NATIONAL STANDARD OF THE

PEOPLE'S REPUBLIC OF CHINA

GB/T 51434-2021

Technical standard for internet security facilities engineering

Issued on: April 9, 2021 **Implemented on: October 1, 2021**

Issued by: Ministry of Housing and Urban-Rural Development of the People's Republic of China;
State Administration for Market Regulation

Table of Contents

1 General

1.0.1 This standard is formulated in order to standardize the construction of Internet network security facilities in my country, ensure that network security facilities and Internet business systems are planned, constructed, and used simultaneously, and that they are technologically advanced, economically reasonable, and safe and applicable.

1.0.2 This standard applies to new construction, reconstruction and expansion projects of Internet network security facilities, covering the technical requirements for the entire process of Internet network security facility engineering planning, design, construction, acceptance, operation and maintenance.

1.0.3 The construction of Internet network security facilities should implement the national network security management guidelines and policies and technical and economic policies.

1.0.4 The construction of Internet network security facilities should fully investigate and analyze the network security requirements and operation and maintenance requirements of the Internet business system, and should consider the impact of new services and new technologies on the structure, function and performance of network security facilities.

1.0.5 The construction of Internet network security facilities should make full use of existing network security facilities, and conduct intensive construction through security capability sharing and centralized management and control.

1.0.6 In addition to implementing this standard, the construction of Internet network security facilities should also comply with the current national standard "Information Security Technology Information System Security Project Management Requirements" GB/T 20282

and other relevant standards.

2.1.1 internet service system

A business system that provides information services to the public through a computer network is composed of hardware and software equipment such as servers, switches, routers, databases, operating systems, and application software.

2.1.2 internet security facilities internet security facilities

Technical facilities such as network security protection facilities, security monitoring facilities, security response facilities, and security recovery facilities constructed to ensure the security, confidentiality, and availability of Internet business systems.

2.1.3 internet security facilities engineering

The process of planning, designing, implementing, checking and accepting, operating and maintaining Internet network security facilities.

2.1.4 Network security protection facilities

A network security facility that protects the security, confidentiality and availability of Internet business systems from external damage.

2.1.5 Network security detecting facilities

Network security facilities that monitor security threats, security vulnerabilities, and security incidents of Internet business systems.

2.1.6 security response facilities network security response facilities

A network security facility that provides technical support for response and disposal work such as analysis, source tracing, blocking, and evidence collection of network attacks.

2.1.7 Security recovery facilities network security recovery facilities

Network security facilities to quickly restore data and services after emergencies such as network security attacks and natural disasters such as earthquakes and floods.

2.1.8 recovery time objective recovery time objective

After a disaster occurs, the time requirement for an information system or business function to recover from a standstill.

2.1.9 recovery point objective recovery point objective

After a disaster, the system and data must be restored to the point in time requirements.

2.2 Abbreviations

IP (Internet Protocol) Internet protocol RPO (Recovery Point Objective) recovery point objective RTO (Recovery Time Objective) recovery time objective SDN (Software Defined Network) software defined network SNMP (Simple Network Management Protocol) Simple Network Management Protocol SSH (Secure Shell) secure shell protocol

3 Engineering planning of network security facilities

3.0.1 The engineering planning of network security facilities should ensure the continuous and stable operation of Internet services, effectively defend and monitor network security threats and attacks, and support emergency response to security incidents and business disaster recovery.

3.0.2 The engineering planning of network security facilities shall meet the needs of network security protection, network security monitoring, network security response, and network security recovery in the short-term and long-term development of Internet business systems, and shall comply with the current national standard "Information Security Technology Network Security Relevant provisions of GB/T 22239 Basic Requirements for Classified Protection.

3.0.3 The functional performance requirements and construction scale of network security facilities shall be determined according to the Internet business development plan, number of users, network bandwidth, network asset scale, and network security management requirements.

3.0.4 The organization plan of network security facilities and the short-term and long-term evolution routes shall be determined according to the use of existing network security facilities, the development plan and business forecast of Internet business systems, and the development of network security technologies.

3.0.5 The project planning of network security facilities should properly handle the relationship between the whole and the parts, and the global network security facilities should adopt the mode of centralized construction and capacity sharing.

3.0.6 The engineering planning of network security facilities should carry out the technical and economic comparison of various schemes.

4.1 General provisions

4.1.1 The network security facility construction route and technical scheme given by the network security facility engineering design should be consistent with the network security planning, and should be further deepened on the basis of the network security planning

combined with specific business scenarios.

4.1.2 The engineering design of network security facilities shall meet the requirements of construction projects such as functions, performance, quality, and engineering investment related to Internet business security assurance.

4.1.3 The network security system design, network security technical scheme design, and network security facility index design should be determined according to the characteristics of Internet services and the relevant requirements for network security level protection.

4.1.4 For new technologies and new applications such as cloud computing, mobile Internet, Internet of Things, SDN, and big data, customized network security design solutions should be adopted, and should comply with the current national standard "Information Security Technology Network Security Level Protection Security Design Technology Requirements" GB/T 25070 related regulations.

4.1.5 Network security reconstruction and expansion projects shall ensure the rational use and full integration of existing network security facilities.

4.1.6 The engineering design of network security facilities shall take into account the specific requirements of Internet business characteristics for security protection facilities, security monitoring facilities, security response facilities, and security recovery facilities, and rationally configure and combine applicable network security facilities to support the entire process of network security management..

4.1.7 The engineering design of network security facilities should achieve network security protection in depth, accurate monitoring, rapid response, and reliable recovery.

4.1.8 The engineering design of network security facilities should include the following contents.

1 Investigate and sort out the status quo of the network and system;

2 Clarify the safety guarantee objectives, including the guarantee objects, function and performance objectives, investment cost objectives, etc.;

3 Network security threats and risk assessment analysis;

4 Network security system design, including protection system design, monitoring system design, response system design, recovery system design, etc.;

5 Network security facility performance design, including network attack scale prediction, data scale calculation, security performance analysis, etc.;

6 Network security facility function, performance analysis and parameter design;

7 equipment selection;

8 Survey the site environment, and determine the final equipment installation configuration,