ICS 35.240.70
CCS A 40

中华人民共和国国家标准

GB/T 43708—2025

科学数据安全要求通则

General rules for scientific data security requirements

2025-01-24 发布　　2025-01-24 实施

国家市场监督管理总局
国家标准化管理委员会　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。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由中华人民共和国科学技术部提出。

本文件由全国科技平台标准化技术委员会(SAC/TC 486)归口。

本文件起草单位：中国标准化研究院、中国科学院计算机网络信息中心、中国网络安全审查技术与认证中心、福建中信网安信息科技有限公司、国家海洋信息中心、北京航空航天大学、国家科技基础条件平台中心、山西华正创新技术研究院有限公司、中科星睿科技(北京)有限公司、中路高科交通科技集团有限公司、自然资源部第一海洋研究所、福建大数据一级开发有限公司、广州物联网研究院、南方电网互联网服务有限公司、中国科学院青藏高原研究所。

本文件主要起草人：王志强、廖方宇、杨青海、胡良霖、甘杰夫、苏靖、金华松、徐凯程、姜晓轶、赵启阳、王漪、赫运涛、朱艳华、叶菱、区东、刘冬梅、宋转玲、李喆、陈鲁鑫、高尚、段静辉、赵琳、梁国霞、李新。

引　言

科学数据是战略性、基础性科技资源，具有传播速度快、影响面宽、开发利用潜力大的特点，深刻影响着国家科技进步和经济发展。《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》与《中华人民共和国网络安全法》是我国网络数据领域治理的基础性法律，标志着我国支撑网络大国、数字大国建设的制度体系更加成熟。《科学数据管理办法》明确提出“应加强科学数据全生命周期安全管理，制定科学数据安全保护措施；加强数据下载的认证、授权等防护管理，防止数据被恶意使用。”本文件是切实提升科学数据领域信息保护与合规运用能力的重要保障，可促进科学数据相关机构数据安全能力提升。

本文件是一项基础的科学数据安全标准，综合考虑科学数据生存周期中的安全要素，形成覆盖科学数据全过程的生存周期维度，以及基于保密性、可用性、完整性、可溯源性、可控性和不可否认性等安全属性维度的要求，同时也统一了科学数据安全通用术语，见附录 A。

科学数据安全要求通则

1 范围

本文件规定了科学数据安全的通用要求，包括总则、科学数据安全基本框架、科学数据生存周期安全要求、科学数据实体安全要求和科学数据安全管理要求。

本文件适用于科学数据的采集加工、存储备份、传输交换、开放共享、使用服务和安全处置等科学数据生存周期中的数据安全。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；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 9361—2011 计算机场地安全要求

GB/T 21052 信息安全技术 信息系统物理安全技术要求

GB/T 34945 信息技术 数据溯源描述模型

GB/T 35274 信息安全技术 大数据服务安全能力要求

GB/T 36092 信息技术 备份存储 备份技术应用要求

GB/T 37939 信息安全技术 网络存储安全技术要求

GB/T 37973 信息安全技术 大数据安全管理指南

GB/T 43705 科学数据安全分类分级指南

GB/T 43710 科学数据安全审计要求

GM/T 0054 信息系统密码应用基本要求

3 术语和定义

下列术语和定义适用于本文件。

3.1

科学数据 scientific data

在自然科学、工程技术科学等领域，科学研究活动中形成的以及通过观测监测、考察调查、检验检测等方式获取的原始及其衍生信息的记录，或可用于科学研究活动的其他数据。

3.2

科学数据安全 scientific data security

通过管理和技术措施，针对国家安全、科技安全、社会公共利益和他人合法权益，确保科学数据持续得到有效保护和合规利用的状态。

[来源：GB/T 37988—2019，3.1，有修改]

