ICS 35.040
CCS L80

# NATIONAL STANDARD OF THE PEOPLE'S REPUBLIC OF CHINA



# GB/T 22239-2019

Replacing GB/T 22239-2008

## Information security technology - Baseline for classified protection of cybersecurity

信息安全技术 网络安全等级保护基本要求

**Issued on: May 10, 2019** **Implemented on: December 1, 2019**

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

# Table of Contents

## 1 Scope

GB/T 22239-2019 is the Chinese national standard on information security technology - baseline for classified protection of cybersecurity, in the field of information technology. The /T suffix marks it as a recommended standard: it is not compulsory by itself, but it becomes binding as soon as a contract, a tender or a customer specification calls it up - which in practice is how most foreign buyers meet it. It was issued on 10 May 2019 by the State Administration for Market Regulation; Standardization Administration of China, and has been in force since 1 December 2019. 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 standard specifies the general security requirements and security extension requirements for the project under classified protection from level 1 to level 4 of the classified protection of cybersecurity. This standard is applicable to guide the security construction and supervision administration of non-confidential objects in different classes.

Note. The class-5 protection object is a very important supervision and management object. It has special management modes and security requirements, so it is not described in this standard.

## 2 Normative references

The following documents are essential to the application of this document. For the dated documents, only the versions with the dates indicated are applicable to this document; for the undated documents, only the latest version (including all the amendments) are applicable to this standard.

GB 17859 Classified criteria for security protection of computer information system

GB/T 22240 Information security technology - Classification guide for classified protection of information system security

GB/T 25069 Information security technology glossary

GB/T 31167-2014 Information security technology - Security guide of cloud computing services

GB/T 31168-2014 Information security technology - Security ability requirements of cloud computing services

GB/T 32919-2016 Information security technology - Application guide to industrial control system security control

## 3 Terms and definitions

The terms and definitions defined in GB 17859, GB/T 22240, GB/T 25069, GB/T 31167-2014, GB/T 31168-2014, GB/T 32919-2016, as well as the following terms and definitions, apply to this document. For ease of use, some of the terms and definitions in GB/T 31167-2014, GB/T 31168-2014, GB/T 32919- 2016 are listed repeatedly.

3.1 Cybersecurity The ability by taking necessary measures to prevent network from attacks, intrusions, interference, destruction and illegal use, as well as accidents, to make the network in a stable and reliable state of operation, and to ensure the integrity, confidentiality and availability of network data.

3.2 Security protection ability The degree to withstand threats, detect security incidents, recover from previous conditions after damage.

3.3 Cloud computing A mode for accessing a scalable, flexible physical or virtual shared resource pool through a network, and self-serving and managing resources on demand.

Note. Examples of resources include servers, operating systems, networks, software, applications, storage devices. [GB/T 31167-2014, definition 3.1]

3.4 Cloud service provider The provider of cloud computing services.

Note. Cloud service providers manage, operate, support computing infrastructure and software for cloud computing; deliver cloud computing resources through the network. [GB/T 31167-2014, definition 3.3]

## 4 Abbreviations

The following abbreviations apply to this document. AP. Wireless Access Point DCS. Distributed Control System DDoS. Distributed Denial of Service ERP. Enterprise Resource Planning FTP. File Transfer Protocol HMI. Human Machine Interface IaaS. Infrastructure-as-a-Service ICS. Industrial Control System IoT. Internet of Things IP. Internet Protocol

## 5 Overview of Classified protection of cybersecurity

5.1 Object under classified protection The object under classified protection refers to the objects in the classified protection of cybersecurity. It usually refers to a system consisting of computers or other information terminals and related device that collects, stores,

transmits, exchanges, processes information in accordance with certain rules and procedures. It mainly includes basic information networks, cloud computing platforms / systems, big data applications / platforms / resources, Internet of Things (IoT), industrial control systems, systems using mobile internet technologies. The object under classified protection is, based on the degree of harm to national security, economic construction, and social life, and the degree of harm to national security, social order, public interests, the legitimate rights and interests of citizens, legal persons, and other organizations after damage, divided into five protection classes from low to high. See GB/T 22240 for the method of determining the security protection level of the protected object.

5.2 Different classes of security protection ability The basic security protection abilities that different classes of protected objects shall possess are as follows: Level 1 security protection ability. It shall be able to protect against critical resource damage caused by malicious attacks from individuals, threat sources with few resources, general natural disasters, other threats of a considerable degree of harm. After the damage, it may restore some functions. Level 2 security protection ability. It shall be able to protect against important resource damage caused by malicious attacks from small external sources, threat sources with a small amount of resources, general natural disasters, other threats of considerable harm. It may find important security loopholes and handle security incidents, restore some functions within a period of time after they are damaged. Level 3 security protection ability. It shall be able to protect against important resource damage caused by malicious attacks from externally organized groups, threat sources with richer resources, more severe natural disasters, other threats of a considerable degree under a unified security policy. It can timely identify and monitor the attack behavior and deal with security incidents in a timely manner. After being damaged, it can quickly recover most of its functions. Level 4 security protection ability. It shall be able to protect against important resource damage caused by malicious attacks from national-level, hostile organizations, resource-rich threat sources, severe natural disasters, other threats of considerable harm under a unified security policy. It can timely identify and monitor the attack behavior and security incidents in a timely manner. After being damaged, it can quickly recover all of its functions. Level 5 security protection ability. omitted.

### 6.1.1 Security physical environment

6.1.1.1 Physical access control At the entrance and exit of the computer room, it shall assign a special person on duty or equip with an electronic access control system to control, identify and record the entering personnel.

6.1.1.2 Protection against theft and vandalism Device or main components shall be fixed and identified with obvious signs that are not easy to remove.

6.1.1.3 Lightning protection All kinds of cabinets, facilities and device shall be safely grounded through the grounding system.