ICS 点击此处添加 ICS 号
CCS 点击此处添加 CCS 号

# 团 体 标 准

T/XXX XXXX—XXXX

# 科学数据 数据存储安全管理要求

Scientific data - Security management requirements for storing data

（征求意见稿）

**在提交反馈意见时，请将您知道的相关专利连同支持性文件一并附上。**



- XX - XX 发布 XXXX - XX - XX 实施

中国信息协会 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。

本文件由中国信息协会提出并归口。

本文件起草单位：

本文件主要起草人：

# 引　言

科学数据又称科研数据或研究数据，是我国重要的基础性、战略性资源，对支撑各领域科学基础的研究和应用、推动各领域经济的创新发展、维护国家安全具有重要作用。科学数据存储安全是保障科学数据安全的基石，《科学数据管理办法》明确要求把数据安全放在首要位置，《中华人民共和国数据安全法》对包含数据存储活动相关的数据处理活动进行规范。科学数据存储安全方面的规范还是空白，亟待补充和完善以推动政策法规的落地实施。为了确保科学数据在全生存周期内的合规使用和有效保护，满足科技创新对科学数据的管理需求，亟需构建通用存储安全解决方案，促进提升科学数据管理水平。

本文件旨在为科学数据的存储安全管理提供指导，从安全管理制度、机房安全、网络安全、人员管理安全等方面提出通用安全要求，同时根据存储在介质上的时间和状态特点界定了临时存储、应用服务存储、长期归档阶段并分别提出存储安全要求。通过遵循本文件并采取有效措施，能够防止数据丢失、覆盖、篡改带来的损失，解决现阶段存储安全问题，提高数据安全保障能力。

# 科学数据存储安全管理要求

## 1 范围

本文件规定了科学数据存储安全的分类，通用安全要求，以及面向临时存储、应用服务和长期归档存储安全要求。

本文件适用于科学数据管理机构数据活动的安全管理。

## 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 18894—2016 电子文件归档与电子档案管理规范
GB/T 20271—2006 信息安全技术 信息系统通用安全技术要求
GB/T 30284—2020 信息安全技术 移动通信智能终端操作系统安全技术要求
GB/T 37988—2019 信息安全技术 数据安全能力成熟度模型
GB/T 39786—2021 信息安全技术 信息系统密码应用基本要求
DA/T 31—2017 纸质档案数字化规范
DA/T 74—2019 电子档案存储用可录类蓝光光盘(BDGR) 技术要求和应用规范

## 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

人类社会科技活动积累的或通过其他方式获取的反映客观世界的本质、特征、变化规律等原始性、基础性数据,以及根据不同科技活动需要进行系统加工整理的各类数据的集合。

注：主要包括在自然科学、工程技术科学等领域，通过基础研究、应用研究、试验开发等产生的数据，以及通过观测监测、考察调查、检验检测等方式取得并用于科学研究活动的原始数据及其衍生数据。

[来源：GB/T 31075—2014，2.2.7，有修改]

3.2

**数据安全** data security

通过管理和技术措施，确保数据有效保护和合规使用的状态，以及具备保障持续安全状态的能力。

[来源：GB/T 37988—2019，3.1，有修改]

3.3

**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]

3.4

**重要数据** important data

我国机构和个人收集、产生的，不涉及国家秘密，一旦遭到篡改、破坏、泄露或者非法获取、非法利用，可能危害国家安全、公共利益的数据。

[来源：GB/T 35274—2017，3.13，有修改]

## 4 科学数据存储安全的分类

根据存储在介质上的时间和状态特点，将科学数据存储安全划分为临时存储的数据存储、应用服务的数据存储和长期归档的数据存储安全阶段。

a) 临时存储的数据存储是指通过传感器、实验室仪器、测量设备、日志文件、调查记录等来源获取数据时，数据在采集终端或临时存储介质上的一种保存状态；
b) 应用服务的数据存储是指数据处于的能为应用端提供访问的保存状态；
c) 长期归档的数据存储是指数据处于归档的保存状态。

