GB

NATIONAL STANDARD OF THE

PEOPLE'S REPUBLIC OF CHINA

ICS 35.030

CCS L 80

GB/T 42447-2023

Information security technology - Data security guidelines for telecom field

信息安全技术 电信领域数据安全指南

Issued on: March 17, 2023 **Implemented on: October 01, 2023**

Issued by: State Administration for Market Regulation;
Standardization Administration of the People's Republic of China.

Table of Contents

Information security technology - Data security guidelines for telecom field

1 Scope

This document provides security principles and general security measures for carrying out data processing activities in the telecom field, as well as corresponding security measures that should be taken during the implementation of data collection, storage, use and processing, transmission, provision, disclosure, destruction, etc.

This document applies for guiding telecom data processors to carry out data security protection work, and is also applies for guiding third-party organizations to carry out telecom data security assessment work.

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 41479-2022 Information security technology - Network data processing security requirements

3 Terms and definitions

For the purpose of this document, the terms and definitions defined in GB/T 41479-2022 and the following apply.

3.1

telecom data

Data generated and collected in the course of telecommunications filed business operations.

NOTE 1: Such as user identity information, call data, location data, signaling data, base station construction and operation and maintenance data, network optimization data, etc.

NOTE 2: Without causing confusion, “telecommunications field data” in this document is referred to as “telecom data”.

3.2

NOTE 1: The identification rules for important data and core data refer to relevant national and industry standards, and other data are general data. Since general data covers a wide range of data, telecom data processors can refine and grade general data according to production and operation needs.

NOTE 2: For links where general measures and enhancement measures are not distinguished, general data, important data, and core data shall be protected with reference to the same measures.

6 Security principles

Telecom data processors shall adhere to the following principles:

a) Principle of three synchronization of security: during the design, construction, and operation of relevant platforms carrying data, achieve synchronous planning, construction, and operation of data security protection measures;

b) Principle of classification and grading protection: classify and grade data, and take appropriate security measures commensurate with data security risks according to differential characteristics such as category attributes, importance, and sensitivity to ensure data security;

c) Principle of minimum necessary: during the collection, storage, use, processing, transmission, provision, disclosure, destruction and other processing activities of data, the type and size of data used are limited to those necessary for business development and have legal, legitimate, and necessary purposes;

d) Principle of full life cycle management and control: data security protection measures cover the entire life cycle of data from generation to destruction;

e) Principle of continuous evaluation and optimization: conduct normalized and comprehensive security evaluation of security measures, and continuously and dynamically optimize data security protection measures based on the evaluation results.

7 General security measures for telecom data

7.1 Organizational guarantee

Telecom data processors should take the following security measures in terms of organizational guarantee.

a) General measures:

1) Clarify the responsible departments for data security management, equip data security managers, formulate data security system specifications and operating procedures, and equip data security technical capabilities;

2) Establish a supervision, inspection, and assessment management system for data security protection, and carry out data security supervision, inspection, and assessment management.

b) Enhancement measures:

1) Establish a data security working system, clarify the data security management organization, set up full-time positions for data security management, and establish a collaboration mechanism between the data security management organization and relevant departments;

2) Clarify key roles such as the person with the primary responsibility for data security management within the organization;

3) Sort out the job positions involving important data and core data processing, clarify job responsibilities, and sign a data security responsibility letter or confidentiality agreement.

7.2 Data classification and grading

Telecom data processors should take the following security measures in terms of data classification and grading.

a) General measures:

1) Regularly sort out data assets, form and update a list of data assets in a timely manner, and carry out data classification and grading in accordance with relevant regulations;

2) Classify organizational data categories based on factors such as business needs, data sources, and uses, and update the data asset list in a timely manner based on changes in data assets and changes in classification and grading requirements.

b) Enhancement measures: Form and update a catalog of important data and core data, and carry out catalog filing work in accordance with relevant regulations.

7.3 Permission management

Telecom data processors should take the following security measures in terms of authority management.

a) General measures:

1) Clarify the data security audit coordinating department, assign security auditors, and conduct security audits on authority allocation approval, data processing logs, etc.;

2) Determine necessary data security audit strategies, clarify audit objects, audit content and implementation cycles, and carry out security audits and data analysis in key scenarios such as major data operations, unauthorized access to data and remote access to data;

3) Promptly deal with, rectify, and track and review problems discovered in the audit, and formulate regular data security audit summaries in accordance with relevant regulations.

b) Enhancement measures:

1) Carry out data security audit technical capacity building (such as 4A), and refine security audit strategies for common risks and prone events;

2) Regularly form a summary of security audits of important data and core data in accordance with relevant regulations.

