Information Security Policy

Purpose

Delton Technology is committed to ensuring the confidentiality, availability and integrity of information. Adhering to the information security policy of "improving information security technology, enhancing information security awareness, strictly abiding by information security policies, and reducing information security risks", Delton Technology 's "Information Security Policy" was released in January 2026 as the core guiding principle to build a credible, secure and sustainable digital cornerstone for all stakeholders.

Scope of application

This policy applies to Delton Technology (Guangzhou) INC. and its subsidiaries.

Our Principles and Positions

(1) Delton commitment

Delton Technology is committed to strictly abide by relevant national and industry laws and regulations on information security, as well as all customer confidentiality agreements, and continuously improve information security technology and improve information security strategies through information security risk assessment.

Delton Technology promises to strengthen information security education for employees at all levels, reduce information security risks, and prevent major information leakage incidents. Compliance with the ISO 27001 information security standard is one of the key objectives of our efforts to meet stakeholder expectations.

(2) Information security governance

Led by the general manager, the information security management team is formed by the top persons in charge of the information center, human resources center, marketing center, finance center, quality center, equipment and facility center, engineering technology center, research institute and other relevant departments, responsible for supervising and reviewing the information security of

Delton Technology, and formulating strategies and coordinating the implementation of information security work in various departments.

Functional departments need to perform information security protection responsibilities in daily operations according to their duties to ensure the implementation of information security protection.

All employees are responsible for information security protection, including but not limited to information security incident reporting and compliance with confidentiality agreements.

(3) Data protection

Technologies including but not limited to dual-link redundant network architecture, gateway firewall, terminal antivirus, intrusion situational awareness platform, server redundant backup, and end-to-end encryption are used to ensure the stability, integrity, and confidentiality of data transmission and storage, and realize real-time threat monitoring and rapid response.

Implement management methods such as hierarchical and classified information management, strict approval processes, and least privilege control to ensure that confidential information is only accessible to authorized full-time personnel.

Regularly perform routine maintenance such as upgrading firewalls and antivirus software, scanning for viruses, checking server hardware and software, and verifying data integrity to ensure terminal security and data integrity.

(4) Information security risk monitoring and continuous improvement

Formulate information security risk management procedures in accordance with the "Information Security Technology Information Security Risk Assessment Specification" (GB/T 20984-2022) and other domestic and international recognized standards, regularly identify information security risks and continuously improve them.

Regularly conduct security vulnerability scans and attack and defense drills to detect and fix potential security risks in a timely manner and continuously enhance overall security response capabilities.

Conduct regular internal audits and ISO 27001 management system assessments to verify compliance with policies and standards, and drive continuous improvement of internal information security systems and management systems.

(5) Employee awareness and training

Regularly carry out information security training and assessment covering all employees, and strengthen employees' awareness of confidentiality and data operation standards.

(6) Supplier information security management

Suppliers must sign a confidentiality agreement with the company and complete information security training annually. All supplier visits must be registered in advance, accompanied by the corresponding procurement personnel throughout the process, and unauthorized entry into the information security area is strictly prohibited.

All suppliers must sign a confidentiality agreement before accessing the company's system, accept the behavior supervision carried out by Fortress Machine, and pass the company's information security qualification review and regular audit. Clarify supplier data protection responsibilities to ensure compliance and improvement of their data protection capabilities.

(7) Customer information security management

The transmission and storage of customer information are managed by full-time personnel, and the information center implements access authorization, password policies and backup mechanisms to ensure that customer privacy data is controllable throughout the life cycle.

Policy Issuance and Review

This policy has been reviewed and approved by the General Manager of Delton Technology Group, and its implementation will be subject to ongoing supervision. Following its issuance, the Information Security Management Team and the ESG Office will conduct periodic reviews and revisions based on changes in the external environment, laws, regulations, and other relevant factors. Any amendments shall be released after review and approval by the Group General Manager.