
系统用户			
申请单位			
联系人		联系电话	
操作系统		操作系统是否改造	
数据库类型			
结构数据存储量		结构数据月增量	
非结构数据量		非结构数据月增量	
所属网络		是否用到VPN	
特殊外设			
商用软件			
关联业务系统名称及其所在网 络		本系统与其他系统耦合程度	
允许系统停机割接时间		系统等级保护级别	
备 注			
二、云基础设施资源需求			
CPU			
内 存			
存 储			
所属网络			
公网带宽			

操作系统	
空间数据库	
云GIS软件	
其他公共软件	
备 注	
三、授理信息	
授理情况	
授理人	
上云时间	

我单位承诺开展了以上应用系统功能、性能及安全测试，符合有关要求。特申请上云。

单位（盖章）

年　月　日

附件：

1. 应用系统开发报告（含系统接口参数）
2. 应用系统测试报告
3. 应用系统定级报告
4. 专家评审意见 等

附件 6

软件工具上云申请表

单位：

一、软件工具详细信息表			
软件名称			
软件简述			
研发单位			
研发联系人		联系电话	
操作系统		操作系统是否改造	
数据库类型			
特殊外设			
商用软件			
备 注			
二、云资源需求			
CPU			
内 存			
存 储			
操作系统			
空间数据库			
云GIS软件			
其他公共软件			
备 注			
三、授理信息			
授理情况			
授理人			
上云时间			

我单位承诺开展了以上软件工具功能、性能及安全测试，符合有关要求。特申请上云。

单位（盖章）

年　月　日

附件：

1. 软件工具开发报告
2. 软件工具测试报告
3. 专家评审意见 等

附件 7

新增软硬件设备申请表

单位：

编号	设备名称	设备型号与参数	备 注

我单位承诺以上设备符合“地质云”技术框架及有关要求。特申请上云。

单位（盖章）：

年　　月　　日

“地质云”用户管理办法（试行）

第一章　总 则

第一条 为规范中国地质调查局（以下简称“地调局”）“地质云”的用户管理，保障“地质云”安全、有序运行，防范应用风险，根据国家的有关法律、技术标准，国土资源部和地调局的有关规定，结合“地质云”实际情况，制定本办法。

第二条 本办法适用于“地质云”平台和所集成的应用系统用户的创建、变更和注销等行为的管理。

第三条 总体要求

（一）统筹规划，分类管理

构建统一的“地质云”用户体系。地质云用户分为管理员用户、局系统用户和社会用户三类。

管理员用户分为地质云超级管理员和系统管理员，系统管理员包括地质云门户系统管理员、地质云基础设施系统管理员、地质云数据管理员、地质云产品管理员、各应用系统管理员、各节点系统管理员等。管理员用户应经过审批。

局系统用户依据其在管理或业务推进体系所承担的职责，分为局领导、局业务部室领导、局机关处长、局机关主办人员、局直属单位领导、局直属单位处（室）负责人、普通职员，和计划协调人、计划首席科学家、工程首席专家、二级项目负责人、项目人员（技术审核）和一般项目人员等用户层级。局系统用户应实名注册并经过审核。

社会用户为登记个人信息并通过实名认证的社会公众，包括中国公民

及外国公民。一般浏览用户不纳入“地质云”用户管理。

（二）统一认证，分系统授权

地质云门户对用户实行统一认证，保存用户基本信息，并授予用户基本权限；各应用系统接受地质云门户认证的用户基本信息，审核用户提供的扩展信息，根据用户角色和其他要求，对用户进行应用系统授权，实现“用户-角色-权限”的一体化管理。

（三）信息真实、操作方便

“地质云”用户采用实名制。用户信息的采集和确认流程遵循必要、自助、在线的原则。确保用户信息安全。

第二章　用户信息构成

第四条　“地质云”门户注册的用户信息包括个人信息、岗位信息和附加信息等用户基本信息；应用系统自行确定用户的扩展信息。通过审核的方式，建立地质云门户用户信息和应用系统用户信息的绑定和同步。

“地质云”门户上注册的用户基本信息包括：

（一）个人信息。为用户注册所需的标识和个人身份信息，包括用户名称（ID）、密码、真实姓名、性别、工作单位、身份证号（外籍人员使用护照号）、移动电话、电子邮箱等。个人信息为必填项，管理员用户、局系统用户和社会用户都应提供。

（二）岗位信息。为用户的管理职务或在业务推进体系中所承担的职责，局系统用户必须提供岗位信息，社会用户仅需要时提供。主要包括以下两类：

1.按组织架构分为：局领导、局业务部室领导、局机关处长、局机关主办人员、局直属单位领导、局直属单位处（室）负责人、普通职员等七种。

2.按地质调查项目业务运行结构分为:计划协调人、计划首席科学家、工程首席专家、二级项目负责人、项目人员（技术审核）、一般项目人员等六种。

3.职务名称：为补充的职务信息，包括行政职务、党内职务、社会兼职等。

（三）附加信息。用于进一步描述用户特征，为选填项，适用于局系统用户和社会用户。具体包括:

1.专业背景：专业、最高学历、学位、职称、技术职级、研究领域。

2.关联信息：涉密证号、单位性质、组织机构代码、法人代表、单位所在地址、机构证明等。

3.资源需求偏好：对地质云资源的需求、偏好等信息。

第三章　管理员用户的设置和职责

第五条 管理员用户是对地质云平台、各应用系统和各节点进行管理的用户，拥有较高权限和较大责任。该类用户应为地调局直属单位的在编人员，应具有较高的政治素养。

（一）地质云主节点设置地质云超级管理员和系统管理员，系统管理员可根据情况细分为地质云门户系统管理员、地质云基础设施系统管理员、地质云数据管理员、地质云产品管理员、地质云应用系统管理员等。各管理员用户的职责包括:

1.地质云超级管理员。负责地质云平台的总体管理和调度，承担地质云所有系统管理员用户的创建、授权和管理。负责对各节点管理员的业务指导。该管理员拥有整个“地质云”用户和资源管理的最高权限。

