Information Security

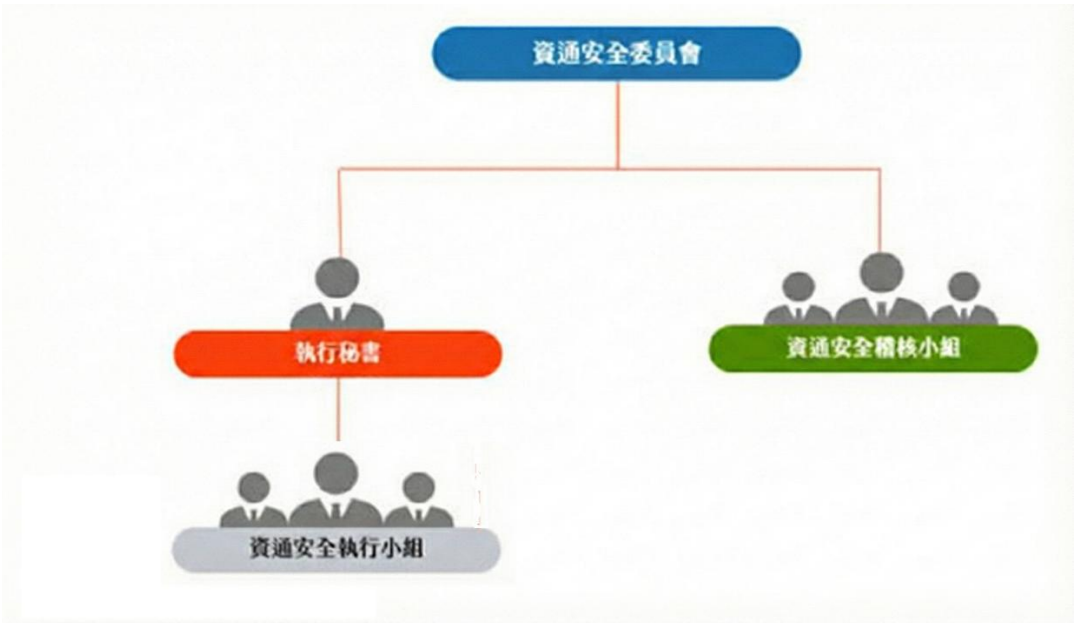
一、Information Security Management Strategy and Framework

The Company views information operations as a crucial part of daily operations. To ensure the security of assets such as data, equipment, personnel, and networks, a comprehensive information security management strategy and framework have been established.

(一) Information Security Risk Management Framework

To effectively promote information security governance, the Company has established a cross-departmental "Information Security Committee" as the highest authority responsible for coordinating policy formulation, execution, and risk management regarding information security and protection.

1. **Organizational Structure：**
    - **Information Security Committee:** Chaired by the General Manager, with third-level managers serving as committee members, and the highest executive of the IT Department acting as the convener. The committee meets as needed to formulate and evaluate security policies and supervise reviews of security incidents.
    - **Executive Secretary:** Appointed by a designated person from the Convener of the Information and Communications Security Committee. In charge of overall management, coordination, and supervision of the information and communications security-related tasks decided by the Committee and the operation of the execution team.
    - **Information and Communications Security Audit Team:** Conducts internal audits of information and communications security, submits audit reports, tracks the status of improvements and the correction of deficiencies.
    - **Information and Communications Security Execution Team:** Served by the company's IT department as a standing information security team , responsible for daily security monitoring, maintenance of IT software, hardware operations, and equipment. It also handles related training and education for information and communications security, and executes the notification and emergency response procedures for security incidents.



