中国科学院网络安全工作管理办法
（试行）

第一章　总　　则

第一条为加强中国科学院网络安全工作、保障我院网络安全，根据《中华人民共和国网络安全法》、《中华人民共和国计算机信息系统安全保护条例》、《中华人民共和国计算机信息网络国际联网管理暂行规定》、《信息安全等级保护管理办法》等国家有关政策、法规及指导性文件，制定本办法。

第二条中国科学院网络安全工作遵循“谁主管谁负责、谁使用谁负责、谁运维谁负责”的原则，实行统一领导、分级治理、定责到人。

第三条网络安全与信息化工作应同步规划、同步建设、同步实施、同步发展。

第四条本办法中的网络，是指由计算机或者其他信息终端及相关设备组成的按照一定的规则和程序对信息进行收集、存储、传输、交换、处理的系统。

网络安全，是指通过采取必要措施，防范对网络的攻击、侵入、干扰、破坏和非法使用以及意外事故，使网络处于稳定可靠运行的状态，以及保障网络数据的完整性、保密性、可用性的能力。

第五条本办法适用于院属单位、院机关（以下统称各单

位）的网络安全工作，其中院属全资及控股企业和双重领导单位应参照执行。

第二章　组织机构

第六条中国科学院网络安全和信息化领导小组（简称院网信领导小组）作为院网络安全工作统筹协调和决策机构，贯彻落实党中央、国务院关于国家网络安全的发展战略、宏观规划和重大政策；按照国家有关部署，组织院网络安全工作；研究制定院网络安全工作的战略、发展规划和重大政策；审定院网络安全工作部署和重要项目部署，对有关重大问题作出决策和决定，协调各方面的工作关系。院网信领导小组办公室（简称院网信办）设在办公厅，作为院网信领导小组的办事机构。

第七条中国科学院安全工作委员会（以下简称院安委会）贯彻落实党中央、国务院关于网络安全工作的方针政策，传达中央重要会议和文件精神，研究部署年度工作；分析全院网络安全工作态势，研究制定院级相关规章制度及管理措施，并部署实施；指导、检查各单位安全工作；研究处理重大问题及重大事件，研究决定重大安全事故责任的处理意见。

第八条中国科学院安全工作委员会办公室（设在办公厅，以下简称院安委办），具体负责落实全院网络安全工作的部署要求，在院安委会领导下，会同院网信办对全院网络安全工作的规划和贯彻实施等工作进行指导、监督和检查。

第九条各分院负责在本系统内贯彻执行党和国家关于网络安全工作的方针政策和法律法规，落实院网络安全工作各项部署。督促、检查本系统单位的网络安全工作，对发现的问题和隐患及时督办整改。组织和督促本系统各单位开展网络安全宣传教育和培训工作。指导和督促本系统单位妥善处理各类网络安全案件、事件、事故并及时上报院安委办。

第十条各单位是网络安全工作的责任主体和实施主体，须设立网络安全工作领导机构或组织，明确主管领导，确定网络安全管理职能部门、网络安全运维部门和具体负责人员，落实网络安全责任。建立本单位包括人员管理、网络建设管理、网络运维管理、安全审计管理等方面切实可行的网络安全管理制度和规范。落实防范网络攻击的物理和环境安全、网络和通信安全、设备和计算安全、应用和数据安全等技术措施。定期开展网络安全检查工作，为国家有关部门依法维护国家安全和侦查犯罪的活动提供支持和协助。根据工作需要和实际情况，确定专兼职技术支撑保障人员。

第三章　安全责任

第十一条　各单位法定代表人是网络安全工作第一责任人，负责对网络安全工作提供政策支持和资源保障，健全和落实可追溯的安全责任体系。分管领导是网络安全工作直接责任人，具体负责网络安全工作的部署、督促、总结、考核和奖惩，定期召开会议，了解工作情况，研究解决重要问

题，组织和开展培训、检查，并对整改工作督办落实。

第十二条 网络安全管理职能部门，负责制定本单位网络安全管理制度和应急预案，并督促贯彻落实；开展网络安全检查、风险处置和隐患整改；每年度开展网络安全教育培训；每半年清查本单位所有网站和信息系统情况并向院安委办报备，原则上对于1个月及以上不维护的、出现漏洞和安全隐患较多的、无法整改漏洞和安全隐患的网站和信息系统予以停用。在发生危害网络安全的事件时，立即启动应急预案，采取相应的补救措施，并按规定向分院、院安委办等部门报告。

第十三条 网络安全运维部门，按照规范和要求具体落实网络安全技术保障措施；采取监测、记录网络运行状态、网络安全事件的技术措施，并按照规定留存相关的网络日志不少于六个月；具体负责网络安全检查事项；及时处置网络安全事件、风险隐患和整改漏洞；定期对运维人员进行保密教育和技能培训。