2.地质云门户系统管理员。负责地质云门户系统的管理，承担在地质云门户注册的“社会用户”的创建、信息维护、身份确认、用户注销和相

关证据存档。

3.地质云基础设施系统管理员。负责地质云基础设施平台的管理，承担对用户申请的基础设施资源进行审核和分配。

4.地质云数据管理员。负责地质云地质数据系统的管理，承担对用户申请的地质数据资源进行审核和处理。

5.地质云产品管理员。负责地质云地质信息产品系统的管理，承担对用户申请的地质信息产品资源进行审核和处理。

6.地质云应用系统管理员。每个应用系统都应设置系统管理员，拥有该应用系统的最高权限，负责该应用系统的管理；承担该应用系统用户管理工作。

（二）在分节点设置节点系统管理员，还可根据情况设节点应用系统管理员。

1.节点系统管理员。 每个节点都应设置系统管理员，拥有该节点系统的最高权限，负责所在节点地质云平台的管理；承担本节点单位局系统用户的创建、信息维护、身份确认、用户注销和相关证据存档等工作。

2. 节点系统管理员还可根据情况创建本节点的应用系统管理员用户，授权负责本节点相关系统的管理工作。

第六条 管理员用户的创建、变更和注销。

（一）所有管理员用户的创建均需填写《管理员用户审批表》（附件1）经所在单位审核后，报局网信办审批。

（二）管理员用户信息发生变更时，需重新填写《管理员用户审批表》，进行审批确认。审批程序同管理员用户创建。

（三）管理员用户注销时，账户应封存，其操作记录和访问日志应长期保存。

第七条 管理员用户的监督

局网信办将以巡查或抽查的方式，对管理员用户的管理行为进行日常

监管和合规性审查。

第四章　局系统用户的管理

第八条 局系统用户创建。局系统用户包括国土资源部机关相关人员、地调局机关人员和局直属单位在编人员以及授权的局直属单位长期聘用人员。其创建流程为:

（一）局系统用户由节点系统管理员依据所在单位人事信息创建，系统自动生成《局系统用户账号申请与变更表》（附件 2）。

（二）节点单位人事部门确认新增用户的信息，并在《局系统用户账号申请与变更表》上确认，由所在节点系统管理员存档管理。

（三）云基础设施系统管理员为用户分配默认的基础设施资源。

（四）各应用系统管理员根据用户基本信息为用户授予访问权限。

（五）节点系统管理员将创建的用户名、口令告知申请人，并要求申请人及时变更口令。

第九条 局系统用户变更。

（一）用户本人在线填写《局系统用户账号申请与变更表》，填写变更事项和理由，提交单位人事部门审核。局系统用户因单位人事信息变化引起的变更，由所在节点系统管理员进行更新，系统自动生成《局系统用户账号申请与变更表》。

（二）节点系统管理员更新用户信息，并将《局系统用户账号申请与变更表》存档管理。

（三）节点系统管理员协调为该用户变更可使用的基础设施资源和应用系统的访问权限。

（四）节点系统管理员通知用户信息变更。

第十条 局系统用户封存。

（一）局系统用户因工作岗位变动、调动、离职等原因需封存其“地质云”账号时，由所在单位人事部门通知本人填写《局系统用户账号申请与变更表》并审核，提交节点系统管理员执行封存。

（二）对于超过半年没有激活或登录使用的局系统用户账户，系统自动进行封存。

（三）用户在出现极端情况（如恶意下载）下，系统自动进行封存。

（四）由所在节点的系统管理员对用户使用记录进行长期存档。

第五章 社会用户的管理

第十一条 “社会用户”通过地质云门户（互联网）进行自助注册创建（附件 3），社会用户注册需提供个人信息，自愿填写岗位信息和附加信息。新产生的社会用户具有默认的基本权限。

第十二条 社会用户的变更。

（一）社会用户如需变更信息，需要在线填写《社会用户账号申请与变更表》（附件 3）。

（二）社会用户如需获得“地质云”应用系统的相关权限，需在线填写《社会用户账号申请与变更表》，补充相应的岗位信息和附加信息以及扩充信息。具体按照各应用系统的要求执行。

（三）社会用户之前经过实名认证的，变更前应提供正确的实名认证信息，由地质云门户系统管理员进行审核。

（四）地质云门户系统管理员对社会用户的信息变更、身份绑定进行审核。

（五）地质云应用系统管理员根据社会用户信息变更，授予相应的应用系统访问权限。

（六）社会用户自动获得信息变更及权限的反馈。

第十三条 社会用户的注销。

（一）社会用户通过“地质云”门户（互联网）自助提交注销申请。

（二）社会用户之前经过实名认证的，注销时应提供正确的实名认证信息，由地质云门户系统管理员进行审核。

（三）一旦社会用户进行注销操作，地质云门户将自动注销其账号，自动回收“地质云”上相关应用系统的权限。

（四）对于超过一年没有激活或登录使用的社会用户账户，自动进行封存。

（五）用户在出现极端情况（如恶意下载）下，自动进行封存。

（六）封存或注销的社会用户，其以往的操作记录和访问日志由地质云门户长期保存。

第六章　用户信息管理

第十四条 “地质云”用户基本信息实行集中存放，并由地质云门户系统管理员负责定期备份、存档。各应用系统的用户信息由各自的应用系统管理员进行定期备份和存档。

第十五条 “地质云”的管理员用户应严格执行国家有关法律，遵守国土资源部、地调局和本单位的相关规章制度，不得将用户信息向任何第三方泄露或公开。

第七章　附 则

第十六条 用户使用须知

地质云门户和应用系统在用户注册时应以“用户使用须知”的形式告知用户使用“地质云”的权利和义务，并设置确认机制。用户须知应至少

包括以下内容:

1. 用户可使用地质云授权的资源;

2. 严格执行国家有关法律、法规;

3. 遵守“地质云”信息系统账户与密码安全管理规定;

4. 遵守“地质云”数据、产品保密及使用范围规定;

5. 用户使用环境应符合网络安全要求;

6. 确认提供的用户信息完整、真实;

7. 免责条款。

第十七条 “地质云”禁止创建任何内容的共同使用的集体帐户。

第十八条 本办法由中国地质调查局网络安全和信息化领导小组办公室负责解释。

第十九条 本办法自发布之日起试行。

附件: 1.管理员用户审批表

2.局系统用户账号申请与变更表

3.社会用户账户申请与变更表

附件 1:

管理员用户审批表

编码：CGS 记录编号：[201　　]　　号

姓　名		工作单位	
身份证号		出生年月	
行政职务		政治面貌	
移动电话		电子邮箱	
管理员类别	☐地质云超级管理员 ☐地质云系统管理员　名称：_____ ☐节点系统管理员 ☐其他：_____		
所在单位			
何时、何地受过何种奖励和处分			
历史上有无问题，是否受过刑事处分			
健康状况能否适应工作			
现工作表现			
人事部门意见	签字：　　年　月　日		
单位意见	（盖　章）　　签字：　　年　月　日		
局网信办意见	（盖　章）　　签字：　　年　月　日		

