数据存储安全管理体系

认证技术规范

文件编号：CTS TBGL140-2026

版本号：B/2

受控状态： （ 受控 ）

编写：技术部

审核：张辉根

批准：周春阳

首次发布：2022-12-20 **首次实施：2022-12-20** **修订实施日期：20260423**

江西腾标认证有限公司

目录

前言

本文件旨在为组织（以下简称“组织”）建立、实施、维护和持续改进数据存储安全管理体系（DSMS）提供要求和指南。本文件采用PDCA（策划-实施-检查-改进）循环模式，与 ISO/IEC 27001:2022《信息安全、网络安全和隐私保护 — 信息安全管理体系 — 要求》 的高阶结构保持一致，并充分融合了 ISO/IEC 27040:2024《信息技术 — 安全技术 — 存储安全》 的特定行业控制要求。

本文件旨在为组织在基于ISO/IEC 27001:2022建立和实施信息安全管理体系的过程中，提供一套专门的数据存储安全控制选择和实施指南。本文件的核心架构与ISO/IEC 27001:2022完全一致，组织可通过实施本文件，建立一个同时满足ISO/IEC 27001和ISO/IEC 27040要求的整合性管理体系。

1. 范围

本文件规定了组织建立、实施、保持和持续改进 数据存储安全管理体系 的要求。本文件适用于

1) 组织建立、实施、保持和改进 数据存储安全管理体系 管理方针和目标；
2) 认证机构对组织进行数据存储安全管理体系认证。

2. 规范性引用文件

下列文件对于本文件的应用必不可少。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。

- ISO/IEC 27000 信息技术 — 安全技术 — 信息安全管理体系 — 概述和词汇
- ISO/IEC 27001:2022 信息安全、网络安全和隐私保护 — 信息安全管理体系 — 要求
- ISO/IEC 27002:2022 信息安全、网络安全和隐私保护 — 信息安全控制
- ISO/IEC 27040:2024 信息技术 — 安全技术 — 存储安全

注：认证审核时引用文件的有效性以审核实施时现行有效的最新版本为准。

3. 术语和定义

ISO/IEC 27000、ISO/IEC 27001:2022界定的以及下列术语和定义适用于本文件。ISO和IEC在以下地址维护用于标准化的术语数据库：

- ISO在线浏览平台：https://www.iso.org/obp
- IEC电子百科：https://www.electropedia.org/

3.1 数据存储

将数据以数字形式保存在计算机系统、存储设备或存储网络中的过程。

3.2 存储基础设施

用于支持数据存储、访问、保护和管理的硬件、软件、固件及其相互作用的环境。包括存储区域网络（SAN）、网络附加存储（NAS）、直接附加存储（DAS）、固态驱动器（SSD）、硬盘驱动器（HDD）、磁带、对象存储、云存储等。

3.3 存储安全

针对存储基础设施及其所存储的数据的保护措施，旨在确保数据的保密性、完整性、可用性和可恢复性。

3.4 数据保留

根据法律、法规、业务或合同要求，将数据保存特定时间段的策略和过程。

3.5 数据销毁

确保数据无法被恢复的过程，包括对存储介质的物理销毁或加密擦除。

3.6 数据迁移

将数据从一种存储设备、格式或位置转移到另一种的过程。

3.7 存储安全控制

用于保护存储基础设施和数据的策略、程序、指南、实践或组织结构。

3.8 存储安全域

具有相同安全要求和信任等级的存储系统或网络区域。

4. 组织环境

4.1 理解组织及其环境

组织应确定与其意图相关的，且影响其实现DSMS预期结果能力的外部和内部事项。

- **外部因素**：适用的数据保护法律和法规（如《网络安全法》、《数据安全法》、《个人信息保护法》等）、监管机构要求（如网信办、工信部、数据局等）、行业标准与最佳实践、勒索软件和网络攻击的威胁趋势、云服务提供商的安全能力、数据跨境传输的法律要求等。
- **内部因素**：组织的规模、治理结构、数据分类与分级策略、存储基础设施的类型与复杂程度（本地、云端、混合）、存储的数据量级与重要性、灾难恢复和业务连续性需求、人员技能与意识、预算约束、以往安全事件记录等。

4.2 理解相关方的需求和期望

组织应确定：

a) 与DSMS有关的相关方；

b) 这些相关方的有关要求；

c) 哪些要求将通过DSMS予以解决。

相关方包括但不限于：监管机构、客户、合作伙伴、供应商（如云存储服务商、存储硬件厂商）、员工、股东、认证机构、公众。

组织应建立、实施并保持程序，以识别相关方，并促其参与到与DSMS相关的已识别的议题中。与相关方的沟通应为一个**持续的过程**。**组织应将促进相关方参与所产生的输出形成文件**。

