许昌市应急管理局文件

许应急〔2019〕46号

许昌市应急管理局
关于转发《应急管理部网络安全管理规定》的
通　知

各县（市、区）应急管理局，局各科（室、队、中心）：

现将《河南省应急管理厅转发应急管理部办公厅关于印发网络安全管理规定的通知》（豫应急办〔2019〕95号）转发给你们，请结合以下要求，一并抓好落实。

一、高度重视网络安全管理。要将网络安全与信息化建设紧密结合，抓好网络信息安全防范。积极组织开展形式多样、针对性强的宣传教育，将网络信息安全意识与责任意识、保密意识结合起来，全面提高信息网络安全防范意识。

二、全面落实网络安全责任。要加强组织领导，明确责任人，落实信息网络安全工作责任追究制度，对因管理不善、工作不力导致责任事故的要严肃处理，按规定追究相关领导和直

接责任人的责任。局办公室负责网络和信息系统的综合管理、协调、监督、检查单位网络安全工作，组织开展网络和信息安全教育培训，以及网络和信息系统的日常保密检查和失泄密事件调查等工作。科技信息化科负责落实网络安全相关法律法规和标准规范，建立健全安全保障体系，审核网络安全建设方案，组织开展网络和信息系统安全风险评估，协助局党组做好网络和信息化系统安全管理的重大事项决策和议事协调等工作。

三、抓好网络安全技术防护。对与互联网有数据交换的信息系统要配备防火墙、网页防篡改、安全网关、入侵防御、网络安全准入管理及访问控制、网络及数据安全审计等安全设备，确保合法终端和服务应用的连接访问控制。

四、开展网络安全防护检查。对于信息系统运行相关的软硬件系统设备，有计划地开展安全防护检查。强化口令控制、病毒扫描、漏洞补丁等基础安全，确保各类硬件设备安全可控。对信息系统的操作行为进行身份标识、口令限制、访问控制和管理。规范数据库管理操作，加强数据操作记录审计和追溯，避免数据信息泄露。

许昌市应急管理局

2019年10月30日

许昌市应急管理局办公室　　2019年10月30日印发

（共印10份）

河南省应急管理厅文件

豫应急办〔2019〕95号

河南省应急管理厅转发应急管理部办公厅关于印发网络安全管理规定的通知

各省辖市应急管理（安全监管）局，省应急厅机关各处室、厅属各单位：

现将《应急管理部网络安全管理规定》转发给你们，请认真遵照执行。

2019年10月18日

河南省应急管理厅办公室　　2019年10月18日印发

校对：韩雪

2272

应急管理部办公厅

应急厅函〔2019〕502号

应急管理部办公厅关于印发网络安全管理规定的通知

中国地震局、国家煤矿安监局，各省、自治区、直辖市应急管理厅（局），新疆生产建设兵团应急管理局，部消防救援局、森林消防局，部机关各司局，驻部纪检监察组，国家安全生产应急救援中心，部所属事业单位：

经部领导同意，现将《应急管理部网络安全管理规定》印发给你们，请认真遵照执行。

应急管理部办公厅

2019年9月26日

应急管理部网络安全管理规定

第一章　总　则

第一条　为规范应急管理部系统网络安全工作，保障应急管理部系统网络安全，依据《中华人民共和国网络安全法》以及相关法规，制定本规定。

第二条　部机关各司局及部所属单位（以下统称各单位）建设、运维、使用网络和信息系统以及开展网络安全监督管理工作，适用本规定。

各省级应急管理厅（局）参照本规定执行。

第三条　本规定所称网络和信息系统，是指各单位使用的非涉密计算机网络以及运行的软硬件和存储数据等。

第四条　网络安全管理工作坚持建设、运维、使用分工负责的原则，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

第五条　部科技和信息化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。

办公厅负责网络和信息系统的综合管理，协调、监督、检查应急管理部系统网络安全工作，组织开展网络和信息安全教育培训

工作；履行部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。

科技和信息化司负责落实网络安全相关法律法规和标准规范，建立健全安全保障体系，审核网络安全建设方案，组织开展网络和信息系统安全风险评估及安全违规事件调查工作。

部所属单位负责本单位网络和信息系统的监测监控、预警处置等安全运维工作。通信信息中心负责部机关网络和信息系统的监测监控、预警处置等安全运维工作。

第六条 各单位应当建立网络安全责任制度。各单位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。

第七条 各单位应当指定网络安全管理工作机构和信息安全员，承担网络安全管理职责，指导、协调、监督、检查本单位网络安全管理工作。

第八条 各单位负责本单位网络和信息系统日常安全管理工作，组织开展网络和信息系统定级、备案、安全建设和整改、等级测评、安全检查等工作。

第三章 网络和信息系统建设安全

第九条 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，网络和信息系统安全防护、密码保护和保密措施与信息化建设同步规划、同步建设、同步运行，不断健全网络安全防

护体系，保障网络和信息系统安全，防止发生网络安全事件。

第十条 网络和信息系统项目单位为网络安全责任单位，应当明确网络安全责任人，组织开展网络安全相关工作。

第十一条 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，开展物理和环境、边界和接入、网络和通信、计算和设备、应用和数据、监督管理等安全建设。