3.3

科学数据生存周期 scientific data lifecycle

科学数据从采集加工、存储备份、传输交换、开放共享、使用服务、安全处置，最终实现再利用的一个

循环过程。

3.4

保密性　confidentiality

信息对未授权的个人、实体或过程不可用或不泄漏的性质。

[来源:GB/T 25069—2022,3.41]

3.5

完整性　integrity

准确和完备的性质。

[来源:GB/T 29246—2023,3.36]

3.6

可用性　availability

可由经授权实体按需访问和使用的性质。

[来源:GB/T 25069—2022, 3.345]

3.7

可控性　controllability

对信息和信息系统可以实施安全监控管理,防止非法利用的性质。

3.8

不可否认性　non-repudiation

抗抵赖性

证明一个已经发生的操作行为无法否认的性质。

[来源:GB/T 25069—2022,3.321]

3.9

可溯源性　provenance

追溯客体的历史、应用情况或所处位置的能力。

3.10

科学数据开放　scientific data opening

按照给定的管理策略和规则,组织向外部提供科学数据的行为和过程。

3.11

科学数据安全分类　scientific data security classification

根据科学数据的安全属性或特征、安全管理需求、多维特征及其相互间客观存在的逻辑关联等将其按照一定的原则和方法进行划分和归类,并建立起一定的层次体系和排列顺序的过程。

3.12

科学数据安全分级　scientific data security grading

根据科学数据的影响对象及其影响程度的不同,确定科学数据安全级别的过程。

注:影响对象通常包括:国家安全、经济运行、社会秩序、公共利益、组织权益、个人权益等。

3.13

安全审计　security audit

对信息系统记录与活动的独立评审和考察,以测试系统控制的充分程度,确保对于既定安全策略和运行规程的符合性,发现安全违规,并在控制、安全策略和过程三方面提出改进建议。

[来源:GB/T 25069—2022,3.24]

3.14

安全处置　security disposition

对科学数据实施移交、销毁、删除或长期归档的一系列活动过程。

3.15

科学数据产品　scientific data product

在各类科学活动中形成的、经包装并能独立提供的、可重复使用和再加工的、生存周期全过程可追溯的、可实现用户特定需求的科学数据集合及其应用软件。

4　总则

4.1　安全目标

对科学数据的采集加工、存储备份、传输交换、开放共享、使用服务、安全处置的过程提出安全要求，以防止科学数据泄露、扩散或破坏，并防止对数据的非授权使用、修改或泄密，确保科学数据的保密性、可用性、完整性、可溯源性、可控性和不可否认性。

4.2　基本原则

4.2.1　技术和管理相结合原则。技术要求和管理措施相结合，共同来确保科学数据的安全。

4.2.2　数据生存周期全覆盖原则。对计算机系统数据的采集加工、存储备份、传输交换、开放共享、使用服务、安全处置等过程分别提出安全要求。充分考虑科学数据生存周期经多次迭代和再利用而形成新的科学数据产品的特点。

