合肥研究院计算机网络与信息安全工作管理办法

第一章　总则

第一条　为加强中国科学院合肥物质科学研究院（简称“合肥研究院”）计算机网络与信息安全工作，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》、《中国科学院计算机网络与信息安全工作管理办法》等有关政策、法规及指导性文件，结合研究院实际情况，制定本办法。

第二条　合肥研究院计算机网络与信息安全（以下简称网络安全）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，实行统一管理、分级治理、责任到人。

第三条　网络安全和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　本办法适用于合肥研究院各研究单元、合肥研究院机关和支撑服务部门（以下简称各单位）的网络安全工作。医院、学校、院属资产公司应参照执行。

第二章　组织机构

第五条　合肥研究院安全工作委员会（以下简称安委会）是合肥研究院网络安全工作的领导机构，负责合肥研究院网络安全工作的总体规划、统筹协调及重大事项决策。

第六条 合肥研究院信息中心作为安委会下设机构，负责落实合肥研究院网络与信息安全的工作部署，开展合肥研究院网络安全工作的技术保障、监督和检查，并向安委会提出有关工作建议。

第七条 合肥研究院各所、中心，应当依据信息系统等级保护的要求，对设置在本所、中心的二级（含）以上信息系统，落实网络安全具体负责人员，并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

第八条 合肥研究院负责人是合肥研究院网络与信息安全工作第一责任人，合肥研究院信息化工作分管领导是网络与信息安全工作主要责任人，合肥研究院各所、中心负责人对本所、中心独立管理的信息系统的安全负具体领导责任。各单位应对网络与信息安全工作高度重视，提供支持，做好保障，健全可追溯的安全责任体系。

第九条 合肥研究院网络安全管理职能部门为合肥研究院院信息中心，负责建立合肥研究院网络安全、保密管理制度，督促网络安全检查与隐患整改，组织网络安全教育培训。

第十条 合肥研究院各所、中心，对其主管或使用的信息系统承担直接责任。

第十一条 计算机网络使用人员，须遵守国家法律法规，服从本单位网络安全管理，增强安全防范意识，坚持上网自律，不故意传播非法和虚假内容信息，遵守合肥研究院相关

保密管理规定

第四章　信息系统安全保护

第十二条　信息系统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。

第十三条　信息系统的安全保护等级应参照国家有关信息系统安全保护等级划分标准确定。

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

（二）新建信息系统，应在规划、设计阶段确定安全保护等级，同步建设相应的防护设施。

（三）信息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。

第十四条　合肥研究院各所、中心，新建信息系统安全保护等级拟定为一级的，应及时到属地公安机关办理信息安全等级保护备案手续；安全保护等级拟定为二级的，须向合肥研究院安委会提交备案申请，审核批准后向公安部门办理备案手续；安全保护等级拟定为三级及以上的，须经合肥研究院安委会审批后向中科院安全工作委员会办公室(以下简称中科院安委办)提交备案申请，审核批准后向公安部门办理备案手续。

第十五条　一、二级信息系统由各单位自主组织等级测评，三级及以上信息系统应在中科院安委办指导下组织等级测评。 测评报告向合肥研究院信息中心报备。

第十六条 信息系统运行场所应完善安全保障措施，严格人员出入管理。

第十七条 信息系统访问权限应根据业务需要和安全要求严格控制，有关人员应签订岗位权限安全责任书。

第十八条 用于科研和办公的台式、便携式计算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设定管理。不具备基本防护能力的办公终端不得接入网络。

第五章 信息系统保密管理

第十九条 合肥研究院从事涉密科研、生产、管理的各部门和科研单元应自觉履行各项保密义务，同时严格遵守合肥研究院信息系统、信息设备和存储设备的保密管理制度及相关策略规定。涉密信息系统、涉密信息设备和涉密存储设备管理的基本要求如下：

