

ICS 35.030
CCS L 80



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

GB/T 45958-2025

**Cybersecurity technology - Security framework for artificial
intelligence computing platform**

网络安全技术 人工智能计算平台安全框架

Issued on: August 1, 2025

Implemented on: February 1, 2026

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

Table of Contents

Preface	III
1 Scope	1
2 Normative references	1
3 Terms and Definitions	1
4 Security Framework	2
5 Safety Features	3
5.1 Resource layer security functions	3
5.2 Scheduling Layer Security Functions	4
5.3 Application Support Layer Security Functions	4
6 Safety Management	5
6.1 Identity Management	5
6.2 Password Management	5
6.3 Log Management	5
6.4 Security Monitoring	5
6.5 Security Audit	6
6.6 Risk Management	6
6.7 Personal Information Protection	6
7 Role Security Responsibilities	6
7.1 Overview	6
7.2 Platform Provider	6
7.3 Data Provider	6
7.4 Model Provider	6
7.5 Application Provider	7
Appendix A (Informative) Platform Composition and Security Risk Examples	8
A.1 Platform Composition	8
A.2 Security Risk Examples	8
Appendix B (Informative) Role Description and Typical Activities	11
Reference	12

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 is proposed and coordinated by the National Cybersecurity Standardization Technical Committee (SAC/TC260).

This document was drafted by: Huawei Technologies Co., Ltd., China Electronics Technology Standardization Institute, Beijing Zhongguancun Laboratory, China Telecom Co., Ltd., the Third Research Institute of the Ministry of Public Security, the National Information Technology Security Research Center, China Mobile Communications Group Co., Ltd., Sichuan University, Institute of Software, Chinese Academy of Sciences, China Electronics Great Wall Internet System Application Co., Ltd., University of Science and Technology of China, Xidian University, Beijing Volcano Engine Technology Co., Ltd., Beijing Digital Certification Co., Ltd., Ant Group Co., Ltd., Information Engineering of the Chinese Academy of Sciences Engineering Research Institute, Nanhu Laboratory, Venusstar Information Technology Group Co., Ltd., Beike Real Estate (Beijing) Technology Co., Ltd., China Power Science Research Institute Co., Ltd., Zhejiang Dahua Technology Co., Ltd., iFLYTEK Co., Ltd., State Grid Xinjiang Electric Power Co., Ltd.

Institute of Mechanical Science, Xi'an Jiaotong University, Shanghai SenseTime Intelligent Technology Co., Ltd., National Industrial Information Security Development Research Center, Huakong Tsinghua University Information Technology (Beijing) Co., Ltd., Beijing Yuanjian Information Technology Co., Ltd., Beijing Tianrongxin Network Security Technology Co., Ltd., and CloudWalk Technology Group Co., Ltd., Shanghai Information Security Evaluation and Certification Center, Beijing Kuaishou Technology Co., Ltd., National Information Center, Beijing Shuanxing Technology Co., Ltd., Zhengzhou Xindajiean Information Technology Co., Ltd., Beijing Jiaotong University, Huazhong University of Science and Technology, Midea Group (Shanghai) Co., Ltd., the First Research Institute of the Ministry of Public Security, Beijing Eyesight Technology Co., Ltd., Shenzhen Insight Wisdom Technology Co., Ltd., Beijing UnionPay Gold Card Technology Co., Ltd., State Grid Blockchain Technology (Beijing) Co., Ltd., Hangzhou Anheng Information Technology Co., Ltd., Qi'anxin Technology Group Co., Ltd.

Co., Ltd., China Electronics Technology Network Security Technology Co., Ltd., Shanghai Enflame Technology Co., Ltd., China United Network Communications Co., Ltd.

Guangdong Branch, Beijing Shanshi Network Technology Co., Ltd., Shenzhen University, Jiangsu Baowanda Software Technology Co., Ltd., Beijing Shuduke Technology Co., Ltd., China Software Evaluation Center (Software and Integrated Circuit Promotion Center of the Ministry of Industry and Information Technology), Inspur (Beijing) Electronic Information Industry Co., Ltd., Wuhan East Lake Big Data Technology Co., Ltd.