4.2.3　数据安全属性和数据生存周期相对应原则。根据科学数据安全属性，明确对应科学数据生存周期各阶段满足各安全属性要求。

4.2.4　数据安全和数据开放相协调原则。在确保科学数据安全的基础上，在一定范围内和一定条件下，实现科学数据开放。

5　科学数据安全基本框架

5.1　概述

科学数据安全基本框架的第一个维度是数据生存周期维度，涵盖科学数据的采集加工、存储备份、传输交换、开放共享、使用服务、安全处置等 6 个阶段。

科学数据安全基本框架的第二个维度是数据安全属性维度，包括数据保密性、可用性、完整性等基本安全属性，以及可溯源性、可控性以及不可否认性等扩展安全属性。

科学数据安全基本框架是在科学数据生存周期中各功能集合所需的安全技术要求和管理要求，满足保密性、可用性、完整性等数据安全属性的各项要求。

科学数据安全的通用术语见附录 A。

科学数据安全基本框架见图 1。

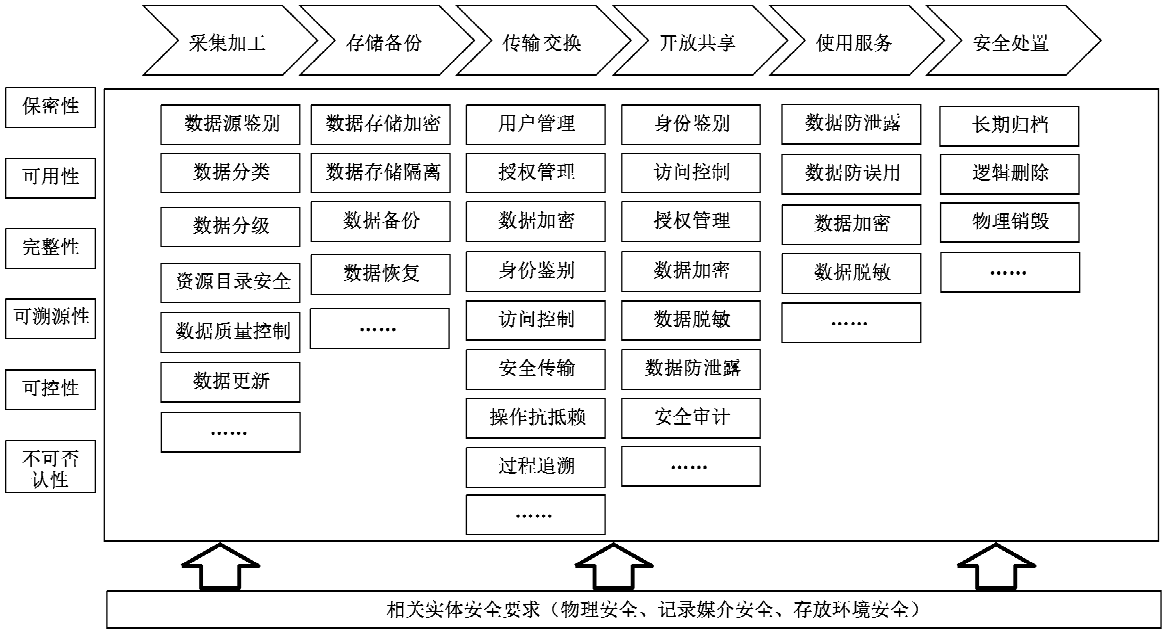

图 1　科学数据安全基本框架

5.2　科学数据生存周期维度

科学数据生存周期分为以下 6 个阶段：

a）　采集加工阶段：科学数据生产方或拥有方内部系统中新产生数据，以及从外部系统收集数据，并对数据进行处理加工的阶段；

b）　存储备份阶段：科学数据以任何数字格式进行存储，并进行备份的阶段；

c）　传输交换阶段：科学数据从一个实体传输到另一个实体，进行科学数据交换的阶段；

d）　开放共享阶段：对科学数据进行分发、出版、共享的阶段；

e）　使用服务阶段：对科学数据进行计算、分析、可视化等操作，对外提供服务的阶段；

f）　安全处置阶段：对科学数据及数据存储媒介通过相应的操作手段，对科学数据进行长期归档，或对科学数据进行销毁删除的阶段。

注 1：特定的科学数据所经历的生存周期由实际的业务所决定，可为完整的 6 个阶段或是其中的几个阶段。

注 2：科学数据生存周期具有多次迭代的特点，对科学数据进行深度挖掘和加工，形成新的科学数据产品，即科学数据再利用，实质上是一种高层次的研发活动，运用信息分析、综合和预测等先进方法，形成新的科学数据产品，它会不断充实数据链条，加快数据流转，适应科技创新需求。

