

ICS 35.030
CCS L 80



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

GB/T 20985.2-2026

Replacing GB/T 20985.2-2020

**Cybersecurity technology - Cybersecurity incident management
- Part 2: Guidelines to plan and prepare for incident response**

网络安全技术 网络安全事件管理 第2部分：事件响应规划和准备指南

(English Translation)

Issued on: July 2, 2026

Implemented on: February 1, 2027

Issued by: State Administration for Market Regulation

Table of Contents

Foreword	
Introduction	
1 Scope	
2 Normative references	
3.1 Terms and Definitions	
3.2 Abbreviations	
4 Network Security Incident Management Strategy	
4.1 General Provisions	
4.2 Stakeholders	
4.3 Contents of Network Security Incident Management Strategy	
5 Network security strategy update	
5.1 General Provisions	
5.2 Association of Strategy Documents	
6 Development of a cybersecurity incident management plan	
6.1 General Provisions	
6.2 Establishing a network security incident management plan based on consensus	
6.3 Stakeholders	
6.4 Contents of the Network Security Incident Management Plan	
6.5 Event Classification	
6.6 Event Forms	
6.7 Documentation process and procedures	
6.8 Trust and Confidence	
6.9 Handling of Confidential or Sensitive Information	
7.1 Overview	
7.2 Establishment of the Incident Management Team	
7.3 Incident Response Team Establishment	
8 Establishing relationships with other organizations	
8.1 Overview	
8.2 Relationship with other departments of the organization	
8.3 Relationships with external stakeholders	
9 Technical and other support	
9.1 General Provisions	

9.2 Technical Support

9.3 Other Support

10 Establishing cybersecurity incident awareness and training

11 Network Security Incident Management Plan Test

11.1 General Provisions

11.2 Drill

11.3 Incident Response Capability Monitoring

12 Lessons Learned

12.1 General Provisions

12.2 Identifying areas for improvement

12.4 Incident Management Team Evaluation

12.5 Identify and improve cybersecurity controls

12.6 Identify and improve the results of cybersecurity risk assessments and management reviews

12.7 Other improvements

Appendix A (Informative) Legal and Regulatory Requirements and Related Considerations

A.1 General Provisions

A.2 Data Protection and Privacy Protection of Personal Information

A.3 Record Saving

A.4 Control measures to ensure the fulfillment of commercial contractual obligations

A.5 Legal issues related to strategies and procedures

A.6 Legal validity check of the disclaimer

A.7 Contracts with external support personnel

A.8 Confidentiality Agreement Requirements

A.9 Enforcement Requirements

A.10 Responsibilities

A.11 Specific regulatory requirements

A.12 Prosecution or enforcement of internal disciplinary procedures

A.13 Legal Aspects

A.14 Acceptable Use Strategies

B.1 Overview

B.2 Example of Recorded Items

B.3 Form Usage Methods

B.4 Form Examples

Appendix C (Informative) Examples of Methods for Classifying, Evaluating, and Prioritizing Cybersecurity Situations and Incidents

C.1 Overview

C.2 Classification of Cybersecurity Incidents

C.3 Network security incident evaluation and prioritization

References

Foreword

This document conforms to GB/T 1.1-2020 "Standardization Work Guidelines Part 1: Structure and Drafting Rules of Standardization Documents".

Drafting is scheduled.

This document is Part 2 of GB/T 20985 "Network Security Technology - Network Security Incident Management". GB/T 20985 has been published.

The following parts were included.

--Part 1: Principles and Processes;

--Part 2: Incident Response Planning and Preparation Guidelines this document replaces GB/T 20985.2-2020 "Information Technology Security Technology - Information Security Incident Management - Part 2: Incidents" the "Response Planning and Preparation Guidelines" differs from GB/T 20985.2-2020 in that, aside from structural adjustments and editorial changes, the main technical changes are as follows.

as follows.

- b) Added content related to the organization's recommendation process (see 6.7);
- c) Changes have been made to content related to vulnerability management (see Chapter 6, Chapter 6 in the 2020 edition);
- d) New roles and responsibilities have been added, including the incident management team and incident coordinator (see 7.2, 7.3).

This document is equivalent to ISO/IEC 27035-2:2023 "Information technology, information security, incident management - Part 2: Incident response".

Planning and Preparation Guide.

The following minimal editorial changes have been made to this document.

--Change the standard title to "Network Security Technology. Network Security Incident Management Part 2: Incident Response Planning and Preparation" guide";

--The abbreviations "ICT" and "IT" have been added;

--Table numbers have been added to the tables in Appendix B.

Please note that some content in this document may involve patents. The issuing organization of this document assumes no responsibility for identifying patents.

This document was proposed and is under the jurisdiction of the National Cybersecurity Standardization Technical Committee (SAC/TC 260).

Introduction

GB/T 20985 "Network Security Technology - Network Security Incident Management" provides guidance for incident management control in GB/T 22081.

The guidelines instruct organizations to implement the controls outlined in GB/T 22081 based on the cybersecurity risks they face. GB/T 20985 is proposed to consist of four parts.

--Part 1: Principles and Processes. The purpose is to present the principles and processes of cybersecurity incident management.

--Part 2: Incident Response Planning and Preparation Guidelines. The purpose is to provide incident response planning and preparation, as well as incident response experience.

A summary guide.

--Part 3: ICT Incident Response Operations Guide. The purpose is to provide guidelines for handling cybersecurity incidents in ICT security operations.

guide.

--Part 4: Collaboration. The aim is to provide guidance on how multiple organizations can collaborate in handling cybersecurity incidents.

Cybersecurity strategies or controls alone cannot guarantee complete protection of information, systems, services, or networks. Even with controls in place...

Measures may still have residual vulnerabilities, reducing the effectiveness of cybersecurity, making cybersecurity incidents more likely, and impacting the organization's business operations.

Direct and indirect potential negative impacts. Furthermore, previously unidentified new threats will inevitably arise if the organization is not prepared to handle such incidents.

Being poorly prepared will diminish the effectiveness of any response, thereby increasing the potential negative impact on the business. Therefore, for any expectation of...

To strengthen the organization of a cybersecurity program, it is essential to adopt a structured and planned approach to conduct the following activities.