FIC Global Inc.

Information Security Policy

Established on June 1, 2023

Article 1 (Purpose of the Policy)

In light of the fact that information security is the foundation for maintaining the safe operation of various services, in order to ensure that FIC Global Inc. (hereinafter referred to as "the Company") has a shared commitment to implementing information security, and in accordance with Article 9 of the "Regulations Governing Establishment of Internal Control Systems by Public Companies" regarding "Computerized Information System Processing," as well as adherence to the management framework of ISO 27001 Information Security Management System, this Information Security Policy (hereinafter referred to as "this document") is established as the highest guiding principle for the Company's information security management system.

Article 2 (Objectives)

The Company's information security objectives are to ensure the confidentiality, integrity, availability, and compliance of the core system management business. Quantitative indicators are defined and measured for each level and function to assess the implementation status of the information security management system and whether the information security objectives are achieved.

- Confidentiality: The Company shall avoid disclosing any sensitive information of the Company on the internet.
- Integrity: Ensure the accuracy of the Company's sensitive data (e.g. customer data, personal data).
- Availability: Ensure that important data held by the Company are properly backed up.
- Compliance: Relevant laws of Taiwan (e.g., Personal Data Protection Act, Trade Secrets Act, intellectual property rights-related laws) shall be followed to prevent infringement of the rights of the Company or third parties.

Article 3 (Applicable Parties)

This "Information Security Policy" applies to all employees of the FIC Group who share the computer room and ERP system.

Article 4 (Dedicated Unit for Information Security Management)

The dedicated unit responsible for managing information security matters within the Company is the Information Security Management Department, which leads the operation of the "Information Security Management Committee" to promote and maintain various information security management, execution, and auditing tasks.

Their powers are as follows:

I. Formulate and revise information security policies, goals, and systems.
II. Follow the ISO 27001 framework for information asset risk management and the implementation and auditing of the information security system.
III. Responsible for promoting the Company's information security policy, implementing security mechanisms, and enhancing the information security awareness of employees.
IV. Responsible for formulating the preservation of all documents, files, and electronic records related to information security policies.
V. Responsible for planning, evaluating, and conducting regular drills for the business continuity plan.
VI. Establish and implement an incident reporting mechanism for information security incidents.
VII. Internal promotion and publication of information security messages, along with training on related protective awareness and advocacy.
VIII. Collect, receive, and update external legal regulations and standard information, and timely release it to internal colleagues, including important information that may affect business operations and information security.
IX. Cross-departmental communication and coordination on information security issues.
X. Cooperate with the auditing team from the accounting firm and external professional verification agencies to conduct audits and verifications of information security management, implementing related improvements based on their recommendations and continuously following up.

Article 5 (Principles of Implementation)

The implementation of the information security management system should follow the Plan, Do, Check, and Act (PDCA) cycle model, ensuring an ongoing and incremental spirit to maintain the effectiveness and sustainability of information security.

- This policy shall be reviewed annually to reflect changes in government regulations, technological developments, business needs, and stakeholder influences, ensuring the achievement of information security operational goals.
- Protect information related to the Company's business activities, strengthen data security, and prevent unauthorized access and inappropriate use such as tampering.
- Information assets (including software, hardware, network communications, data, and personnel) shall be adequately protected and evaluated for risks on a regular basis every year for improvement.
- Establish backup recovery measures, conduct regular drills, and ensure that the Company¡s important information management systems remain stable and available for use.
- Implement automated information security monitoring and enhance defensive alert capabilities to reduce unauthorized intrusions, malicious damage, or disclosure of information.
- Ensure standardized operational procedures for daily operations are effectively implemented, and conduct regular internal and external audits to ensure the effectiveness of internal control systems and related procedures.
- All information security incidents or suspicious security events should be reported immediately in accordance with the "Information Security Incident Management Procedures", allowing the responsible unit to investigate and address the matter.
- Third-party contractors and visitors must comply with the "Third-Party Management Procedures". If they come into contact with the Company's related information, they should sign the "Third-Party Non-Disclosure Agreement" to protect the security of the Company's information assets.
- Provide information security education and training to strengthen employees' awareness of information security and their understanding of related responsibilities.

Article 6 (Review and Evaluation)

I. This document shall be evaluated and reviewed at least once a year, considering the latest conditions regarding laws and regulations, technological changes, stakeholder expectations, business activities, internal management, and resources, to ensure the effectiveness of information security practices.
II. This document shall be revised based on the review results and issued by the Chairman of the Information Security Committee before it becomes effective.
III. After this document is established or revised, it should be communicated to stakeholders, such as employees, suppliers, customers, and external auditors, in an appropriate manner (e.g., via email, website announcement, or printed copies).
IV. Information security-related files and documents shall be backed up and stored in a safe place.

Article 7 (Information Security Manual)

According to the Company¡s "Information Security Policy" and related regulations, an "Information Security Manual" has been established as the guideline for the Information Security Management System (ISMS). For details, please refer to the issued ISMS-01-02_ Information Security Manual.