ICS 35.03
CCS L80

T/STRSA

团 体 标 准

T/STRSA 001—2023

空间科学数据安全存储规范

Specification for security storage of space science data

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、华为技术有限公司、曙光信息产业（北京）有限公司、北京中科行远科技有限公司、中国科学院计算机网络信息中心、中国科学院高能物理研究所、中国科学院国家天文台、北京开运联合信息技术集团股份有限公司、中科星图维天信（北京）科技有限公司、中国标准化研究院。

本文件主要起草人：刘宇、李晓翠、许琦、佟继周、王明轩、吕磊、罗宾、郭洪星、李晓楠、闫振中、张埕钢、黎超、张红梅、王爽、陶一寒、王有芬、陈昕、刘宁、冯德财、陈昌硕、亢瑞卿、李达、王志强、杨青海、徐凯程。

空间科学数据安全存储规范

1 范围

本文件规定了空间科学数据安全存储原则、要素与等级要求。

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安全存储管理和保护。

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 22239-2019 信息安全技术 网络安全等级保护基本要求

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 术语和定义

3.1.1

空间科学 space science

以航天、航空飞行器以及地面工作为主要平台，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]

3.1.2

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衍生数据。

3.1.3

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]

3.2 略缩语

下列略缩语适用于本文件。

CIS：互联网安全中心（Center for Internet Security）

RAID：独立磁盘冗余阵列（Redundant Array of Independent Disks）

SSH：安全外壳协议（Secure Shell）

CMS：内容管理系统（Content Management System）

WORM：一写多读（Write Once Read Many）

4 空间科学数据安全存储原则

4.1 准确性

准确性是信息和数据与真实情况的接近程度。应保证空间科学数据真实、准确，信息的表述不会引起歧义，能够反映信息的真实状态，不得有虚假记载或误导性陈述。

4.2 完整性

完整性是信息在存储和传输的过程中，不被非法授权修改、破坏、插入、延迟、乱序和丢失的特性。应保证空间科学数据信息完整，没有重大遗漏或信息歪曲失真的情况发生。

4.3 可用性

可用性是授权实体在需要时可有效访问和可利用的属性。应保证提供空间科学数据信息服务的网络、信息系统随时可用，使合法授权的用户可以及时获取所需的数据信息。

4.4 时效性

时效性是信息仅在一定时间段内对决策具有价值的属性。应保证空间科学数据及时提供和更新。

4.5 可信性

可信性是提供确实可信任服务的属性。应保证提供的空间科学数据来源明确，数据信息加工处理经过审核确认。

4.6 合规性

合规性是符合并遵守法律、政策、规章、程序及合同的能力。应在采集、加工、处理和提供数据信息时不违反知识产权、著作权等法律法规要求。

4.7 保密性

保密性是空间科学数据信息对未授权个人、实体或过程不可用或不可泄漏的特性。应通过完备的信息安全体系，保证未授权者无法使用信息，在信息使用和传输过程中不会被非法泄漏而扩散。

4.8 可控性

可控性是信息的传播及内容具有控制能力的特性。应掌握、控制信息的流向和使用范围等，以便国家相关监管部门审查。

5 空间科学数据安全存储要素

空间科学数据安全存储要素包括：数据安全、系统安全及管理安全。

5.1 数据安全

数据安全要素包括：数据完整性、数据保密性、数据可用性、数据访问控制。

5.2 系统安全

系统安全要素包括：系统可靠性、设备状态监控、软件安全、系统完整性保护、系统加固、程序行为安全、软件供应链安全、信息安全等级保护。

5.3 管理安全

管理安全要素包括：认证鉴权、证书管理、密钥管理、安全审计、安全事件应急。

6 空间科学数据安全存储等级

空间科学数据安全存储共分为3个等级,见表1。

表1 空间科学数据安全存储等级说明

	等级说明
等级1	数据存储需具备基本安全功能，包括数据安全要素、系统安全要素及管理安全要素。
等级2	与等级1相比，增强了数据安全中数据完整性、数据保密性、数据可用性及数据访问控制要求，增强了系统安全中系统可靠性、系统加固及信息安全等级保护要求，增强了管理安全中认证鉴权、证书管理、密钥管理、安全审计及安全应急事件要求。
等级3	与等级2相比，增强了数据安全中数据完整性、数据保密性、数据可用性要求，增强了系统安全中系统完整性保护、系统加固、软件供应链管理及信息安全等级保护要求，增强了管理安全中认证鉴权、证书管理、密钥管理、安全审计及安全应急事件要求。

