中国地震局文件

中震测发〔2020〕69 号

关于印发《中国地震局网络安全管理办法》的通知

各省、自治区、直辖市地震局，各直属单位，机关各内设机构：

《中国地震局网络安全管理办法》已经 2020 年 9 月 22 日召开的中国地震局第 6 次局务会议审议通过，现予印发，请各单位遵照执行。

中国地震局

2020 年 10 月 16 日

（信息公开形式：依申请公开）

中国地震局网络安全管理办法

第一章 总　则

第一条 为规范地震系统网络安全工作，保障地震系统网络安全，依据《中华人民共和国网络安全法》、《应急管理部网络安全管理规定》、《中国地震局网络安全事件应急预案（试行）》以及相关规定，制定本办法。

第二条 本办法适用于地震系统开展非涉密网络和信息系统建设、运维、使用，以及网络安全监督管理工作。

第三条 中国地震局网络安全工作坚持谁主管谁负责、谁使用谁负责的原则，做到统一领导、统一规划、分级管理、保障应用。

第二章 网络安全职责

第四条 中国地震局网络安全和信息化领导小组（以下简称局网信领导小组）负责网络和信息系统安全管理的重大事项决策和议事协调等工作。

监测预报司负责网络和信息系统安全的综合管理，协调、监督、检查地震网络安全工作，组织制定地震网络安全管理制度和相关政策，建立健全网络安全体系，审核网络安全建设方案，组织开展网络和信息安全教育培训工作。

局办公室负责协调推进网站、邮件和电子公文系统等政务系

统的保密管理，履行地震局保密委员会办公室职责，负责网络和信息系统的日常保密检查和失泄密事件调查工作。

公共服务司（法规司）负责协调推进地震网络安全标准体系建设。

规划财务司负责归口地震网络安全项目投资和财务管理。

局网信办其他成员单位发挥各自职能，配合做好本领域的网络安全管理工作。

第五条 中国地震台网中心（以下简称台网中心）牵头负责地震网络安全防护能力建设和业务协调组织，协助局网信办实现地震行业网络安全工作的统一监管、整体防护、综合分析、集中审计和联防联控。

第六条 局属各单位应当加强网络安全责任落实，建立网络安全责任制度，主要负责人是网络安全工作第一责任人，主管网络安全的领导班子成员是直接责任人。

局属各单位网信办为本单位网络安全管理工作机构，网信办主任为信息安全员，承担本单位网络安全管理职责，指导、协调、监督、检查本单位网络安全管理工作。

第三章 网络和信息系统建设安全

第七条 各单位应当严格执行国家网络安全等级保护制度及相关标准规范，在网络和信息系统建设过程中要做到网络安全“同步规划、同步建设、同步运行”。

第八条 网络和信息系统建设应当按照统一的安全策略和标准规范，组织开展安全物理环境、通信网络、区域边界、计算环境建设，所需软硬件产品应当符合国家关于安全可信的要求，关系国家安全和公共利益的信息系统所使用的重要网络产品和服务应当经过网络安全审查。

第九条 网络和信息系统应当具备用户管理、权限管理、日志审计等安全功能，不得在代码中植入恶意代码或留有后门程序，不得脱离安全管控。软件源代码应当留存备案。

第十条 网络和信息系统中的数据资源应当根据分级分类的管理要求授权使用，实施不同的安全保护策略和安全技术措施，着重加强重要数据和个人信息安全防护。

第十一条 新建网络和信息系统验收前，建设单位应组织完成网络安全等级保护定级工作，并向当地公安机关备案。对安全保护等级二级及以上的网络安全和信息系统，应组织第三方测评机构开展网络安全等级保护测评，测评通过方可申请验收。

第十二条 网络和信息系统竣工验收后，建设单位、运行管理单位应进行应用系统、硬件设备、相关文档资料等移交，移交前的运行安全由建设单位负责。

第四章 网络和信息系统运维安全

第十三条 网络和信息系统经过网络安全等级保护测评，确保安全后方可上线运行。

第十四条 上线运行的网络和信息系统，应当在首页底端标明网络安全责任单位、运维单位及联系方式。在互联网运行的网站类系统，还应当在首页底端链接（标明）党政机关事业单位网站标识、ICP 备案号、国际联网备案号。