备 注	

件附 2:

局系统用户账号申请与变更表

编码：CGS 记录编号：[201] 号

用户信息				
个人信息	用户名称（ID）		真实姓名	
	性 别	□男 □女	工作单位	
	身份证号*			
	移动电话		电子邮箱	
岗位信息	职务类别	□局领导，职务：_____ □局业务部室领导，部室：_____ □局机关处长，处室：_____ □局机关主办人员，处室：_____ □直属单位领导，职务：_____ □直属单位处（室）负责人，处室：_____ □普通职员，处室：_____ □其他，_____		
	项目职责	□计划协调人，所属计划：_____ □计划首席科学家，所属计划：_____ □工程首席专家，所属工程：_____ □二级项目负责人，所属项目：_____ □项目人员（技术审核），所属项目：_____ □一般项目人员，所属项目：_____		

<table>
<tr><td rowspan="4"></td><td></td><td colspan="3">□其他，_____</td></tr>
<tr><td colspan="4">职务名称（补充）</td></tr>
<tr><td>行政职务</td><td></td><td>党内职务</td><td></td></tr>
<tr><td>社会兼职</td><td></td><td>其他</td><td></td></tr>
<tr><td rowspan="8">附加信息</td><td colspan="4">专业背景</td></tr>
<tr><td>专 业</td><td></td><td>职 称</td><td></td></tr>
<tr><td>最高学历</td><td></td><td>学 位</td><td></td></tr>
<tr><td>职 级</td><td></td><td>研究领域</td><td></td></tr>
<tr><td colspan="4">关联信息</td></tr>
<tr><td>涉密证号</td><td></td><td></td><td></td></tr>
<tr><td colspan="4">其 他</td></tr>
<tr><td>资源偏好</td><td></td><td></td><td></td></tr>
<tr><td colspan="5">申请和变更</td></tr>
<tr><td>申请类型</td><td colspan="4">□新建 □变更 □封存</td></tr>
<tr><td>申请(变更)说明</td><td colspan="4"></td></tr>
<tr><td>申请人</td><td colspan="4">签字: 年 月 日</td></tr>
<tr><td>单位人事部门审核意见</td><td colspan="4">签字: 年 月 日</td></tr>
<tr><td>地质云门户落实情况记录</td><td colspan="4">签字: 年 月 日</td></tr>
</table>

备 注	

* 外籍人员可填写护照号。

附件 3:

社会用户账号申请与变更表

编码：CGS 记录编号：[201　]　号

用户信息				
个人（必填）	用户名称（ID）		真实姓名	
	性　　别	□男　□女	工作单位	
	身份证号*			
	移动电话		电子邮箱	
岗位信息（选填）	项目职责	□二级项目负责人，所属项目：_____ □项目人员（技术审核），所属项目：_____ □一般项目人员，所属项目：_____ □其他，_____		
	职务名称			
	行政职务		党内职务	
	社会兼职		其他	
附加信息（选填）	专业背景			
	专　业		职　称	
	最高学历		学　位	
	职　级		研究领域	
	关联信息			
	涉密证号		单位性质	
	组织机构代码		法人代表	
	机构证明**		单位地址	
	其　他			
	资源偏好			
申请和变更				
申请类型	□新建　□变更　□封存			

申请(变更)说明	
申请人	签字: 年 月 日
地质门户系统管理员处理情况	签字: 年 月 日
地质云应用系统管理员落实情况	签字: 年 月 日
备 注	

* 外籍人员可填写护照号。

** 以附件提交组织机构证明的

“地质云”网络安全组织管理规定（试行）

第一章　总　则

第一条　为推进“地质云”建设，加强地质调查局网络安全和信息化组织的管理，提高网络安全组织建设的制度化、规范化水平，协调组织相关力量开展地质调查网络安全活动，保障地质调查网络和信息系统安全稳定运行，依据国家网络安全法和有关技术标准、国土资源部网络安全有关规定、“地质云”网络安全管理办法等，制定本规定。

第二条　本规定适用于中国地质调查局（以下简称“地调局”）“地质云”建设主节点和各分节点单位（以下简称“各单位”）的网络安全组织管理。

第二章　组织机构

第三条　各单位应建立包括领导层、管理层和执行层的三层网络安全管理组织架构。

1. 领导层：由各单位网络安全和信息化领导小组（以下简称“网信领导小组”）承担。

2. 管理层：由各单位网络安全和信息化领导小组办公室（以下简称“网信办”）承担。

3. 执行层：由各单位相关网络安全部门、专家顾问团队和外部服务商组成。

第四条 各单位网络安全机构设置要求。

1. 网信领导小组：一般由本单位主要领导担任组长。在成员构成上，至少应包括行政、信息化、人事、财务、科技、资产等管理部门负责人和业务生产部门负责人。

2. 网信办：一般设在本单位网络安全归口管理的部门，成员可由相关人员兼任。

3. 执行部门：一般由本单位网络系统运行维护的部门牵头，其他涉及应用系统网络安全的部门参加。

第三章 职责分工

第五条 各单位网络安全机构的职责分工。

1. 网信领导小组：作为本单位网络安全管理工作的最高领导机构，负责对安全重大事项进行决策，审定本单位网络安

全工作方针、政策和整体规划，协调解决网络安全相关的重大问题。

2. 网信办：全面负责管理本单位网络安全方面的各项工作。主要包括组织编制网络安全管理相关制度、办法及标准；组织开展网络安全等级保护和安全评估工作；组织开展单位内部的网络安全检查；组织开展网络安全知识的培训和宣贯工作；组织并协调网络安全重大事件的处理；负责单位内部、外部组织和机构的网络安全沟通、协调和合作工作。

3. 执行部门：配合相关工作的开展。

第六条 各类岗位的设置要求与职责分工。

1. 网络安全主管。一般为本单位网信办成员，分工负责网络安全管理工作；按照国家相关要求，组织开展网络安全及监督检查工作。

2. 网络安全管理员。协助网络安全主管开展各项工作。主要负责组织本单位网络安全等级保护和安全评估工作、组织开展本单位网络安全检查和整改，协调网络安全重大事件的处理。建有等级保护第三级系统（或有较多信息系统）的单位要求专职。

3. 机房管理员。负责机房安全管理，主要包括基础设施、各业务系统硬件环境的日常巡检、故障排查等工作。

4. 网络管理员。负责单位网络的运行维护工作；负责对单位内网络、各专线网络、业务系统相关网络、通讯网络以及网络相关设备等进行部署配置、日常巡检、故障排查、优化升级等工作。