7 空间科学数据安全存储等级1

7.1 数据安全

7.1.1 数据完整性

应支持空间科学数据存储过程中的数据完整性检测功能，并针对检测出的错误提供必要的恢复措施。

7.1.2 数据保密性

应支持对空间科学数据保密性进行保护，并针对关键数据采用非明文存储，包含以下要求：

a) 敏感信息不得使用明文存储在本地，且需加密保护；
b) 不在日志、错误信息、调试信息中暴露口令、密钥等敏感信息。

7.1.3 数据可用性

7.1.3.1.1 备份与恢复

应支持数据备份与恢复的功能，包含以下要求：

a) 对数据进行手动备份；
b) 对数据进行全备份；
c) 对数据进行异步备份；
d) 对数据进行本地备份；
e) 卷镜像的方式提供数据的备份与恢复功能；
f) 快照的方式提供数据的备份与恢复功能。

7.1.3.1.2 防病毒

应支持防病毒软件扫描，防止文件被病毒感染。

7.1.3.1.3 数据冗余

应支持通过技术手段保障存储数据的可靠性，如配置RAID。

7.1.4 数据访问控制

应支持策略控制下的访问控制功能，包含以下要求：

a）访问策略范围应包括与资源访问相关的主体、客体及他们之间的操作；
b）对访问的内容、操作权限应不超出预定范围，保障最小特权原则；

c） 支持业务面和管理面无法相互访问；
d） 支持对访问控制的策略配置。

7.2 系统安全

7.2.1 系统可靠性

应支持管理模块冗余、电源模块冗余、控制模块冗余，并提供容错和故障恢复功能。

7.2.2 设备状态监控

应支持设备状态自动检测功能，至少可检测硬件故障、网络中断、网络连接错误、业务异常等内容，并采取告警措施。

7.2.3 软件安全

应保证系统软件及软件运行环境不存在高风险级别漏洞。

7.2.4 系统加固

应支持系统加固功能，包含以下要求：
a） 应遵从业界配置加固规范，如CIS；
b） 应支持最小化裁剪，裁撤不必要的组件和服务。

7.2.5 程序行为安全

应持程序行为安全功能，包含以下要求：
a） 应支持关键文件入侵检测，设置入侵检测前检查功能，避免文件被篡改；
b） 应支持异常行为检测，支持Rootkit入侵检测功能；
c） 应支持进程及网络入侵检测，设置周期性非法接入检测功能和关键进程看护功能。

7.2.6 软件供应链安全

存储厂商应对使用的第三方开源软件进行生命周期管理：如漏洞管理、应急响应、版本升级等。

7.3 管理安全

7.3.1 认证鉴权

7.3.1.1.1 身份标识管理

应支持对用户的标识功能，并保障每个用户拥有唯一的身份标识。

7.3.2 账号安全管理

应支持账号管理功能，包含以下要求：
a） 系统中的账号具有唯一性；
b） 所有账号都可被系统管理；
c） 账号的授权应基于最小特权原则；
d） 系统账号不能修改自身权限。

7.3.2.1 鉴别机制管理

应支持身份鉴别功能，包含以下要求：
a） 在用户对数据存储进行操作之前，先对该用户进行鉴别；
a） 应在服务端进行鉴别处理，并遵循先鉴别，再执行的原则。

7.3.2.2 口令安全管理

应支持口令检测功能，包含以下要求：
a） 提供口令复杂度检测功能，若设置口令不符合复杂度要求，系统不准许设置成功并给出合理的提示；

b） 口令复杂度满足长度至少6个字符、包含至少两种字符组合、口令不可与账号相同；
c） 不得使用缺省口令；
d） 不应存在用户无法修改的口令，对于出厂时缺省设置的账号、口令或用于传输的加密密钥应提供修改机制，提醒用户修改及定期更新，并提示风险，口令应保障至少每6个月更换一次；
e） 提供的口令输入框不支持口令复制与粘贴功能；
f） 操作界面中的口令不得明文显示；
g） 密码口令文件应设置访问权限，管理用户不可读取或拷贝加密的内容；
h） 用户修改自己口令时应验证旧口令。

