

ICS 35.030

CCS M 10



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

GB/T 47324-2026

**Cybersecurity protection requirements for internet of vehicles
platforms**

车联网平台网络安全防护要求

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

1	Scope
2	Normative references
3	Terms and definitions
4	Abbreviated terms
5	Security protection content
6	Level 1 security protection requirements
6.1	Physical environment security requirements
6.2	Security management requirements
6.2.2	Security management organizations and personnel
6.2.3	Platform security construction management
6.3	Security technical requirements...
7	Level 2 security protection requirements...
7.1	Physical environment security requirements...
7.2	Security management requirements...
7.3	Security technical requirements...
8	Level 3 security protection requirements...
8.1	Physical environment security requirements...
8.2	Security management requirements...
8.3	Security technical requirements...
9	Level 4 security protection requirements...
9.1	Physical environment security requirements...
9.2	Security management requirements...
9.3	Security technical requirements...

1 Scope

GB/T 47324-2026 is the Chinese national standard covering the platform behind a connected fleet - the authentication of vehicles and users, the isolation of the command paths that can act on a vehicle, the protection of the location and behaviour data collected, the monitoring and the incident response. A compromise of this platform reaches every vehicle connected to it, which is why the document runs to 22,000 words. 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 cyber security protection requirements for internet of vehicles platform, including Level 1, Level 2, Level 3, Level 4 and Level 5 requirements for physical environment security, security management and security technology. This document applies to intelligent and connected vehicle manufacturers, internet of vehicles platform operators and other relevant organizations in carrying out graded cyber security protection of internet of vehicles platforms.

2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

GB/T 22239, Information security technology - Baseline for classified protection of cybersecurity

GB/T 25069, Information security technology - Glossary

3 Terms and definitions

Terms and definitions determined by GB/T 25069 and the following ones are applicable to this document.

3.1 internet of vehicles Complex network and related systems that, through next-generation network communication technologies, achieve deep integration with the automotive, electronics, road traffic and transportation sectors, and achieve comprehensive interconnection and information interaction among vehicles, roads, people, and platforms, thereby enhancing driving safety, transportation efficiency and services, and supporting the development of automated driving.

3.2 common middleware A type of software that facilitates interaction among software components and provides connections between system software and application software.

Note. It mainly includes microservice middleware, message middleware, web service middleware, etc.

3.6 sensitive personal information Personal information that, once leaked or used illegally, may lead to discrimination against vehicle owners, drivers, passengers, people outside the vehicle, etc., or serious harm to their personal or property safety.

Note. This includes vehicle movement trajectory, audio, video, images and biometric information.

4 Abbreviated terms

For the purposes of this document, the following abbreviated terms apply. CPU. Central Processing Unit DTC. Diagnostic Trouble Code FTP. File Transfer Protocol HTTP. Hyper Text Transfer Protocol HTTPS. Hypertext Transfer Protocol Secure IP. Internet Protocol OTA. Over-the-Air POP

3.Post Office Protocol-Version 3 SMTP. Simple Mail Transfer Protocol SSL. Secure Socket Layer TLS. Transport Layer Security VIN. Vehicle Identification Number

5 Security protection content

Enterprises involved in internet of vehicles platforms shall determine the cyber security protection classification of IoV platforms and take security protection measures to ensure cyber security of IoV platforms. In terms of security protection content, the security protection of IoV platforms is divided into three categories. physical environment security requirements, security management requirements, and security technology requirements. Physical environment security requirements include physical location selection, physical access control, protection against theft and vandalism, lightning protection, fire protection, water and moisture protection, electrostatic discharge protection, temperature and humidity control, dust protection, power supply, and electromagnetic protection. Security management requirements include security management systems, security management organizations and personnel, platform security construction management, and platform security operation and maintenance management. Security technology requirements include infrastructure security protection and application service security protection. Infrastructure security protection includes requirements for computing environment security protection, communication network security protection, security protection of zone boundaries, security management center, virtualization security protection, container security protection, common middleware security protection, and general-purpose interface security protection. Application service security protection includes general requirements, requirements for software update services, remote control, remote monitoring, remote diagnosis, and charging management and monitoring.

6.1 Physical environment security requirements

6.1.1 Physical location selection Requirements for physical location selection shall include the following.

- a) Requirements for the basic site selection conditions of the computer room shall comply with the provisions for Level 2 specified in GB/T 22239;
- b) The computer room shall be located away from areas prone to geological disasters, such as mudslides and landslides;

c) The load-bearing capacity of the computer room shall meet the requirements for the computer room building.

6.1.2 Physical access control Requirements for physical access control shall include the following.

- a) Requirements for the management of computer room entrances and exits shall comply with the provisions for Level 2 specified in GB/T 22239;
- b) Visitors requiring access to the computer room shall be subject to an application and approval process, and their activities shall be restricted and monitored.

6.1.3 Protection against theft and vandalism Requirements for protection against theft and vandalism shall include the following.

- a) Requirements for the protection of equipment against theft and vandalism shall comply with the provisions for Level 2 specified in GB/T 22239;
- b) Major equipment shall be placed in the computer room;
- c) Media shall be classified and labeled, and stored in media or archives rooms;
- d) Necessary anti-theft alarm facilities shall be installed in the main computer room.

6.1.4 Lightning protection Requirements for lightning protection shall include the following.

- a) Requirements for lightning protection of various cabinets, facilities and equipment shall comply with the provisions for Level 2 specified in GB/T 22239;

6.2 Security management requirements

6.2.1 Security management systems Requirements for security management systems shall include the following.

- a) Security management systems appropriate to the current operational conditions of the internet of vehicles platform operators shall be established, including routine management and operation procedures, emergency response mechanisms, update service procedures;
- b) Security management systems shall be formally and effectively issued and shall be subject to version control.

6.2.2 Security management organizations and personnel

6.2.2.1 Requirements for security management organizations Requirements for security management organizations shall include the following.

- a) Requirements for post establishment, personnel allocation, authorization and approval shall comply with the provisions for Level 1 specified in GB/T 22239;
- b) Dedicated positions for the internet of vehicles platform, such as system administrator