## 5 科学数据存储安全框架

针对科学数据存储安全的三个阶段，分别提出科学数据存储安全要求。科学数据存储安全框架见图1。

a) 通用安全要求包括安全管理制度、机房安全、网络安全和人员管理安全要求，见第6章；
b) 临时存储安全要求包括临时存储安全管理制度、采集设备安全和临时存储系统安全等要求，见第7章；
c) 应用服务存储安全要求包括安全管理策略、系统安全、网络安全、人员管理安全等要求，见第8章；
d) 长期归档数据存储安全要求包括长期归档操作规范、归档介质安全、人员管理安全等要求，见第9章。

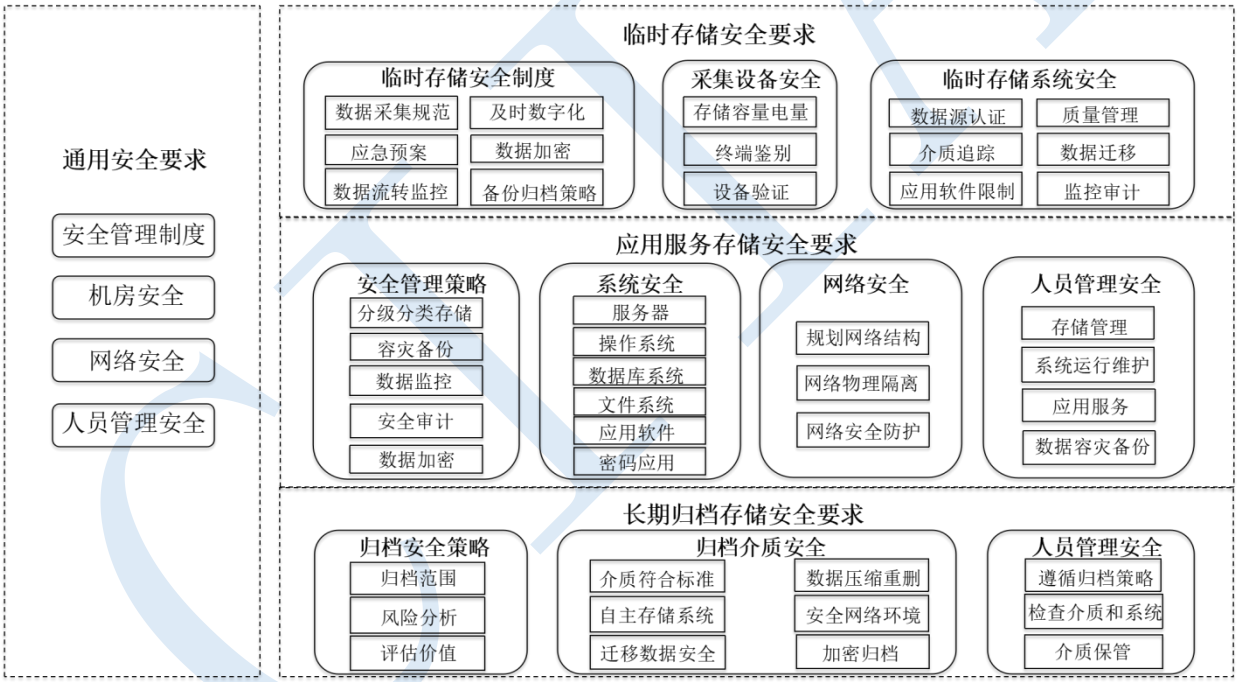


图1 科学数据存储安全框架

## 6 通用安全要求

### 6.1 安全管理制度

6.1.1 应规范数据存储安全管理活动，根据数据安全等级制定数据存储安全管理制度；应规范管理人员、操作人员的日常管理操作；应形成由安全管理政策、管理办法和细则构成的安全管理制度体系。
6.1.2 应对安全管理制度进行评审，根据征求意见进行修改，并发布实施。
6.1.3 应定期开展安全管理制度相关培训和宣贯。
6.1.4 应参考行业最佳实践，根据实施情况持续修订。