7.3.3 登录身份鉴别

应支持登录身份鉴别功能，包含以下要求：
a） 管理接口应提供接入鉴别机制，所有可对系统进行管理的人机接口以及跨信任网络的机机接口应有安全的接入鉴别机制，标准协议没有鉴别机制的除外；
b） 设备外部可见的可对系统进行调试或管理的物理接口应有接入鉴别机制；
c） 对于人机接口或跨信任网络的机机接口的登录身份鉴别应支持口令防暴力破解机制，当重复输入错误口令次数超过阈值时采取保护措施。

7.3.4 证书管理

应支持数字证书管理功能，包含以下要求：
a） 使用通用格式的证书，且使用安全的证书签名算法；
b） 设置合理的证书有效期；
c） 支持验证证书的有效性功能。

7.3.5 密钥管理

应支持密钥管理功能，包含以下要求：
a） 对密钥进行分层管理；
b） 用于敏感数据加密的密钥，不可写在源代码中。

7.3.6 安全审计

7.3.6.1 审计数据产生

应支持对于以下事件进行安全审计，并生成审计数据：
a） 审计功能的开启和关闭；
b） 针对数据的备份、恢复、删除、迁移等操作；
c） 用户活动和关键操作行为；
d） 其他与系统安全有关的事件；
e） 所有事件的审计记录应包括：用户名、被访问资源名称、访问发起端地址或标识、事件的日期和时间、事件类型、事件是否成功、及其他与审计相关的信息。

7.3.6.2 审计数据管理

应支持审计数据管理功能，包含以下要求：
a）只有具有相应权限的用户才可读取对应的审计数据；
b）以可被处理的形式提供审计数据。

7.3.6.3 审计数据存储

应保障审计数据的存储安全，包含以下要求：
a） 应确保审计记录的留存时间符合法律法规要求；
b） 应检测或防止对审计的未授权修改。

7.3.6.4 安全事件应急

应具备安全事件应急能力，包含以下要求：

a） 应设立负责数据安全事件管理和应急响应的岗位和人员；
b） 应明确数据安全事件管理和应急响应的策略和具体方案。

8 空间科学数据安全存储等级 2

8.1 数据安全

8.1.1 数据完整性

8.1.1.1 存储数据的完整性

应支持空间科学数据存储过程中的数据完整性检测功能，并针对检测出的错误提供必要的恢复措施。

8.1.1.2 传输数据的完整性

应支持在存储内部不同组件、部件之间传输的数据提供完整性保护功能，能够检测传输中的数据完整性错误。

8.1.1.3 处理数据的完整性

应支持在数据处理过程中进行完整性保护功能。

8.1.2 数据保密性

应支持对空间科学数据保密性进行保护，并针对关键数据采用非明文存储，包含以下要求：
a） 敏感信息不得使用明文存储在本地，且需加密保护；
b） 不在日志、错误信息、调试信息中暴露口令、密钥等敏感信息；
c） 在非信任网络之间进行数据传输时，应支持采用安全传输通道或加密传输；
d） 对敏感数据的访问要有认证、授权或加密机制，对于认证凭据的安全存储，在不需要还原明文的场景下应使用不可逆算法加密。

8.1.3 数据可用性

8.1.3.1 备份与恢复

应支持数据备份与恢复的功能，包含以下要求：
a） 对数据进行手动备份；
b） 对数据进行自动备份；
c） 对数据进行全备份；
d） 对数据进行增量备份；
e） 对数据进行异步备份；
f） 对数据进行同步备份；
g） 对数据进行本地备份；
h） 对数据进行异地备份；
i） 卷镜像的方式提供数据的备份与恢复功能；
j） 快照的方式提供数据的备份与恢复功能；
k） 通过远程复制方式提供数据的备份与恢复功能。

8.1.3.2 防病毒

应支持防病毒软件扫描，防止文件被病毒感染。

8.1.3.3 数据冗余

应支持通过技术手段保障存储数据的可靠性，如配置RAID。

8.1.4 数据访问控制

应支持策略控制下的访问控制功能，包含以下要求：

a）访问策略范围应包括与资源访问相关的主体、客体及他们之间的操作；
b） 对访问的内容、操作权限应不超出预定范围，保障最小特权原则；
c） 对访问的内容、操作权限应不超出预定范围，保障最小特权原则；
d） 支持业务面和管理面无法相互访问；
e）支持对访问控制的策略配置。

