ICS 01.020
CCS A 00

T

团 体 标 准

T/CI 1.2—2024

智慧科研机构安全体系建设导则

Guidelines for the construction of security system for intelligent scientific research institutions

征求意见稿

2023-XX-XX 发布 2024-XX-XX 实施

中国国际科技促进会 发布

目 次

前　　言

本文件按照GB/T 1.1—2020《标准化工作导则 第1部分：标准化文件的结构和起草规则》的规定起草。

本文件由中国国际科技促进会标准化工作委员会提出。

本文件由中国国际科技促进会归口管理。

本文件起草单位：xxx、

本文件主要起草人：xxx、

本文件由中国国际科技促进会标准化工作委员会制定并负责解释。

智慧科研机构安全体系建设导则

1 范围

本标准从规定了智慧科研机构安全体系建设的术语和定义、体系的构成、体系建设的基本原则和目标、体系建设的基本要求、建设流程。

本标准适用于从事自主创新技术研究的智慧型科研机构的安全体系建设。

2 规范性引用文件

下列文件中对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 25069-2010 信息安全技术 术语

GB/T 25070-2019 信息安全技术 网络安全等级保护安全设计技术要求标准

3 术语和定义

GB/T 25069-2010 界定的以及下列术语和定义适用于本文件。

3.1

智慧研究机构 Smart Research Institutions

基于知识构筑的智慧化组织，其组织、决策、运营、市场营销、管理和科研生产模式是以知识应用为基础，以创新驱动发展为目的，具有自学习、自成长、自优化、自适应的特征，是支撑我国科研院所未来自主创新的核心科研组织。

3.2

智慧研究机构安全 Security Of Smart Research Institutions

在智慧研究机构中对信息的保密性、完整性和可用性的保持，以及依此提供的信息安全、网络安全和运行安全。

3.3

智慧研究机构安全体系建设 Construction Of Safety System For Scientific Research Institutions

智慧科研机构安全体系建设是指通过建立健全的安全管理制度、技术防范体系和应急响应机制，确保科研机构的信息安全，网络安全和运行安全。

3.4

智慧研究机构安全管理者 Security Manager of Smart Research Institutions

智慧科研机构信息安全组织建设、机制建设，以及协调监督的实体。

3.5

智慧研究机构安全建设者 Security Builder for Smart Research Institutions

智慧科研机构信息安全工程实施，部署智慧研究机构安全技术防护措施的实体。

3.6

智慧研究机构安全运维者 Construction Of Safety System For Scientific Research Institutions

负责智慧科研机构安全事件的监测、预警、响应、应急处置和恢复的实体。

4 缩略语

下列缩略语适用于本文件。

5 智慧科研机构安全目标

围绕智慧科研机构安全保护对象，智慧科研机构安全提供者、安全管理者、智慧科研机构建设者、智慧科研机构安全运维者等安全角色相互协作，实现以下安全目标：

a) 保证智慧科研机构信息系统安全运行，尤其是保证重要关键信息系统的可用性和可靠性；
b) 保证智慧科技机构的数据资产的真实性、保密性、完整性、可用性和可靠性；
c) 保证智慧科研机构应用和服务的可用性、可靠性和可核查性；
d) 保证智慧科技机构整体安全的合理性、鲁棒性和可扩展性。

6 智慧科研机构安全体系概述

智慧科研机构安全体系建设是指通过建立健全的安全管理制度、技术方法体系和应急响应机制，确保科研机构的信息安全、网络安全和运行安全，并且审核信息安全职能（责任）部门制定的信息安全管理策略、工作流程和各种规章制度，监督信息安全措施的落实和执行，领导信息安全检查工作。

6.1 智慧科研机构安全保护的对象

智慧科研机构安全保护对象分为硬件设备、软件设备、信息系统、数据资产与应用服务。

硬件设备是智慧科研机构中具有独立工作能力的信息采集或处理设备，包括终端、网络设备、安全设备、服务器等。

软件设备是服务于智慧科研机构的工具和业务应用系统等。

信息系统指应用服务、数据资产、硬件设备之外的 ICT 基础服务，为科研机构提供网络、存储、计算等基础资源服务，包括虚拟化平台和云服务等。

数据资产是智慧科研机构收集、存储、传输、处理和产生的各种电子数据。

应用服务是应用系统提供的数据共享服务及数据服务和数据计算服务等。

6.2 智慧科研机构安全体系框架

智慧科研机构安全体系框架是实现智慧科研机构安全目标的参考模型，由智慧科研机构的安全保护对象、安全要素、安全角色及其相互关系组成，如图 1 所示。其中安全要素包含安全管理、安全技术、安全建设、安全运营和配套安全产品及工具等方面。