第十四条 网络使用人员，应遵守国家法律法规，服从本单位网络安全管理，增强安全防范意识，保管好账号和密码，避免泄露；坚持上网自律，不故意传播非法和虚假内容信息。

第十五条 院级非法人单元、院属单位分支机构及各类组织等，所依托的法人单位对其主管或使用的网络信息系

统安全负责，对其使用网络的行为负责。

第四章　系统安全保护

第十六条　网络安全等级保护所涉及的定级指导、备案审查、系统测评、方案论证、安全咨询、安全检查等工作，应在相关部门和行业专家指导下开展。

第十七条　系统的安全保护等级必须参照国家有关网络安全保护等级划分标准确定。

（一）已投入使用的系统，必须确定安全保护等级，按相应管理规范和技术标准实施保护。

（二）新建或改建系统，必须经网络安全管理部门审批备案后方可建设或改建，在规划阶段确定安全保护等级，在设计阶段落实网络安全要求，原则上由具有相应资质的单位实施，同步建设相应的防护设施，上线运行前必须依据国家规定进行安全性测试。

（三）系统业务的重要程度或系统遭到破坏后的危害程度发生重大变化时，应及时调整安全保护等级，落实相应网络安全防护措施。

（四）网站和系统停用，必须及时清除所有系统内容，并注销所有备案信息。

（五）所有系统必须及时向分院、院安委办报备。

第十八条　网络安全保护等级拟定为第一、二级的，应及时到属地公安机关办理网络安全等级保护备案手续；拟定

为第三级及以上的，须向院安委办提交备案申请，院安委办审核批准后向公安部门办理备案手续。

第十九条 网络安全保护等级为第一、二级系统可由各单位原则上每两年自主组织等级测评，测评报告向所在分院报备。第三级及以上系统应在院安委办指导下组织等级测评。

第二十条 系统应按等级保护政策、标准和规范要求，制定相应的安全保护实施方案。其中，第三级及以上系统的安全保护实施方案须报院安委办审核批准后实施。

第二十一条 信息化基础设施和支撑重大科研任务的重要信息系统建设项目验收前，建设单位应组织对其进行等级保护测评，测评报告应作为验收评价的重要依据。

第二十二条 对信息化系统的设计方案、实施方案、拓扑图、软件代码、系统设置、系统管理账户、运维账户、密码等关键信息资料要严加管理，严禁外泄；要与系统建设方、运维方签署协议，明确其保密职责，明确追责条款，并严格管理。

第二十三条 信息系统的防护要重视边界防护，更要高度重视内部防护，要合理分区和隔离，合理设置权限和配置防护措施，坚决避免出现“一点突破，畅通无阻”的严重后果。

第二十四条 关键信息基础设施的各单位除履行相关

网络安全规定外，还应做好如下方面工作：

（一）设置专门安全管理部门和安全管理负责人，并对该负责人和关键岗位的人员进行安全背景审查；

（二）定期对从业人员进行网络安全教育、技术培训和技能考核；

（三）对重要系统和数据库进行容灾备份；

（四）自行或者委托网络安全服务机构对网络的安全性和可能存在的风险每年至少进行一次检测评估，并将检测评估情况和改进措施报送院安委办；

（五）法律、法规规定的其他要求。

第二十五条 用于科研和办公的台式机、便携式计算机、打印机和移动终端等应具备防病毒、抗攻击、补漏洞等基本安全防护能力，严格系统密码和账户权限以及 IP 地址操作权限设定管理，避免对外泄露。不具备基本防护能力的办公终端不得接入本单位网络。

第五章 互联网地址安全管理

第二十六条 各单位必须对互联网地址（以下称 IP 地址）进行审计，原则上每季度不少于 1 次。建立健全接入审批和登记管理制度，任何部门或个人未经允许不得改变网络拓扑结构。IP 地址分配、使用定责到人，信息记录应保存一年以上。

第二十七条 IP 地址用于对外服务的，须经网络安全

管理部门审核、备案。严禁使用未经电信主管部门批准开展跨境活动的虚拟专用网络服务商。IP 地址传输的邮件、发布的信息及其他各类数据内容，须严格遵守国家相关法律法规要求。