8.2 系统安全

8.2.1 系统可靠性

应保证系统可靠性运行，包含以下内容：
a） 应支持管理模块冗余、电源模块冗余、控制模块冗余，并提供容错和故障恢复功能；
b） 应支持对内存的检测与纠错功能；
c） 应支持对硬盘检测与修复功能。

8.2.2 设备状态监控

应支持设备状态自动检测功能，至少可检测硬件故障、网络中断、网络连接错误、业务异常等内容，并采取告警措施。

8.2.3 软件安全

应保证系统软件及软件运行环境不存在高风险级别漏洞。

8.2.4 系统完整性保护

应支持系统完整性保护功能，包含以下要求：
a）对软件安装包进行完整性保护并确保完整性校验流程安全可靠；
b）支持在固件升级和安装过程中对固件进行合法性检验，例如：进行签名校验，未被篡改的软件包可以正常进行安装和升级；被篡改的软件包进行安装和升级时，流程会失败，无法进行正常的安装和升级；
c） 支持对软件包内部文件进行数字签名，同时软件包里应提供对应的CMS签名文件。

8.2.5 系统加固

应支持系统加固功能，包含以下要求：
a）应遵从业界配置加固规范，如CIS ；
b）应支持最小化裁剪，裁撤不必要的组件和服务；
c）应支持补丁管理，支持实时漏洞修复；
d） 应支持权限最小化，支持对文件和目录设置访问权限。

8.2.6 程序行为安全

应持程序行为安全功能，包含以下要求：
a）应支持关键文件入侵检测，设置入侵检测前检查功能，避免文件被篡改；
b）应支持异常行为检测，支持Rootkit入侵检测功能；
c）应支持进程及网络入侵检测，设置周期性非法接入检测功能和关键进程看护功能。

8.2.7 软件供应链安全

存储厂商应对使用的第三方开源软件进行生命周期管理：如漏洞管理、应急响应、版本升级等。

8.2.8 信息安全等级保护

应保证系统至少符合GB/T 22239-2019信息安全等级保护第三级要求。

8.3 管理安全

8.3.1 认证鉴权

8.3.1.1 身份标识管理

应支持对用户的标识功能，包含以下要求：

a）为每个用户提供唯一的身份标识；

b）对每个用户身份标识进行管理、维护，确保其不被非授权地访问、修改或删除。

8.3.1.2 账号安全管理

应支持账号管理功能，包含以下要求：

a） 系统中的账号具有唯一性；

b） 所有账号都可被系统管理；

c） 账号的授权应基于最小特权原则；

d） 系统账号不能修改自身权限。

8.3.1.3 鉴别机制管理

应支持身份鉴别功能，包含以下要求：

a）在用户对数据存储进行操作之前，先对该用户进行鉴别；

b）应在服务端进行鉴别处理，并遵循先鉴别，再执行的原则；

c）当用户连续鉴别失败达到设定次数后，系统应阻止用户的进一步请求；

d）用户操作超时断开后，再次连接需重新进行鉴别；

e）用户鉴别信息应非明文存储，且认证数据不被未授权查阅和修改。

8.3.1.4 口令安全管理

应支持口令检测功能，包含以下要求：

a）提供口令复杂度检测功能，若设置口令不符合复杂度要求，系统不准许设置成功并给出合理的提示；

b）口令复杂度满足长度至少6个字符、包含至少两种字符组合、口令不可与账号相同；

c）不得使用缺省口令；

d）不应存在用户无法修改的口令，对于出厂时缺省设置的账号、口令或用于传输的加密密钥应提供修改机制，提醒用户修改及定期更新，并提示风险，口令应保障至少每6个月更换一次；

