ICS 35.030
CCS L80

NATIONAL STANDARD OF THE PEOPLE'S REPUBLIC OF CHINA

GB/T 43697-2024

Data security technology - Rules for data classification and grading

数据安全技术 数据分类分级规则

Issued on: March 15, 2024 **Implemented on: October 1, 2024**

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

Table of Contents

Foreword

This document is in accordance with the provisions of GB/T 1.1-2020 "Guidelines for standardization work Part

1.Structure and drafting rules for standardization documents" Drafting. Please note that some of the contents of this document may involve patents. The issuing organization of this document does not assume the responsibility for identifying patents. This document was proposed and coordinated by the National Cybersecurity Standardization Technical Committee (SAC/TC260). This document was drafted by: China Electronics Technology Standardization Institute, University of Science and Technology of China, National Computer Network Emergency Response Technical Processing Coordination Center, National Information Technology Security Research Center, China Information Security Evaluation Center, China Cyberspace Research Institute, China Cyber Security Review Center Technology and Certification Center, National Industrial Information Security Development Research Center, National Information Center, Beijing Municipal Government Information Security Center (Beijing Beijing Information Security Evaluation Center), the

Third Research Institute of the Ministry of Public Security, China Academy of Information and Communications Technology, Tsinghua University, China People's Public Security University, China Academy of Science and Technology Software Research Institute of the College, Ministry of Transport Science and Technology Research Institute, Hangzhou Anheng Information Technology Co., Ltd., 360 Digital Security Technology Group Co., Ltd., Beijing Douyin Information Service Co., Ltd., Beijing Kuaishou Technology Co., Ltd., China Nuclear Energy Association, China Petrochemical Corporation Co., Ltd., China UnionPay Co., Ltd., China Postal Savings Bank Co., Ltd., Alibaba (Beijing) Software Services Co., Ltd. Ant Group Co., Ltd., Huawei Technologies Co., Ltd., Beijing Baidu Netcom Technology Co., Ltd., China Mobile Communications Group Co., Ltd. Co., Ltd., China Telecom Group Co., Ltd., Beijing iQiyi Technology Co., Ltd., Shuku (Shanghai) Technology Co., Ltd., Beijing Qihoo Technology Co., Ltd. Ltd., Sangfor Technologies Co., Ltd., Venustech Information Technology Group Co., Ltd., Qi'anxin Technology Group Co., Ltd. company. The main drafters of this document are. Yao Xiangzhen, Zuo Xiaodong, Hu Ying, Zhou Chenwei, Wu Mengting, Chen Qi, Zhou Yachao, Shangguan Xiaoli, Lu Lei, Ren Yingjie, Chen Te, Yan Hui, Yang Chen, Yang Xiaowei, Li Wenting, Zhuo Zihan, Xing Xiao, Yang Tao, Li Min, Duan Jinghui, Xu Jinghui, Li Yuan, Ren Weihong, Jin Bo, Hu Zhenquan, Geng Guining, Shan Boshen, Xu Wanxiu, Zhang Min, Yan Min, Du Jing, Yang Guang, Jiang Wei, Yang Shuaifeng, Sun Yan, Liu Bei, Guo Mingduo, Zhang Xiye, Cao Jing, Lu Tianliang, Yang Xiaohan, Yang Bolong, Luo Hongwei, Wang Xin, Hao Chunliang, Zhu Xuefeng, Sha Rui, Jiang Nan, Guo Yanling, Liu Lei, Tian Xin, Zhang Fang, Zhu Chenhong, Peng Juntao, Yong Sun, Xiaoyuan Bai, Jin Peng, Xinmiao Chang, Shi Li, Haitang Wang, Shuxiang Zhong, Xiao Zhang, Yanting Zhang, Weiqiang Jiang, Dongyuan Fan, Libao Yang, Chenchao Xu, Qingjun Fan, Zhang Yuguang, Lan Yuna, Zhang Yi, Lu Zhongming, Ye Runguo, Song Botao, Yao Zhuo, Song Xiaopeng, Liu Qianwei, An Jincheng.

On September 1, 2021, the "Data Security Law of the People's Republic of China" was officially implemented, which clearly stipulates that "the state shall establish a data classification and grading protection system. The system proposes that "according to the importance of data in economic and social development, and once it is tampered with, damaged, leaked or illegally obtained, The data shall be classified and protected according to the degree of harm caused to national security, public interests, or the legitimate rights and interests of individuals and organizations. To carry out data classification and grading protection work, we first need to classify and grade the data, identify the important data and core data involved, and then This document is under the guidance of the National Data Security Coordination Mechanism and is based on the Data Security Law, Cybersecurity Law of the People's Republic of China, Personal Information Protection Law of the People's Republic of China and related regulations give data The general rules for classification and grading are used to guide various industries, regions, departments and data processors in carrying out data classification and grading work. Data security technology data classification and grading rules

1 Scope

GB/T 43697-2024 is the standard that makes the Chinese Data Security Law operable. The law requires data to be protected according to its importance and requires important data to receive particular treatment, but it does not say how to decide which data is which; this document does. It sets the principles, the framework, the methods and the processes for classifying and grading data, and it provides the guidelines for identifying important data, which is the determination with the sharpest regulatory consequences, since it triggers risk assessment, reporting and cross-border transfer requirements. It is written for two audiences: the competent regulatory departments that have to produce sector-specific classification and grading rules, and the regions, departments and data processors that have to apply them. Data involving state secrets and military data are outside its scope. It takes effect on 1 October 2024, and for any company handling Chinese data at scale it is essential reading.

This document specifies the principles, framework, methods and processes for data classification and grading, and provides guidance for identifying important data. This document is applicable to the competent (regulatory) departments of the industry for reference in formulating data classification and grading standards and specifications in this industry and field. Carry out data classification and grading work in various regions and departments, and provide reference for data processors to carry out data classification and grading. This document does not apply to data involving state secrets and military data.

2 Normative references

The contents of the following documents constitute the essential clauses of this document through normative references in this document. For referenced documents without a date, only the version corresponding to that date applies to this document; for referenced documents without a date, the latest version (including all amendments) applies to This document.

GB/T 25069-2022 Information Security Technical Terminology

3 Terms and definitions

The terms and definitions defined in GB/T 25069-2022 and the following apply to this document.

3.1 data Any recording of information by electronic or other means.

3.2 Important data keydata Once leaked, tampered or damaged, it may directly endanger the Data on national security, economic operation, social stability, and public health and safety.

Note. Data that only affects the organization itself or individual citizens is generally not considered important data.

3.3 Core Data If the information has high coverage, high precision, large scale, or certain depth in a field, group, or region, it will be used illegally or shared. Sharing important data that may directly affect political security.

Note. Core data mainly include data related to key areas of national security, data related to the lifeline of the national economy, important people's livelihood, and major public interests. Other data determined by relevant departments through evaluation.

3.4 General data Other data besides core data and important data.

3.5 Personal information Various information related to an identified or identifiable natural person recorded electronically or otherwise.

3.6 Personal information that, once leaked or illegally used, may easily cause infringement upon a natural person's personal dignity or endanger personal or property safety.