2. **Operational Mechanism (PDCA Management Cycle)**：
   The Company ensures the effectiveness of security management based on the Plan-Do-Check-Act (PDCA) cycle：
   - **Plan (Organization & System):** Establishment of the Information Security Committee, formulation of security guidelines, and compilation of standard operating procedures and work instructions.
   - **Do (Information Security Operations):** Execution of security advocacy, training, information classification management, operation security controls, disaster recovery drills, and preservation of evidence for security incidents.
   - **Check (Analysis & Review):** Analysis of security incidents and causes of deficiencies, security threat warnings, and tracking of improvement progress.
   - **Act (Information Security Assessment):** Implementation of security into daily operations and internalization into organizational culture through daily inspection records, KPI reviews, and internal/external audits.

(二) Information Security Policy

The Company formulates its information security policy in accordance with the "Guidelines for Information Security Control of Listed Companies" issued by the Financial Supervisory Commission. The policy goal is to ensure information assets are protected from internal or external, intentional or accidental threats and destruction, avoiding alteration, disclosure, destruction, or loss of business information.

(三) Concrete Management Measures

To implement the security policy, the Company adopts several concrete measures：

1. **Network and Operation Security Control:** Establishing control mechanisms for IT operations, regulating network access and equipment maintenance, and implementing information classification and management.
2. **Disaster Recovery Mechanism:** Conducting periodic disaster recovery drills to ensure information systems can rapidly resume operations during major accidents.
3. **Incident Reporting and Evidence Preservation:** Establishing procedures for handling security incidents, including evidence preservation and deficiency analysis, to ensure effective response when incidents occur.
4. **Continuous Improvement:** Conducting regular daily security inspections and reviewing the compliance and effectiveness of security management through internal and external audit mechanisms.
5. **External Security Rating Monitoring:** Using a third-party security platform to manage the Company's external security risks; the current score is maintained at a low-risk level of over 90 points, with no medium or high risks.

二、Resources Invested in Information Security Management

The Company attaches great importance to information security investment. The main resources invested are as follows：

1. **Dedicated Organization and Manpower：**
   - Establishment of the "Information Security Committee" and a permanent "Information Security Executive Team," with dedicated personnel from the IT Department responsible for daily operations and monitoring.
   - Establishment of an "Emergency Response Team" responsible for immediate response to major incidents.
2. **Education, Training, and Advocacy**：
   To enhance the security awareness of all employees, training and advocacy are conducted regularly. Implementation status in recent years：
   - **Irregular Advocacy:** Issuing internal announcements regarding the latest security threat warnings and precautions.
   - **2025/06/30:** General Information Security Video & Test (Course duration: 2 hours).
   - **2025/11/19:** Online advocacy courses on "Prevention of Insider Trading" and "Integrity Management, Intellectual Property Rights, and Trade Secret Protection."

三、Major Information Security Incidents

In the most recent year and up to the present, the Company has not suffered any major losses or impact on operations due to major information security incidents (such as hacker intrusion, virus infection, data leakage, etc.).

四、Information Security Risks and Countermeasures

(一) Information Security Risk Assessment

With the development of digital technology, corporate security risks (including cyberattacks, ransomware, system vulnerabilities, etc.) are becoming increasingly complex. Although the Company has established protective measures, it cannot guarantee complete immunity from all malicious software or hacker attacks. Potential risks may include：

1. **Operational Interruption:** Attacks on core systems could lead to temporary suspension of business.
2. **Data Leakage:** Theft of confidential information or personal data could affect the Company's reputation and violate laws.

(二) Countermeasures

To reduce the aforementioned risks, the Company adopts the following strategies：

1. **Multi-layered Defense:** Constructing a defense-in-depth network by combining firewalls, endpoint protection, intelligent security operation platforms, and permission controls.
2. **Backup and Recovery:** Implementing data backup mechanisms and regular disaster recovery drills to ensure data availability.
3. **Continuous Monitoring:** Detecting potential threats early and handling them through daily monitoring and anomaly alerts.
4. **Joining Joint Defense Organizations:** Joining the government's TWCERT/CC information sharing organization to obtain security warning intelligence, threat updates, and vulnerability information.