e）提供的口令输入框不支持口令复制与粘贴功能；

f）操作界面中的口令不得明文显示；

g）密码口令文件应设置访问权限，管理用户不可读取或拷贝加密的内容；

h）用户修改自己口令时应验证旧口令。

8.3.1.5 登录身份鉴别

应支持登录身份鉴别功能，包含以下要求：

a） 管理接口应提供接入鉴别机制，所有可对系统进行管理的人机接口以及跨信任网络的机机接口应有安全的接入鉴别机制，标准协议没有鉴别机制的除外；

b）设备外部可见的可对系统进行调试或管理的物理接口应有接入鉴别机制；

c） 对于人机接口或跨信任网络的机机接口的登录身份鉴别应支持口令防暴力破解机制，当重复输入错误口令次数超过阈值时采取保护措施。

8.3.2 证书管理

应支持数字证书管理功能，包含以下要求：

a）使用通用格式的证书，且使用安全的证书签名算法；

b） 设置合理的证书有效期；

c） 支持验证证书的有效性；

d）证书的私钥应加密保存，私钥保护口令应满足复杂度要求并加密保存，同时控制私钥文件和证书文件的访问权限；

e）支持周期性检查设备上各种类型证书是否过期或即将过期。

8.3.3 密钥管理

应支持密钥管理功能，包含以下要求：

a） 应对密钥进行分层管理；

b） 用于敏感数据加密的密钥，不可写在源代码中；

c） 密钥及相关信息在本地存储时需提供完整性保护和机密性保护。

8.3.4 安全审计

8.3.4.1 审计数据产生

应支持对于以下事件进行安全审计，并生成审计数据：

a）审计功能的开启和关闭；

b）针对数据的备份、恢复、删除、迁移等操作；

c）用户活动和关键操作行为；

d）其他与系统安全有关的事件。

e）所有事件的审计记录应包括：用户名、被访问资源名称、访问发起端地址或标识、事件的日期和时间、事件类型、事件是否成功、及其他与审计相关的信息；

f） 审计数据产生时的时间应由存储所在系统范围内唯一确定的时钟产生，以确保审计分析正确性；

g） 会话事件审计数据产生时还应包括：网络程序名称、协议类型、源地址、目的地址、源端口、目的端口、会话总字节等信息。

8.3.4.2 审计数据管理

应提供对审计数据的管工功能，包含以下要求：

a）只有具有相应权限的用户才可读取对应的审计数据；

b）以可被处理的形式提供审计数据。

8.3.4.3 审计数据存储

应保证审计数据的存储安全，包含以下要求：

a）应确保审计记录的留存时间符合法律法规要求；

b） 应检测或防止对审计记录的未授权修改；

c）审计数据被未授权修改时，对该操作进行审计；

d）审计存储已满、存储失败时，确保审计记录不丢失。

8.3.4.4 安全事件应急

应具备安全事件应急能力，包含以下要求：

a）核心业务应设立负责数据安全事件管理和应急响应的岗位和人员；

b）核心业务应明确数据安全事件管理和应急响应的策略和具体方案；

c）应明确数据安全事件应急预案，定期开展应急演练活动。

9 空间科学数据安全存储等级 3

9.1 数据安全

9.1.1 数据完整性

9.1.1.1 存储数据的完整性

应支持对空间科学数据存储过程中的数据进行完整性保护功能，包含以下要求：

a） 应支持数据存储过程中的数据完整性检测功能，并针对检测出的错误提供必要的恢复措施；

b） 应支持WORM功能。

9.1.1.2 传输数据的完整性

应对存储内部不同组件、部件之间传输的数据提供完整性保护功能，包含以下内容：

a）可检测存储传输中的数据完整性错误；
b）检测到数据完整性错误时，采取必要的数据恢复措施。

9.1.1.3 处理数据的完整性

应支持对处理中的数据进行完整性保护功能。

9.1.2 数据保密性

9.1.2.1 数据保密性

应支持对空间科学数据保密性进行保护，并针对关键数据采用非明文存储，包含以下要求：
a）敏感信息不得使用明文存储在本地，且需加密保护；
b）不在日志、错误信息、调试信息中暴露口令、密钥等敏感信息；
c）在非信任网络之间进行数据传输时，应支持采用安全传输通道或加密传输；
d）对敏感数据的访问要有认证、授权或加密机制，对于认证凭据的安全存储，在不需要还原明文的场景下应使用不可逆算法加密；
e）存储设备应提供数据加密能力，对用户业务数据进行加密存储。

9.1.2.2 剩余信息保护

应支持剩余信息保护功能，包含以下要求：
a） 支持对鉴别信息和敏感数据所在的存储空间进行完全清除；
b） 支持硬盘数据安全擦除，数据擦除后不可恢复；
注：应按照业界数据擦除安全标准（如DoD 5220.22-M(ECE)或者VSITR）对硬盘执行数据安全销毁的功能。
c） 支持硬盘在脱离存储设备后，通过鉴别或加密等机制保障数据不被恶意获取或篡改。