5.3　数据安全属性维度

5.3.1　保密性要求

保密性的要求如下：

a）　应对密钥进行有效的管理，包括对密钥的产生、存储、分配、更换、保管、使用和处置的全过程；密钥的分配可采用人工和自动相结合的方式；密钥的产生和检验工作应由专门的密钥管理部门和授权的人员负责，密钥存储要按照国家有关规定，确保密钥的机密性、完整性和认证性；

b）　应根据所传输或存储的科学数据安全分级和信息特征，确定对科学数据加密保护的方式（传输数据的用户加密、线路加密、存储数据的局部或全部加密、数据库内或库外加密等）；

c）　应对传导和辐射产生的电磁信号泄露进行有效的抑制和屏蔽，以保证数据在一定范围内不被

泄露。

5.3.2 可用性要求

可用性的要求如下：

a) 用户身份的鉴别：应确保授权用户经鉴别身份后允许进入系统；
b) 访问控制：应采用访问控制机制来保证合法用户只能访问与其身份相适应的一定种类和一定分级的数据资源；
c) 安全审计：应对访问数据资源的有关事件和有关操作进行安全审计，以便获得完整的记录，根据记录进行安全性的分析，并及时采取处理措施。

5.3.3 完整性要求

完整性的要求如下：

a) 数据完整性：应对科学数据进行完整性检验；应定期检查存储数据媒介的物理损伤情况，尽量减少误操作、软件故障、硬件故障和强电磁干扰等意外事件，以保证数据的完整性；
b) 软件完整性：应对软件确认其功能的正确性；为了防止软件被非法复制，软件应有唯一的标识，且能检验这种标识是否存在，以及是否被绕过；为了防止软件被非法修改，软件应具有抗分析能力和完整性检验的手段。

5.3.4 可溯源性要求

可溯源性要求如下：

a) 数据可追溯：应记录和更新科学数据从产生、处理，再到成果等各个环节的数据信息，保障科学数据的高效利用；
b) 行为可追溯：应确保每一条数据都可查询其使用者及其源头；在数据的传输、处理、交换环节中，从用户、设备、应用的视角审计这些实体的行为，实时追踪数据的来龙去脉，为数据安全事件提供溯源、取证。

科学数据溯源的信息描述模型应符合 GB/T 34945 的规定。

5.3.5 可控性要求

可控性要求如下：

a) 应具备访问权限控制的管理机制；
b) 应验证对各软件资源和数据的访问、操作和使用的权限；
c) 应验证软件、固件和配置文件的升级、加载和安装的权限；
d) 应对接入安全系统的软件、固件和配置文件进行安全测试。

5.3.6 不可否认性要求

不可否认性要求如下：

a) 发送不可否认：应具有在请求的情况下，为数据发送方提供数据原发证据的功能；数据发送方不能否认发过数据，不能诬陷收方伪造数据；
b) 接收不可否认：应具有在请求的情况下，为数据接收者提供数据接收证据的功能，数据接收方应能证实数据是由确认的数据发送方发来的，内容是真实的，对收到的数据不能修改和抵赖。

6 科学数据生存周期安全要求

6.1 科学数据采集加工的安全要求

6.1.1 对采集到的数据应按核定的内容和范围，及时登记和编制目录，且应按照 GB/T 43705 确定科学数据安全分类和科学数据安全分级，并按相应级别规定的要求分类管理。

6.1.2 应对数据的收集和获取过程建立安全控制措施，保证各类数据采集活动的合规性和安全性。

6.1.3 在数据执行清洗、转换与加载的过程中执行保护措施，应确保数据的保密性、完整性和可用性。

6.2 科学数据存储备份的安全要求

6.2.1 科学数据应按照 GB/T 36092 的要求进行备份。

6.2.2 科学数据如果采用网络存储方式，应符合 GB/T 37939 的要求。

6.2.3 应通过分析组织机构的数据量增长、数据存储安全需求和合规性要求制定适当的存储架构，以实现对存储数据的有效保护。

6.2.4 存储科学数据如需加密，要求如下：

a) 对存储在各种存储媒介上的科学数据应按照 GB/T 43705 确定的级别，进行加密，防止明文内容的泄露，防止非授权者从已加密的科学数据中获得明文，防止非授权的检索和修改科学数据；

