ICS 35.030
CCS M 10

NATIONAL STANDARD OF THE PEOPLE'S REPUBLIC OF CHINA

GB/T 44462.4-2026

Industrial internet enterprise cybersecurity - Part 4: Data protection requirements

工业互联网企业网络安全 第4部分：数据防护要求

Issued on: March 31, 2026 **Implemented on: October 1, 2026**

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

Table of Contents

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. This document is Part 4 of GB/T 44462 "Enterprise Cybersecurity for Industrial Internet". GB/T 44462 has already published the following... part.

1.Protection Requirements for Industrial Enterprises Applying the Industrial Internet;

2.Protection Requirements for Platform Enterprises;

3.Identifier Resolution Enterprise Protection Requirements;

4.Data Protection Requirements. 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 by the Ministry of Industry and Information Technology of the People's Republic of China. This document was prepared by the National Telecommunications Standardization Technical Committee (SAC/TC485) and the National Cybersecurity Standardization Technical Committee (SAC/TC260). Under the same jurisdiction. This document was drafted by: National Industrial Information Security Development Research Center, China Academy of Information and Communications Technology, Tsinghua University, and Fujian Provincial Department of Industry and Information Technology. Information Industry Development Research Center, University of Chinese Academy of Sciences, CATL (Contemporary Amperex Technology Co., Limited), China Industrial Internet Research Institute China Software Testing Center (Software and Integrated Circuit Promotion Center of the Ministry of Industry and Information Technology), Fujian Normal University, Yantai Zhongke Network Technology Research Institute Institute, Shanghai Guanan Information Technology Co., Ltd., Shanghai Baoxin Software Co., Ltd., Zhengzhou Xinda Jiean Information Technology Co., Ltd. Company, Beijing Topsec Network Security Technology Co., Ltd., Hubei Provincial Institute of Electronic Information Product Quality Supervision and Inspection, Beijing Ruihang Zhizhen Technology Co., Ltd. The company, Shandong Provincial Information Technology Industry Development Research Institute (China Saibao (Shandong) Laboratory), Beijing Shuanxing Technology Co., Ltd., and Beijing Anhua Jinhe Technology Co., Ltd., Hangzhou Anheng Information Technology Co., Ltd., Changyang Technology (Beijing) Co., Ltd., Hunan Provincial Electronic Information Technology Co., Ltd. Industry Research Institute, Guizhou Provincial Network and Information Security Evaluation and Certification Center, Tsinghua Sichuan Energy Internet Research Institute, Qingdao Hisense Communication Co., Ltd. Sangfor Technologies Inc., Schneider Electric (China) Co., Ltd., Beijing Luoan Technology Co., Ltd., Beijing Shenzhou Green Alliance Technology Co., Ltd., Fengtai Technology (Beijing) Co., Ltd. The main drafters of this document are. Li Jun, Liu Caiyun, Yang Shuaifeng, Sun Yan, Qu Haikuo, Jiang Yan, Liu Yitong, Zhang Xueying, Ke Haoren, Chen Jie, and Yang Chunrui. Wang Jianmin, Wang Chen, Zheng Lina, Li Rui, Zhang Yuqing, Hu Haishan, Wang Ning, Jin Hengze, Zha Qiwen, Zhang Jiahuan, Xu Li, Zhou Zhaobin, Wang Haiyang, Chu Jie Xie Jiang, Chen Wei, Liu Weihua, Kou Zengjie, Xu Xu, Jiang Shouyi, Chen Yi, Liu Yuhong, Tan Junnan, Wang Xiaoxiang, Zhang Yajing, Zhang Xin, Li Yuan, Luo Dingling, Song Liang, Zhang Xuejie, Song Botao, Wang Ping, Kong Lingwu, Cheng Luyang, and Wang Qimeng.

The number of industrial internet enterprises varies, their levels of informatization development differ, and the types of businesses they undertake are diverse, leading to different patterns in cybersecurity protection across industries. Significant differences exist, and to address the issue that existing cybersecurity protection requirements cannot meet

the actual needs of industrial internet enterprises, it is necessary to implement industrial... The document outlines the classification and grading management of cybersecurity for internet enterprises and the development of relevant standards. GB/T 44462, "Cybersecurity for Industrial Internet Enterprises," serves as a guide. The basic standards for industrial internet enterprises to carry out cybersecurity classification and grading are designed to target industrial enterprises and industrial sectors that apply the industrial internet. This paper proposes different levels of network security management and protection for internet platform companies, industrial internet identifier resolution companies, and enterprise data security. Technical requirements are used to guide enterprises in implementing security protection measures appropriate to their own level. Due to the different needs of users of the document, it is divided into four departments. Composition.

1.Protection Requirements for Industrial Enterprises Applying the Industrial Internet. The purpose is to propose protection requirements for industrial enterprises applying the Industrial Internet. The security protection requirements that need to be implemented in carrying out network security classification and grading protection work.

2.Protection Requirements for Platform Enterprises. The purpose is to propose classification and grading protection measures for cybersecurity for industrial internet platform enterprises. Safety protection requirements that need to be implemented in protection work.

3.Protection Requirements for Identifier Resolution Enterprises. The purpose is to propose cybersecurity requirements for industrial internet identifier resolution enterprises. The safety protection requirements that need to be implemented in the classification and grading protection work.

4.Data Protection Requirements. The purpose is to propose the data protection requirements for industrial internet enterprises to implement classified and graded network security protection measures. Data security protection requirements to be implemented. This document proposes data... In accordance with security protection requirements, this document outlines measures to ensure data security protection for enterprises during the implementation of network security classification and grading management, and to strengthen enterprise security. It provides guidance on building overall data security protection capabilities and improving the level of enterprise data security protection. Industrial Internet Enterprise Cybersecurity Part

1 Scope

GB/T 44462.4-2026 is the Chinese national standard covering protecting the data of an industrial enterprise - the classification of production, process and product data by sensitivity, the protection at rest and in transit, the control over what leaves the plant to a supplier's cloud and the retention and destruction. Part 4 of the series, first edition, in force

since 1 October 2026. It was issued on 31 March 2026 and takes effect on 1 October 2026, as a first edition. This page is published from the official record of the 2026 edition; the clause text of a standard this recent is not yet in circulation, and the figures, limits and tables it contains are those of the document itself, delivered in full with the English translation.

This document specifies the data security protection requirements for industrial internet enterprises, including industrial internet data classification and grading requirements, and industrial internet... Requirements for graded protection of network data throughout its entire lifecycle and requirements for data security management. This document is applicable to industrial internet enterprises when carrying out data security protection work and conducting data security assessments.

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 25069 Information Security Technical Terminology

GB/T 35273-2020 Information Security Technology - Personal Information Security Specification

GB/T 35295-2017 Information Technology Big Data Terminology

GB/T 41479-2022 Information Security Technology - Security Requirements for Network Data Processing

GB/T 41778-2022 Terminology for Big Data in Information Technology Industry

3 Terms and Definitions

The terms and definitions defined in GB/T 25069, GB/T 35295-2017 and GB/T 41778-2022, as well as the following terms and definitions, apply to this standard. document.

3.1 Data generated and collected by various industries and sectors under the Industrial Internet model.

Note. This includes any electronic or other records collected and generated during the research and development, design, manufacturing, operation and management, maintenance, and platform operation processes. The data.

3.2 data processor Organizations or entities that collect, store, use, process, transmit, provide, disclose, and destroy industrial internet data. personal.