5. 系统管理员。负责主机操作系统、数据库系统、终端的运行维护工作；负责对操作系统、数据库、终端等进行部署配置、日常巡检、故障排查、优化升级、防病毒等工作。

6.应用系统管理员。负责各个应用系统的运行维护工作，以及处理业务人员提出的相关业务需求等工作。

第四章　工作沟通协调机制

第七条　　单位内部的工作沟通协调机制。

1. 单位网络安全相关部门，在本单位网信办的组织协调下，承担网络安全的相关工作。

2. 单位网络安全相关岗位人员，在本单位网络安全主管的组织协调下，配合执行各项有关任务。

3. 单位业务和其他部门，在本单位网信领导小组办公室的组织协调下，配合执行相关管理制度和各项有关任务。

第八条　　地调局与各单位之间的工作沟通协调机制。

1. 各单位网信领导小组，在地调局网信领导小组的指导下，组织开展各项活动。

2. 各单位网信办，在本单位网信领导小组领导下，在局网信办指导下，组织开展各项活动。

第九条 地调局与国土资源部网络安全组织沟通机制。

1. 局网信办负责与国土资源部网络安全和信息化领导小组办公室定期沟通。

2. 各节点网络安全组织，接受国土资源部网络安全组织的检查、指导。

第十条 各单位与地方网络安全管理组织沟通机制。

各单位网信办负责与所在地政府网络安全管理机构开展沟通协调工作。

第十一条 外部沟通交流机制。

各节点网络安全组织，根据业务需要，构建与外部机构（政府部门、供货商、电信运营商、兄弟单位等）的沟通交流机制。

第五章 附 则

第十二条 本规定由中国地质调查局网络安全和信息化领导小组办公室负责解释。

第十三条 本规定自发布之日起试行。

“地质云”网络安全等级保护管理规定（试行）

第一章　总　则

第一条　为推进“地质云”建设，规范地质调查网络安全等级保护管理，提高网络安全保障能力和水平，依据国家网络安全法和有关技术标准、国土资源部网络安全有关规定、“地质云”网络安全管理办法等，制定本规定。

第二条　本规定适用于中国地质调查局（以下简称“地调局”）“地质云”所涵盖的非涉密网络和信息系统的安全等级保护管理工作。

第三条　“地质云”建设主节点和各分节点单位（以下简称“各单位”）是该节点运行维护的信息系统的安全责任单位，应当按照网络安全等级保护制度的要求，履行安全保护义务，保障网络免受干扰、破坏或者未经授权的访问，防止网络数据泄露或被窃取、篡改。

第二章　系统定级

第四条 界定定级对象。定级对象应具有如下三个基本特征：

1.具有唯一确定的安全责任单位。作为定级对象的信息系统应能够唯一地确定其安全责任单位。

2.具有信息系统的基本要素。作为定级对象的信息系统应该是由相关的和配套的设备、设施按照一定的应用目标和规则组成的有形实体。

3.承载单一或相对独立的业务应用。定级对象承载单一的业务应用是指该业务应用的业务流程独立，且与其他业务应用没有数据交换，且独享所有信息处理设备。

为了体现重要部分重点保护，可将较大的信息系统划分为若干个较小的、可能具有不同安全保护等级的定级对象。

第五条 确定安全保护等级。根据定级对象系统在国家安全、经济建设、社会生活中的重要程度，信息系统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安全保护等级。安全保护等级划分为以下五级：

第一级，信息系统受到破坏后，会对公民、法人和其他组织的合法权益造成损害，但不损害国家安全、社会秩序和公共利益。

第二级，信息系统受到破坏后，会对公民、法人和其他组织的合法权益产生严重损害，或者对社会秩序和公共利益造成损害，但不损害国家安全。

第三级，信息系统受到破坏后，会对社会秩序和公共利益造成严重损害，或者对国家安全造成损害。

第四级，信息系统受到破坏后，会对社会秩序和公共利益造成特别严重损害，或者对国家安全造成严重损害。

第五级，信息系统受到破坏后，会对国家安全造成特别严重损害。

第六条 对信息系统中的业务信息和系统服务可分别进行安全保护定级。作为定级对象的信息系统的安全保护等级由业务信息安全保护等级和系统服务安全保护等级的较高者决定。

由于业务信息和系统服务受到破坏时所侵害的客体和对客体的侵害程度可能会有所不同，在定级过程中，需要分别处理这两种危害。

第七条 编制定级报告。信息系统的安全责任单位依据公安部《信息安全等级保护管理办法》和国家标准《信息系统安全等级保护定级指南》（GB/T 22240）相关要求，编制信息系统安全保护等级定级报告。

第八条 专家评审。安全责任单位组织信息安全领域的专家和业务专家，对初步定级结果的合理性进行论证、评审，出具专家评审意见。对拟确定为第四级以上信息系统的，应当请国家信息安全保护等级专家评审委员会评审。

第九条　审核批准。通过专家评审的信息系统定级报告，经过安全责任单位研究同意后，报上级主管单位批复。各单位负责运行的信息系统，安全定级报告经地调局网络安全与信息化领导小组办公室（以下简称“局网信办”）审核后，报地调局批复；地调局运行维护的信息系统，安全定级报告由局网信办负责报送国土资源部相关部门批复。

第十条　新建信息系统在设计、规划阶段应确定安全保护等级。

第十一条　跨省级行政区或全国联网运行的信息系统由局网信办统一确定安全保护等级。

第十二条　特定定级对象定级说明。

对于基础信息网络、云计算平台、大数据平台等起支撑作用的定级对象，应根据其承载或将要承载的等级保护对象的重要程度确定其安全保护等级，原则上应不低于其承载的等级保护对象的安全保护等级。

关键信息基础设施的安全保护等级应不低于第三级。

第三章　系统定级备案

第十三条　已运行的第二级以上信息系统，应当在安全保护等级确定后 30 日内，由信息系统安全责任单位到所在地设区的市级以上公安机关办理备案手续。

新建第二级以上信息系统，应当在投入运行后 30 日内，由安全责任单位到所在地设区的市级以上公安机关办理备案手续。

全国联网的地质调查信息系统，由局网信办负责向公安部办理备案手续。全国联网的的地质调查信息系统在各地运行、应用的分系统，应由分系统安全责任单位当向当地设区的市级以上公安机关备案。