The main drafters of this document are: Ge Xiaoyu, Yan Minrui, Xu Xiaogeng, Liu Yong, Zhang Yuguang, Gu Hongxun, Zhang Kan, Xu Hao, Lu Zhen, Guo Xiaolei, Jiang Weiqiang, Zhang Feng, Zhang Rui, Chen Xingshu, Zhang Liwu, Min Jinghua, Zuo Xiaodong, Li Xinghua, Chen Yan, Yuan Jing, Guo Jianling, Zhang Yongqiang, Lin Guanchen, Wang Rui, Jing Lihua, Chen Zhiyu, Zhang Lei, Tang Wen, Wang Zitian, Jiang Faqun, Li Zhi, Hu Yue, Ma Mengna, Liu Dong, Hao Qinfen, Chen Jiong, Wang Xiaohui, Li Daoxing, Zheng Bihuang, Zhang Yu, Wen Liangjun, Wang Hong, Xie Zhenghan, Bian Chaoyi, Wu Xiaojie, Chen Jianbo, Mei Rui, Ye Bo, Yang Huiting, Zhang Yan, Lin Chenhao, Qiu Yunxiang, Yu Jinhao, Lu Yifan, Yang Tao, Wang Chao, Wang Yuchen, Wu Geng, Zhu Qianqian, Wang Yunwei, Jin Chen, Shen Chao, Wang Xueqiang, Yan Jianhui, Lei Xiaofeng, Yang Xiansen, Zhang Junyan, Ren Yongpan, Luo Hongwei, Gu Chen, Zhang Heng, Wang Hejun, Li Ang, Liu Yuhong, Liu Weihua, Wang Wei, Liu Jingkai, Li Ruixuan, Cai Yasen, Wang Zhaohao, Liu Jun, Yang Chunlin, Yao Ming, He Hao, Peng Yuxiang, Hu Shiyang, Yang Bo, Wang Dong, Yang Ke, Liu Bo, Li Jianfeng, An Jincheng, Cao Zhantao, Mei Jingqing, Wang Sishan, Zeng Chuxuan, Cheng Wei, Wu Jiang, He Yisheng, Liu Weili, Xie Jiang, Ge Song, Jin Yinyu, Liu Yunlong, Gao Guolu, and Du Le. Cybersecurity Technology Artificial Intelligence Computing Platform Security Framework

1 Scope

This document establishes the security framework of the artificial intelligence computing platform and specifies security functions, security management, and role security responsibilities.

This document applies to the design, construction, application, and operation and maintenance of artificial intelligence computing platforms.

2 Normative references

GB/T 22239-2019

GB/T 31168-2023

GB/T 35273-2020

GB/T 41479-2022

3 Terms and Definitions

The following terms and definitions apply to this document.

3.1

Provides a software and hardware system with efficient and scalable resource environment and supporting components for the development and operation of artificial intelligence

applications.

Note. Artificial intelligence computing platforms are usually used in data centers and edge computing scenarios.

3.2 [Source. GB/T 42018-2022, 3.5, with modifications]

A server that provides high-performance computing processing capabilities for artificial intelligence applications.

Note. AI servers usually integrate AI acceleration processors (3.3), AI acceleration cards (3.4) or AI acceleration modules (3.5) to meet the requirements of Accelerated computing needs for artificial intelligence applications.

3.3 [Source. GB/T 42018-2022, 3.8, with modifications]

An integrated circuit with a computing microarchitecture adapted to artificial intelligence algorithms and capable of accelerating computing processing for artificial intelligence applications.

Note. Typical AI acceleration processors include graphics processors, neural network processors, and tensor processors.

3.4 The extended acceleration component of the computing microarchitecture

Designed specifically for AI computing, it complies with the AI server (3.2) hardware interface and integrates an AI acceleration processor (3.3) or