ICS 35.040
CCS L80

NATIONAL STANDARD OF THE PEOPLE'S REPUBLIC OF CHINA

GB 42250-2022

Information security technology - Security technical requirements for specialized cybersecurity products

信息安全技术 网络安全专用产品安全技术要求

Issued on: December 29, 2022 **Implemented on: July 1, 2023**

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

Table of Contents

Foreword

This document was drafted in accordance with the rules given in GB/T 1.1-2020 "Directives for standardization - Part

1.Rules for the structure and drafting of standardizing documents". Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. The issuing authority shall not be held responsible for identifying any or all such patent

rights. This document was proposed by and shall be under the jurisdiction of Ministry of Public Security of the People's Republic of China.

This document is formulated to implement Article 23 of the Cybersecurity Law of the People's Republic of China. Specialized cybersecurity products are developed, produced, serviced and tested in accordance with the security technical requirements of this document and other technical specifications stipulated by relevant national authorities. This document is the baseline requirement that all specialized cybersecurity products and their providers need to meet. Information security technology - Security technical requirements of specialized cybersecurity products

1 Scope

GB 42250-2022 is the Chinese national standard on information security technology - security technical requirements for specialized cybersecurity 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 29 December 2022 by the State Administration for Market Regulation; Standardization Administration of China, and has been in force since 1 July 2023. Classification: ICS 35.040, 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 stipulates the security function requirements, own security requirements and security assurance requirements of specialized cybersecurity products. This document is applicable to the research and development, production, service, and testing of specialized cybersecurity products sold or provided.

2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

GB/T 25069, Information security techniques -- Terminology

3 Terms and definitions

For the purposes of this document, the terms and definitions defined in GB/T 25069 as well as the followings apply.

3.1 specialized cybersecurity products Specialized hardware and software products used to

secure networks.

3.2 specialized cybersecurity products provider Developers, producers or maintenance service providers of specialized cybersecurity products.

3.3 security domain A collection of assets and resources subject to a common security policy.

3.4 personal information Various information related to identified or identifiable natural persons recorded electronically, excluding anonymized information.

3.5 user information Electronically recorded information generated, collected, stored, transmitted, and processed by individuals, legal persons, or other organizations during the installation and use of specialized cybersecurity products.

3.6 malicious program Programs with network attack functions such as destroying networks and information systems, interfering with the normal use of networks and information systems, stealing or maliciously encrypting network and system data.

4 Security functional requirements

4.1 Access control Specialized cybersecurity products with access control functions should have the following functions.

4.2 Intrusion prevention Specialized cybersecurity products with intrusion prevention functions should have the following functions.

4.3 Security audit Specialized cybersecurity products with security audit functions should have the following functions.

4.4 Malicious program prevention Specialized cybersecurity products with malicious program prevention functions should have the following functions.

5 Own security requirements

5.1 Identification and authentication Specialized cybersecurity products should have the following functions.

5.2 Own access control Specialized cybersecurity products should have the following functions.

5.3 Own security audit Specialized cybersecurity products should have the following functions.

5.4 Communication security Specialized cybersecurity products should provide security measures to ensure the confidentiality and integrity of product remote management network communication data.

5.5 Support system security Specialized cybersecurity products should not contain disclosed medium- and high-risk vulnerabilities.

5.6 Product upgrade Specialized cybersecurity products should have the following functions.

5.7 User information security Specialized cybersecurity products should have the following functions.

5.8 Password requirements Any content related to the use and management of passwords in this document shall be in accordance with relevant standards.

6 Security requirements

6.1 Supply chain security Specialized cybersecurity products provider should meet the following security assurance requirements.

6.2 Design and development Specialized cybersecurity products provider should meet the following security assurance requirements.

6.3 Production and delivery Specialized cybersecurity products provider should meet the following security requirements.

6.4 Operation and maintenance service guarantee Specialized cybersecurity products provider should meet the following security assurance requirements.