b) 对数据加密时，应保证有足够的系统资源，不应过多影响查询、检索速度及数据维护的操作时间。

6.2.5 存入系统中的数据应由专人录入和核对。数据在存储之前，应确保数据准确性。

6.3 科学数据传输交换的安全要求

6.3.1 应提供满足数据传输安全策略相应的安全控制技术方案，包括安全通道、可信通道、数据加密等。

6.3.2 应提供在构建传输通道前对两端主体身份进行鉴别和认证的技术方案和工具。

6.3.3 应利用加密、数字签名、数字证书、鉴别和认证等机制对数据传输进行安全管理，防止数据遭泄露和篡改。

6.3.4 应采用符合 GM/T 0054 规定的密码技术，保证传输交换过程中数据的保密性和完整性。

6.3.5 在关键的业务网络架构汇总时，宜考虑数据传输的可靠性和网络的可用性，对关键的网络传输链路、网络设备节点实行冗余建设。

6.3.6 如需进行线下传输，应在密封、媒介、运输途径等方面采取必要的安全措施。

6.4 科学数据开放共享的安全要求

6.4.1 通过业务系统和数据产品对外部客户提供数据时，以及通过合作的方式与第三方合作伙伴开放共享数据时，应执行对数据交换过程的安全风险控制，以实现对数据价值保护的有效性和合规性。

6.4.2 应通过在数据发布的过程中对发布数据的格式、适应范围、发布者与使用者权利和义务执行必要控制，以实现数据发布过程中数据的安全可控与合规。

6.4.3 应通过基于组织机构数据存储安全需求和合规性要求建立数据访问控制机制，防止对存储数据的未授权访问风险。

6.4.4 应根据数据使用过程中的安全和业务需求，明确敏感数据的脱敏需求，制定相应数据脱敏规则，对敏感数据进行数据脱敏处理以保证数据的可用性和安全性的平衡。

6.4.5 应规定开放共享数据的范围、权限、级别，并能防止越权操作。

6.4.6 科学数据开放共享时，不得对科学数据原始记录做任何篡改或损坏。科学数据共享完毕后，应

检查并确保数据的原始状态。

6.4.7 应根据科学数据安全级别处理相应的科学数据。未经批准，不得在低级别环境中处理高级别数据。

6.4.8 在处理数据时，应采取措施防止因声、光干扰，以及电、磁等传导和辐射干扰所造成的数据泄露与破坏。

6.4.9 应建立良好的人机操作环境，以减少操作数据的失误。

6.5 科学数据使用服务的安全要求

6.5.1 科学数据使用服务安全应符合 GB/T 35274 的要求。

6.5.2 应通过针对组织机构内部使用相关计算、开发平台/系统建立分布式处理的安全保护机制，防止分布式处理过程中数据泄漏、未授权访问等安全风险。

6.5.3 应通过在数据分析过程中对国家安全、业务价值、个人数据保护的安全需求分析，采取适当的安全控制措施以防止由于数据分析而可能带来的数据价值泄露风险。

6.5.4 基于国家相关法律法规对数据使用和分析处理的相关要求，应通过对数据使用过程中的相关责任、机制的建立保证数据的正当使用。

6.5.5 应按规定授权原则确定不同用户的数据访问权限，并由专人负责编制授权表。

6.5.6 应划分用户类别和权限，使数据的使用被限制在工作确需的范围内。

6.5.7 应规定科学数据安全分类、科学数据安全分级、用户使用的许可等级和相应的数据使用规则，以保证数据的安全使用。

6.5.8 应规定数据的安全级别和相应的数据流控制规则，以保证数据使用时，不允许安全级别低的数据流向同级或安全级别高的数据。

6.5.9 应采取数据保护措施，以保证使用数据的完整性和准确性。

6.5.10 应采取容错、备份和恢复措施，以保证数据使用的可靠性。

6.5.11 为防止合法用户因误操作而造成数据丢失，应用程序应保证在操作者执行修改或删除时有醒目的提示。经过操作者确认后，才能存储修改后的数据，并记录版本的更新情况。

