ICS 35.240
CCS L 04

NATIONAL STANDARD OF THE PEOPLE'S REPUBLIC OF CHINA

GB/T 43705-2025

Guidelines for security classification and grading of scientific data

科学数据安全分类分级指南

Issued on: January 24, 2025 **Implemented on: January 24, 2025**

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

Table of Contents

0 Introduction

The scientific data gathered by the national scientific data centres is classified mainly by discipline, by industry or by use. That arrangement makes the data easy to use and to access, but it leaves a problem: scientific data under one and the same heading may be subject to different security management needs. Managing a whole heading according to its strictest security requirement leads to insufficient sharing; the opposite choice leaves security risks and does not meet the needs of scientific data security management.

The document was drawn up against those problems, following the classification and grading management requirements set for scientific data by the relevant national laws and measures, with the aim of raising the level of open sharing while keeping scientific data secure.

On the basis of the relevant regulations and measures it puts forward a security classification framework for scientific data and settles the division into security levels and the grading principles, so that institutions holding multi-discipline, large-volume scientific data can carry out security classification and grading, build a suitable security classification catalogue and, on that basis, determine the level of the data.

1 Scope

This document provides the principles, framework, elements, methods and process of security classification and grading of scientific data.

It applies to the security classification and grading of scientific data, and may also serve as a reference for scientific data centres or related working organizations carrying out security classification and grading.

2 Normative references

The contents of the following documents constitute indispensable provisions of this document through normative reference in the text. For dated references, only the edition corresponding to that date applies; for undated references, the latest edition, including all amendments, applies.

GB/T 25069 Information security technology - Terminology.

GB/T 43697-2024 Data security technology - Rules for data classification and grading.

GB/T 43707 Provenance metadata of scientific data.

GB/T 43708-2025 General rules for security requirements of scientific data.

3 Terms and definitions

The terms and definitions given in GB/T 25069, GB/T 43697-2024 and GB/T 43708-2025 apply, together with those listed below.

3.1 Scientific data: records of original information and of information derived from it, formed in the course of scientific research activities in the fields of natural science, engineering technology science and the like, and obtained by means such as observation and monitoring, survey and investigation, inspection and testing; or other data usable for scientific research activities. Source: GB/T 43708-2025, 3.1.

3.2 Scientific data security classification: the process of dividing and grouping scientific data according to set principles and methods, on the basis of its security attributes or characteristics, its security management needs, its multi-dimensional features and the logical links objectively existing among them, and of establishing a hierarchy and an order of arrangement. Source: GB/T 43708-2025, 3.11.

3.3 Scientific data security grading: the process of determining the security level of scientific data according to the different impact objects and degrees of impact.

3.4 Impact object: the entity whose lawful rights and interests may be affected when scientific data is leaked, tampered with or damaged, or is obtained, used or shared in a non-compliant way. Note: impact objects usually include national security, economic

operation, social order, public interest, organizational rights and interests, and personal rights and interests.

3.5 Impact degree: the size or severity of the loss or damage caused to the impact object when scientific data is leaked, tampered with or damaged, or is obtained, used or shared in a non-compliant way.

3.6 Key data: data of a specific field, a specific group or a specific area, or reaching a certain precision and scale, which once leaked, tampered with or destroyed may directly endanger national security, economic operation, social stability, public health and safety. Note: data affecting only the organization itself or individual citizens is normally not treated as key data. Source: GB/T 43697-2024, 3.2.

3.7 Core data: key data with a relatively high coverage of a field, a group or an area, or reaching a relatively high precision, a relatively large scale or a certain depth, which once used or shared unlawfully may directly affect political security. Note: core data mainly includes data of key fields bearing on national security, data bearing on the lifelines of the national economy, on important aspects of people's livelihood and on major public interests, and other data assessed and determined by the relevant national departments. Source: GB/T 43697-2024, 3.3.

3.8 General data: data other than core data and key data. Source: GB/T 43697-2024, 3.4.

4 Principles for security classification and grading of scientific data

4.1 Principle of integrated planning. Following the overall national requirement of coordinating development and security, different treatments are adopted according to the impact object identified when the level of the scientific data is settled. Where the impact object concerns only the rights and interests of individuals or organizations, the level is settled together with the security classification, after weighing up the development value brought by open sharing against the security cost; otherwise the level should be settled on the principle of taking the higher rather than the lower. Where several factors may affect the grading, the level is settled by the highest impact degree among the impact objects that could be caused.

4.2 Principle of dynamic updating. The security classification catalogue and the grading results are adjusted periodically as the business attributes, the importance and the possible impact degree of the scientific data change.

4.3 Principle of extensibility of the classification. The classification attributes in the security classification framework may be added to as actually needed, so as to suit the characteristics of different disciplines and fields. After the framework has been adjusted, its soundness should be reviewed before use.

5 Security classification of scientific data

5.1 Classification framework. The security classification framework for scientific data is shown in Table 1 and is made up of multi-level classification attributes over several dimensions. Table 1 has three columns: classification dimension, first-level classification attribute and second-level classification attribute. The first dimension, security topic (01), carries five first-level attributes: national security (01), with the second-level attributes political security (01), territorial security (02), military security (03), economic security (04), cultural security (05), social security (06), science and technology security (07), information security (08), ecological security (09), resource security (10), food security (11), energy security (12), nuclear security (13) and biological security (14); public interest (02), with public health (01), social order (02) and public economic rights (03); organizational rights and interests (03), with work order (01), reputation and image (02), public credibility (03) and competitiveness (04); personal rights and interests (04), with personal privacy (01), personal economic rights and interests (02) and personal safety (03); and security management (05), with cross-border data transfer management (01), personal information protection (02), protection of human genetic information (03) and other security management requirements (04). The second dimension, discipline field (02), carries the first-level attributes discipline classification of the Ministry of Education (01), discipline classification of the National Natural Science Foundation (02) and economic industry classification (03), with no second-level attribute. The third dimension, data form (03), carries original data (01), derived data, that is analysed, processed or handled data (02), and archived data (03), again with no second-level attribute.

When a scientific data management institution carries out security classification work, it may do so together with the classification of the scientific data and the needs of the research work. Only the setting of the security topic is obligatory; the other classifications may be adjusted according to the characteristics of the data itself, by trimming, replacing or adding, so as to build a security classification framework suited to a particular discipline field.

5.2 Classification method and process. Security classification of scientific data is carried out with reference to Clause 6, Basic methods of information classification, of GB/T 7027-2002, using the faceted classification method to place the data into the specific classification attributes of the framework. The main steps are: a) obtain the basic information of the scientific data, including name, description, access environment, operating environment, related parties, format and size, then sort the data and form an asset inventory; b) select suitable classification attributes according to the current state of the data and, taking into account the features of the discipline and the characteristics and management needs of the sector, build the security classification framework on the basis of Table 1, Annex A giving an extract of the postgraduate discipline and specialty catalogue issued by the Ministry of Education, Annex B an example framework for agricultural scientific data and Annex C an