

ICS 03.080.99

CCS A 16



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

GB/T 45085-2024

**Specification for network information evidence preservation of
recyclable resources recovery**

再生资源回收利用网络信息存证规范

Issued on: November 28, 2024

Implemented on: June 1, 2025

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

Table of Contents

1 Scope	1
2 Normative references	1
3 Terms and definitions	1
4 Basic principles	1
4.1 Truthfulness	1
4.2 Accuracy	2
4.3 Security	2
4.4 Traceability	2
5 System operating requirements	2
5.1 Basic requirements	2
5.2 Data security	2
5.3 Privacy protection	2
6 Evidence preservation requirements	3
6.1 Authentication of the preserving party	3
6.2 Information collection	3
6.3 Information storage	4
6.4 Information enquiry	5
6.5 Information verification	5
7 Verification method	5
Bibliography	6

1 Scope

This document defines the terms relating to the preservation of evidence of network information in the recovery and use of recyclable resources, establishes the basic principles for such preservation, specifies the system operating requirements and the evidence preservation requirements for network information in the recovery and use of recyclable resources, and describes the corresponding verification method.

This document applies to the preservation of evidence of network information in the recovery and use of recyclable resources, whether on a self-built platform or on a third-party service platform.

3 Terms and definitions

3.1 network information. Information arising in the course of a recyclable resources transaction which is transmitted and stored over a network. Note: it includes the contract for the recyclable resources transaction, the goods, the funds, the invoices and the like.

3.2 preserve evidence. The act of collecting, storing, querying and verifying network information by technical means, so as to ensure that it is complete, true and unalterable, and to make it traceable.

3.3 preserve evidence subject. The organizations and individuals which take part in recyclable resources trading activities and which carry out evidence preservation.

3.4 hash value. The value obtained by carrying out a logical operation on information by means of a particular secure hash algorithm.

4 Basic principles

4.1 Truthfulness. Objective facts, or judgements with a basis in fact, are taken as the ground; the objective situation is reflected as it is; and there is no false record.

4.2 Accuracy. The content is complete, precise and valid, and shall be free of material omission, ambiguity or unusability.

4.3 Security. Hidden dangers in the system can be identified and effective control measures taken to remove them, so as to prevent unlawful intrusion, information leakage, system collapse and similar problems.

4.4 Traceability. The whole lifecycle of the data, from creation to destruction, can be traced, and the data are not modified or damaged without authorization.

5 System operating requirements

5.1.1 The system shall have records of the basic equipment, including but not limited to the type, model, function and physical location of the equipment, and a surveillance system shall be installed at and around the basic equipment.

5.1.2 Routine maintenance and monitoring of the system shall be carried out, including but not limited to virus scanning and removal, system vulnerability scanning and the installation of patches.

5.1.3 The system shall be capable of data export and migration, redundant backup and storage expansion.

5.1.4 The system shall use multi-role division of rights, and important operations shall be authorized by several people jointly and carried out at the same time.

5.1.5 A complete log record shall be established for the evidence preservation system.

5.1.6 The operating situation of the system shall be disclosed regularly and made public to

the interested parties.

5.1.7 A third-party evidence preservation service platform shall reach the level three basic requirements of GB/T 22239-2019 and shall undergo a graded protection assessment once a year.

5.1.8 A third-party evidence preservation service platform shall run stably without interruption, and the availability of the system shall reach 99.99 per cent.

5.1.9 A third-party evidence preservation service platform shall have operation and maintenance capability, with a recovery time objective (RTO) for the business system of not more than 240 minutes and a recovery point objective (RPO) of not more than 120 minutes.

5.2.1 An information security management system shall be established in accordance with GB/T 22080.

5.2.2 The system and the software shall be fully controllable, the system interfaces and system configuration shall be correct and reliable, and the system and software code shall be kept from being decompiled or tampered with.

5.2.3 Measures shall be taken to safeguard the security of the evidence preservation database, preventing access beyond the rights granted and the theft or destruction of data.

5.2.4 The preserved information shall be encrypted with a key, and the necessary protection mechanism shall be applied to the key.

5.2.5 The system shall have an emergency response scheme and a recovery strategy, so that emergencies are responded to in time.

5.3.1 The following measures shall be taken to safeguard privacy: a) following the principle of the minimum necessary, only the personal information and enterprise information that are necessary shall be collected and kept; b) the identity of the party making an enquiry shall be identified, and the complete information preserved shall be returned only to the party that submitted it; c) the enquiry operations of the system administrator shall be recorded in full; d) sensitive information in the enquiry results shall be de-identified.

5.3.2 Multi-factor authentication should be used to confirm the identity of a user, including but not limited to a one-time password by text message, a one-time password app, a physical USB key, face recognition and fingerprint verification.

5.3.3 The collection, storage and use of personal information shall comply with the principles and requirements of GB/T 35273.

6 Evidence preservation requirements

6.1 Authentication of the preserving party. When network information is preserved as evidence, the preserving party shall first be authenticated. The cases include but are not

limited to the following: a) where the preserving party is a natural person, verification of truthfulness and real-name authentication shall be carried out by biometric recognition, by authentication through the national unified identity authentication platform or by similar means, the authentication record shall be kept, and the undertaking of the natural person and the agreement entrusting the handling of taxes and fees shall be retained; b) where the preserving party is an individual industrial and commercial household, verification of truthfulness and real-name authentication shall be carried out by biometric recognition, by authentication through the national unified identity authentication platform, by comparison of certificates and licences or by similar means, and the authentication record shall be kept; c) where the preserving party is a corporate enterprise, verification of truthfulness and real-name authentication shall be carried out by authentication through the national unified identity authentication platform, by comparison of certificates and licences or by similar means, and the authentication record shall be kept.

6.2.1 The content collected shall be the information on the preserving party, the contract or agreement, the goods, the funds, the invoices and the like.

6.2.2 The content collected falls into three types: required, meaning that the content is mandatory and shall not be missing; conditionally required, meaning that the content is required under certain conditions, the conditions being listed in the column headed type explanation; and optional, meaning that the content is optional according to the actual situation.

6.2.3 The several items of content collected shall each be assigned to the contract or agreement, the goods, the funds or the invoices in the accounting of the tax-related business. The contract, the goods, the funds and the invoices shall correspond to one another.

6.2.4 The content and type requirements for information collection shall comply with Table 1. Table 1 sets out, for each category of evidence, the item collected, whether it is required, conditionally required or optional, and the condition under which a conditionally required item applies. For the preserving party it covers the details of a natural person and of an individual household or enterprise together with the verification and authentication result; for the contract or agreement it covers the contract image or electronic contract and the particulars it has to carry; for the goods it covers delivery, quality, price, place and process together with the transport documents and the records they depend on; and for the vouchers it covers the invoice, the payment record and the internal voucher used where an invoice cannot lawfully be obtained. The rows of the table dealing with goods transport and with processing were not legible with certainty in the copy consulted, so the individual item-to-type pairings there are not reproduced here. A footnote to the table states that processing covers only simple operations such as washing, picking, shredding, cutting, dismantling and baling, which change the physical state of the recyclable resource, that is its density, moisture, length, purity, fineness or hardness.