（一）禁止将涉密信息系统、涉密信息设备和涉密存储设备接入互联网及其他公共信息网络。

（二）禁止在未采取防护措施的情况下，在涉密信息系统、涉密信息设备和涉密存储设备与互联网及其他公共信息网络之间进行信息交换。

（三）禁止未经安全技术处理，将退出使用的涉密信息设备和涉密存储设备赠送、出售、丢弃或者改作其他用途。

（四）禁止擅自卸载、修改涉密信息系统、涉密信息设备和涉密存储设备的安全技术程序、管理程序。

（五）禁止擅自访问、下载、存储、传输知悉范围以外

的国家秘密。

（六）禁止擅自扫描或者检测涉密信息系统的网络基础设施、安全保密产品以及应用系统等。

（七）禁止修改、删除涉密计算机保密技术防护专用系统的监控程序报警回联地址。

（八）禁止故意隐藏涉密信息设备和涉密存储设备，规避检查。

（九）未经审批，禁止更换涉密信息设备存储部件。

（十）未经审批，禁止重装涉密计算机操作系统。

第二十条 非涉密信息设备和非涉密存储设备：

（一）合肥研究院工作内网的保密管理执行《合肥研究院工作内网保密管理规定》。

（二）工作单机：禁止连接互联网和其他公共信息网络；禁止安装、配备和使用摄像头、麦克风等视音频输入设备和无线设备。

（三）互联网计算机：禁止在互联网计算机存储、处理涉密信息和内部信息。

第六章 互联网地址安全管理

第二十一条 使用互联网地址（以下称IP地址）须履行接入审批程序，并作好登记、审计工作，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。

第二十二条 IP 地址用于对外服务的，须经合肥研究院信息中心审核、备案。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。

第二十三条 合肥研究院科学岛园区内实行互联网、外网出入口集中管理。科学岛园区内新增互联网络接入或新 IP 地址段须经过合肥研究院信息中心的技术核验，向合肥研究院安保办备案，研究院信息化分管领导审批后方可实施。

第二十四条 各所、中心依据业务需要在其他地域使用独立网络出口的，须配套相应的网络安全管理设施，并经合肥研究院信息中心技术核验，向合肥研究院安保办备案，研究院信息化分管领导审批后方可实施。

第二十五条 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在可控范围内。

第七章 互联网信息服务安全管理

第二十六条 各单位应对自建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。

第二十七条 对外网站采用分级发布审核制度：各所、中心及课题项目网站上线前应报所信息化分管领导审核批准，合肥研究院门户网站需经合肥研究院信息化分管领导审核批准，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。网站 ICP 备案按《合肥研究院单位用户新增域名备案流程及说明》办理。

第二十八条 对电子公告板、论坛、聊天室、博客空间等交互式网站，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。

第二十九条 合肥研究院互联网站信息发布实行审核制度，内设机构及各部门开发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。

第三十一条 各单位应做好停止运维网站的注销和关停工作，具体流程参见《中科院合肥研究院院属网站注销流程》。同时信息中心应对内实时发布和更新合肥研究院所属网站列表，完善网站运营期间的内部监控工作。

第八章 互联网信息服务安全管理

第三十二条 合肥研究院信息中心和各二级及以上信息系统的业务主管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，制定重要信息系统应急预案，定期开展应急演练。

第三十三条 合肥研究院信息中心应建立网络安全信息报告工作机制，了解和掌握网络安全状况，及时报告突发网络安全事件。

第九章　监督检查

第三十四条　各单位应组织网络安全自查，检查范围包括安全责任划分、人员安全意识、对外开放服务、重要系统运行、系统软件漏洞、权限管理、系统维护、安全审计以及机房物理环境安全等。

安全保护等级为四级的信息系统每半年至少自查一次。安全保护等级为三级的信息系统及对外网站和电子邮件系统 每年至少自查一次。

第三十五条　依据《中国科学院网络安全事件与漏洞处理流程合肥研究院》，合肥研究院信息中心将定期或及时发布或转发安全通报；针对发现的重大安全风险隐患，以安全隐患告知书的形式督促整改，各单位要在接到安全隐患告知书 15 个工作日内修复隐患风险。对管理不善且超过 30 日未予整改的，合肥研究院信息中心将采封闭其端口或网络接入，注销相关注册信息等技术措施。

第三十六条　信息中心负责落实各单位的网络安全工作，对信息系统底数、信息安全等级保护、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

第三十七条　网络安全工作纳入合肥研究院年终安全工作先进集体、先进个人评选范围，对成绩显著或者做出突出贡献的集体和个人，予以表彰、奖励；发生重大网络安全事件的单位和个人，实行一票否决，取消所有评优资格。

第三十八条 对网络安全工作管理不力或存在网络安全重大隐患且长期未予整改的部门或个人，予以通报，同时上报合肥研究院安委会，追究相关人员的责任。

第十章 附则

第三十九条 本办法由合肥研究院信息中心负责解释。

第四十条 本办法自印发之日起施行。