

ICS 35.030
CCS L 80



**NATIONAL STANDARD OF THE
PEOPLE'S REPUBLIC OF CHINA**

GB/T 47685-2026

Cybersecurity technology - Guidelines for storage security

网络安全技术 存储安全指南

(English Translation)

Issued on: May 25, 2026

Implemented on: December 1, 2026

Issued by: State Administration for Market Regulation

Table of Contents

Preface
1 Scope
2 Normative References
3 Terms and Definitions
4 Abbreviations 5.
5 Overview 7.
6 Storage organization and management measures
7 Personnel Management Measures for Storage
8 Physical control measures for storage
9 Technical control measures for storage
Appendix A (Informative) Comparison of this document with the structural numbering of ISO/IEC 27040:2024
Appendix B (Informative) Summary of Storage Security Management and Control Measures
Reference

Foreword

This document complies with the provisions of GB/T 1.1-2020 "Standardization Work Guidelines Part 1: Structure and Drafting Rules of Standardization Documents".

Drafting.

This document is modified to adopt ISO/IEC 27040:2024 "Information technology security technology - Storage security".

This document has undergone significant structural adjustments compared to ISO/IEC 27040:2024. A comparison of the structural numbering changes between the two documents is provided.

See Appendix A for a list.

The technical differences between this document and ISO/IEC 27040:2024, and the reasons therefor, are as follows.

---Change the requirement clauses in ISO/IEC 27040:2024 to recommendation clauses to adapt to the development of guideline standards in my country.

Requirements (see Chapters 1, 6-9);

---In the "Terms and Definitions" introductory section, ISO/IEC 27000 has been replaced with GB/T 29246-2023, and GB/T 25069 has been added.

References to GB/T 37939 and GB/T 43697-2024 (see Chapter 3);

---The sections "Storing data", "Transmitting data", "Equipment", "Fibre Channel protocol", and "Network-attached storage" from ISO/IEC 27040:2024 have been removed.

Storage, Storage Area Network, Storage Media, Demagnetize, Destroy, Clean, Clear, Storage Clear, Logical Storage Clear, Media "Clean up", "Data security compromised", "Data integrity compromised", "Multi-factor authentication", "Malware", "Security strength", "Strong authentication", "Archived" Terms and definitions such as "evidence," "metadata," and "out-of-band" are defined and professionally in national standards related to cybersecurity.

There is no inconsistency in understanding among users, in accordance with the drafting rules of my country's standardization documents;

---The definition of the term "fiber optic channel" has been changed to enhance the accuracy of the definition (see 3.1.4);

---The definition of the term "storage" has been changed to combine the verb and noun definitions to better suit Chinese reading habits (see 3.1.7);

---Added the terms and definitions for "storage infrastructure" and "chain of custody" to improve readability and facilitate application of this document (see [link]).

3.1.10, 3.6.1);

---Added abbreviations such as "AD", "OAuth", "iWARP", "LDAP", "PSK", "RFC", "RoCE", "SAML", and "WAN" (see below) Chapter 4) removed shortenings such as "AES", "BCM", "DDos", "Dos", "ICT", "ID", "ISMS", "PII", "SHA", and "VM".

Abbreviations;

---Added examples of compliance issues in data security risks that fail to meet statutory, regulatory, or legal requirements, to adapt to my country's data security situation.

All relevant laws and regulations are required (see 5.4.5);

---The descriptions of "organizational control" and "personnel control" have been revised to enhance the accuracy of the descriptions (see 5.5, Chapter 6, and Chapter 7);

---GB/T 22080-2025 replaced ISO/IEC 27001, and GB/T 22081-2024 replaced ISO/IEC 27002.

At the same time, the format of the management and control measures labels was changed to comply with the requirements for the compilation of guideline standards in my country (see 5.5);

---Added a mapping of storage security management and control measures to their corresponding codes to improve organizational, personnel, physical, and technical security.

Readability of technical management and control measures (see Table 2);

---The descriptions concerning data levels have been revised to align with my country's definition of data levels (see 6.2, 9.2.2.2);

---The presentation of IRBC concepts and methodologies in this document has been changed to improve readability (see 6.3);

---Added examples of data confidentiality measures implemented during storage to enhance the practicality of the controls (see 6.4);

---Examples of physical access restrictions for the management interface have been added to enhance the usability of the control measures (see 8.3);

---The control measures for secure initialization have been changed to reflect secure firmware initialization, in order to ensure the storage infrastructure is secure during the boot process.

Integrity (see 9.2.2.4);

---The control measures for data integrity protection technology have been modified to reflect the comprehensiveness of data integrity protection technology (see 9.2.3.4);

---Added reference to GB/T 15843 (all parts), listing strong authentication and centralized identity authentication solutions, in order to this demonstrates the comprehensiveness of the relevant identification technology solutions (see 9.4.2.1);

---Added controls for digital certificate management to ensure the security and validity of digital certificates used in storage management activities.

Sex (see 9.4.2.2);

---Added controls for remote management session security to enhance the security of remote storage management processes (see 9.4.3);

---The encryption process and encryption method have been modified to improve the readability of this document (see 9.5.1);

---The clauses concerning cryptographic algorithms have been amended to suit my country's technical conditions (see 9.5.2~9.5.5, 9.16);

---Added factors affecting the speed of data access through encryption to better evaluate the suitability of storage encryption solutions (see 9.5.3);

---The control measures for protecting stored encryption keys have been changed, and a reference to GM/T 0110-2021 has been added to provide more comprehensive protection.

Key security (see 9.5.5);

---The 10.6 "Storage Clearance" clause and content of ISO/IEC 27040:2024 have been deleted to better align with information clearing in my country.

Standards harmonization;

---Controls for the secure use of snapshots have been changed to better protect the integrity of snapshots (see 9.7.4);

---Change "Disk Array" to "Disk Array" to reflect the current diversity of storage media materials (see 9.10.2.1);

---A centralized mechanism has been added to implement identity authentication and access control measures to ensure the comprehensiveness of the NFS access control scheme.

(See 9.12.2).

The following editorial changes have been made to this document.

---To maintain consistency with the naming conventions of my country's cybersecurity standards, the standard's name has been changed to "Cybersecurity Technology Storage Security Guidelines";

---The description of the scope of storage security has been moved from Chapter 1 to 5.3 (see 5.3);

---The URLs for the ISO and IEC terminology databases in ISO/IEC 27040:2024 have been removed;

---Informative citation FIPS 140-3 has been removed;

---The footnote to clause 6.3 of ISO/IEC 27040:2024 has been deleted;

---Notes 10.5.5j) and 10.9.1b) of ISO/IEC 27040:2024 have been deleted.

Please note that some content in this document may involve patents. The issuing organization of this document assumes no responsibility for identifying patents.

This document was proposed and is under the jurisdiction of the National Cybersecurity Standardization Technical Committee (SAC/TC260).

1 Scope

This document defines relevant concepts and definitions of storage security, and provides information on threats and related technologies in typical storage scenarios and storage technology fields.

Guidelines on accounting and management control.