ICS 35.03
CCS L80

T/STRSA

团 体 标 准

T/STRSA 002—2023

空间科学数据汇交安全管理规范

specification for space science data submission security management

2024-02-01 发布　　2024-02-01 实施

中关村国基条件科技资源共享服务创新联盟　　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。

本文件由中国科学院国家空间科学中心提出。

本文件由中关村国基条件科技资源共享服务创新联盟归口。

本文件起草单位：中国科学院国家空间科学中心、中国科学院高能物理研究所、中国科学院计算机网络信息中心、中国科学院国家天文台、北京中科行远科技有限公司、中科星图维天信（北京）科技有限公司、北京开运联合信息技术集团股份有限公司、中国标准化研究院。

本文件主要起草人：许琦、佟继周、胡晓彦、贾博、张红梅、王爽、陈昕、刘宁、陶一寒、王有芬、熊森林、冯德财、陈昌硕、亢瑞卿、李达、王志强、杨青海、徐凯程。

空间科学数据汇交安全管理规范

1 范围

本文件规定了空间科学数据汇交安全管理框架、基本原则与管理要求。

本文件适用于空间科学数据管理机构、科研机构或行业相关机构对空间科学数据汇交安全管理。包括但不限于空间物理与空间环境、空间天文、月球与行星科学、空间地球科学及其他交叉学科领域的科学数据汇交安全管理工作。

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 22239 信息安全技术 网络安全等级保护基本要求
GB/T 30523 科技平台 资源核心元数据
GB/T 32843 科技资源标识
GB/T 33132 信息安全技术 信息安全风险处理实施指南
GB/T 35273 信息安全技术 个人信息安全规范
GB/T 36626 信息安全技术 信息系统安全运维管理指南
GB/T 39908 科技计划形成的科学数据汇交 通用代码集
GB/T 39909 科技计划形成的科学数据汇交 通用数据元
GB/T 39912 科技计划项目形成的科学数据汇交 技术与管理规范
T/CIIA 031-2022 空间环境科学数据安全分级指南

3 术语和定义

下列术语和定义适用于本文件。

3.1

空间科学 space science

以航天、航空飞行器以及地面工作平台，研究发生在地球、日地空间、太阳系乃至整个宇宙的物理、化学及生命等自然现象及其规律的学科。

注：主要领域为空间物理学、空间天文学、月球和行星科学、空间地球科学、空间生命科学和微重力科学等。

［来源：GB/T 30114.1-2013 5.3］

3.2

空间科学数据 space science data

通过航天、航空飞行器以及地面工作平台进行科学探测、以及通过试验检验、仿真模拟、融合同化等方式取得并用于空间科学领域科学研究活动的原始数据及其衍生数据。

3.3

数据安全 data security

是指通过采取必要措施，确保数据处于有效保护和合法利用的状态，以及具备保障持续安全状态的能力。

［来源：中华人民共和国数据安全法 第一章 第三条］

3.4

真实性 authenticity

指信息和数据与真实情况的接近程度。

［来源：GB/T 25069—2022, 3.345 有修改］

3.5

完整性 integrity

没有遭受以未授权方式所作的更改或破坏的特性。

［来源：T/CIIA 031-2022 3.8]

3.6

可获取性 availability

可由经授权实体按需访问和使用的性质

［来源： T/CIIA 031-2022 3.7］

3.7

保密性 confidentiality

指信息对未授权个人、实体或过程不可用或不可泄漏的特性。

［来源：GB/T 25069—2022,3.41 有修改］

3.8

科学数据提交方 submitting organization of scientific data

按规定程序和要求向科学数据管理方提交数据的组织。

［来源：GB/T 39912—2021,3.4］

3.9

科学数据管理方 scientific data management organization

利用信息、网络等现代技术，对科学数据进行搜集、加工、汇交、整合、安全存储和管理，并向用户提供科学数据开放共享服务的专业机构。

［来源：GB/T 39912—2021,3.5]

4 概述

4.1 安全管理框架

空间科学数据汇交过程根据GB/T 39912中的有关要求，包括科学数据汇交计划制定、科学数据制备、科学数据提交、科学数据审核与编目、出具数据汇交凭证等过程。空间科学数据汇交安全管理应遵守空间科学数据汇交安全管理框架（见图1），遵循空间科学数据汇交安全管理基本原则，以分级保护为基础，针对不同安全级别的数据，明确在数据采集加工整理、数据传输、数据编目标识与临时存储与综合保障等方面的安全管理要求，防止汇交过程中可能存在数据泄露、伪造、篡改、窃取、丢失、传输中断等风险，全面加强对汇交数据的安全保护能力。