4.3 确定DSMS的范围

组织应确定DSMS的边界及其适用性，以建立其范围。在确定范围时，组织应考虑：

a) 4.1中提到的外部和内部事项；

b) 4.2中提到的要求；

c) 组织实施的活动与其他组织实施的活动之间的接口和依赖关系（特别是与云存储服务商、外包运维方之间的接口）。

范围应形成文件化信息并可用。

4.4 数据存储安全管理体系（DSMS）

4.4.1 组织应按照本标准的要求，建立、实施、保持和持续改进数据存储管理体系，包括所需过程及其相互作用。

组织应确定数据存储管理体系所需的过程及其在整个组织中的应用，且应：

a) 确定这些过程所需的输入和期望的输出；

b) 确定这些过程的顺序和相互作用；

c) 确定和应用所需的准则和方法（包括监视、测量和相关绩效指标），以确保这些过程的有效运行和控制；

d) 确定这些过程所需的资源并确保其可获得；

e) 分配这些过程的职责和权限；

f) 按照 6.1 的要求应对风险和机遇；

g) 评价这些过程，实施所需的变更，以确保实现这些过程的预期结果；

h) 改进过程和数据存储管理体系。

4.4.2 在必要的范围和程度上，组织应：

a) 保持成文信息以支持过程运行；

b) 保留成文信息以确信其过程按策划进行。

5. 领导作用

5.1 领导作用和承诺

最高管理者应通过以下活动，证实其在对DSMS的领导作用和承诺：

a) 确保建立数据存储安全方针和目标，并与组织战略方向一致；

b) 确保将DSMS要求融入组织的业务过程；

c) 确保DSMS所需的资源可获得；

d) 沟通有效的数据存储安全管理的重要性；

e) 确保DSMS达成其预期结果（如数据可用、安全、合规）；

f) 指导并支持相关人员为DSMS的有效性做出贡献；

g) 促进持续改进；

h) 支持其他相关管理角色在其职责范围内发挥领导作用。

5.2 方针

最高管理者应建立数据存储安全方针，该方针应：

a) 与组织的宗旨相适宜；

b) 包括信息安全目标（见6.2）或为设定信息安全目标提供框架；

c) 包括对满足适用信息安全要求的承诺；

d) 包括对持续改进DSMS的承诺；

e) **特别应包括对保护存储数据的保密性、完整性、可用性和可恢复性的承诺。**

信息安全方针应：

f) 形成文件化信息并可获取；

g) 在组织内得到沟通；

h) 适当时，可被相关方获取（如监管机构、客户）。

5.3 组织的岗位、职责和权限

最高管理者应确保与数据存储安全相关岗位、职责和权限在组织内得到分配和沟通。

最高管理者应**指定一名或多名管理者**（如信息安全负责人、数据存储管理员），不论其是否负有其他职责，应使其具有以下方面的岗位、职责和权限：

a) 确保DSMS符合本文件的要求；

b) 向最高管理者报告DSMS绩效，供其评审并作为持续改进的依据；

c) 确保在整个组织内提高对数据存储安全重要性的意识；

d) 协调与DSMS有关的内部和外部沟通（特别是与存储服务商和监管机构）。

同时，最高管理者应明确**指定一个存储安全协调点**，负责跨部门沟通。

6. 策划

6.1 应对风险和机会的措施

6.1.1 总则

当策划DSMS时，组织应考虑4.1中提到的事项和4.2中提到的要求，并确定需要应对的风险和机会，以：

a) 确保DSMS可达到预期结果；

b) 预防或减少不良影响（如数据泄露、数据丢失、勒索软件攻击、合规处罚）；

c) 达到持续改进。

组织应策划：

d) 应对这些风险和机会的措施；

e) 如何将此措施整合到DSMS过程中并予以实现及评价其有效性。

6.1.2 存储安全风险评估

组织应定义并应用风险评估过程，以建立并维护风险准则（包括风险接受准则和评估实施准则）；识别与存储基础设施及其数据的安全相关的风险（如物理破坏、逻辑错误、未授权访问、存储介质故障、供应商锁定、合规风险）；分析并评价风险。风险评估应特别考虑不同的存储类型（块存储、文件存储、对象存储、备份存储）的特定威胁。组织应保留有关风险评估过程的文件化信息。