6.5.12 应按照 GB/T 43710 的要求，进行科学数据安全审计。

6.6 科学数据安全处置的安全要求

6.6.1 数据使用后，应将存储过科学数据的媒介妥善保管，必要时进行长期归档或经过评估后销毁。

6.6.2 应通过建立数据归档存储的规范化流程和安全保护措施，实现对归档数据的有效保护。

6.6.3 应根据科学数据再利用的要求，科学数据宜进行长期归档，必要时计算机存储媒介内的残留数据应及时清除，以防止数据泄露。

6.6.4 应通过建立针对数据内容的清除、净化机制，防止因对存储介质上的数据内容的恶意恢复而导致的数据泄露风险。

6.6.5 对如确实需要销毁的科学数据，应进行鉴定审核后，再行销毁。

7 科学数据实体安全要求

7.1 计算机系统的物理安全要求

7.1.1 计算机系统的物理安全应符合 GB/T 21052 的要求。

7.1.2 处理科学数据的计算机应根据不同级别要求选用，其防电击、防火灾、防能量危害等安全防护性能应符合有关标准的规定。

7.1.3 处理科学数据的计算机及有关设备应有备份。

7.1.4 计算机及有关设备在电磁发射和敏感度方面应符合有关标准的要求。

7.1.5 计算机的防病毒保护应符合相关国家标准的要求。

7.1.6 计算机系统应具有识别与认证用户身份的手段以限定操作人员。

7.2 科学数据记录媒介的安全要求

7.2.1 针对组织机构内需要对数据存储介质进行访问和使用的场景，应提供有效的制度流程和技术工具保证，防止对介质的不当使用而可能引发的数据泄露风险。

7.2.2 应通过建立对介质的安全销毁的规程和技术手段，防止因介质丢失、被窃或未授权的物理访问而导致的介质中的数据面临泄露的安全风险。

7.2.3 应根据媒介上记录内容的重要性、类别和级别，将媒介分为相应的类型。分类分级应遵循GB/T 43705的要求。

7.2.4 应对科学数据记录媒介的存放、传递等提出保护性要求。应根据本地存储、云存储、分布式存储等存储方式，分别提出保护要求，科学数据记录媒介的保护性要求应符合相关国家标准的规定。

7.2.5 当记录不同类别和级别科学数据时，记录媒介应由专人负责，保存在一定安全要求的物理环境，科学数据记录媒介的管理要求应符合相关规定。应采用存储备份等必要的手段，确保物理介质物理保存时间大于科学数据的保存时间。