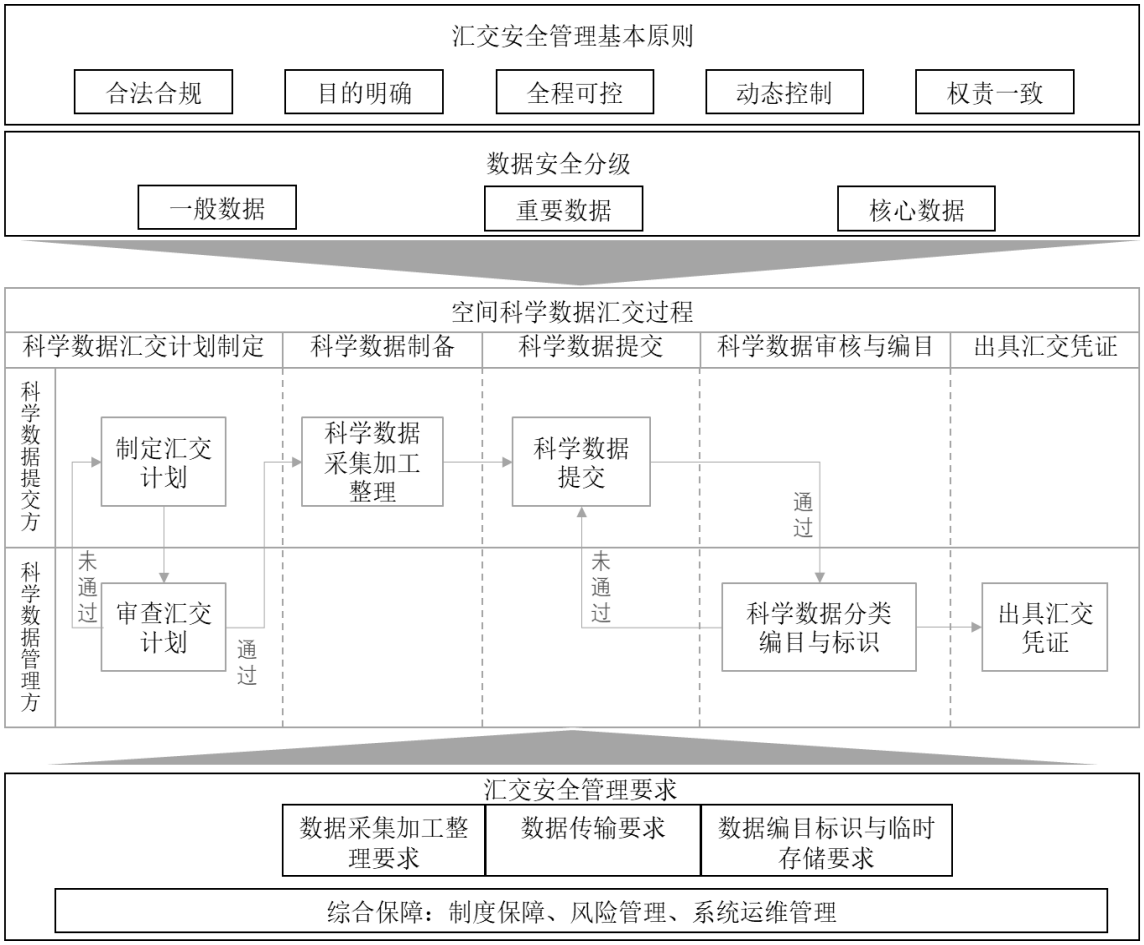

图 1 空间科学数据汇交安全管理框架

4.2 分级保护

空间科学数据按照国家及和行业主管部门的有关要求，安全级别由高到低划分为核心数据、重要数据和一般数据。

空间环境科学数据宜按照T/CIIA 031-2022相关要求，安全级别由高到低划分为5级、4级、3级、2级、1级。4级数据执行本文中重要数据安全管理要求，5级数据执行核心数据安全管理要求。