### 6.2 机房安全

6.2.1 机房场地安全应符合 GB/T 20271—2006 中 4.1.1.1 的要求，保障机房有良好的运行环境和工作环境，保障数据库服务器、数据库所在环境、网络设备的物理安全，确保存储数据的安全。建筑物结构的耐火等级应符合 GB/T 9361—2011 第 6 章的规定，火灾报警及消防设施应符合 GB/T 9361—2011 第 10 章的规定，应设置防盗报警器。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。

6.2.2 设备安全应符合 GB/T 20271—2006 中 4.1.2.2 的要求，应能提供基本运行支持，满足安全可用和不间断运行需求。定期进行设备的全面检查并及时更换，定期进行例行维护、巡检和处置废弃设备。

6.2.3 存储介质性能监控应符合 GB/T 37988—2019 中 8.1.2.3 的 b)和 c)的要求，设置超过安全阈值的预警，对所有设备的访问和使用行为记录并审计。对存储重要数据的介质应增强对其访问的控制。

6.2.4 应制定针对机房意外事件和环境条件和工作条件变化风险的规避措施，如自然灾害、人为破坏、工作失误、设备故障、盗抢事件、介质失效、电磁传导和辐射干扰等。

6.2.5 应制定机房突发事件应急处置安全预案，对各类安全事件进行及时响应和处置，降低损失。完善应急技术队伍建设和物资保障。

### 6.3 网络安全

6.3.1 应实行网络设备安全措施，包括但不限于设备接入安全认证、设备安全管理、设备链路冗余、网络设备处理能力保证、漏洞扫描、设备安全加固。

6.3.2 应保障网络通道安全，实行网络访问控制措施。

6.3.3 采用网络传输安全机制，确保传输过程中数据完整性和保密性：

a) 应明确传输范围、频次和有效期，使用传输安全协议、经过安全认证或访问控制机制的接口和安全传输通道，定期评估传输的安全性，防止数据窃取和数据篡改；
b) 应建立数据加密保护和签名机制，使用加密传输协议；
c) 应开展数据传输过程的质量验证工作，校验传输数据的完整性。

### 6.4 人员管理安全

6.4.1 应制定人员安全管理规范，各类人员应遵循相关规章制度。包括但不限于：

a) 授权和审批制度；
b) 待离岗人员交接制度；
c) 相互检查和监督的人员安全管理制度；
d) 人员考勤管理制度。

6.4.2 人员分工负责，有效配合，岗位设置和职责应包括但不限于：

a) 总体负责岗：负责统筹数据管理、应用服务及运行维护工作，负责人才队伍的建设和培养；
b) 数据存储管理岗：负责数据通信交换、数据生产和数据存储管理业务的运行与维护；
c) 应用服务岗：负责应用服务业务的运行维护，服务和应用的巡检；
d) 运行维护岗：负责维护物理环境及运行环境的稳定运行。

6.4.3 应加强人员技术储备，同时定期进行安全意识教育和培训考核，提高安全能力水平。

## 7 临时存储安全要求

### 7.1 临时存储安全制度

7.1.1 应制定数据采集原则，明确数据源、数据采集范围和频度、临时存储的数据格式。

7.1.2 应采取应急活动响应措施，建立应急预案管理机制和安全事件处置机制，保存故障日志，防止软件故障、硬件故障、网站故障与攻击等不可预料的未知故障的发生。

7.1.3 应及时将纸质文件数字化，保证数据完整性和保密性。

7.1.4 应制定存储和备份策略，根据安全级别要求，定期将临时存储的数据备份和归档，对数据流转过程进行监控与审计。定期对数据的有效性和可用性进行检查。

7.1.5 应同时存储元数据（包含辅助数据）和原始数据，通过加密、过滤等技术存储重要数据。

### 7.2 采集设备安全

7.2.1 存储电子数据时应确保采集终端的存储容量和蓄电量，避免数据被覆盖和未及时保存导致的数据丢失。
7.2.2 应采取终端鉴别措施，存储安全级别高的数据应结合口令密码、设备指纹、物理位置等方式验证数据采集设备，具体要求应符合 GB/T 30284—2020 中 4.1 和 4.2 的要求。