7.3 科学数据记录媒介存放环境的安全要求

7.3.1 存放科学数据记录媒介的科学数据中心建筑物结构的耐火等级应符合GB/T 9361—2011中第6章的规定。

7.3.2 存放科学数据记录媒介的科学数据中心建筑物的火灾报警及消防设施应符合GB/T 9361—2011第10章的规定。

7.3.3 存放科学数据记录媒介的科学数据中心建筑物应具备通风条件和配备空调装置，并根据存放媒介的要求，确定其合适的温、湿度值。

7.3.4 存放科学数据记录媒介的科学数据中心建筑物，根据其所存放的媒介要求，应具有防霉、防震、防风、防水、防有害物质、防核辐射以及防盗等安全措施。

7.3.5 存放科学数据记录媒介的建筑物应采用铁门、铁窗、铁柜及其他高安全性能的锁具；存放科学数据记录媒介的建筑物应设置防盗报警器。

8 科学数据安全管理要求

8.1 科学数据安全管理要求应符合国家和有关行政机构现行的安全管理规定。

8.2 科学数据安全管理应符合GB/T 37973的要求。

8.3 运行科学数据的硬件基础和网络的安全管理要求应符合相关国家标准要求。

8.4 应按照GB/T 43710的要求，进行科学数据安全审计。

8.5 应按照GB/T 43705的要求，进行科学数据安全分类分级。

8.6 为了保证科学数据安全，应建立并健全各种规章制度。主要的规章制度包括但不限于：

a) 数据安全管理制度；
b) 数据媒介及其存放环境管理制度；
c) 数据管理人员安全培训、考核制度；
d) 数据管理部门安全职责范围的规定；
e) 数据管理人员安全职责范围的规定；
f) 数据安全应急预案、恢复措施的规定。

附 录 A
（资料性）
科学数据安全通用术语

A.1 总体类

A.1.1

科学数据安全特性 scientific data security feature

科学数据的保密性、可用性、完整性、可溯源性、可控性和不可否认性等安全特性。

A.1.2

真实性 authenticity

科学数据可验证可重复的特性。

A.1.3

数据完整性 data integrity

数据所具有的特性，即无论数据形式作何变化，数据的准确性和一致性均保持不变。

[来源：GB/T 25069—2022，3.574]

A.1.4

可靠性 reliability

与预测行为和结果一致的性质。

[来源：GB/T 29246—2023，3.55]

A.1.5

原始科学数据 original scientific data

由观测、实验、模拟等手段直接获取的科学数据。

A.1.6

衍生科学数据 derived scientific data

由原始科学数据经二次加工而产生的科学数据。

A.1.7

科学数据生存周期管理 scientific data lifecycle management

面向科学数据生存周期对数据质量、知识产权、数据安全等进行的计划、组织、协调和控制。

A.1.8

科学数据安全风险管理 scientific data security risk management

识别、控制、消除或最小化可能影响科学数据安全的不确定因素的风险评估、风险应对、风险容忍及风险交流等过程。

A.1.9

科技平台 general science and technology(S&T) infrastructure

运用现代信息技术等手段，有效整合科技资源，为科技创新和社会经济发展提供共享服务的网络化、社会化的组织体系。

[来源：GB/T 31075—2014，2.1.1]。

A.1.10

科学数据中心 scientific data center

利用信息、网络等现代技术，对科学数据进行整合汇交、分类分级、加工整理和分析挖掘，保障科学数据安全，推动科学数据开放共享，加强国内外科学数据交流与合作的专业化平台或组织。

A.2 技术类

A.2.1

科学数据安全能力 scientific data security capability

针对科学数据的安全保障，组织在机构建设、制度流程、技术工具以及人员素质等方面所具备的综合条件。

[来源：GB/T 37988—2019，3.5，有修改]

A.2.2

科学数据采集 scientific data acquisition

以明确的目标、规范的流程、合理的工具、标准的格式在科研活动中记录、收集、识别和筛选科学数据的过程。

A.2.3

科学数据收割 scientific data harvesting

对分布式资源库科学数据增量进行批次获取和集中式建库的操作。

A.2.4

科学数据汇交 scientific data archiving

科学数据所有方将各类科学数据按标准的格式和规范的步骤进行汇集和提交，以实现统一管理、共享和利用的过程。

A.2.5

科学数据加工 scientific data processing

对科学数据进行甄选、清洗、挖掘、聚合、关联、演化和推理的过程。

A.2.6

无条件共享 unconditional sharing

科学数据通过互联网或其他方式直接公开发布、不再召回的共享方式。

A.2.7

协议共享 sharing according to agreement

通过协议对科学数据的使用进行约束的共享方式。

A.3 管理类

A.3.1

安全分级 security classification

根据业务信息和系统服务的重要性和受损后的影响，确定实施某种保护的等级。

[来源：GB/T 25069—2022，3.6]

