

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

JR/T 0223-2021

**Financial Data Security Data Life Cycle Security Specification
(English Translation)**

Issued on: January 1, 1970

Implemented on: January 1, 1970

Issued by: People's Bank of China

Table of Contents

- 1 Scope
- 2 Normative references
- 5.1 Security Framework
- 5.2 Hierarchical protection
- 6 Data Security Principles
- 7.2 Data transmission

1 Scope

This document specifies the life cycle security principles, protection requirements, organization guarantee requirements and information system operation and maintenance guarantee requirements for financial data.

Establish a security framework covering data collection, transmission, storage, use, deletion and destruction.

This document is applicable to guide financial institutions to carry out electronic data security protection work, and to carry out data protection for third-party evaluation agencies and other units.

Provide reference for safety inspection and evaluation work.

2 Normative references

The contents of the following documents constitute the essential provisions of this document through normative references in the text. Among them, the dated citation documents, only the version corresponding to the date applies to this document; for undated reference documents, the latest version (including all amendments) applies used in this document.

5.1 Security Framework

The life cycle of financial data refers to the collection, processing and management of financial data by financial institutions in the process of business development and management.

The entire process of transmission, storage, use, deletion, and destruction. The Data Lifecycle Security Framework (see Figure 1) follows data security principles to Based on data security classification, establish a security protection system covering the entire

process of the data life cycle, and establish a sound data security organization Structure and clarify the data security requirements in the operation and maintenance of information systems, and comprehensively strengthen the data security protection capabilities of financial institutions.

The data life cycle security protection requirements are the core of the data life cycle security framework. For data with different security levels, specify its the security protection requirements of all links in the data life cycle such as collection, transmission, storage, use, deletion, and destruction are the requirements of financial institutions.

The basic basis for carrying out data security protection work. Combining financial data business rules and financial data characteristics, build a financial data life the security protection mechanism of the whole process of the cycle is the top priority of the data security protection work of financial institutions, and it is also the key to ensuring the security of financial data.

The only way.

Data security organizational guarantee and information system operation and maintenance guarantee are also essential components of the data life cycle security framework, which together constitute it is the cornerstone to ensure that the data life cycle security protection mechanism can be effectively implemented and strictly enforced. Data Security Organization Guarantees Ensure Data Security the work has a complete management system including the decision-making level, management level, executive level and supervision level, which provides a basis for the organization and implementation of data security-related work.

really lay the foundation. In the daily operation of financial institutions, the data security prevention and control work in the information system operation and maintenance process cannot be ignored.

Strengthen data security in the process of border control, access control, security monitoring, security audit, inspection and evaluation, emergency response and incident disposal.

The comprehensive risk prevention and control capability can effectively guarantee the effective implementation of the data security protection mechanism and the timely discovery and response of data security issues.

5.2 Hierarchical protection

The security level of financial data is in accordance with the relevant requirements of JR/T 0197-2020, according to the scope and degree of influence after the security is breached the security level of financial data is divided into 5, 4, 3, 2 and 1 from high to low.

The security of financial data referred to in this document mainly refers to ensuring the

security of financial data at each stage of its life cycle.

Measures to minimize or reduce the possible security impact of data security breaches to an acceptable range. Among them, the level 1 data is in principle, there is no confidentiality requirement for public data, and its security protection should refer to the relevant integrity and availability security requirements of this document; Level 2 to Level 4 Data security protection should be on the basis of balancing security needs and business needs, and according to different data security levels, appropriate measures should be taken with emphasis.

Level 2 data should give priority to business needs, level 4 data should give priority to security needs, and level 5 data should be protected in accordance with national standards.

The relevant requirements of national and industry authorities shall be implemented.

The data security classification and data security protection work in the securities industry shall be implemented in accordance with the relevant requirements of the securities industry such as JR/T 0158-2018, Yunhuan the data security of the environment should meet the relevant requirements of the national and industry authorities. Overseas branches, subsidiaries and branches of financial institutions for data collected and generated in the course of conducting business, its security rating and data protection work shall be implemented in accordance with the relevant requirements for cross-border data.

Content involving personal financial information, in addition to meeting the requirements of this document, should also be implemented in accordance with the relevant requirements of JR/T 0171-2020.

Note: The terms of the specific security level are not specified in this document, which are the general security requirements that all data with security level 1 to 4 should meet; the specific security level has been specified.

All levels of clauses are additional security requirements that need to be implemented for this level of data protection.

6 Data Security Principles

In order to prevent and defend against financial data security risks, financial institutions follow the following data in the process of conducting business and daily management Basic safety requirements.

- a) The principle of legality and legitimacy. the legality and legitimacy of data activities in all links of the financial data life cycle should be ensured.
- b) The principle of clear purpose. a financial data security protection strategy should be formulated, and the security protection purpose of each link in the financial data life cycle should be clarified.

standards and requirements.

c) The principle of choosing consent. the purpose, method, scope, rules, etc. of data collection and processing should be clearly stated to the subject of personal financial information, Formulate a comprehensive privacy policy, and obtain their authorization and consent before data collection and processing.

d) The principle of minimum sufficiency. Financial institutions should only process financial data authorized and agreed by the subject of personal financial information, and the processed financial data the data is the minimum financial data type and quantity necessary for the business.

e) The principle of full controllability. security control mechanisms and technical measures that match the security level of financial data should be adopted to ensure that financial data According to the confidentiality, integrity and availability of each link in the whole life cycle, to avoid unauthorized access to data in the whole life cycle, destruction, tampering, leakage or loss, etc.

f) The principle of dynamic control. the security control strategy and security protection measures for financial data should not be one-time and static, but should be based on Real-time and dynamic adjustments are made to factors such as business requirements, security environment attributes, and system user behavior.

g) The principle of consistency of powers and responsibilities. The relevant departments and responsibilities of the organization's data security protection work should be clarified, and relevant departments and personnel should actively Implement relevant measures and perform data security protection responsibilities.

7.1.1 Overview

Data collection refers to the direct or indirect collection of personal financial data by financial institutions in the provision of financial products and services, business management and other activities.

Financial information entities, as well as the process of obtaining data by external organizations such as corporate customers and external data suppliers. Data leakage during data collection Exposure, data source forgery, privileged account abuse, data tampering and other security risks.

The data collection process realizes data collection and extraction, conversion and standardization, information upload, and provides built-in security audit and supervision, etc.

Auxiliary tools. According to the collection mode, it can be divided into data collection from external institutions and personal financial information subjects, see Appendix A.