第十四条 向公安机关办理信息系统安全保护等级备案手续时，应当填写《信息系统安全等级保护备案表》，所提供材料以当地公安机关要求为准。

第十五条 信息系统备案后，将收到公安部门的信息系统安全等级保护备案证明。备案材料若不符合相关要求的，应及时予以纠正、补充；若公安机关认为安全等级保护定级不准的，安全责任单位应及时组织重新进行信息系统定级，重新办理备案手续。

第四章　系统定期检查

第十六条 局网信办组织对第三级以上的信息系统的安全等级保护工作进行定期检查。对第三级信息系统每年至少检查一次，对第四级信息系统每半年至少检查一次，对第五级信息

系统，配合国家专门部门进行检查。局网信办组织的检查可和公安部门进行的检查一同进行。检查事项主要包括:

（一） 信息系统安全需求是否发生变化，原定保护等级是否准确;

（二） 安全责任单位安全管理制度、措施的落实情况;

（三） 安全责任单位及其主管部门对信息系统安全状况的检查情况;

（四） 系统安全等级测评是否符合要求;

（五） 信息安全产品使用是否符合要求;

（六） 信息系统安全整改情况;

（七） 备案材料与安全责任单位、信息系统的符合情况;

（八） 其他应当进行监督检查的事项。

第十七条 信息系统安全责任单位应当接受公安机关、国家指定的专门部门的网络安全监督、检查、指导，如实向公安机关、国家指定的专门部门提供下列有关信息安全保护的信息资料及数据文件:

（一） 信息系统备案事项变更情况;

（二） 安全组织、人员的变动情况;

（三） 信息安全管理制度、措施变更情况;

（四） 信息系统运行状况记录;

（五） 安全责任单位及主管部门定期对信息系统安全状况的检查记录;

（六） 对信息系统开展等级测评的技术测评报告;

（七） 信息安全产品使用的变更情况;

（八） 信息安全事件应急预案，信息安全事件应急处置结果报告;

（九） 信息系统安全建设、整改结果报告。

第五章　等级测评

第十八条　选择测评机构。第三级以上信息系统应当选择符合下列条件的等级保护测评机构进行测评:

（一） 在中华人民共和国境内注册成立（港澳台地区除外);

（二） 由中国公民投资、中国法人投资或者国家投资的企事业单位（港澳台地区除外);

（三） 从事相关检测评估工作两年以上，无违法记录;

（四） 工作人员仅限于中国公民;

（五） 法人及主要业务、技术人员无犯罪记录;

（六） 使用的技术装备、设施应当符合本规定对信息安全产品的要求;

（七） 具有完备的保密管理、项目管理、质量管理、人员管理和培训教育等安全管理制度;

（八）对国家安全、社会秩序、公共利益不构成威胁。

第十九条 等级测评。信息系统建设完成后，定期对信息系统安全等级状况开展等级测评。

第三级信息系统应当每年至少进行一次等级测评;

第四级信息系统应当每半年至少进行一次等级测评;

第五级信息系统应当依据特殊安全需求进行等级测评。

第二十条 自查。各单位应当定期对信息系统安全状况、安全保护制度及措施的落实情况进行自查。第三级信息系统应当每年至少进行一次自查,第四级信息系统应当每半年至少进行一次自查,第五级信息系统应当依据特殊安全需求进行自查。

第二十一条 经测评或者自查,信息系统安全状况未达到安全保护等级要求的，应当制定方案进行整改。

第六章 安全建设整改

第二十二条 建设整改。信息系统安全责任单位根据信息系统安全等级，按照国家政策、标准开展安全建设整改;

第二十三条 收到公安机关发出的整改通知后,信息系统安全责任单位应当根据整改通知要求,按照管理规范和技术标准进行整改。整改完成后，应当将整改报告向公安机关备案，并接受公安机关可能组织的整改情况检查。

第七章 等级变更与终止

第二十四条 当等级保护对象所处理的信息、业务状态和系统服务范围发生变化，可能导致业务信息安全或系统服务安全受到破坏后的受侵害客体和对客体的侵害程度发生变化时，应根据本制度要求重新确定定级对象和安全保护等级，完成变更备案，并重新进行等级测评。

第二十五条 信息系统终止阶段是等级保护实施的最后环节。当信息系统被转移、终止或废弃时，应慎重处理系统内的敏感信息。对还要有部分信息转移到新系统的拟终止或废弃信息系统，在终止处理中应确保信息转移、设备迁移和介质销毁等方面的安全。

在信息系统终止阶段关注信息转移、暂存和清除，设备迁移或废弃，存储介质的清除或销毁等活动。

第八章 附 则

第二十六条 本规定由中国地质调查局网络安全和信息化领导小组办公室负责解释。

第二十七条 本规定自发行之日起试行。

“地质云”网络安全事件管理规定（试行）

第一章　总 则

第一条　为推进“地质云”建设，加强地质调查网络信息系统安全事件的管理，降低网络安全事件带来的损失和影响，提高信息系统安全事件管理的制度化、规范化水平，依据国家网络安全法、国土资源部网络安全有关规定、“地质云”网络安全管理办法等，制定本规定。

第二条　本规定所称网络安全事件，是指由于自然或者人为以及软硬件本身缺陷或故障等原因，对信息系统造成危害、或对社会造成负面影响的事件。

第三条　本规定适用于“地质云”所涵盖的非涉密网络和信息系统的安全事件管理。

第二章　网络安全事件的分类分级

第四条　根据网络安全事件的起因、表现、结果等，网络安全事件分为以下七类:

（一）有害程序事件，是指蓄意制造、传播有害程序，或

是因受到有害程序的影响而导致的网络安全事件。有害程序危害系统中数据、应用程序或操作系统的保密性、完整性或可用性，或影响信息系统的正常运行。有害程序事件包括计算机病毒事件、蠕虫事件、特洛伊木马事件、僵尸网络事件、混合攻击程序事件、网页内嵌恶意代码事件和其它有害程序事件等 7 个子类。

（二）网络攻击事件，是指通过网络或其他技术手段，利用信息系统的配置缺陷、协议缺陷、程序缺陷或使用暴力攻击对信息系统实施攻击，并造成信息系统异常或对信息系统当前运行造成潜在危害的网络安全事件。网络攻击事件包括拒绝服务攻击事件、后门攻击事件、漏洞攻击事件、网络扫描窃听事件、网络钓鱼事件、干扰事件和其他网络攻击事件等 7 个子类。

（三）信息破坏事件，是指通过网络或其他技术手段，造成信息系统中的信息被篡改、假冒、泄漏、窃取等而导致的网络安全事件。信息破坏事件包括信息篡改事件、信息假冒事件、信息泄漏事件、信息窃取事件、信息丢失事件和其它信息破坏事件等 6 个子类。