第十五条 网络和信息系统中各类软硬件设备在上线运行时应当注册登记；维修时应当有本单位运维人员在场，并确保数据安全；退网时应当申报注销，并进行安全处理。

第十六条 上线运行的软件系统和硬件设备应当定期进行系统加固、补丁升级、漏洞修复、病毒查杀等安全维护工作。

第十七条 不同网络间应设置物理或逻辑隔离，按照最小权限的原则对网络进行分区分域管理，实施严格的设备系统接入和访问控制策略。

第十八条 各单位应制定机房进出入管理办法，严格控制机房和设备间的进出访问，加强安全监控和巡检，确保机房符合有关规定要求。

第十九条 各单位应遵循最小授权、最小安装原则开展主机账号、口令、应用、服务、端口的安全管理，定期进行漏洞扫描和恶意代码检测，及时安装安全补丁和更新恶意代码库。

第二十条 各单位应建立信息发布多控审核机制，严格管控门户网站等媒体信息的发布。

第二十一条 各单位应严格邮件系统用户注册审批和注销管理，严禁将工作邮件自动转发至私人或境外邮箱，避免存在弱口

令和访问钓鱼邮件等情况。

第二十二条 在地震行业网、电子政务外网和互联网上开展安全攻防测试必须报局网信办批准并接受台网中心指导。核心地震业务系统须采取主、备、测分离策略，确保测试不影响正常业务运行。

第二十三条 各单位应当对网络和信息系统建设项目的承建单位、运维单位、外包服务单位及相关人员进行资格审查，签订安全责任书、保密协议，对其工作进行全程监督。

第二十四条 确定为关键信息基础设施的网络和信息系统，应当严格落实《中华人民共和国网络安全法》及关键信息基础设施相关法律法规有关要求，采取有效措施，确保安全。

第二十五条 各单位应保障数据采集、传输、存储、处理、交换、共享和销毁等数据全生命周期安全，对重要地震数据和应用系统进行容灾备份，对个人信息等敏感数据部署加密措施，遵循合法、正当、必要的原则进行数据收集和使用。

第五章 网络和信息系统使用安全

第二十六条 各单位开发的网络和信息系统应当实行以数字证书为主要载体的实名制身份认证和授权访问，并实行网络行为监测和安全审计。用户不得使用他人数字证书。

第二十七条 用户不得擅自扫描、探测、入侵、攻击测试网络和信息系统，不得违规干扰、屏蔽、卸载、拆除安全监控程序或

者监测设备，不得越权访问、查询、下载网络和信息系统数据资源，不得擅自篡改地震信息资源或者审计信息，不得泄露网络和信息系统中不宜对外公开的数据，不得对抗安全检查或者阻挠、妨碍安全事件调查。

第二十八条 部署在公有云上的系统和数据在使用过程中应按照国家关于公有云的相关网络安全标准规范做好防护。

第二十九条 传输、处理和存储个人信息的网络和信息系统，应当符合国家有关个人信息保护的法律法规要求。任何组织和个人不得窃取或者以其他非法方式获取个人信息，不得非法出售或者非法向他人提供个人信息。

第三十条 三个月以上未使用的网络和信息系统应当采取断电、断网等清理措施，再次上线使用前应先进行漏洞修补、病毒库更新等安全加固工作。

第六章 终端设备安全管理

第三十一条 各单位应当建立计算机终端台账，对计算机终端进行全生命周期管理。

第三十二条 计算机终端、外设及办公软件应当按照财务有关制度要求，纳入资产管理范围，统一采购、统一编号、统一标识、统一发放、统一报废。

计算机终端及外设应当按照国家有关要求采购安全可信产品，安装使用正版操作系统、办公软件及防病毒软件。

第三十三条 计算机终端及外设应当遵循“谁使用，谁负责”的原则，明确终端安全的使用和管理责任，定期开展针对终端的弱口令检查、病毒查杀、漏洞修补、操作行为管理和安全审计等工作。

第三十四条 个人终端设备原则上不得接入办公网络，确需接入的，须经运维部门技术审查确保安全。

第三十五条 计算机终端需送外维修时，应当采取数据安全防护措施，确保重要数据安全。重新联入办公网络前，应当进行安全性检查。

移动存储介质应当定期清理、整理，不得长期、大量存储信息。

第三十六条 计算机终端、移动存储介质报废应当交固定资产管理部门统一处置，报废前应当做好数据备份和清除，必要时应当拆除硬盘、存储卡等数据存储介质并交保密部门销毁，同时从计算机终端卸载软件。

第七章 使用人员安全管理

第三十七条 各单位应当加强网络和信息系统使用人员管理，严把入口关，严格权限分配，及时清理离岗离职人员访问账户及权限。确因工作需要，可对外部人员开放临时性账户，需签订并严格履行安全保密协议，工作结束后及时注销临时账户。