9.1.3 数据可用性

9.1.3.1 备份与恢复

应支持对数据进行备份和恢复的功能，包含以下要求：
a）对数据进行手动备份；
b）对数据进行自动备份；
c）对数据进行全备份；
d）对数据进行增量备份；
e）对数据进行异步备份；
f）对数据进行同步备份；
g）对数据进行本地备份；
h）对数据进行异地备份；
i）卷镜像的方式提供数据的备份与恢复功能；
j）快照的方式提供数据的备份与恢复功能；
k）通过远程复制方式提供数据的备份与恢复功能。

9.1.3.2 防病毒

应支持防病毒软件扫描，防止文件被病毒感染。

9.1.3.3 数据冗余

应支持通过技术手段保障存储数据的可靠性，如配置RAID。

9.1.3.4 高可用

应支持高可用功能，当一个数据中心的存储系统发生故障时，业务自动切换到另一个数据中心。

9.1.3.5 防勒索

应支持防勒索功能，包含以下要求：

a) 应支持对接第三方提供防勒索检测能力或是提供内置的防勒索检测能力；
b) 应支持文件拦截功能，能够阻止已知勒索病毒文件写入；
c) 在系统被勒索的情况下，应支持通过安全快照、法规级 WORM 等安全能力快速恢复用户数据；
d) 应支持 AirGap 功能，对远程复制链路进行关断控制，将数据复制到隔离区，形成更安全的数据保护效果。

9.1.4 数据访问控制

应支持策略控制下的访问控制功能，包含以下要求：
a) 访问策略范围应包括与资源访问相关的主体、客体及他们之间的操作；
b) 对访问的内容、操作权限应不超出预定范围，保障最小特权原则；
c) 对访问的内容、操作权限应不超出预定范围，保障最小特权原则；
d) 支持业务面和管理面无法相互访问；
e) 支持对访问控制的策略配置。

9.2 系统安全

9.2.1 系统可靠性

应保证系统可靠性运行，包含以下内容：
a）应支持管理模块冗余、电源模块冗余、控制模块冗余，并提供容错和故障恢复功能；
b）应支持对内存的检测与纠错功能；
c）应支持对硬盘检测与修复功能。

9.2.2 设备状态监控

应支持设备状态自动检测功能，至少可检测硬件故障、网络中断、网络连接错误、业务异常等内容，并采取告警措施。

9.2.3 软件安全

应保证系统软件及软件运行环境不存在高风险级别漏洞。

9.2.4 系统完整性保护

应支持系统完整性保护功能，包含以下要求：
a）对软件安装包进行完整性保护并确保完整性校验流程安全可靠；
b）支持在固件升级和安装过程中对固件进行合法性检验，例如：进行签名校验，未被篡改的软件包可以正常进行安装和升级；被篡改的软件包进行安装和升级时，流程会失败，无法进行正常的安装和升级；
c）支持对软件包内部文件进行数字签名，同时软件包里应提供对应的CMS签名文件；
d）应提供安全启动功能，防止系统被篡改；
e）存储系统启动时，应支持从信任根开始逐层进行签名校验，按照信任根校验BIOS签名、BIOS校验操作系统签名、操作系统校验存储系统关键业务文件签名的启动顺序，逐级验证。任何一个关键文件被篡改，则系统启动失败，设备记录签名校验异常相关日志。

9.2.5 系统加固

应支持系统加固功能，包含以下要求：
a）应遵从业界配置加固规范，如CIS；
b）应支持最小化裁剪，裁撤不必要的组件和服务；
c）应支持补丁管理，支持实时漏洞修复；
d）应支持权限最小化，支持对文件和目录设置访问权限；
d） 应支持安全沙箱功能，使用安全隔离技术屏蔽操作系统，减少系统暴露面；
e） 安全沙箱应只能操作存储系统配置、维护需要的命令，减小系统的安全风险；
g）通过SSH登录存储系统的时候，应默认进入安全沙箱，不能进入存储系统的linux后台；

h）通过SSH登录存储系统的时候，应禁止root用户远程登录SSH；
i）应支持SSH加固，通过加密和认证机制实现安全访问。

9.2.6 程序行为安全

应持程序行为安全功能，包含以下要求：
a）应支持关键文件入侵检测，设置入侵检测前检查功能，避免文件被篡改；
b）应支持异常行为检测，支持Rootkit入侵检测功能；
c）应支持进程及网络入侵检测，设置周期性非法接入检测功能和关键进程看护功能。