7.6 Risk monitoring and early warning

Telecom data processors should take the following security measures in terms of risk monitoring and early warning: carry out data security risk monitoring; conduct monitoring and inspections of data assets, data processing environments, network and system equipment, data processing accounts, and internal and external data flows; conduct investigation and early warning for abnormal flows and other behaviors; and take remedial measures in a timely manner. Risks that may cause major or greater safety incidents shall be reported in accordance with relevant regulations.

7.7 Emergency response

Telecom data processors should take the following security measures in terms of emergency response.

a) General measures:

1) Develop an emergency plan for data security incidents, and clarify the division of emergency response responsibilities, work processes, and disposal measures according to the level of the incident;

2) Develop an emergency drill plan for data security incidents, conduct regular drills for typical data security incidents such as data leakage, loss, theft, damage, abuse, tampering, illegal access, and illegal transmission, and formulate a drill summary report;

3) After a data security incident occurs, carry out emergency response in a timely manner according to the emergency plan. After the incident is handled, carry out rectification in accordance with relevant regulations, and form a summary report and submit in a timely manner.

b) Enhancement measures: For security incidents involving important data and core data, report in accordance with relevant regulations, while carry out tracking and analyzing of the incident, and take relevant measures in a timely manner to reduce the impact of the incident.

7.8 Security assessment

Telecom data processors should take the following security measures in terms of security assessment.

a) General measures:

1) Regularly sort out and self-examine the organization's overall data security protection level, key business, and platform system data security;

2) Record the self-examination and summary process, form a summary report, analyze the causes of the problems found, and clarify improvement measures and plans.

b) Enhancement measures:

1) Carry out risk assessment of important data and core data, and take timely and effective measures to eliminate potential security risks found in the assessment based on important data processing scenarios;

2) Submit risk assessment reports to relevant departments in accordance with relevant regulations.

7.9 Education and training

Telecom data processors should take the following security measures in terms of education and training.

a) General measures:

1) Develop an education and training plan for personnel in data security positions, and conduct regular education and training for personnel in data security-related positions;

2) Clarify the annual training duration for data security positions, and conduct assessments and evaluations for those who participate in the training.

8.3 Data use and processing

Telecom data processors should take the following security measures when conducting data use and processing activities.

a) General measures:

1) Clarify the approval process and processing rules for data use and processing;

2) If data is used for automated decision-making, it shall carry out data processing algorithm management to ensure the transparency of automated decision-making and the fairness and rationality of the results.

b) Enhancement measures: Use technical measures such as access control and data desensitization to ensure the security of important data processing.

8.4 Data transmission

Telecom data processors should take the following security measures when conducting data transmission activities.

a) General measures:

1) According to business processes, network deployment, security risks, etc., divide network system security domains. According to the type, level and application scenarios of data transmitted, clarify the data security policy and take protective measures;

2) Develop work specifications for security management of data transmission interfaces, and clarify interface security management and protection measures. Sort out the interface situation, form an interface list and update it regularly, and take corresponding measures for interfaces that are found to have security issues or have gone offline through monitoring.

b) Enhancement measures:

1) For activities that transmit important data across networks and security domains, conduct security approval in advance and adopt measures such as verification technology, cryptography technology, secure transmission channels (such as VPN) or secure transmission protocols (such as SSL) to ensure the security of important data transmission;

2) Equip interface authentication capabilities; support the restriction of unauthorized or illegal device access through MAC address, IP address or port number binding, etc.; have interface security monitoring capabilities; support the discovery of unauthorized or illegal device access, and provide alerts and actions;

3) Have the ability to limit and block interface traffic, and support handling measures for abnormal interface calling behaviors and abnormal important data transmission events.

8.5 Data provision

Telecom data processors should take the following security measures when conducting data provision activities.

a) General measures:

1) Clarify the scope, categories, conditions, procedures, etc. of data provision, and regularly sort out the data provision list to ensure that the content of the list is complete and accurate;

2) Clarify the data security protection terms in the service contract or agreement, and clarify the data scope, usage rights, purpose, and security protection responsibilities that the data receiver can access;

3) When data provision involves data export, it shall be conducted in accordance with relevant national regulations and relevant standards.

b) Enhancement measures: Verify the data security protection capabilities of the data receiver, assess security risks, and adopt security measures such as data desensitization and data encryption.

8.6 Data disclosure

Telecom data processors should take the following security measures when conducting data disclosure activities:

a) General measures: Clarify the scope, categories, conditions, procedures, etc. of data disclosure, analyze and determine the possible impact on national security and public interests before data disclosure, and do not disclose data if there is a significant impact;

b) Enhancement measures: Establish an important data disclosure approval mechanism, and use data desensitization technology to protect data required to be disclosed by laws and regulations.

8.7 Data destruction

Telecom data processors should take the following security measures when conducting data destruction activities.

a) General measures:

This is an excerpt of the PDF (Some pages are marked off intentionally)

------ The End ------