### 7.3 临时存储系统安全

7.3.1 应采用数据源认证技术保障来源真实，对数据进行质量管理，实现采集过程可追溯，如采集数据与存储数据的一致性校验，通过监控采集、建立采集日志并定期对用户行为审计。
7.3.2 应采用身份识别、介质追踪和访问控制机制。对用户、应用和进程进行唯一标识。
7.3.3 应执行应用软件限制策略，数据交换应进行严格的权限审批。
7.3.4 应提供密码支持，对安全级别高的数据应进行加密技术保护。
7.3.5 应具备数据整体迁移功能，并具备迁移数据完整性检测的能力。

## 8 应用服务存储安全要求

### 8.1 安全管理制度

8.1.1 应采用分级分类数据存储架构，采取在线存储、近线存储或离线存储方式，定期评估存储数据安全级别和风险，及时调整存储策略。
8.1.2 制定数据容灾备份的操作规范，应执行数据备份和恢复策略，保障存储数据的安全。
8.1.3 应实施重要数据数据加密、脱敏和密文处理的安全保护措施，恢复原始数据时应经过严格的审批。
8.1.4 建立数据监控制度，应监控存储系统日志、收集接口的日志记录，监测端口安全。
8.1.5 应确保存储数据的质量，留存值班人员记录表，形成存储业务操作场景、策略的文档。应建立完整的技术文档和维护方案，建立审计制度，定期审计。

### 8.2 系统安全

#### 8.2.1 服务器安全

服务器安全应符合下列要求：

a) 服务器配置满足基本要求，包括但不限于实现内外网分离、用户账户管理、注册表安全配置、服务管理、文件及目录控制功能；
b) 设立安全风险协议，更新服务器补丁，保护服务器及数据安全。

#### 8.2.2 操作系统安全

操作系统安全应符合下列要求：

a) 包括但不限于丢失保护、密码支持、用户数据保护、标识和鉴别、安全管理、数据加密、安全审计、残留信息清除、会话管理和资源限制功能实现；
b) 应启用访问控制、漏洞扫描、防火墙防御、安装入侵检测和入侵防御系统、安装杀毒软件、及时更新补丁、数据备份和安全加固。

#### 8.2.3 数据库管理系统和文件系统安全

数据库管理系统和文件系统安全应符合下列要求：

a) 应具备冗余能力，存储架构可伸缩。包括但不限于访问控制、漏洞扫描、安全审计和更新补丁等。支持用户权限设置、用户配额、目录配额等设置，支持对目录设置宽限期和保护期，阻止用户越权操作；
b) 应制定数据加密和安全查询方案，防止数据被窃取和篡改，并支持密文存储状态下的安全查询。对加密密钥集中化与分发管理，将密钥与存储数据分离保存，加强密钥的产生、获取、存储、备份、恢复等全生命周期管理，并加入密钥访问时间、访问用户等策略配置的日志记录，提高密钥安全性；
c) 应支持双活等灾备方案，支持多种快照的数据恢复方式；

d) 应实施纠删、副本，以及强一致性、弱一致性等多种数据保护机制。

#### 8.2.4 应用软件安全

应用软件安全应符合下列要求：

a) 能及时获得授权和更新；
b) 支持数据访问控制、身份鉴别、安全审计、剩余信息保护、通信完整性和保密性、抗抵赖、软件容错、资源控制和数据流控制等功能。

#### 8.2.5 密码应用安全

密码应用安全应符合下列要求：

a) 信息系统密码通用要求符合 GB/T 39786—2021 第 5 章的要求；
b) 物理和环境安全、网络和通信安全、设备和计算安全以及应用和数据安全的密码应用基本要求应符合 GB/T 39786 的相关要求。