第二十八条 无线网络的使用应加强监督管理和安全防护，外来人员临时接入网络应做访问登记。

第六章 互联网信息服务安全管理

第二十九条 各单位应对互联网信息服务内容负责，对外开放的共享业务须审核登记，强化 FTP、系统共享和网络流量代理的安全监管。

第三十条 网站建设前应经网络安全管理职能部门审核备案，报分管领导同意后，依照有关互联网信息服务行政法规要求，办理经营许可、ICP 备案及国际联网备案登记等手续。

第三十一条 对电子公告板、论坛、聊天室、博客空间、微信、自媒体等交互式网站，应加强建站需求、制度保障、账户注册、安全维护、审计能力等方面安全管理。

第三十二条 各单位应建立健全网站信息发布审核制度，内设机构的门户网站须建立信息发布审核机制，确保信息内容准确、真实、可追溯，确保不涉及国家秘密和内部敏感信息。

第三十三条 对外网站应明确运营责任人和技术负责

人。运营责任人须由固定人员担任，负责网站信息发布、系统运行以及留言评论等互动栏目的安全管理。社会公众能够直接访问的交互式网站，须明确网站、系统和信息管理员，运营管理要实行专人负责。原则上仅限本单位内部 IP 具有更改网站内容的权限。

第七章　监测预警与应急处置和信息报告

第三十四条　院安委办统筹协调有关部门加强网络信息收集、分析和通报工作。

第三十五条　各单位应结合业务实际，完善相应的应急协调机制，规范安全事件应急响应和处置流程，制定网络安全事件应急预案，定期开展应急演练。

网络安全事件应急预案应当按照事件发生后的危害程度、影响范围等因素对网络安全事件进行分级，并规定相应的应急处置措施。

第三十六条　关键信息基础设施运营单位应建立网络安全监测预警和信息通报制度，并按照要求报送网络安全监测预警信息。

第三十七条　发生网络安全事件，各单位应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，采取技术措施和其他必要措施，消除安全隐患，防止危害扩大。

发生网络安全事件的单位应该按院安委办要求增加网络安全保障设施。

第三十八条 各单位应建立网络安全信息报告工作机制，了解和掌握本单位网络安全状况，及时报告突发网络安全事件。

第八章 监督检查

第三十九条 各单位应组织网络安全自查，检查范围包括本单位网络基本情况、安全责任划分、人员安全意识、对外开放服务、系统漏洞、权限管理、系统维护、安全审计以及机房物理环境安全等。

网络安全保护等级为第三级以上的系统每半年至少自查一次。网络安全保护等级为第三级及以下的系统及对外网站和电子邮件系统每年至少自查一次。将检查报告上报分院和院安委办。

第四十条 分院每年度应组织对系统单位的网络安全工作落实、信息系统底数、网络安全等级保护、部门职责及人员安全意识等情况进行监督检查。

第九章 奖 惩

第四十一条 网络安全工作纳入安全工作先进集体、先进个人评选范围，对成绩显著或者作出突出贡献的集体和个人，应予以表彰、奖励；发生网络安全事件、重大网络安全事件的，取消周期内评优资格。

第四十二条 对向院安委办瞒报、漏报网站和信息系统的单位，应予以通报，情节严重的追究相关人员责任。

第四十三条 对网络安全工作管理不力或存在网络安全隐患较多且长期未予整改的单位或个人，应予以通报，并追究相关人员的责任。

第十章 附 则

第四十四条 本办法由院安委办负责解释。

第四十五条 涉及国家秘密的网络安全工作，按保密相关规定执行。

第四十六条 本办法自印发之日起施行。《中国科学院计算机网络与信息安全工作管理办法》（科发办字〔2015〕56号）同时废止。

附件：各单位网络安全管理制度框架

附件

各单位网络安全管理制度框架

一、总则

制定依据，体系说明，工作总方针，安全保密协议等。

二、组织机构及职责

组织机构，管理人员、运维人员、管理员岗位职责，网络安全检查规范、网络安全宣传教育机制、奖惩措施等。

三、人员管理

内部访问安全、外部访问安全，培训计划、人员安全管理规定、管理规范，员工上岗、离职签订责任书，人员变动、外部人员安全管理，员工信息安全行为准则等。

四、项目及系统建设管理

项目及系统建设安全管理要求，建设前的申报和审批，系统定级方案，设计、实施过程安全管理，产品采购和使用安全要求、自行开发软件安全要求、外包软件安全要求，测试验收安全要求，系统交付管理，系统备案、等级测评管理，安全服务要求，验收与投产安全管理等。

五、系统运维管理

机房管理办法，机房管理制度张贴内容，物理与环境安全实施规范，存储介质、访问控制实施规范，操作系统、网络设备、数据库加固规范，安全产品、防病毒、终端管理操作规范，计算机病毒防治管理办法，日常安全运维管理，数

据备份要求，网络安全策略，信息安全审计制度、审计规范、配置手册，系统补丁、用户账号及口令管理，系统变更管理，信息资产分类及安全、风险评估等信息资产管理，存储介质管理等。

六、网络安全事件应急预案

编制目的、依据、范围、体系原则，组织机构及职责，网络安全事件分级，监测与预警，应急响应与处理，调查与评估，安全事件管理规范，预防工作，保障措施等。