

ICS 35.040
CCS L 80



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

GB/T 22081-2016

**Information technology -- Security techniques -- Code of
practice for information security controls**

信息技术 安全技术

(English Translation)

Issued on: August 29, 2016

Implemented on: March 1, 2017

**Issued by: General Administration of Quality Supervision, Inspection and
Quarantine**

Table of Contents

Foreword
Introduction
0.1 Background and Environment
0.2 Information Security Requirements
0.3 Control Selection
0.4 Preparation of the organization's own guidelines
0.5 life cycle considerations
0.6 Relevant standard
1 Scope
2 Normative references
3 Terms and definitions
4 standard structure
4.2 Control Category
5 Information Security Strategy
5.1 Information Security Management Guide
6.1 Internal Organization
6.2 Mobile Devices and Remote Work
7 Human Resources Security
7.1 Before Appointment
7.2 Appointment
7.3 Termination and Change of Appointments
8.1 Responsibilities relating to assets
8.2 Information Classification
8.3 Media Handling
9.1 Access Control Business Requirements
9.2 User Access Management
9.3 User Responsibilities
9.4 System and Application Access Control
10 password
10.1 Password Control
11.1 Safety Zone
11.2 Equipment

12 Operational safety
12.1 Operational Procedures and Responsibilities
12.2 Malware Prevention
12.3 Backup
12.4 Logs and Surveillance
12.5 Running Software Control
12.6 Technical Vulnerability Management
12.7 Information System Audit Considerations
13.1 Network Security Management
13.2 Information Transmission
14.1 Information System Security Requirements
14.2 Security During Development and Support
14.3 Test Data
15.1 Information Security in Supplier Relationships
15.2 Supplier Service Delivery Management
16.1 Management and Improvement of Information Security Incidents
17.1 Continuity of Information Security
17.2 Redundancy
18.1 Compliance with law and contractual requirements
18.2 Information Security Review
References

1 Scope

This standard provides guidelines for the organization's information security standards and information security management practices, including the organization of information security risk ring

Environment control of the choice, implementation and management.

This standard is designed to organize.

- a) Selection control, that is, selection control based on GB/T 22080 [10] in the process of implementing an information security management system;
- b) to achieve universal, acceptable information security control;
- c) Develop an organization's own guidance on information security management.

2 Normative references

The following documents for the application of this document is essential. For dated references, only the dated version applies to this article

Pieces. For undated references, the latest edition (including all amendments) applies to this document.

ISO /IEC 27000 information technology security technology information security management system overview and vocabulary (Informationtechnology-

Security technologies - Information security systems systems - Overview and vocabulary.

3 Terms and definitions

ISO /IEC 27000 defined terms and definitions apply to this document.

4 standard structure

This standard includes 14 safety control chapters, contains a total of 35 major safety categories and 114 controls.

Section 4.1

Define each chapter of safety controls, containing one or more major safety categories.

The order of the chapters in this standard does not indicate its importance. Depending on the circumstances, safety control in any or all sections is possible

Is important, so every organization that applies this standard should identify the controls that are applicable, how important these controls are, and how they are used

To each business process. In addition, the list of this standard has no priority.

4.2 Control Category

Each of the major safety control categories includes.

- a) a control goal that states what is to be achieved;
- b) One or more controls that can be used to achieve this control objective.

The description of the control structure is as follows.

control

To meet the control objectives, give a statement that defines a specific control.

Realize the guide

To support the realization of this control and meet the control objectives, provide more

detailed information. This guide may not be entirely applicable or inadequate

In all cases, it may or may not meet the organization's specific control requirements.

other information

Provide further information to consider, such as legal considerations and references to other standards. If there is no other information, this will be

Not given.

5.1 Information Security Management Guidance

Goals. Based on business requirements and relevant laws and regulations, provide management guidance and support for information security.

5.1.1 Information Security Policy

control

Information security policy sets should be defined, approved by the manager, and published, communicated to all employees and external parties.

Realize the guide

At the highest level, the organization should define an "information security policy" that should be approved by management and establish an organization that manages its information

The safety goal of the method.

Information security policy should be concerned about the following requirements.

- a) business strategy b) laws, regulations and contracts;
- c) The current and expected information security threat environment.

This information security policy should include statements regarding.

- a) definition of information security, goals and principles to guide all information security related activities;
- b) Assign general and specific responsibilities for information security management to defined roles;
- c) Handling deviations and surprises.

At a lower level, this information security strategy should be supported by a thematic-specific strategy that further mandates information

Security controls are implemented and are often structured to emphasize the needs of certain target groups within the organization or to cover certain topics.