（四）信息内容安全事件，是指利用信息网络发布、传播危害国家安全、社会稳定和公共利益的内容的安全事件。信息内容安全事件包括违反宪法和法律、行政法规的网络安全事件；针对社会事项进行讨论、评论形成网上敏感的舆论热

点，出现一定规模炒作的网络安全事件；组织串连、煽动集会游行的网络安全事件；其他信息内容安全事件等 4 个子类。

（五）设备设施故障，是指由于信息系统自身故障或外围保障设施故障而导致的网络安全事件，以及人为的使用非技术手段有意或无意的造成信息系统破坏而导致的网络安全事件。设备设施故障包括软硬件自身故障、外围保障设施故障、人为破坏事故和其它设备设施故障等 4 个子类。

（六）灾害性事件，是指由于不可抗力对信息系统造成物理破坏而导致的网络安全事件。灾害性事件包括水灾、台风、地震、雷击、坍塌、火灾、恐怖袭击、战争等导致的网络安全事件。

（七）其他事件类别，是指不能归为以上 6 种基本分类的网络安全事件。

第五条 考虑网络安全事件中信息系统的重要程度、系统损失和社会影响等方面要素，将网络安全事件划分为四个级别：

（一）特别重大事件（Ⅰ级），是指能够导致特别严重影响或破坏的网络安全事件，包括以下情况：

1. 会使特别重要信息系统遭受特别严重的系统损失；

2. 产生特别重大的社会影响。

（二）重大事件（Ⅱ级），是指能够导致严重影响或破坏的网络安全事件，包括以下情况：

1．会使特别重要信息系统遭受严重的系统损失、或使重要信息系统遭受特别严重的系统损失;

2．产生的重大的社会影响。

（三） 较大事件（Ⅲ级），是指能够导致较严重影响或破坏的网络安全事件，包括以下情况:

1．会使特别重要信息系统遭受较大的系统损失、或使重要信息系统遭受严重的系统损失、一般信息系统遭受特别严重的系统损失;

2．产生较大的社会影响。

（四） 一般事件（Ⅳ级），是指不满足以上条件的网络安全事件，包括以下情况:

1．会使特别重要信息系统遭受较小的系统损失、或使重要信息系统遭受较大的系统损失，一般信息系统遭受严重或严重以下级别的系统损失;

2．产生一般的社会影响。

第三章　网络安全事件的处理流程

第六条　安全事件管理分为安全事件监控和安全事件处理。

安全事件监控，包括预防预警和对安全事件迹象的日常检测分析。通过公安网络监控部门等安全组织发布的安全预

警信息，及时发布可能招致攻击的网络互联设备和计算机的安全漏洞、病毒的动态变化趋势等预警信息；建立网络和信息系统的监测体系，对异常流量来源实行监控及控制。

安全事件处理是对被发现的安全事件的响应处理过程，主要处理流程包括报告、响应处理、评价整改等。

第七条 报告。

（一）当事人发现网络安全事件时，应立即向本单位网络安全主管报告，由本单位网络安全主管初步分析和判断事件类型及级别，并通知相关人员处理。重大事件（II级）及以上事件，本单位网络安全主管须1小时内向本单位网络安全和信息化领导小组办公室领导汇报，并在2小时内向中国地质调查局网络安全与信息化领导小组办公室报告，对涉及人为故意破坏事件应同时报告公安机关。

（二）报告方式分为口头电话报告和书面报告。如遇紧急情况，可先电话报告，随后附上书面报告。无论是口头报告还是书面报告，参与响应、处理等相关人员都需做好书面记录，以便跟踪和统计。

第八条 响应处理。

（一）网络安全技术人员可对安全事件做出最初响应，并在网络安全管理部门负责人或单位分管领导的指导下，针对不同类型的安全事件，按照国家有关部门发布的技术规范、“地

质云”地质调查网络安全管理办法以及相关管理规定，对安全事件做进一步处理。

（二）事件响应及处理者在处理安全事件时应考虑以下优先次序：

1. 保护人员的生命与安全；

2. 保护重要的数据资源；

3. 保护敏感的设备和资料；

4. 防止系统被损坏；

5. 将单位遭受的损失降至最小。

第九条 评价整改。

（一）网络安全事件处理完成之后，网络安全管理部门应对事件或故障的类型、严重程度、发生的原因、性质、产生的损失、责任人进行调查确认，并在事件处理完成 5 个工作日内形成网络安全事件评价书面报告。

（二）总结网络安全事件中的教训，分析事件发展的趋势和模式；确定新的或经过优化的安全防护措施并立即付诸实施。

第四章 其 他

第十条 对于观察到的或怀疑的任何系统或服务的网络安全弱点，单位员工或外部人员应做好书面记录，并及时向

网络安全管理部门报告，经确认后，由相关的技术人员进行处置。

第十一条 未经网络安全管理部门允许，单位员工和外部人员禁止利用测试等方法去证明他们怀疑的网络安全弱点。测试弱点可以被解释为对系统可能的滥用，可能导致信息系统和服务的损坏。

第十二条 各单位网络安全管理部门应定期对相关人员进行培训或进行相关案例警示，减少安全事件再次发生概率，提高相关人员遇到事件的处理能力。

第五章 附 则

第十三条 本规定由中国地质调查局网络安全和信息化领导小组办公室负责解释。

第十四条 本规定自发布之日起试行。

“地质云”信息系统账户与密码安全管理规定（试行）

第一章　总　则

第一条 为推进“地质云”建设，规范地质调查网络和信息系统的账户及密码管理，保障信息系统安全、有序、稳定运行，依据国家网络安全法和相关技术标准、国土资源部网络安全有关规定、“地质云”网络安全管理办法、“地质云”用户管理办法等，制定本规定。

第二条 本规定适用于“地质云”所涵盖的非涉密网络和信息系统的用户账户及密码管理。

第三条 本规定从安全角度对“地质云”平台和各应用系统的用户账户设置和密码管理做出具体规定。

第二章　账户的创建

第四条 根据网络安全的需要，“地质云”平台和各应用系统用户账户分为以下三类:

（一）系统超级管理员账户，拥有创建、初始（密码）、变更（权限）、删除、禁止系统管理员账户和进行其他计算机信息系统安全审计等权限的账户。

（二）系统管理员账户，拥有管理普通用户、设定普通用

户访问许可、修改系统配置、安装系统组件等权限的账户。

（三）普通用户账户，拥有在被授权范围内登陆和使用信息系统的权限的账户，普通账户又细分为地调局系统工作人员账户和社会账户。

第五条 系统超级管理员原则上只配置一个；创建系统管理员账户，则需向中国地质调查局网络安全和信息化领导小组办公室（以下简称“局网信办”）提出书面申请，经核实批准后，实施账户和密码的初始化程序，并登记备查；创建普通用户，需向系统管理员提出书面申请，经其核准后，由系统管理员实施账户和密码的初始化，并登记备查。

第六条 在创建账户时，应遵循下列安全规定：

（一）账户名是账户的唯一标识码，在创建账户时应予明确，一般由用户姓名字符和数字构成；与账户捆绑的用户手机号也可作为账户名。

（二）严格限制创建公用账户，且公用账户不得具有访问敏感信息以及“写”和“执行”的系统权限。不得创建匿名账户，及时关闭任何缺省的匿名账户。

（三）细化各类账户角色，根据各系统需求，实现账户权限的最小化。

（四）系统开启对用户账户、用户权限和登录管理的日志审计功能。

（五）禁止使用空密码或与用户名相同的密码，作为初始

密码。

（六）系统管理员在通知用户初始密码时，必须采用加密或其他安全传输途径，以确保初始密码不会被中途截取。

（七）系统管理员必须强制用户在第一次登录时，修改其初始密码。

（八）严禁以任何明文形式传递和存放用户的初始密码。

（九）需要创建临时用户账户时，则由相关负责人向系统管理员提出书面申请，经核准后，再由系统管理员统一创建（临时用户账户的密码由该负责人统一指定和保管）；并且严禁在生产系统中创建临时用户或测试用户。使用完毕后，立即删除所有临时的用户账户。

第七条 密码设置标准

密码长度应最小 8 位，复杂度为数字、大写字母、小写字母、特殊符号这四类字符中的至少两种。

第三章　普通账户与密码的管理

第八条 用户密码的变更。

（一）在系统管理员创建或初始化用户账户和密码后，用户需要立即改变初始密码。

（二）用户密码必须定期进行变更，周期应不多于 3 个月，最大程度确保密码的安全性。

（三）用户丢失或遗忘密码，必须向系统管理员提出书面

密码初始化申请，经核准后，由系统管理员具体实施密码的初始化程序，然后通知有关用户，并登记备案。

（四）系统管理员在发现任何企图非法使用某用户账户的情况时，应立即强制该用户更改密码，并记录备案。

第九条 用户账户的禁止。

（一）一天内，用户连续登录失败超过 5 次时，系统应自动锁住该用户账户。

（二）用户账户在一年内没有使用，系统应自动禁用该用户账户。

（三）用户没有按密码定期变更的规定定期修改密码，超过系统设定的时限后，系统应自动禁用该用户账户。

（四）用户违反网络安全管理的有关规章制度，在经教育无效后，由信息系统管理部门负责人授权，系统管理员手工禁用该用户账户。

（五）当用户发现账户由于其他原因被禁止时，应及时报告系统管理员，系统管理员在查明原因后再为其开通，并记录在案。

第十条 用户账户的停用与封存。

（一）用户因岗位变动而不再需要使用信息系统时，系统管理员在收到该用户所在部门的书面通知后，应对该用户账户的权限进行封存，对用户以往操作记录和访问日志进行保存归档。

（二）用户离职后，系统管理员在接到该用户所在部门的书面通知后，应对该用户账户的权限进行封存，对用户以往操作记录和访问日志保存归档。

（三）为了其他特殊原因临时开设的用户账户，如不再需要，经由相关负责人或信息系统管理部门负责人同意后，应对该用户账户的权限进行封存，对用户以往操作记录和访问日志进行保存归档。

第十一条 用户账户权限的变更。

（一）用户因岗位变动或其他工作原因需要修改信息系统访问权限，其部门主管需要书面通知有关系统管理员，由系统管理员修改权限。

（二）系统管理员需要依照“账户权限的最小化”原则对用户权限分配情况进行定期检查，如有必要，将修改用户权限，并通知该用户。

第十二条 系统管理员必须对存有用户账户和密码的数据库和注册表进行严格的访问控制，严禁对其进行任何远程访问。

第十三条 系统管理员必须开启系统内建的用户账户、用户权限管理和登录管理的审计功能，并对其生成的日志文件进行妥善保管，以确保日志文件的安全性和完整性。

第十四条 系统管理员必须定期对用户账户进行清查工作，及时删除无用、无主的用户账户。

第十五条 严禁以任何理由，使用他人账户访问信息系统资源。

第四章　系统管理员账户与密码的管理

第十六条 局网信办必须对系统管理员的账户和密码采用备份保护措施。备份账户和密码记录在纸质介质上，按照系统管理员备份账户封存流程，签封后由所在部门主管人员统一管理。

第十七条 如果系统管理员密码遗忘或泄漏，或者发生紧急情况且需要使用系统管理员账户的情况下，按照系统管理员备份账户启用流程，经局网信办领导审批同意后，启用封存的系统管理员账户和密码。申请、审批和使用信息必须及时记录。封存的账户和密码一旦启用后，系统管理员必须及时变更账户和密码，并重新按照系统管理员备份账户封存流程，予以签封保存。

第十八条 系统管理员离开岗位后，新系统管理员应立即进行有关各级账户密码的修改，并按系统管理备份账户封存流程，将新的管理员账户和密码重新签封保存。

第五章　其　他

第十九条 使用数字证书实施电子认证的信息系统，应加

强证书介质和证书私钥的管理。数字证书管理遵循“专人专用，按需发放，用毕交回”原则，按照“谁持有谁负责，谁申请谁监管”的原则管理，不得转借他人使用或盗用他人证书。数字证书自签发之日起有效，有效期为1-3年。

第六章　附　则

第二十条　本办法由中国地质调查局网络安全和信息化领导小组办公室负责解释。

第二十一条　本办法自发布之日起试行。

“地质云”机房安全管理规定（试行）

第一章　总　则

第一条　为推进“地质云”建设，保障机房的物理环境安全和重要信息基础设施的稳定运行，为数据、信息提供可持续的网络支撑环境，依据国家网络安全法、国土资源部网络安全有关规定、“地质云”网络安全管理办法等，制定本规定。

第二条　本规定适用于“地质云”主节点、备份节点和分节点机房的安全管理。

第三条　各节点单位承担所在节点机房的安全管理工作，机房管理和使用人员应牢固树立“安全第一”的思想。机房管理实行安全责任制。机房管理人员年终考核评优实行安全工作“一票否决制”。