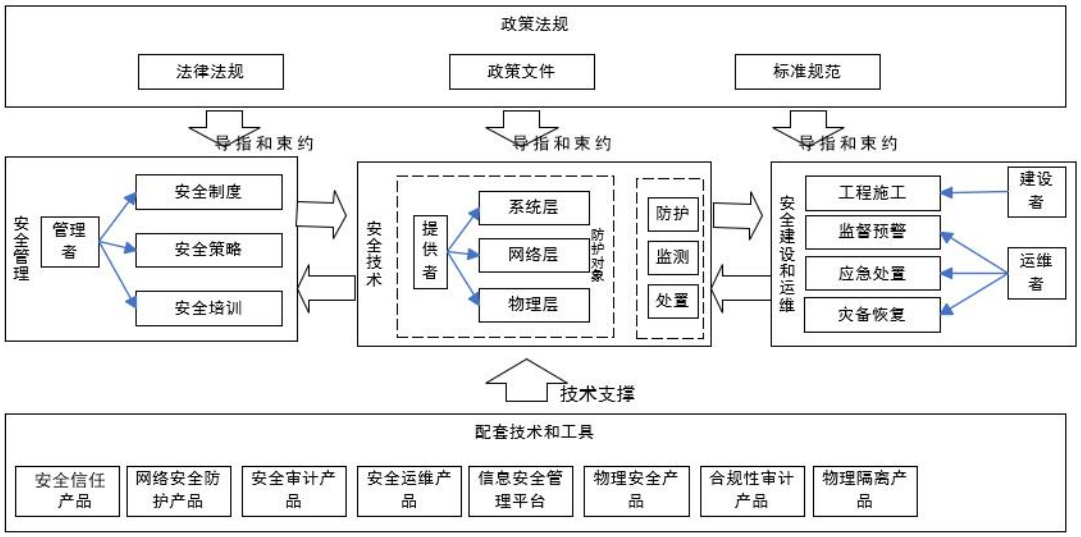

图 1. 智慧科研机构安全体系框架

6.3 智慧科研机构安全角色

6.3.1 智慧科研机构安全管理者

智慧科研机构安全管理者的职责包括但不限于：

a) 制定智慧科研机构安全管理机制；
b) 制定智慧科研机构安全人才培养和安全意识教育计划；
c) 为智慧科研机构建设者、安全运营者提供指导和必要支持。
d) 定期开展智慧科研机构安全应急演练活动；
e) 及时报告安全威胁信息与安全事件；

6.3.2 智慧科研机构安全建设者

智慧科研机构安全建设者的职责包括但不限于：

a) 实施智慧科研机构安全工程建设；
b) 部署有效的智慧科研机构安全防护措施；
c) 测试智慧科研机构信息工程建设安全建设方案；
d) 定期对智慧科研机构安全建设方案进行评审和改进；

6.3.3 智慧科研机构安全运维者

智慧科研机构安全运维者的职责包括但不限于：

a) 负责智慧科研机构安全运行与维护管理；
b) 监测智慧科研机构安全风险，分析安全态势；
c) 发现智慧科研机构安全事件和脆弱性、防范、阻断网络攻击；
d) 应急处置智慧科研机构安全风险与安全事件；
e) 制定、评估并修订智慧科研机构安全事件应急预案；
f) 实现对恶意行为的取证和追踪溯源；
g) 保证灾后智慧科研机构信息系统快速恢复正常运转状态；
h) 有效控制智慧科研机构安全事件造成的负面影响。

6.3.4 智慧科研机构安全提供者

a) 设计开发安全产品与应用，并提供维护技术服务；
b) 按照智慧科研机构安全管理策略部署安全技术措施；
c) 协助智慧科研机构安全建设者进行工程建设，提供安全产品、服务及技术服务支持；
d) 协助智慧科研机构安全运营者完成应急恢复及调查取证，提供安全产品、服务及技术支持。

6.4 智慧科研机构安全要素

智慧科研机构安全管理主要包括管理制度建设、应急响应机制、人员安全意识培训、教育培训和演练等。

智慧科研机构安全技术由智慧科研机构服务提供者研究、开发和设计应用，在物理层、网络通信层、计算与存储层、数据及服务融合层以及智慧应用层五个层次分别部署安全技术防御措施，应对智慧科研机构安全风险。

智慧科研机构安全建设与运营主要包括信息安全工程实施和安全运营。智慧科研机构信息安全工程实施是指信息系统/设备开发、采购、集成、组件、配置及测试。智慧科研机构安全运营是对信息系统运行状态的维护、监测，对安全事件的报告、应急处置、恢复，确保并维持智慧科研机构的各项业务安全有序运行。

7 智慧科研机构安全管理

7.1 信息安全管理制度建设

信息安全管理制度建设包括但不限于以下内容：

a) 应建立安全保卫制度；
b) 应建立保密管理制度；
c) 应建立信息安全风险评估制度；
d) 应建立规范的信息安全管理流程。

7.2 应急响应机制

应急响应机制包括但不限于以下内容：

a) 安全事件应急预案及其有效性评估；
b) 应急处置机制；
c) 安全事件教育培训；
d) 应急智慧体系。

7.3 人员安全意识培训和演练

人员安全意识培训要求的主要内容：

a) 加强对科研人员的教育培训，提高他们的信息安全意识和安全技能，增强他们的安全责任干和风险意识。
b) 定期组织演练，提高科研人员在面对安全事件时的应变能力。

7.4 安全管理体系建设

安全管理体系建设要求的主要内容：

a) 建立健全的安全管理体系，包括安全组织架构、安全管理流程、安全培训计划等，确保安全管理工作的有效开展。
b) 制定信息安全总体策略，明确机构安全工作的总体目标、范围、原则和安全框架等内容，其安全体系也应围绕其总体策略建设。

