

Contemporary Amperex Technology Co., Limited

Information Security Management Policy

1. Purpose

This Policy aims to clarify the information security management responsibilities and strategies of Contemporary Amperex Technology Co., Limited ("CATL"), control information security risks, and ensure the confidentiality, integrity, and availability of the Company's information.

2. Scope

This Policy applies to CATL, its branches, and its controlling subsidiaries (collectively, the "Company"), as well as the Company's employees, suppliers, and partners. It covers CATL's information security management system requirements, management responsibilities, internal audits, and improvements to the information security management system.

3. Governance Structure

CATL has established a Security and Confidentiality Committee, under which a Security and Confidentiality Office oversees the Company's information security and confidentiality management. The Office comprises four teams - security and confidentiality management, operations, technology, and supervision - and works with external professional security firms, consultancies, and audit bodies to build a

comprehensive information security defense covering all of the Company's production bases.

4. General Principles

Guided by the information security policy of "risk-focused, prevention-oriented, awareness-led, combining technology with management, and engaging all employees", the Company places high priority on information security management.

Drawing on international best practices in its business operations, the Company is building a data security management system of high standards and full coverage that meets regulatory requirements, laying a solid information security foundation for serving customers at home and abroad.

5. Control Measures

5.1 Security and Confidentiality Management

5.1.1 The Company has established, implemented, maintained, and continuously improved its Information Security Management System (ISMS), ensuring that all employees understand and comply with the ISMS requirements and continually improving the effectiveness of the system.

5.1.2 The Company upholds the principle that all employees share responsibility for confidentiality. Through institutional regulations, ongoing training, and cultural promotion, it deeply integrates security and confidentiality requirements into the job responsibilities of each position. Through annual information security training and assessments, the Company continuously enhances employees' security awareness and protective capabilities.

5.2 Security and Confidentiality Operations

5.2.1 The Company regularly conducts security and confidentiality risk assessments in collaboration with CCRC-certified organizations. For example, it performs security assessments on live environments through simulated hacker attacks to test the effectiveness of existing defense mechanisms, identify and remediate potential security vulnerabilities.

5.2.2 The Company conducts annual business continuity management activities. Through interviews and incident analysis, it assesses the current state of business continuity management, performs gap analyses based on applicable national standards, client audit requirements, and industry best practices, develops an overall business continuity management plan.

5.2.3 The Company has established a supply chain security management mechanism covering its partner ecosystem. From admission assessments, contractual obligations to ongoing oversight, the Company works with external partners to jointly build a secure and trustworthy collaborative environment, and continuously provides information security training to suppliers.

5.3 Security and Confidentiality Technology

5.3.1 The Company is committed to building a proactive and intelligent security defense system. It enhances the efficiency of security operations by leveraging threat intelligence analysis and automated response mechanisms, and continuously strengthens overall security resilience through regular offensive and defensive drills.

The Company continuously updates and improves its security and confidentiality technologies.

5.3.2 To achieve and maintain protection of the Company's data, and to ensure that data receives an appropriate level of protection against unauthorized access, tampering, or destruction, security controls are integrated throughout the entire data lifecycle - including data collection, encrypted transmission, encrypted storage, encrypted external transmission, use, sharing, and destruction - to prevent leaks and ensure that only authorized users can modify or access sensitive information.

5.4 Security and Confidentiality Supervision

5.4.1 Group-Level Management: To ensure the effective implementation of risk management measures, the Company has established a comprehensive information security audit system. The Company conducts at least one internal audit of the information security management system and one third-party information security audit annually (including ISO/IEC 27001 audits, TISAX certification, Cybervadis certification, etc.).

5.4.2 Supply Chain Management: The Company regularly conducts security and confidentiality audits of the supply chain, provides guidance to suppliers on corrective actions and improvements, strengthens the prevention and control of security and confidentiality risks in the supply chain.

5.4.3 The Company has established a monitoring and reward/punishment mechanism. If internal employees or third-party personnel discover security incidents, vulnerabilities, or risks, they shall handle them in accordance with the incident handling procedures or the incident emergency response mechanism, document the incident process and outcome, analyze the causes of the incident, draw lessons learned, and formulate preventive measures.

6. Appeals and Handling Procedure

You may report the following to the SSO mailbox (SSO@catl.com):

- 1) Objections regarding your understanding of this policy or affected decisions;
- 2) Reports of security and confidentiality vulnerabilities and risks;
- 3) Reports of security and confidentiality violations by CATL employees or related incidents;
- 4) Other leads regarding information leaks or theft of confidential information.

7. Policy Revision and Effective Date

This policy takes effect on the date of its issuance and will be revised in a timely manner in the event of significant changes to the Company's information security organizational structure, internal and external environment, information security risks, and relevant laws and regulations, or in the event of significant changes to the Company's business processes.

Contemporary Amperex Technology Co., Limited

September 2026