核心数据的保护应按照国家及行业主管部门的有关要求执行。

空间科学数据汇交过程中如有涉及个人信息的数据，除满足本文件要求外，还应该按照GB/T 35273相关要求执行。

5 基本原则

空间科学数据汇交安全管理应遵循基本原则如下：

a) 合法合规性原则。应遵守国家法律法规及科学数据管理责任主体的有关规定；
b) 目的明确原则。应制定空间科学数据安全防护策略，明确空间科学数据安全防护目标和要求；
c) 全程可控原则。应采取与空间科学数据安全级别相匹配的安全管理措施，确保空间科学数据汇交过程的保密性、完整性和可获取性，避免汇交过程中数据被未授权访问、破坏、篡改、泄漏或丢失等；
d) 动态控制原则。空间科学数据的安全管理措施不应是一次性和静态的，应可基于业务需求、安全环境属性、系统用户行为等因素实施实时和动态调整；
e) 权责一致原则。应明确落实空间科学汇交数据机构的数据安全管理人员与职责，保证有关部门及人员应积极落实相关措施，履行数据安全防护职责。

6 汇交安全管理

6.1 数据采集加工整理

数据采集加工整理是应进行规范化的科学数据实体采集与处理，按照GB/T 30524、GB/T 39909、GB/T 39908等相关要求形成科学数据的元数据，并应覆盖数据来源、数据处理方法、数据质量控制等方面的说明文档。数据采集加工整理过程存在数据泄露、数据源伪造、数据篡改等安全风险。数据采集加工整理安全管理要求如下：

a） 应明确数据源、数据采集范围和频度，数据处理方法、数据质量控制措施，针对重要数据、核心数据应开展数据安全影响评估；

注：数据安全影响评估：针对数据处理活动，检验其合法合规程度，判断其对相关方合法权益造成损害的各种风险，以及评估相关保护措施有效性的过程；

b） 应明确数据采集加工整理过程中重要数据、核心数据的知悉范围和安全管控措施，确保采集数据的完整性和真实性。；

c） 通过系统批量采集加工整理的数据应采用摘要、消息认证码、数字签名等密码技术确保采集过程数据的完整性；

d） 应对人工批量采集加工整理数据的环境进行安全管控，并通过人员权限管控、信息碎片化等方式，防 止采集过程出现数据泄露；

e） 应对数据采集加工整理进行日志记录，并采取技术措施确保信息来源的可追溯性；

f） 针对重要数据的采集加工整理过程中对数据进行加密，用于采集加工处理该类数据的设备或系统及其网络安全建设、监督管理应满足GB/T 22239中的网络安全等级保护3级要求；

g） 针对核心数据的采集加工整理过程中对数据进行加密，用于采集加工处理该类数据的设备或系统及其网络安全建设、监督管理应满足 GB/T 22239 中的网络安全等级保护 4 级要求。

6.2 数据传输

数据传输是科学数据提交方按照科学数据汇交计划的要求通过线上传输或线下传输等方式提交到科学数据管理方。数据传输包括线上传输和线下传输方式，线上传输包括客户端传输、FTP传输和VPN传输等。线下传输包括物理介质现场拷贝。数据传输安全管理要求如下：

a） 线上传输时采取措施加强数据传输过程中的网络和数据安全，满足以下基本要求：

1） 应加强软件开发安全管理，保障数据传输工具的安全性，工具上线前应开展必要的渗透测试、支持库漏洞查找等工作，以防止工具使用过程中遭受恶意破坏、篡改、信息窃取等攻击；

2） 应采用防火墙、入侵检测等安全技术或设备，确保数据传输的安全性；

3） 终端应采取准入控制、终端鉴别等技术措施，防止非法或未授权终端接入传输网络；

4） 应对通信双方进行身份认证，确保数据传输双方是可信任的；

5） 应采用数字签名、时间戳等方式，确保数据传输的抗抵赖性；

6） 应采用密码技术或非密码技术等方式，确保数据的完整性；

7） 重要数据和核心数据的传输应事先经过审批授权采取数据加密措施，应明确传输通道加密、数据内容加密、签名验签、身份鉴别、数据传输接口安全管理方式与要求，应明确对数据传输安全策略的变更进行审核的技术方案；

