ICS 35.030
CCS L 80

NATIONAL STANDARD OF THE PEOPLE'S REPUBLIC OF CHINA

GB/T 46796-2025

Data security technology - Methods for monitoring the security risk of data interfaces

数据安全技术 数据接口安全风险监测方法

Issued on: December 2, 2025 **Implemented on: July 1, 2026**

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.Abbreviations 1
5 General Rules 2
5.1 Relationship of Data Interface Security Risk Monitoring Elements 2
5.2 Data Interface Security Risk Monitoring Methods 3
5.3 Data Interface Security Risk Monitoring Process 3
5.4 Data Interface Security Risk Monitoring Process Control 4
6.Monitoring Preparation 4
6.1 Establish a monitoring team 4
6.2 Identify the monitoring targets 5
6.3 Develop a monitoring plan 5
7.1 Monitoring Information Collection 5
7.2 Monitoring Information Processing 6
7.3 Risk Source Identification 6
8.1 Risk Analysis 7
8.2 Event Analysis 7
9.1 Monitoring and Early Warning 8
9.2 Monitoring and Handling 8
15 Appendix E (Informative) Example 16 of Data Interface Security Risk Mitigation Measures Reference 18

Foreword

This document complies with the provisions of GB/T 1.1-2020 "Standardization Work Guidelines Part

1.Structure and Drafting Rules of Standardization Documents". Drafting. Please note that some content in this document may involve patents. The issuing organization of this document assumes no responsibility for identifying patents. This document was proposed and is under the jurisdiction of the National Cybersecurity Standardization Technical Committee (SAC/TC260). This document was drafted by: Quanzhi Technology (Hangzhou) Co., Ltd., the Third Research Institute of the Ministry of Public Security, and the China

Electronics Technology Standardization Institute. State Information Center, China Academy of Information and Communications Technology, China Information Security Evaluation Center, China Cybersecurity Review and Certification and Market Supervision Big Data Center According to the Center, the National Information Technology Security Research Center, the Information Center of Yunnan Power Grid Co., Ltd., Sangfor Technologies Inc., Beijing Haohan Deep Information Technology Co., Ltd., Rockchip Technology Group Co., Ltd., Beijing Data Security Technology Co., Ltd., Shenzhen Information Security Management Center, State Grid Siji Network Security Technology (Beijing) Co., Ltd., Guangdong Provincial Information Security Evaluation Center, China Telecom Co., Ltd. The company's Jiangxi branch, Shanghai Hehe Information Technology Co., Ltd., Alibaba Cloud Computing Co., Ltd., and Beijing Yahong Century Technology Development Co., Ltd. The company, Venustech Information Technology Group Co., Ltd., Jiangsu Provincial Institute of Electronic Information Product Quality Supervision and Inspection (Jiangsu Provincial Information Security) (Full Testing Center), Zhejiang University of Technology, Beijing Topsec Network Security Technology Co., Ltd., Qi An Xin NetSec Information Technology (Beijing) Co., Ltd. The company, Shenzhen CESI Information Technology Co., Ltd., China Telecom Cloud Technology Co., Ltd., China United Network Communications Group Co., Ltd., and the Chinese Academy of Sciences Information Engineering Research Institute, China Southern Power Grid Data Platform and Security (Guangdong) Co., Ltd., Jiangxi Provincial Government Information Center, China Mobile Communications Group Limited Liability Company, Minyuxing (Beijing) Technology Co., Ltd., Shanghai Wenyao Information Technology Co., Ltd., Beijing Jianheng Xin'an Technology Co., Ltd. The main drafters of this document are. Fang Xing, He Yanzhe, Wei Fengling, Zhou Dunke, Xu Kechao, Chen Yan, Liu Bei, Yan Guixun, Chen Tian, Cao Jing, and Song Jing. Xiao Peng, Du Jing, Feng Xiaoxiao, Tian Yuxuan, Fan Hua, Wang Zhelin, Liu Nan, Song Botao, Gong Panpan, Li Wei, Yang Gaofeng, Liu Yuhong, Dong Anbo, Mu Duanduan Sun Lei, Yu Ning, Guo Li, Song Hongyu, Sun Yong, Gu Yuan, Yang Tianshi, Zhou Ruiqun, Zhang Tengbiao, Xuan Qi, Jin Gang, Lu Junjie, Bi Siwen, Zhang Yu, Cao Mi, Liang Ruigang, Du Haowen, Wen Jian, Jiang Weiqiang, Zhang Jian, Zhong Kaitao, Qian Lipei. Data security technology Data Interface Security Risk Monitoring Method

1 Scope

GB/T 46796-2025 is the Chinese national standard covering watching the API surface of an organisation - discovering the interfaces that exist including the ones nobody documented, classifying the data each exposes, detecting the abnormal volumes and patterns that mean data is leaving, and the response. Undocumented and over-permissive APIs are how most large data breaches now happen. First edition. Issued on 2 December 2025, it has been in force since 1 July 2026.

This document describes the relationships between key elements and monitoring methods for data interface security risk monitoring, and outlines the data interface security risk

monitoring process. Explanation of the stages. This document is intended to guide data processors and third-party organizations in conducting data interface security risk monitoring, and is implemented by the competent (regulatory) department. This can be used as a reference when supervising and managing data interface security risks.

2 Normative references

The contents of the following documents, through normative references within the text, constitute essential provisions of this document. Dated citations are not included. For references to documents, only the version corresponding to that date applies to this document; for undated references, the latest version (including all amendments) applies. This document.

GB/T 20986-2023 Information Security Technology - Guidelines for Classification and Grading of Network Security Incidents

GB/T 43697-2024 Data Security Technology - Data Classification and Grading Rules

GB/T 45577-2025 Data Security Technology - Data Security Risk Assessment Methods

3 Terms and Definitions

The terms and definitions defined in GB/T 43697-2024 and GB/T 45577-2025, as well as the following terms and definitions, apply to this document.

3.1 data interface Between different network areas or information systems, the caller and the provider follow a data transmission format agreed upon by one or both parties and complete the data transfer. According to the interface of the transmission and exchange service. Note

1.This does not include physical hardware interfaces (such as USB) as well as internal logical interfaces and protocol interfaces of the system. Note

2.Typical data interface structures, technologies, and business models are shown in Appendix A.

3.2 Threats and vulnerabilities that could compromise the confidentiality, integrity, availability, and proper processing of data carried by the data interface. Sexuality, problems, and hidden dangers, etc.

Note. In this document, "risk sources" are referred to as such. They include both sources where security threats exploit vulnerabilities in data interfaces, potentially leading to data security incidents, and sources related to data processing. Improper handling of management activities may lead to illegal or irregular incidents. [Source: GB/T 45577-2025, 3.5, with modifications]

4.Abbreviations The following abbreviations apply to this document.