9.2.7 软件供应链安全

应支持软件供应链安全功能，包含以下要求：
b）存储厂商应对使用的第三方开源软件进行生命周期管理：如漏洞管理、应急响应、版本升级等；
c）存储厂商应提供软件供应链安全能力成熟度等级证明，如中国信息通信研究院安全研究所提供的SSC-CMM软件供应链安全能力成熟度等级证书等；
d）存储厂商应积极参与第三方专业安全机构的检测和认证，同时提供对应的安全证书。

9.2.8 信息安全等级保护

应保证系统至少符合GB/T 22239-2019信息安全技术网络安全等级保护第四级要求。

9.3 管理安全

9.3.1 认证鉴权

9.3.1.1 身份标识管理

应支持对用户的标识功能，包含以下要求：
a）为每个用户提供唯一的身份标识；
b）对每个用户身份标识进行管理、维护，确保其不被非授权地访问、修改或删除；
c）将用户身份标识和该用户的所有审计事件相关联。

9.3.1.2 账号安全管理

应支持账号管理功能，包含以下要求：
a）系统中的账号具有唯一性；
b）所有账号都可被系统管理；
c）账号的授权应基于最小特权原则；
d）系统账号不能修改自身权限；
e）应用系统人机账号、机机账号分离，用于程序间通信的机机账号不可作为系统维护的人机账号。

9.3.1.3 鉴别机制管理

应支持身份鉴别功能，包含以下要求：
a）在用户对数据存储进行操作之前，先对该用户进行鉴别；
b）应在服务端进行鉴别处理，并遵循先鉴别，再执行的原则；
c）当用户连续鉴别失败达到设定次数后，系统应阻止用户的进一步请求；
d）用户操作超时断开后，再次连接需重新进行鉴别；
e）用户鉴别信息应非明文存储，且认证数据不被未授权查阅和修改；
f）提供多种鉴别机制及相应的鉴别规则；
g）支持重要的操作强制要求用户重新输入口令等鉴别信息，并在服务端完成鉴别；
h）应支持基于密码技术的身份鉴别机制。

9.3.1.4 口令安全管理

应支持口令检测功能，包含以下要求：

a）提供口令复杂度检测功能，若设置口令不符合复杂度要求，系统不准许设置成功并给出合理的提示；

b）口令复杂度满足长度至少6个字符、包含至少两种字符组合、口令不可与账号相同；

c）不得使用缺省口令；

d）不应存在用户无法修改的口令，对于出厂时缺省设置的账号、口令或用于传输的加密密钥应提供修改机制，提醒用户修改及定期更新，并提示风险，口令应保障至少每6个月更换一次；