6.1.3 存储安全风险处置

组织应定义并应用风险处置过程，以选择适当的处置方案（通过 **ISO/IEC 27001:2022附录A** 及 **ISO/IEC 27040:2024** 中的控制措施）。组织应**制定并维护一个《适用性声明》**，包含所选控制措施及删减的合理性说明，并制定正式的风险处置计划。组织应保留有关风险处置过程的文件化信息。

注： 组织应**建立并保持合规义务登记册**，以识别和跟踪与数据存储安全相关的法律法规、标准及其他要求。

6.2 数据存储安全目标及其实现的策划

组织应在相关职能和层级上建立数据存储安全目标。目标应：

a) 与数据存储安全方针一致；

b) 可测量（如备份恢复成功率、存储系统可用性百分比、存储安全事件数量、加密覆盖率、介质销毁合规率）；

c) 考虑适用的要求；

d) 予以监视；

e) 予以沟通；

f) 视情况予以更新。

策划如何实现这些目标时，组织应确定要做什么、需要什么资源、由谁负责、何时完成、如何评价结果。

6.3 针对变更的规划

当组织确定需要对DSMS进行变更时（如引入新的存储技术、扩充存储容量、切换存储供应商、数据中心搬迁、法律法规变更），变更应系统地予以策划和实施。

7. 支持

7.1 资源

组织应确定并提供建立、实施、维护和持续改进DSMS所需的资源。资源包括：具备相应能力的人员（存储管理员、安全运维人员）、存储基础设施（硬件、软件、网络）、安全工具（如加密机、密钥管理系统、数据防丢失系统、日志审计系统）、财务资源、技术资源等。

7.2 能力

组织应：确定从事会影响组织数据存储安全绩效的工作人员的必要能力（如存储管理、备份恢复、加密技术、介质销毁）；基于适当的教育、培训或经验确保其胜任；适用时采取措施获得必要能力（如存储安全培训、厂商认证），并评估有效性；保留适当的文件化信息作为能力的证据（如培训记录、认证证书）。

7.3 意识

在组织控制下工作的人员应了解：

a) 数据存储安全方针；

b) 其对DSMS有效性的贡献；

c) 不符合DSMS要求的潜在影响（如导致数据丢失、业务中断、合规处罚）。

7.4 沟通

组织应确定与DSMS相关的内部和外部沟通的需求，包括：沟通什么（如存储容量预警、备份状态、安全事件通知、供应商审计结果）、何时沟通、与谁沟通、谁来沟通、怎么沟通。特别地，应建立与云存储服务商关于数据安全事件的沟通机制。

7.5 文件化信息

7.5.1 总则

组织的DSMS应包括：本文件要求的文件化信息（如DSMS手册、风险评估报告、风险处置计划、适用性声明、备份恢复计划等）；组织为DSMS有效性所确定的必要的文件化信息（如存储配置清单、安全策略、操作流程）。

7.5.2 创建和更新

创建和更新文件化信息时，组织应确保适当的标识和说明、形式、载体以及评审和批准。

7.5.3 文件化信息的控制

DSMS及本文件所要求的文件化信息应得到控制，以确保：在需要的场合和时机可获得并适用；予以妥善保护（避免泄密、不当使用或缺失）。为控制文件化信息，适用时，组织应分发、访问、检索和使用；存储和防护；更改控制；保留和处置（存储相关文件化信息的保留期限应符合法规和业务需要）。

8. 运行

8.1 运行的策划和控制

组织应策划、实施和控制为满足要求和实施第6章所确定的措施所需的过程，包括建立过程准则，并按照准则实施控制。组织应控制计划内和计划外的变更，确保外部提供的过程、产品和服务受控。

8.2 存储安全风险评估

组织应考虑6.1.2a) 所建立的准则，按计划的时间间隔或当重大变更发生时（如引入新存储系统、发生重大安全事件），执行存储安全风险评估。应保留风险评估结果的文件化信息。