A.3.2

科学数据定制服务 customized service of scientific data

按照用户的特定需求所提供的科学数据服务。

A.3.3

科学数据版本 scientific data version

同一科学数据产品在生存周期中所呈现的不同形态。

A.3.4

数据论文 data paper

对特定在线数据集进行描述、按照一定学术规范出版并可被检索的元数据文件。

A.3.5

数据文件　data file

由数据项、文本或者图像等组成的用于存储数据，并能够在信息系统间交换和处理的单个计算机文件。

A.3.6

科学数据提供方　scientific data provider

按约定和规范生产和提供科学数据的组织机构。

[来源：GB/T 37932—2019，3.2，有修改]

A.3.7

科学数据使用方　scientific data user

按约定和规范接收和使用科学数据的组织机构。

[来源：GB/T 37932—2019，3.3，有修改]

A.3.8

科学数据运营方　scientific data operator

按约定和规范管理和运营科学数据的组织机构。

A.3.9

科学数据承接方　scientific data contractor

在科学数据运营方兼并、重组、破产的情况下，按约定和规范承接科学数据资源的组织机构。

A.3.10

科学数据共享　scientific data sharing

按照给定的管理策略和规则，不同组织之间相互使用科学数据的行为和过程。

A.3.11

科学数据利用　scientific data usage

通过对科学数据的分析、处理和挖掘，提取并发挥科学数据潜在价值的活动。

A.3.12

科学数据在线下载　down loading of on-line scientific data

用户以在线的方式对科学数据进行的下载。

A.3.13

科学数据离线共享　sharing of off-line scientific data

用户以离线的方式对科学数据进行的共享。

A.3.14

科学数据出版　scientific data publishing

组织按照统一规范的质量管理和控制机制，利用互联网及其他方式公开发布其在科研中产生的原始数据，或对原始数据进行收集、整理和再加工形成的数据的活动。

A.3.15

科学数据相关权利　rights related to scientific data

赋予相关主体在科学数据生产、管理、共享、服务活动中的各项权利。

A.3.16

科学数据相关权利界定　rights definition of scientific data

界定科学数据在生产、管理、共享、服务等活动中的各项权利及其权利主体。

参 考 文 献

[1] GB/T 5271.1—2000 信息技术 词汇 第1部分:基本术语

[2] GB/T 25069—2022 信息安全技术 术语

[3] GB/T 29246—2023 信息安全技术 信息安全管理体系 概述和词汇

[4] GB/T 31075—2014 科技平台 通用术语

[5] GB/T 32923—2016 信息技术 安全技术 信息安全治理

[6] GB/T 35273—2020 信息安全技术 个人信息安全规范

[7] GB/T 37373—2019 智能交通 数据安全服务

[8] GB/T 37932—2019 信息安全技术 数据交易服务安全要求

[9] GB/T 37939—2019 信息安全技术 网络存储安全技术要求

[10] GB/T 37973—2019 信息安全技术 大数据安全管理指南

[11] GB/T 37988—2019 信息安全技术 数据安全能力成熟度模型

[12] GB/T 39477—2020 信息安全技术 政务信息共享 数据安全技术要求

[13] GB/T 39725—2020 信息安全技术 健康医疗数据安全指南

[14] T/CIIA 017—2022 科学数据 安全标准体系

[15] T/CIIA 018—2022 科学数据 安全管理指南

[16] T/CIIA 019—2022 科学数据 安全能力成熟度模型

[17] T/CIIA 020—2022 科学数据 安全传输技术要求

[18] T/CIIA 021—2022 科学数据 安全防护技术要求

[19] T/CIIA 024—2022 科学数据 数据安全分级程序

[20] T/CIIA 025—2022 科学数据 数据安全分类质量评价指标

[21] 中华人民共和国数据安全法

[22] 中华人民共和国网络安全法

[23] 中华人民共和国个人信息保护法

[24] 科学数据安全管理办法