8 智慧科研机构安全技术

技术防范体系建设与网络安全防护包括但不限于以下内容：

8.1 物理层提供基础的安全保障

对实验室、办公场所、网络设备等物理场所进行安全控制，避免设备被破坏、数据被泄露等情况的发生。

8.2 网络层提供安全的通信信道

a) 局域网
b) 广域网
c) 互联网等。

8.3 系统层提供技术支持和防护措施

a) 软件
b) 硬件
c) 计算与存储
   1） 数据内容、数据与服务融合资源的防护措施；
   2） 数据存储安全；
   3） 基础软件安全，包括但不限于操作系统、数据库、中间件和资源管理软件的安全。
d) 通信网络
   1） 科研网络应支持资源分层隔离安全
   2） 不同保护等级的业务应分区域进行保护
   3） 应支持细粒度网络层安全策略访问控制
e) 智慧应用
   1） 智慧应用的可靠性和可扩展性；
   2） 应用软件、职能终端、网站等防护措施；
f) 数据安全及通信网络安全
   1） 物理或虚拟计算资源安全；
   2） 物理或存储资源安全；
   3） 身份鉴别；
   4） 访问控制；
   5） 网络接入安全；。

8.4 内生安全

a) 可获得性
   1） 软硬件基础设施资源应可持续获得
   2） 软硬件维护与安全支持服务应可持续获得
b) 安全可控
   1） 软件资源应遵从安全规范开发
   2） 硬件设备应支持可信启动
   3） 软硬件及算法模块无后门
   4） 重要网络环境 CPU、OS、服务应符合安全可靠测评要求
c) 安全韧性
   1） IT 架构无单点故障风险
   2） 网络应遵从服务分层与分区域隔离
   3） 产品部件应具备一定故障恢复能力
   4） 产品部件宜具备初步入侵感知、阻断能力（密码爆破、输入校验等）
d) 安全功能配置
   1） 产品材料应包含安全配置说明
   2） 应支持配置文件备份与还原
   3） 配置项应默认为安全选项
   4） 应支持弱口令防范机制、审计机制

8.5 高价值资产安全

智慧科研机构场所存在高价值专用设备、高性能通用与专用计算能力、机密科研实验与成果数据，宜在分层防御的基础上需针对此类高价值资产进行安全增强保护。

a) 算力安全
   1） 支持算力运行状态监控
   2） 支持大规模算力节点认证管 1i6
   3） 支持机密计算能力
b) 数据安全
   1） 支持敏感数据混淆与脱敏能力
   2） 科研成果数据如大模型微调与权重数据使用增强的访问控制
   3） 参考“3+2+1”数据安全备份机制，侧重隔离独立保存
   4） 存储与网络支持重要数据勒索防范机制
c) 密码安全
   1） 使用证书进行设备与算力节点认证
   2） 密码技术产品符合密码测评安全要求
   3） 对重要数据进行加密存储
d) 设备安全
   1） 专用设备应隔离部署
   2） 支持物理与网络访问控制
   3） 具备紧急关停等熔断机制

8.6 事件响应层提供监测预警和处理安全事件

安全监控和预警应包括但不限于以下内容：

a) 按照《国家网络安全事件应急预案》的规定进行预警分级、监测预警、预警研判及预警响应与解除；
b) 基础硬件设备的监测监控；
c) 漏洞和恶意代码识别、修补和防范机制；
d) 安全态势感知。

整体安全态势感知应整合各类应用服务与设备告警日志、关键流量，进行安全分析，防范单点绕过，发现隐藏的威胁。

1） 应具备网络设备的安全资产全景、风险现状、入侵事件及处置状态的统一呈现
2） 应支持与多元感知数据来源对接
3） 应支持对收集的日志与事件进行查询、管理
4） 应具备运维入侵感知能力，可对接审计能力，及时发现口令暴力破解、异常登录行为、非法账号创建等行为
5） 宜支持基于资产的风险管理与配置核查
6） 应支持高级威胁分析
7） 宜支持安全事件的处置闭环

8.7 安全服务层提供专业的安全服务

安全服务包括但不限于业务上线安全检测、安全基线检查、安全配置加固，安全镜像管理，安全漏洞修复，可通过安全咨询、运营、运维服务提供。

1） 安全咨询
2） 安全检测
3） 安全加固等。

9 智慧科研机构安全建设与运营

9.1 工程实施

应对项目过程进行安全管理，对相关安全角色进行授权与保密培训，管控项目验收编制安全要求，确保安全交付有效性，业务处于被保护状态。

9.2 监测预警与应急处置

9.3 灾备恢复

应制定灾备恢复计划，明确灾备恢复原则与保护对象，安全角色依据计划进行安全备份与归档及灾备资源的储备和使用，定期进行安全恢复检验与测试，确保业务和数据可用，灾备方案有效。