Q/SYY

中 科 大 数 据 研 究 院 企 业 标 准

Q/SYY BZ204.01—2022

网络与信息安全管理制度

Network and Information Security Management System

2022－07－15 发布　　2022－08－01 实施

中科大数据研究院　　发 布

网络与信息安全管理制度

1 范围

本文件规定了中科大数据研究院网络与信息安全的管理等内容。本文件适用于中科大数据研究院各中心所有职工及使用单位网络的所有人员。

2 规范性引用文件

本文件没有规范性引用文件。

3 网络与信息安全管理架构

3.1 网络与信息安全领导小组

设立网络与信息安全领导小组，小组组长为院长王元卓，副组长为总工程师兼大数据创新平台中心主任冯凯，组员为各中心主任助理及大数据创新平台中心运维人员。

网络与信息安全领导小组主要职责如下：

1) 根据国家和卫健委有关网络与信息安全的政策、法律和法规，制定中科院计算技术研究所大数据研究院网络与信息安全总体规划、管理规范和技术标准等。
2) 发挥集中统一领导作用，统筹领导中科院计算技术研究所大数据研究院网络与信息安全相关工作。
3) 贯彻执行上级单位、相关单位下发的网络与信息安全文件要求及精神。
4) 协调、督促各中心的网络与信息安全工作，处理网络与信息安全隐患，参与信息系统工程建设中的安全规划，监督安全措施的执行。
5) 统筹领导处理网络与信息安全事故，组织进行事件调查，评估安全事件的严重程度，负责网络与信息安全事故的后续处理及防范措施等。

3.2 网络与信息安全工作

网络与信息安全工作具体内容包括：

1) 保障网络与信息系统安全运行。
2) 按照网络与信息安全等级保护制度对中科院计算技术研究所大数据研究院网络进行建设和整改工作。
3) 网络与信息安全突发事件处置、应对、整改。
4) 开展网络与信息安全宣传教育与培训。
5) 开展网络与信息安全检查与自查工作。
6) 负责中科院计算技术研究所大数据研究院网络与信息安全应急预案的编制并组织测试和演练。
7) 开展其他网络与信息安全工作。

4 网络与信息安全管理

网络与信息安全管理要求如下：

1) 网络与信息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。
2) 办公室负责对中科院计算技术研究所大数据研究院外网、内网（以下统称“网络” ）及设备和系统进行规划、建设、统一管理、日常维护、安全保障等工作。
3) 接入并利用中科院计算技术研究所大数据研究院网络进行工作的人员，应自觉遵守相关规章制度，建立良好的使用习惯，杜绝潜在的网络与信息安全隐患和漏洞。
4) 使用中科院计算技术研究所大数据研究院网络必须遵守相关法律法规，遵守公共秩序，尊重社会公德，不得利用网络从事危害国家安全、泄露国家秘密，不得侵犯国家、社会、集体的利益和公民的合法权益，不得从事违法犯罪活动。
5) 严禁通过中科院计算技术研究所大数据研究院网络进行传播反动、暴力、淫秽内容等违法行为，严禁利用中科院计算技术研究所大数据研究院网络制作、复制、发布、传播病毒、流氓软件及进行其他影响网络正常运行或影响其他用户正常使用的行为。
6) 在使用网络与信息设备时应保持清洁、安全、良好的工作环境，禁止在信息设备应用环境中放置易燃易爆、强腐蚀、强磁性等损害设备的物品。
7) 所有网络和信息设备未经中科院计算技术研究所大数据研究院办公室授权同意，严禁擅自拆、换任何零件、配件、外设。
8) 各中心主任助理对本部门信息设备安全管理负责。

