ICS 35.030
CCS L 80

NATIONAL STANDARD OF THE PEOPLE'S REPUBLIC OF CHINA

GB/T 37939-2026

Replacing GB/T 37939-2019

Cybersecurity technology - Technical requirements for network storage security

网络安全技术 网络存储安全技术要求

Issued on: May 25, 2026 **Implemented on: December 1, 2026**

Issued by: State Administration for Market Regulation;
Standardization Administration of the PRC

Table of Contents

Foreword

GB/T 37939-2026 | Cybersecurity technology - Technical requirements for network storage security

GB/T 37939-2026 English version. Cybersecurity technology - Technical requirements for network storage security ICS

80 National Standards of the People's Republic of China Replaces GB/T 37939-2019 Network security technology and network storage security requirements Published on

2026-05-

25 Implemented on December 1, 2026 State Administration for Market Regulation The State Administration for Standardization issued a statement.

1.Scope This document specifies the security function requirements and security assurance requirements for network storage. This document applies to the design, development, testing, and evaluation of network storage.

4.Abbreviations The following abbreviations apply to this document. CER. Certificate CPU. Central Processing Unit DER. Distinguished Encoding Rules JKS. Java Keystore PEM. Privacy Enhanced Mail PKCS Requirements in areas such as security management. See Appendix A for a description of the security function requirements for each level of network storage. If no specific level of requirements is specified in this chapter, it means that Level 1, Level 2, and Level 3 all must comply with the requirements of this chapter; if there are explicit requirements... If a specific level of security function requirements is specified in a relevant chapter or clause, then that specific level must comply with the requirements of that chapter or clause. See the corresponding chapters or clauses for different levels of security function requirements. Table B.1 in Appendix B.

6.2 General Requirements It should comply with the requirements of Chapter 5 of GB 42250-2022 regarding identification and authentication, self-access control, self-security auditing, communication security, and support. It supports requirements regarding system security, product upgrades, user information security, and passwords.

6.3 Access Security

6.3.1 Access Authentication Applications accessing network storage should be authenticated and meet the following requirements.

a) Provide a unique identifier for the application and associate the identifier with all auditable events associated with it;

b) Authentication information should not be stored in plaintext, and authentication data should not be accessed or tampered with without authorization;

c) There is no access method that can bypass the authentication mechanism.

6.3.2 Access Control The design should be based on access control security policies to implement policy-controlled access control functions and meet the following requirements.

a) The scope of access control policies includes the subjects, objects, and operations between them related to resource access;

b) The content and operation permissions accessed to resources do not exceed the preset scope and comply with the principle of least privilege;

c) The networks connecting the server and storage, as well as the management network,

should be isolated from each other and unable to access each other;

d) It has log auditing functionality;

e) If multi-protocol access is available, set up a unified access control policy.

6.4.1.1 Level

1 Safety Function Requirements It should have functions such as redundancy of management modules, power modules, and control modules, and provide fault tolerance and fault recovery capabilities.

6.4.1.2 Level

2 Safety Function Requirements It should meet the following requirements.

a) Centralized storage devices feature redundancy in management modules, power modules, and control modules, and provide fault tolerance and disaster recovery capabilities. Recovery ability;

b) It has the function of memory detection and error correction;

c) It has the function of detecting hard disks and solid-state drives.

6.4.1.3 Level

3 Safety Function Requirements It should meet the following requirements.

a) Centralized storage devices feature redundancy in management modules, power modules, and control modules, and provide fault tolerance and disaster recovery capabilities. Recovery ability;

b) It has the function of memory detection and error correction;

c) It has the function of detecting hard disks and solid-state drives;

d) It has the function of detecting CPU anomalies.

6.4.2 Equipment operating status monitoring It should have the function of automatically detecting the working status of the equipment, including but not limited to detecting hardware failures, network interruptions, network connection errors, and quota limitations. It includes functions such as quantity warning and business anomaly warning, and issues alarms for detected abnormal equipment status.

6.4.3 Software and Software Operation Security The system software and its operating environment should not contain vulnerabilities that are known to be classified as high-risk or medium-risk.

6.4.4.1 Level

2 Safety Function Requirements System integrity protection functions should be provided, meeting the following requirements.

a) The software installation package is protected for integrity;

b) It has the function of verifying the integrity of firmware during firmware upgrades and installations.

6.4.4.2 Level

3 Safety Function Requirements System integrity protection functions should be provided, meeting the following requirements.

a) The software installation package is protected for integrity;

b) It has the function of verifying firmware integrity during firmware upgrades and installations;

c) Digitally sign the software package.

6.4.5 Safety reinforcement Level 2 and Level 3 should have safety reinforcement functions and meet the following requirements.

a) The operating system, database, and file system should be hardened for security.

b) Disable unnecessary system services, default shares, and ports;

c) It has the function to disable insecure access protocols, and this function is disabled by default;

d) You cannot log in remotely using the root account directly.

6.4.6 Web Security Level 2 and Level 3 should provide web security features and meet the following requirements.

a) For each request that requires authorized access, verify whether the user's session ID is valid and whether the user is authorized to perform this operation;

b) It has the function of content verification for all data from untrusted data sources, and rejects any data that fails the verification;

c) If the data output to the client comes from an untrusted data source, then the data is encoded or escaped accordingly;

d) When uploading files via the web, a whitelist should be used on the server side to classify the file types uploaded to the web content directory. Line restrictions;