（一）机房管理处室负责人对机房的安全工作全面负责，并有对机房管理人员进行安全培训的责任和对机房日常安全工作进行检查监督的权力。

（二）机房管理员负责机房的环境、设备以及日常巡视等工作，负责机房的人员出入管理。

（三）机房管理处室负责人指定一人为机房安全员协助机

房管理员开展工作，并负责定期检查工作设备的安全状况，发现隐患必须及时排除。

第二章　物理环境管理

第四条　机房应实行一体化管理，按照机房功能划分不同区域，不同区域应通过门禁进行管控。

第五条　机房物理环境应达到国家相关标准，满足包括温湿度、防尘、防静电、防磁、防雷接地以及供水、供电、消防等要求。

第六条　机房应每周进行一次保洁，保持机房墙面、地面清洁、设备、机柜等无明显灰尘、活动地板无损坏，不得在通道、入口、设备前后、消防器材放置处和窗口附近堆放物品和杂物，严禁带入或存放易燃、易爆等危险品，减少安全隐患，巡检保洁结果应有记录。

第七条　每个工作日均应进行机房人工巡检，内容包括温度、湿度以及供电、照明、UPS、空调、漏水、门禁系统、监控系统等设施及各种现场可直接观察到的状况。

第八条　UPS 后备电池以及机柜 PDU 接线板至少每 5 年更换一次；UPS 主机至少每 8 年更新升级一次。

第九条　交换机、路由器、服务器、磁盘阵列等设备进入机房前，应填写登记表，经允许后安全固定在指定的机柜内，

设备金属壳体必须与保护接地装置可靠连接。

第十条 设备上架运行或现场维修完成后，包装箱、维修材料、工具、部件等物品禁止在机房存放，及时清理出机房。

第十一条 机房内机柜电源开关、配电柜电源开关，除机房管理人员外，不得私自开启或关闭。

第十二条 严禁在机房内抽烟、用火，以及使用除工作设备以外的大功率电器、设备。

第十三条 严禁在机房内随意拉设强、弱电线缆。

第三章 设备安全管理

第十四条 机房内所有设备实行专人负责制：谁使用的设备谁负责其运行安全。设备物理安全由机房所在处室负责，设备使用安全、故障维修由应用方负责。

第十五条 设备进入机房运行前应进行登记、验收、上架、加电测试等环节。设备上架应按照机房管理员指定的位置安装，配电由机房管理员负责分配和连接。

第十六条 非机房管理人员及系统管理人员，不得上机操作或触动机房内各种设备开关、按钮及键盘。

第十七条 硬件设备维修人员应按照操作规程操作设备，不得违规或越权操作；应认真按照维修手册或说明中的操作规程进行。

第十八条 对机房内的设备拆、装、维修时，设备应断电，严禁带电作业，不得在通电情况下进行设备或板卡的更换（支持热插拔设备除外）、拆卸。操作人员应采取防静电措施。

第十九条 对确需异地维修的设备，应卸载留存敏感、重要数据的存储介质，提出申请并填报登记表，经批准后搬离机房维修。应及时维修，尽快返回机房恢复部署。

第二十条 闲置的设备应及时清除出机房并作好记录。

第二十一条 机房设备应有标识，标识内容至少包含设备名称、IP 地址、系统管理员、责任处室。网络设备已使用的端口、网络线、配线架端口都应有标识，标识内容应简明清晰，便于查对。

第四章 系统管理和安全运行

第二十二条 为防止泄密，机房内所有计算机应严格执行涉密不上网，上网不涉密的规定。

第二十三条 系统上线运行前应通过系统安全功能测试、等保定级备案、ICP 备案等一系列审批，通过后方能进入机房部署运行。

第二十四条 外部迁入机房的信息系统，应通过系统安全检测，经确认没有安全隐患后才能部署到机房。

第二十五条 服务器设备系统应按照如下要求配置:

（一）遵循开启最小服务的原则和最少端口开放的原则;

（二）所有服务器系统要安装最新的系统补丁，并及时升级;

（三）所有服务器系统要开启本机防火墙，并及时升级;

（四）所有服务器均应安装杀毒软件，并经常进行升级;

（五）未经允许，任何人都不得在机房设备上随意安装软件或处理与工作无关的文件。

第二十六条 机房断电维护应经过所在单位审批同意。机房断电维护前应对设备和系统进行配置备份，并评估配电恢复后系统或设备是否能正常启动运行，以便有针对性地提前做好预案。

第二十七条 系统对不同安全域开放服务或端口，应提交申请并填写申请单。

第二十八条 系统和数据备份及安全管理，由系统管理员及责任处室负责。

第五章 机房出入及人员管理

第二十九条 机房是重要的业务场所，只限机房管理人员以及授权的系统维护人员、硬件维护人员等进入，非授权人员不得进入机房。进入机房的人员应严格遵守机房管理的各项规章制度，服从机房管理员的管理。

第三十条 非机房管理人员进入机房，需要填写机房进出登记表，外部参观人员还应留存有效证件复印件，经机房管理员和机房管理处室负责人签字确认后，方可在管理人员陪同下进入机房指定区域开展工作。机房进出登记表由专人保管。

第三十一条 机房管理人员应对进出人员进行安全教育和现场安全监督检查。

第六章 安全监控和应急处置

第三十二条 机房应安装信息化的监控系统。系统应具备监视摄像、温湿度监测报警、烟感监测报警、漏水监测报警、电源监测报警、门禁记录等功能，视频数据保存时间不应少于六个月。

第三十三条 机房工作时间实行有人值守式安全监控和管理，非工作时间可实行短信报警的无人值守式监控和管理。

第三十四条 机房管理员应确保门禁系统、视频监控系统正常工作，如有失效应立即通知相关人员检查并排除故障。环境监控设备应定期进行检测，确保问题及早发现，尽快处理。

第三十五条 机房管理人员应对进入机房操作的人员进行行为管理和监控，随时制止违规行为。

第三十六条 在日常监控和巡检过程中，发现或遇到安全事故或安全威胁时，应进行安全处置和逐级上报。

第三十七条 机房防火监控和处置由所在单位相关部门实行统一管理，机房管理人员和责任处室应予密切配合。

第七章 附 则

第三十八条 涉密计算机机房管理规定另行制定。其他机房和设备间管理可参照此规定执行。

第三十九条 本规定由中国地质调查局网络安全和信息化领导小组办公室负责解释。

第四十条 本规定自发布之日起试行。