ICS 35.030
CCS L80

NATIONAL STANDARD OF THE PEOPLE'S REPUBLIC OF CHINA

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 1, 2023**

Issued by: State Administration for Market Regulation;
Standardization Administration of the PRC

Table of Contents

Foreword

This document was issued on 17 March 2023 by the State Administration for Market Regulation; Standardization Administration of the PRC and takes effect on 1 October 2023.

It is a GB/T standard: recommended rather than compulsory, but it is the text a Chinese reviewer applies when assessing a submission.

1 Scope

GB/T 42447-2023 covers how a telecom operator or any other telecom data processor protects the data it holds, from the principles down to the measures that attach to each stage of processing. Clause 6 states those principles, among them the rule that security is planned, built and operated in step with the platform carrying the data rather than bolted on once it runs. Clause 7 sets out the general measures - organizational responsibility first, then the management and technical controls that apply whatever is being done with the data - and clause 8 works through the processing activities themselves, from collection and storage onward through the data life cycle, each with the measures that belong to it. The terms are taken from GB/T 41479-2022, so the vocabulary lines up with the wider telecom data security framework. A carrier sees who contacts whom, from where and how often, for most of the population, and that record is valuable in the same measure that losing it is damaging; it is also scattered across signalling, billing, customer service and analytics, which is why the measures are organized by processing activity rather than by system. For carriers and telecom service providers, their platform vendors, and the auditors and regulators who review them.

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;