### 8.3 网络安全

8.3.1 应规划网络结构，承载不同业务或职责的网络应相互独立，数据、业务、管理三隔离，实现数据安全防护。

8.3.2 网络结构应从逻辑上对虚拟机和服务器的数据访问相互隔离。

8.3.3 应加强网络安全保障，实现网络物理隔离，核心网络应建立防火墙、采取入侵检测等安全措施。

8.3.4 应建立访问控制、身份认证、数据加密、反爬虫机制、攻击防护和流量监控等网络安全的防护措施。

8.3.5 应合理分配网络资源，监控网络运行情况，制定网络安全紧急预案。

### 8.4 人员管理安全

8.4.1 存储管理人员应按规定的时间、手段、方法、步骤检查存储设备的工作情况、安全日志、安全补丁及反病毒升级包的更新，按照规范（系统安装规范、系统管理规范、数据备份规范等）操作，明确检查的详细内容、手段、方法、步骤、时间等。

8.4.2 系统维护人员应对日常行为的日志定期审查。加强口令的安全管理，定期更换管理密码。应对数据库系统的配置参数及相关文件进行备份，当配置发生变更时，应重新备份，以便系统故障时能尽快恢复系统配置。对系统运行状况进行实时或定期监控，例行维护管理并定期评估总结。

8.4.3 应用服务人员应配额管理存储资源，保障业务数据及元数据的备份安全。应事先预估及计算存储空间，合理规划存储数据的位置，便于查找、应用和管理。应定期开展安全检查评估、检测磁盘空间、数据更新。

8.4.4 数据容灾备份人员应遵循相关管理制度，定期备份和恢复数据，进行风险评估，进行本地、异地、异质备份，检测磁盘空间。应检查数据存储、备份与容灾的数据量和业务要求的符合性，对发现的问题按工作流程与故障预案进行通知、报备并及时处理。

## 9 长期归档存储安全要求

### 9.1 归档安全策略

9.1.1 应基于安全的网络环境或专用离线存储介质，根据不同等级实行在线归档或离线归档策略；

9.1.2 应符合 GB/T 18894—2016 第 6 章的要求归档，通过电子档案管理系统客户端或归档接口完成电子文件及纸质档案的归档。包括不限于：原始数据、过程数据、加工的产品级数据、相关辅助数据和元数据进行归档。

9.1.3 应建立归档数据的备份机制，安全级别高的数据异质、异地容灾备份。

9.1.4 应定期开展归档数据存储安全的风险分析活动，制定风险预防方案和容错机制、不断调整并监督实施。

9.1.5 应定期评估数据的保存价值，调整归档策略。

## 9.2 归档介质安全

9.2.1 归档存储介质应符合通用标准，采用不可更改的存储介质，避免存储数据被修改或删除；

9.2.2 电子档案管理系统应保障归档数据的系统性、真实性、完整性和有效性，并应符合 GB/T 18894—2016 第 5 章的要求：

a) 支撑电子档案管理系统运行的网络应与网络物理隔离，联网设备之间的数据传输应通过一次性写入或满足物理隔离要求的数据交换设备实施；

b) 应采用通用和兼容的存储技术及自主可控的存储系统，以规避技术设备升级、迭代、停产带来的不可控风险；

c) 应能满足不同级别的响应要求，实现数据压缩、重删和数据迁移。

## 9.3 人员管理安全

9.3.1 应明确负责长期归档的人员的职责，按照 DA/T 31—2017 的 5.1 要求执行，保证数据资源质量和需要迁移的数据安全传输和存储。

9.3.2 介质保管应符合要求，如避免擦、划、触摸记录介质涂层。定期对长期归档设备及运行环境进行检查和维护，如归档设备的静默数据检验。

9.3.3 应定期对存储软件和数据格式进行检查并更新，定期备份、检查和报告归档数据的状态，应符合 DA/T 74—2019 的要求，适时迁移，并做好迁移记录。

9.3.4 应确保需要删除的数据不可恢复。

# 参 考 文 献

[1] GB/T 25069—2022 信息安全技术 术语
[2] GB/T 31075—2014 科技平台 通用术语
[3] GB/T 35274—2017 信息安全技术 大数据服务安全能力要求
[4] GB/T 37973—2019 信息安全技术 大数据安全管理指南