第十二条 信息系统应当具备统一用户管理、权限管理、日志审计等安全功能，不得留有后门程序，不得脱离安全管控。软件源代码应当留存备案。

第十三条 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。应当建立数据备份机制，对重要数据和应用系统进行备份。

第四章 网络和信息系统运维安全

第十四条 网络和信息系统建设完成后应当经过等级保护测评并完成安全整改，确保安全后方可上线运行。

第十五条 上线运行的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，其中在互联网运行的网站类信息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。

第十六条 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。

第十七条 上线运行的软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。

第十八条 网络和信息系统应当具备安全审计功能，记录访问行为和软硬件设备的运行状态，安全审计日志应当完整、真实、可溯源。

第十九条 在应急指挥信息网、电子政务外网和互联网上开展安全攻防测试必须报部办公厅批准，并接受部科技和信息化司指导。

第二十条 各单位网络安全运维机构应当加强网络安全监测与预警，采取有效措施，堵塞安全漏洞，严防网络安全事件发生。

第二十一条 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，开展安全教育，督促落实安全管理措施，对其工作进行全程监督。

第二十二条 网络和信息系统所需软硬件产品应当符合国家关于安全可靠的要求，关系国家安全和公共利益的信息系统使用的重要网络产品和服务，应当经过网络安全审查。

第二十三条 网络和信息系统确定为关键信息基础设施的，应当严格落实《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。

第二十四条 未经网络和信息系统网络安全责任部门、运维部门同意，不得私自从数据库中拷贝数据。

第二十五条 拟报废的网络和信息系统，应当采取措施做好数据备份、数据删除等工作，防止数据泄露。

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 各单位网络和信息系统应当保持相对独立，未经允许，不得将网络和信息系统延伸到其他单位。

第二十八条 用户不得擅自扫描、探测、入侵、攻防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，不得擅自篡改应急管理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。

第六章　终端设备安全管理

第三十条　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。

第三十一条　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靠产品，安装使用正版操作系统、办公软件及防病毒软件。

第三十二条　计算机终端及外设应当遵循“谁使用，谁负责”的原则，明确安全责任人，落实安全责任。

第三十三条　便携式计算机原则上不接入部机关网络，确需接入的，须经运维部门技术审查确保安全。

涉密计算机终端和存储介质严禁接入非涉密网络。

第三十四条　计算机终端应当交运维部门统一维修，不得私自带离办公区域。需送外维修时，应当采取数据备份、数据清除等措施，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。

第三十五条　计算机终端、移动存储介质报废应当交运维部门统一处置，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

第三十六条　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。

第三十七条　各单位应当着力提高工作人员网络安全意识，持续开展网络安全宣传教育，注重宣传教育效果。在国家网络安全宣传周活动期间，应当举行网络安全宣传活动。

第三十八条　各单位应当注重提高工作人员网络安全技能，开展网络安全教育培训，对网络使用人员、安全管理人员、安全技术人员进行培训。

网络安全管理培训应当包含网络安全政策、安全标准规范、网络安全检查、风险管理、应急处置、灾备管理等内容。网络安全技术培训应当包括网络、信息系统、关键信息基础设施、数据等安全防护内容。

第八章　网络安全检查

第三十九条　各单位应当制定年度网络安全检查计划，每年至少开展一次网络安全普查，专项检查可根据实际随时开展，检查报告应当报送部办公厅。

第四十条　开展网络安全检查应当制定检查方案，明确检查

工作机构、检查范围、检查内容、检查进度安排等。定期汇总检查结果、分析风险隐患，针对存在的问题应当制定整改方案，及时整改并报送本单位网络安全管理部门。

第九章　网络安全事件应急处置

第四十一条　部所属各单位应当依据《国家网络安全事件应急预案》编制本单位网络安全事件应急预案并及时修订，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、网络侵入、数据泄露等安全风险。

第四十二条　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部办公厅。部办公厅应当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。

第十章　保障和处罚措施

第四十三条　各单位应当建立网络安全责任制考评制度，将网络安全管理纳入年度工作绩效考核评价。

第四十四条　各单位应当将网络和信息系统安全防护设施的建设、运维及安全检查、测评、整改等费用列入年度经费预算。

第四十五条　各单位应当将网络和信息系统安全管理宣传、教育和培训，列入人员晋升和专业训练规划。

第四十六条　对扰乱网络和信息系统正常运行秩序或者妨碍

安全管理的相关责任人员按照国家和应急管理部有关规定予以处分；构成犯罪的，依法追究刑事责任。

第十一章　附　则

第四十七条　中国地震局、国家煤矿安监局及部消防救援局、森林消防局分别负责本级和所属单位的网络安全工作，依据网络安全相关法律法规制定本领域网络安全管理制度。

第四十八条　本规定由部办公厅负责解释，自印发之日起施行。

（信息公开形式：不予公开）

应急管理部办公厅　　2019年9月29日印发

承办单位：办公厅　　经办人：郑志峰　电话：83933098　共印125份