

ICS 35.030
CCS L80



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

GB/T 31500-2024

**Cybersecurity technology - Security specification of data
recovery service for storage media**

网络安全技术 存储介质数据恢复服务安全规范

Issued on: October 26, 2024

Implemented on: May 1, 2025

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

Table of Contents

1 Scope	1
2 Normative references	1
3 Terms and Definitions	1
4 Principle	2
5 General Requirements	3
6 Safety Management Requirements	3
6.1 Institution	3
6.2 Personnel	3
6.3 Environment	4
6.4 Quality Control	5
6.5 Security Audit	6
7 Security Implementation Requirements	6
7.1 Overview	6
7.2 Media Reception	6
7.3 Media Detection	7
7.4 Data Recovery	7
7.5 Data Delivery	8
7.6 Data Destruction	8
8 Safety Management Evaluation Methods	8
8.1 Organization	8
8.2 Personnel	9
8.3 Environment	10
8.4 Quality Control	13
8.5 Security Audit	14
9 Safety Implementation Evaluation Methods	15
9.1 Media Reception	15
9.2 Media Detection	15
9.3 Data Recovery	16
9.4 Data Delivery	16
19 Reference	20

Foreword

This document is in accordance with the provisions of GB/T 1.1-2020 "Guidelines for standardization work Part

1. Structure and drafting rules for standardization documents" Drafting. This document replaces GB/T 31500-2015 "Information Security Technology Storage Media Data Recovery Service Requirements" and GB/T 31500- Compared with.2015, in addition to structural adjustments and editorial changes, the main technical changes are as follows:

- a) The scope of application of the document has been changed (see Chapter 1, Chapter 1 of the.2015 edition);
- b) Added terms and definitions such as "logical failure", "mirror data", and "data recovery service", and changed the terms and definitions of "storage media". righteousness (see Chapter 3);
- c) The relevant requirements of the "confidentiality principle" have been changed, and the "compliance principle" and "grading principle" clauses have been added (see Chapter 4,.2015 Edition). Chapter 4 of);
- d) Added general requirements (see Chapter 5);
- e) The requirements for practitioners have been changed, further divided into two categories, and the clauses have been refined accordingly (see 6.1,.2015 edition). 5.1);
- f) Changed the requirements for practitioners, further divided the requirements into two categories, and detailed the clauses accordingly (see 6.2,.2015 edition) 5.2);
- g) Changed the relevant requirements of "Environment" and detailed the relevant provisions of service places, facilities and equipment, and storage media (see 6.3,.2015 Versions 5.3, 5.4, 7.3, and 7.4);
- h) Added "quality control" requirements (see 6.4);
- i) Added "Safety Audit" requirements (see 6.5);
- j) Changed the relevant requirements of "Security Implementation Requirements" and changed "Service Process Requirements" to "Security Implementation Requirements" (see Chapter 7,.2015 Chapter 6 of the.2001 edition);
- k) Added "Safety Management Evaluation Method" to describe the evaluation method of safety management requirements in Chapter 6 (see Chapter 8);
- l) Added "Safety Implementation Evaluation Method" to describe the evaluation method for the safety implementation requirements in Chapter 7 (see Chapter 9);

1 Scope

GB/T 31500-2024 sets the security requirements for data recovery services on storage media in China. The service is an unusual security problem: a customer hands over a failed disk that may contain everything the organisation has, to a third party that will necessarily read all of it, often in a cleanroom with the drive dismantled, and the customer has no way to observe what happens. The standard therefore governs the provider rather than the technique. It sets the principles and general requirements and then the security management requirements in detail: the institution and its qualification, the personnel with their vetting, training and confidentiality obligations, the physical environment and access control of the recovery facility, the quality control of the process, the handling and custody of the media and of the recovered data at each stage, the equipment and tools used, the destruction of intermediate copies, the records and traceability, and the incident handling. For an organisation choosing a recovery provider, or a provider seeking to demonstrate competence, this is the reference. It takes effect on 1 May 2025.

This document establishes the security principles of storage media data recovery services, stipulates security management requirements and security implementation requirements, and describes the requirements for Evaluation methods for meeting safety management requirements and safety implementation requirements. This document is intended to guide storage media data recovery service agencies in the implementation and management of data recovery services that do not involve state secrets. Self-evaluation and third-party supervision and review of data recovery service agencies for storage and storage media, as well as procurement of data recovery services by storage service users evaluation.

2 Normative references

The contents of the following documents constitute the essential clauses of this document through normative references in this document. For referenced documents without a date, only the version corresponding to that date applies to this document; for referenced documents without a date, the latest version (including all amendments) applies to This document.

GB/T 25069-2022 Information Security Technical Terminology

GB/T 42446-2023 Information security technology - General requirements for the competence of network security practitioners

GB 50073 Cleanroom Design Specifications

GB 50174 Data Center Design Specification

3 Terms and Definitions

The terms and definitions defined in GB/T 25069-2022 and the following apply to this document.

3.1 electronic data Objective data formed by electronic technology such as computer application and communication, used to represent text, graphic symbols, multimedia, etc. information.

Note. Electronic data includes static data and dynamic data stored, processed or transmitted in electronic form.

3.2 storage medium Storage Media Various media or devices that carry electronic data (3.1), including but not limited to computer hard disks, tapes, floppy disks, CDs, various forms of storage media, Memory cards, memory chips, etc. [Source: GB/T 25069-2022, 3.94, modified]

3.3 data recovery Regenerate (restore) lost or damaged electronic data in storage media (3.2) through specialized computer software and hardware technology (3.1) process.