8.3 存储安全风险处置

组织应实现存储安全风险处置计划。应保留风险处置结果的文件化信息。

8.4 数据存储安全特定控制措施（依据ISO/IEC 27040:2024）

组织应按本章节要求实施和运行特定的存储安全控制措施，这些措施补充和细化了ISO/IEC 27001:2022附录A中的相关控制。

8.4.1 存储安全策略（依据ISO/IEC 27040:2024第6章）

控制

应制定和维护存储安全策略，以管理组织的存储安全。

实施要求：

a) 制定并维护文件化的《数据存储安全策略》，该策略应由最高管理层批准。

b) 该策略应涵盖：存储分类（如内部、外部、云存储）；数据分类与存储位置映射；访问控制原则（如最小权限、职责分离）；加密要求（静态和传输中）；数据备份与恢复要求；数据保留与销毁要求；事件响应要求；合规要求。

c) 该策略应定期评审和更新（至少每年一次）。

8.4.2 存储基础设施的分类与安全域（依据ISO/IEC 27040:2024第6.2条）

控制

应根据安全要求对存储基础设施进行分类，并建立安全域。

实施要求：

a) 对存储基础设施进行分类（如：生产环境存储、测试环境存储、备份存储、归档存储）。

b) 根据安全等级建立**存储安全域**，不同域之间应有逻辑或物理隔离（如VLAN、防火墙、存储级访问控制）。

c) 数据应根据其分类存储在相应的安全域中。

8.4.3 物理安全——存储设备（依据ISO/IEC 27040:2024第7章）

控制

应保护存储设备所在的环境免受物理威胁。

实施要求：

a) 存储设备（硬盘、磁带、固态盘、存储阵列）应放置在受控的物理安全区域内（如数据中心、机房）。

b) 应实施多层次的物理访问控制（如门禁、生物识别、视频监控、人员登记）。

c) 对存储设备的物理访问应授权和记录。

8.4.4 访问控制——存储系统（依据ISO/IEC 27040:2024第8章及附录E）

控制

应实施访问控制措施，防止对存储系统的未授权访问。

实施要求：

a) 存储系统管理接口（如管理软件、CLI、Web控制台）应使用**强身份验证**（如多因素认证）。

b) 严格执行**最小权限原则**，为存储管理员、备份操作员等分配不同的角色和权限。

c) 实施**职责分离**（如：系统管理员和审计员角色分离）。

d) 存储网络（SAN/NAS）应使用访问控制策略（如LUN遮蔽、端口绑定、IP限制）限制主机对存储资源的访问。

e) 对存储管理系统和存储用户的所有访问应进行**日志记录**。

8.4.5 加密与密钥管理（依据ISO/IEC 27040:2024第9章及附录A）

控制

应使用加密技术保护存储数据的保密性。

实施要求：

a) 应实施**静态数据加密**：对存储介质（硬盘、磁带、对象存储桶）中的数据进行加密。可采用存储设备自带的加密功能、文件级加密、卷级加密或应用级加密。

b) 应实施**传输中数据加密**：对在存储网络（SAN/NAS/iSCSI）上传输的数据进行加密（如IPsec、FC-SP）。

c) 应**管理加密密钥**：使用企业级密钥管理系统（KMS）；密钥生成、存储、分发、轮换和销

毁应遵循安全策略；硬件安全模块（HSM）可用于保护根密钥。

d) 应记录并保留加密相关的元数据和审计日志。

8.4.6 数据备份与恢复（依据ISO/IEC 27040:2024第10章）

控制

应建立数据备份与恢复机制，以防止数据丢失和中断。

实施要求：

a) 应制定并实施**数据备份策略**：确定备份范围（哪些数据、多长时间）、备份频率（按需、小时、日、周）、备份类型（全量、增量、差异）、保留周期。

b) 备份数据应**异地存储**，且与生产数据物理或逻辑隔离（如离线、不可变存储），以抵御勒索软件攻击。

c) 备份数据的加密要求应与生产数据一致。

d) 应定期对备份数据进行**恢复测试**，验证其完整性和可用性（至少每季度一次）。

e) 恢复流程应文档化并定期演练。

8.4.7 灾难恢复与业务连续性（涉及存储部分）（依据ISO/IEC 27040:2024第10.3条）

控制

存储基础设施应支持组织的灾难恢复和业务连续性计划。

实施要求：

a) 存储设计应考虑**高可用性**（如RAID、冗余控制器、冗余路径）。

b) 应配置**数据复制**（同步或异步）到灾备站点（本地或云端）。

c) 应对灾备站点的存储设备和链路的可用性进行定期测试。

8.4.8 数据防泄露（DLP）（新增）

控制

应部署数据防泄露措施，以保护存储在存储基础设施上的敏感数据免受未授权的传输、泄露或篡改。