8） 用于传输重要数据的系统及其网络安全建设、监督管理应满足GB/T 22239中的网络安全等级保护3级要求；

9） 用于传输核心数据的系统及其网络安全建设、监督管理应满足GB/T 22239中的网络安全等级保护4级要求；

10） 应在数据传输完成后进行校验，以保证数据的一致性；

11） 应在数据传输不完整时清除传输缓存数据；

12） 应在数据传输完成后立即清除传输历史缓存数据；

13） 应定期检查或评估数据传输通道的安全性和可靠性。

b） 线下通过物理介质传输重要数据和核心数据时应对数据进行加密或脱敏，并由专人负责收发、登记、编号、传递、保管和销毁等，传输过程中可采用密封、双人押送、视频监控等方式确保物理

介质安全到位，传递过程中物理介质不应离开相关责任人、监控设备等的监视及控制范围，且不应在无人监管情况下通过第三方进行传递，国家及行业主管部门另有规定的除外。

6.3 数据标识编目与临时存储

数据标识编目与临时存储是科学数据管理方在接收科学数据后，应按照一定规范对科学数据进行分类、编目、标识操作以及临时存储。数据标识编目与临时存储管理要求如下：

a) 分类宜按照学科领域特点划分为空间物理与空间环境、空间天文、月球与行星科学、空间工程与应用、交叉学科及其他等五大类，可依据探测方式、探测对象或区域在大类下进一步划分；
b) 编目应按照一定的规范将数据实体、数据标签、元数据、索引、说明文档信息进行组织与关联，并按一定的规范将数据文件、数据集、数据集合和数据卷进行组织；
c) 数据标识注册应符合GB/T 32843的有关要求；
d) 临时存储一般数据时采取一定措施确保数据临时存储的完整性；
e) 临时存储重要数据和核心数据时，应采取加密、权限控制等技术措施保证数据临时存储的保密性；
f) 临时存储重要数据的信息系统，其网络安全建设及监督管理宜满足网络安全等级保护3级要求；
g) 临时存储核心数据的信息系统，其网络安全建设及监督管理宜满足网络安全等级保护4级要求；
h) 文件系统中存放含有重要数据和核心数据的文件，宜采用整个文件加密存储方式进行保护；
i) 重要数据及核心数据的临时存储应使用密码算法加密存储；
j) 应制定数据临时存储介质销毁操作规程，明确数据临时存储介质销毁场景、销毁技术措施，以及销毁过程的安全管理要求，并对已共享或者已被机构内部部门使用的数据提出有针对性的数据存储介质销毁管控规程；
k) 一般数据的临时存储介质如还需继续使用，应采用删除索引、删除文件系统的方式进行数据销毁，并进行进行数据的尝试恢复及检查，验证数据销毁结果，确保介质中的数据不可再被恢复或者以其他形式被利用；
l) 重要数据和核心数据的临时存储介质不应移作他用，销毁时应采用物理销毁的方式对其进行处理，如消磁或磁介质、粉碎、融化等。；
m) 重要数据和核心数据的临时存储介质的销毁应参照国家及行业涉密载体管理有关规定，由具备相应资质的机构或数据销毁部门进行专门处理，并由科学数据管理方相应人员对其进行全程监督。

6.4 综合保障

在汇交过程中，制度保障、风险管理和系统运维等综合保障安全管理要求如下：

a) 制度保障。为了保证空间科学数据安全，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：
   1) 数据安全管理制度；
   2) 数据存储介质管理制度；
   3) 数据管理人员安全培训、考核制度；
   4) 数据管理部门安全职责范围的规定；
   5) 数据管理人员安全职责范围的规定；
   6) 数据安全应急预案、恢复措施的规定。
b) 风险管理。在空间科学数据汇交过程中，科学数据提交方和管理方应依据有关信息安全管理制度、标准和规范同时按 GB/T 33132 规定，对其面临的信息安全风险进行管理。
c) 系统运维管理。用于接收汇交数据与临时存储的系统运维应符合 GB/T 36626 的要求。

参 考 文 献

[1] 中华人民共和国数据安全法
[2] 中华人民共和国网络安全法
[3] 中华人民共和国个人信息保护法
[4] 科学数据管理办法
[5] GB/T 25069—2022 信息安全技术 术语
[6] GB/T 30114.1-2013 空间科学及其应用术语 第1部分：基础通用
[7] GB/T 37025-2018 信息安全技术 物联网数据传输安全技术要求
[8] GB-T 37973-2019 信息安全技术 大数据安全管理指南
[9] GB/T 37988-2019 信息安全技术 数据安全能力成熟度模型
[10] GB/T 39912-2021 科技计划形成的科学数据汇交 技术与管理规范
[11] JR/T 0223—2021金融数据安全 数据生命周期安全规范