ICS 35.030
CCS L80

NATIONAL STANDARD OF THE PEOPLE'S REPUBLIC OF CHINA

GB 46864-2025

Data security technology - Technical requirements for information sanitization of electronic products

数据安全技术 电子产品信息清除技术要求

Issued on: December 2, 2025 **Implemented on: January 1, 2027**

Issued by: State Administration for Market Regulation;
Standardization Administration of China

Table of Contents

3 Introduction... 4
1 Scope... 5
2 Normative References... 5
3 Terms and Definitions... 5
4 Abbreviations... 7
5 Basic Requirements... 8
6 Function Requirements of Information Sanitization... 9

1 Scope

GB 46864-2025 is the Chinese national standard on data security technology - technical requirements for information sanitization of electronic products, in the field of information technology. It carries no /T suffix, which in the Chinese system means compliance is mandatory: a product or a practice within its scope has to meet it to be lawfully made, sold or carried out in China. It was issued on 2 December 2025 by the State Administration for Market Regulation; Standardization Administration of China, and takes effect on 1 January 2027. Classification: ICS 35.030, CCS L80. This page is published from the official record of the standard held by the Chinese standards administration: the identification, the dates, the classification and the issuing body are taken from there. The clause text, the tables and the numeric limits are in the document itself, which is delivered complete in English translation.

This Document specifies the basic requirements and functional requirements for information sanitization on electronic products, as well as the process requirements for information sanitization on the used electronic products. This Document applies to electronic products manufactured and sold domestically that have non-volatile storage media. It also applies to electronic product manufacturers; third parties developing information sanitization functions for electronic products; and recycling operators' information sanitization on used electronic products. This Document does not apply to electronic products handling state secrets. Electronic products involving state secrets shall be handled in accordance with relevant national regulations on guarding state secrets.

2 Normative References

This document has no normative references.

3 Terms and Definitions

For the purposes of this Document, the following terms and definitions apply.

3.1 Storage media Materials or devices that are used for storing data. NOTE

1.Based on whether data is retained after power loss, storage media are divided into volatile and non-volatile storage media. Volatile storage media loses stored data immediately upon power loss, such as memory, Central Processing Unit (CPU) cache, and video memory, and the like Random Access Memory (RAM). Non-volatile storage media retain data for a long time after power loss, such as Hard Disk Drive (HDD), Solid State Drive (SSD), Embedded Multi-Media Card/Universal Flah Storage (eMMC/UFS) embedded storage chips, USB flash drives, and Secure Digital/Trans Flash (SD/TF) cards. NOTE

2.Based on storage materials and storage principles, electronic product storage media are mainly divided into magnetic media and semiconductor media. Magnetic media uses the magnetization state of magnetic materials to record data, such as HDDs, magnetic tapes, and magnetic cards. Semiconductor media uses the electrical properties of semiconductor materials to record data, such as RAM, SSDs, eMMC, UFS, and USB flash drives, etc.

3.2 Electronic products Hardware and software equipment and accessories that are manufactured using electronic information technology. NOTE. Electronic products in this Document refer to electronic products that have the function of storing user data and use non-volatile storage media.

3.3 User data Data that are generated and written by users during the use of electronic products. NOTE. User data does not include cloud data, electronic product usage status and lifespan data, or product exit-factory settings data such as operating system and pre-installed applications, etc.

3.4 Information sanitization Data stored in electronic products is processed technically to make it inaccessible or unrecoverable. NOTE

1.Information sanitization in this Document refers to the irreversible sanitization of data from the storage media. NOTE

2.Information sanitization prevents the use of technical means to access or recover the data.

3.5 Data Overwrite Write fixed or random meaningless data into an electronic product, overwriting each storage unit related to user data to achieve information sanitization.

3.6 Block erase Perform an erasure operation on the physical blocks of the storage media by invoking instructions on the storage media, erasing all data within the physical blocks. NOTE

1.Block erase is typically applicable to semiconductor-based electronic products that support hardware erasure instructions. After invoking the instruction, it is usually implemented using methods such as charge release. Its smallest erasure unit is counted in

physical blocks. NOTE

2.Clearing only the mapping relationship between logical and physical addresses or marking data as invalid, without erasing user data in the physical blocks, is not considered block erase.

3.7 Destroy Using physical or chemical methods to destroy the usability of the storage media of an electronic product to achieve information sanitization.

4 Abbreviations

The following abbreviations apply to this Document. CPU. Central Processing Unit eMMC. Embedded Multi-Media Card HDD. Hard Disk Drive RAM. Random Access Memory SD. Secure Digital SSD. Solid State Drive TF. Trans Flash UFS. Universal Flah Storage

5 Basic Requirements

The information sanitization shall meet the following requirements.

a) Clear all user data stored on the electronic product, including but not limited to. 1) All files generated or downloaded by the user, such as text, images, audio, and video files; 2) User's address book, call logs, SMS messages, MMS messages, calendar, memos, location, and activity logs; 3) User-installed applications; 4) Application data generated by user-installed and pre-installed applications, and cross- application shared data; 5) User identity-related security data, such as accounts, passwords, biometric information, and application certificates; 6) Information from external devices such as smart cards linked to the user, such as bank cards, transportation cards, and access cards; 7) User's system settings, such as network settings, permission settings, Bluetooth settings, desktop and personalization settings; 8) User data backed up in the electronic product; 9) Cache data generated by the user using the electronic product.

b) For electronic products that encrypt user data, clear or destroy the encryption key and all copies of the key to the user data.

c) Log out all pre-installed application user accounts on the electronic product. After the information sanitization, disable automatic account login, automatic synchronization of user data to the cloud, and activation using the original password. NOTE

1.Prompt the user to actively log out of the account, or force log out during the information sanitization function. NOTE