实施要求：

a) 应识别并标记存储在存储系统中的敏感数据（如PII、知识产权、财务数据）。

b) 应部署**数据防泄露（DLP）** 技术，监控和阻止敏感数据通过存储网络、电子邮件、USB接口或云存储应用进行未授权的传输。

c) 应对DLP事件进行记录、告警和调查。

8.4.9 恶意软件防护（存储相关，依据ISO/IEC 27040:2024第11章及附录D）

控制

应保护存储基础设施免受恶意软件（特别是勒索软件）的攻击。

实施要求：

a) 应在存储访问通路上部署恶意软件扫描和防护功能（可在文件服务器或NAS上部署）。

b) 应考虑部署**不可变或一次写入多次读取（WORM）** 的存储功能，以防止恶意加密和数据

篡改。

c) 对存储系统本身的固件和软件应进行漏洞扫描和补丁管理。

8.4.10 数据保留与销毁（依据ISO/IEC 27040:2024第12章）

控制

应根据法律、法规和业务要求管理数据的保留和销毁。

实施要求：

a) 制定数据保留策略，明确不同类型数据的保留期限。

b) 当数据不再需要时，应根据敏感度进行**安全销毁**：

- **逻辑销毁**：对数据进行多次覆写（如DOD 5220.22-M标准）或加密擦除。
- **物理销毁**：对物理存储介质（如硬盘、磁带）进行消磁、粉碎或焚毁。

c) 所有销毁操作应有**审批记录**和**见证记录**。供应商应提供销毁证明。

8.4.11 第三方和云存储服务（依据ISO/IEC 27040:2024第14章）

控制

应确保第三方和云存储服务满足组织的数据存储安全要求。

实施要求：

a) 在选择云存储服务商或第三方存储运维商时，应评估其安全能力（如ISO 27001认证、数据加密能力、合规性）。

b) 与云存储服务商签订的服务协议（SLA）中应明确：数据所有权、数据隔离、加密要求、数据备份与恢复、事件通知流程、数据删除与返还条款。

c) 定期对云存储服务商进行安全审计或要求其提供审计报告（如SOC 2）。

8.4.12 存储安全事件响应与监控（修订）

控制

应建立存储相关的安全事件响应机制和监控措施。

实施要求：

a) 定义存储安全事件的类型（如存储设备故障、数据泄露、勒索软件攻击、性能异常、数据防泄露告警、未授权访问尝试）。

b) **监控存储系统日志、性能数据和警报**（如容量预警、健康状态、备份失败、访问日志异常）。应使用安全信息和事件管理（SIEM）系统进行集中分析。

c) 事件响应计划中应包含**存储数据恢复**的具体步骤和角色。

d) 应定期测试事件响应计划的有效性（至少每年一次）。

9. 绩效评价

9.1 监视、测量、分析和评价

组织应确定：需要被监视和测量的内容（包括存储性能、容量、可用性、安全事件指标、备份成功率、加密覆盖率等）；适用的方法；何时执行；谁应执行；何时分析和评价结果。组

织应评价数据存储安全绩效以及DSMS的有效性。**确保用于监视与测量的资源（如存储管理平台、日志分析工具）的准确性**。

9.1.2 合规性评价

组织应建立、实施并保持程序，以定期评价其对适用法律法规（特别是数据安全法）、标准及自身DSMS要求的遵守情况。**合规性评价应至少每年进行一次**，并**保留合规性评价报告作为成文信息**。

9.2 内部审核

组织应按策划的时间间隔进行内部审核，以提供有关DSMS符合性及有效性的信息。审核员应确保客观性和公正性。审核结果应报告给相关管理层。

9.3 管理评审

最高管理者应按计划的时间间隔评审DSMS，以确保其持续的适宜性、充分性和有效性。管理评审应考虑：

a) 以往管理评审措施的状态；

b) 内外部的变化（如新的法规、新的存储威胁、技术迭代）；

c) 绩效信息（包括：存储安全事件趋势、备份恢复成功率、**外部供方（如云存储服务商、存储设备供应商）的绩效**、合规性偏差、风险评估与处置状态、改进机会等）；

d) 持续改进的机会。

评审输出应包括与持续改进机会及DSMS变更需求相关的决定。

10. 改进

10.1 持续改进

组织应持续改进DSMS的适宜性、充分性和有效性。

10.2 不符合与纠正措施

当发生不符合时，组织应：做出应对、控制并纠正，处置后果；评价是否需要采取措施消除原因；实施所需的措施并评审有效性；必要时对DSMS进行更改。应保留文件化信息作为不符合性质及后续采取措施的证据。**推荐预防措施**以防范潜在不符合的发生（例如，通过定期容量预警和健康检查，预防存储满故障）。

————————————————