5 内网安全管理

内网安全管理要求如下：

1) 接入内网的设备和软件，应进行充分的安全评估和杀毒扫描，只允许经过授权软件运行。
2) 临时接入内网的设备在接入前须进行病毒查杀，并由负责信息安全的工作人员辅助执行。
3) 内网接入设备实行白名单制度，所有接入内网的设备应由办公室进行授权备案。
4) 办公室建立内网系统配置清单，并进行配置审计。
5) 对重大配置变更应制定变更计划并进行影响分析，配置变更实施前进行严格安全测试。
6) 负责信息安全的工作人员密切关注重大安全漏洞及其补丁发布， 发现漏洞及时上报办公室，由办公室统一指定和进行升级措施。
7) 接入内部网络的设备严禁使用桥接、双网卡等方式直接接入互联网。
8) 对重要的业务数据、 关键程序建立健全的本地和异地、自动和手动相配合的多重备份机制。定期检查备份数据的完整性。
9) 接入内部网络的设备严禁使用各类型的移动存储设备，包括但不限于 U 盘、移动硬盘、软盘、光盘等。因业务拓展需要时，应由办公室进行统一推送部署。

6 外网安全管理

外网安全管理要求如下：

1) 新增设备接入外网，应报办公室进行备案。
2) 工作人员在使用接入外网的设备时，应做好基础的安全防护工作。安装防火墙和杀毒软件并定期查杀病毒和修补漏洞。
3) 禁止安装与工作无关的软件，禁止运行来源不明的软件和程序。

4) 禁止未经授权私自通过外接路由器、US 网卡等方式建立无线网络环境。
5) 因工作需要连接各类外来移动存储设备时，应进行病毒扫描等基础安全防护工作。

7 网络与信息安全事故管理

网络与信息安全事故管理要求如下：

1) 办公室负责制定安全事件应急响应预案，当遭受安全事故导致系统出现异常或故障时，应立即采取紧急防护措施，防止事态扩大，并上报院领导及信息化主管部门，同时注意保护现场，以便进行调查取证。
2) 办公室负责网络与信息安全事故应急预案的编制，并组织演练。
3) 网络与信息安全事故概念：
   (a) 普通网络与信息安全事故
   - 网络与信息系统发生 24 小时内故障瘫痪；
   - 安全事故影响范围仅限部分科室和部分设备；
   - 安全事故得到及时遏制和处理，未发生蔓延；
   - 安全事故没有造成数据丢失和泄密，没有造成经济损失；

   (b) 严重网络与信息安全事故
   - 网络与信息系统发生 24 小时以上 48 小时以内故障和瘫痪。
   - 安全事故影响范围包含大部分中心和设备；
   - 安全事故没有及时遏制和处理，但未蔓延；
   - 安全事故没有造成数据丢失和泄密，没有造成经济损失；
   - 安全事故造成一定影响，但在可控范围内。
   - 没有发生不利于单位的舆情信息。

   (c) 重大网络与信息安全事故
   - 网络与信息系统发生 48 小时以上的故障和瘫痪。
   - 信息系统受到较大面积病毒感染和渗透、攻击。
   - 安全事故没有及时遏制和处理，发生蔓延；
   - 安全事故造成数据丢失和泄密，造成经济损失；
4) 出现网络与信息安全事件时，发现者及时上报中心主任助理和办公室，做到及时、全面、准确报送，不得瞒报、缓报、谎报网络与信息安全情况。
5) 出现严重或重大网络与信息安全事故时，办公室及时上报信息化主管部门。
6) 发生网络与信息安全事故时，网络与信息安全小组应及时对故障进行排查、处理，第一时间阻止事故发生蔓延。若无法处理，应立即联系软件服务商或联系信息化主管部门人员寻求协助处理。

8 网络与信息安全教育与管理

网络与信息安全教育与管理要求如下：

1) 员工入职后应参加办公室组织的网络与信息安全培训，以提升其网络与信息安全意识及技术水平。
2) 办公室不定期对各中心员工的网络与信息安全防护行为进行考核评估，对发现具有安全隐患的行为，应限期监督整改。

3) 员工离职时应返还属于中科院计算技术研究所大数据研究院的全部信息设备，不得在离职时以任何形式带走任何信息。