e）提供的口令输入框不支持口令复制与粘贴功能；

f）操作界面中的口令不得明文显示；

g）密码口令文件应设置访问权限，管理用户不可读取或拷贝加密的内容。

h）用户修改自己口令时应验证旧口令。

9.3.1.5 登录身份鉴别

应支持登录身份鉴别功能，包含以下要求：

a） 管理接口应提供接入鉴别机制，所有可对系统进行管理的人机接口以及跨信任网络的机机接口应有安全的接入鉴别机制，标准协议没有鉴别机制的除外；

b）设备外部可见的可对系统进行调试或管理的物理接口应有接入鉴别机制；

c） 对于人机接口或跨信任网络的机机接口的登录身份鉴别应支持口令防暴力破解机制，当重复输入错误口令次数超过阈值时采取保护措施；

e）允许口令错误次数及用户锁定时长的配置。

9.3.2 证书管理

应支持数字证书管理功能，包含以下要求：

a）使用通用格式的证书，且使用安全的证书签名算法；

b） 设置合理的证书有效期；

c） 支持验证证书的有效性；

d）证书的私钥应加密保存，私钥保护口令应满足复杂度要求并加密保存，同时控制私钥文件和证书文件的访问权限；

e）支持周期性检查设备上各种类型证书是否过期或即将过期；

g）支持第三方可信机构颁发的数字证书；

h）支持对证书的吊销状态进行验证。

9.3.3 密钥管理

应支持密钥管理功能，包含以下要求：

a）应对密钥进行分层管理；

b）用于敏感数据加密的密钥，不可写在源代码中；

c）密钥及相关信息在本地存储时需提供完整性保护和机密性保护；

d）应支持密钥管理产品对存储进行必要的密钥管理支持。

9.3.4 安全审计

9.3.4.1 审计数据产生

应支持对于以下事件进行安全审计，并生成审计数据：

a）审计功能的开启和关闭；

b）针对数据的备份、恢复、删除、迁移等操作；

c）用户活动和关键操作行为；

d）其他与系统安全有关的事件；

e）所有事件的审计记录应包括：用户名、被访问资源名称、访问发起端地址或标识、事件的日期和时间、事件类型、事件是否成功、及其他与审计相关的信息；

f） 审计数据产生时的时间应由存储所在系统范围内唯一确定的时钟产生，以确保审计分析正确性；

g）会话事件审计数据产生时还应包括：网络程序名称、协议类型、源地址、目的地址、源端口、目的端口、会话总字节等信息。

9.3.4.2 审计数据管理

应提供对审计数据的管工功能，包含以下要求：

a）只有具有相应权限的用户才可读取对应的审计数据；

b）以可被处理的形式提供审计数据；

c）支持条件化检索审计数据，如：搜索、排序、分类等。

9.3.4.3 审计数据存储

应保证审计数据的存储安全，包含以下要求：

a）应确保审计记录的留存时间符合法律法规要求；

b）应检测或防止对审计记录的未授权修改；

c）审计数据被未授权修改时，对该操作进行审计；

d）审计存储已满、存储失败时，确保审计记录不丢失。

9.3.4.4 安全事件应急

应具备安全事件应急能力，包含以下要求：

a）应设立负责数据安全事件管理和应急响应的岗位和人员；

b）应明确数据安全事件管理和应急响应的策略和具体方案；

c）应明确数据安全事件应急预案，定期开展应急演练活动；

d）安全事件管理和响应机制应随着组织实际情况不断调整、更新和完善，并定期对相关员工开展流程培训和宣贯。

10 数据安全级别与数据安全存储等级关系

空间科学数据按照国家及行业主管部门有关要求，安全级别由高到低划分为核心数据、重要数据和一般数据三个级别。综合考虑空间科学数据安全存储中数据安全、系统安全及管理安全三个要素，建议各个级别的空间科学数据安全存储等级要求如表2。

表 2 空间科学数据安全级别与安全存储等级关系

数据安全级别	建议的安全存储等级
核心数据	等级 3
重要数据	等级 2
一般数据	等级 1

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级数据参照本文中重要数据的安全存储等级执行，5级数据参照本文中核心数据的安全存储等级执行。国家及行业主管部门另有规定的除外。

附 录 A
（规范性）
安全存储等级中要素对照表

各个安全存储等级的安全存储要素对照见表A

表A 安全存储要素对照表

安全存储要素		等级1	等级2	等级3
数据安全	数据完整性	✓	✓✓	✓✓✓
	数据保密性	✓	✓✓	✓✓✓
	数据可用性	✓	✓✓	✓✓✓
	数据访问控制	✓	✓✓	✓✓
系统安全	系统可靠性	✓	✓✓	✓✓
	设备状态监控	✓	✓	✓
	软件安全	✓	✓	✓
	系统完整性保护		✓	✓✓
	系统加固	✓	✓✓	✓✓✓
	程序行为管理	✓	✓	✓
	软件供应链管理	✓	✓	✓✓
	信息安全等级保护		✓	✓✓
管理安全	认证鉴权	✓	✓✓	✓✓✓
	证书管理	✓	✓✓	✓✓✓
	密钥管理	✓	✓✓	✓✓✓
	安全审计	✓	✓✓	✓✓✓
	安全应急事件	✓	✓✓	✓✓✓
注：空白表格表示本级无要求；“✓”表示本级有要求；本级要求与上一级相比增加“✓”表示本级要求有增强。				

参 考 文 献

[1] GB/T 25069-2022 信息安全技术 术语
[2] GB-T 22240-2008 信息安全技术 信息系统安全等级保护定级指南
[3] GB/T 30114.1-2013 空间科学及其应用术语 第1部分：基础通用
[4] GB/T 36618-2018 信息安全技术 金融信息服务安全规范
[5] GB/T 37939-2019 信息安全技术 网络存储安全技术要求