第三十八条 局网信办牵头制定地震系统网络安全培训规划

和年度计划，并定期组织开展教育培训。

第三十九条 局属各单位应当着力提高工作人员网络安全意识，定期开展本单位的网络安全宣传教育和业务技能培训。

第八章 网络安全监督检查

第四十条 台网中心受局网信办委托，承担地震系统网络安全监督检查及督促整改任务，配合公安部和应急管理部等部门做好地震网络安全监督检查工作。监督检查主要包括自查、技术检测和现场检查。

第四十一条 各单位应当组织开展本单位网络安全自查，制定年度网络安全自查计划，每年至少开展一次网络安全自查工作，专项自查可根据实际随时开展，自查报告报送台网中心，台网中心汇总分析后形成地震系统网络安全自查工作总结报局网信办。

第四十二条 台网中心组织相关技术力量对各单位的信息系统开展远程技术检测，及时发现网络安全漏洞、隐患、问题和风险，通知相关单位限期整改。对于通报整改的情况，各单位要及时整改反馈。

第四十三条 局网信办不定期组织开展现场检查，听取被检查单位网络安全工作汇报，了解被检查单位网络安全工作情况，对于前期发现的网络安全漏洞、隐患，进行实地督办、复核整改工作情况。

第九章 网络安全事件应急处置

第四十四条 各单位应当编制本单位网络安全事件应急预案，每年组织开展应急演练，及时处置系统漏洞、计算机病毒、网络攻击、网络入侵、数据泄露等安全风险，定期检验、评估、完善应急预案。

第四十五条 发生网络安全事件后，各单位应当立即启动应急预案，采取有效处置措施，并在 24 小时内将有关情况报送局网信办。局网信办根据有关规定将网络安全事件相关情况及时报送国家网络安全主管部门。

第四十六条 各单位应在网络安全事件发生后 30 天内，完成对事件起因、性质、影响、责任等情况调查与评估，提出处理意见和改进措施，并报局网信办。

第十章 监测预警与信息通报

第四十七条 按照“分工负责、协作配合、资源共享、力量协同”的原则，开展网络安全监测预警和信息通报。

局网信办牵头建立健全地震系统网络安全监测预警和信息通报管理制度，规范监测预警和信息通报工作。

台网中心牵头地震系统网络安全监测预警和信息通报工作，对地震系统网络运行状况开展实时监控，发布网络安全预警信息。

局属各单位应加强本单位网络安全监测预警能力建设，完善信息通报机制，加强本单位风险漏洞和网络安全事件的预警、处

置和信息通报工作。

第四十八条 网络安全信息通报工作主要包括日常信息通报、特殊保障时期信息通报和网络安全事件信息通报。

日常信息通报。局属各单位每月向台网中心报送网络安全月报。台网中心向国家网络安全主管部门和局网信办报送网络安全季报和年度总结报告，向局属各单位通报国家网络安全主管部门和应急管理部发布的网络安全报告和预警信息。

特殊保障时期信息通报。在重要节假日、国家重大活动和重大地震应急响应等特殊时期，局属各单位实行网络安全每日“零报告”制度，台网中心每日向国家网络安全主管部门和中国地震局报送网络安全保障工作情况。

网络安全事件信息通报。局属各单位发生《中国地震局网络安全事件应急预案（试行）》中规定的网络安全事件时，在迅即处置的同时，第一时间将情况上报局网信办。局网信办或台网中心监测到或收到国家有关部门转来的局属单位网络安全事件信息，局网信办应向事发单位印发网络安全整改通知，事发单位立即对问题进行核实、处置并及时上报处置情况。

第十一章 考核评价

第四十九条 局网信办和局属各单位加强网络安全责任分级考评，以网络安全管理、攻防演练、渗透测试、在线监测、信息通报和应急响应等方面情况作为主要考核依据，纳入年度局属单

位工作目标考核。

第五十条 对于在网络安全监督检查中发现重大安全隐患且未及时整改到位，谎报、瞒报网络安全事件造成不良影响，扰乱网络和信息系统正常运行秩序等行为，按照国家和中国地震局有关规定启动问责程序，进行逐级追责，构成犯罪的，依法追究刑事责任。

第十二章 附则

第五十一条 各单位依据网络安全相关法律法规和本办法制定修订本单位网络安全管理制度。

第五十二条 使用应急管理部网络和信息资源的单位或个人，应当遵守应急管理部网络安全相关管理规定。

第五十三条 本规定由局网信办负责解释，自印发之日起施行。

中国地震局 2020年10月19日印发