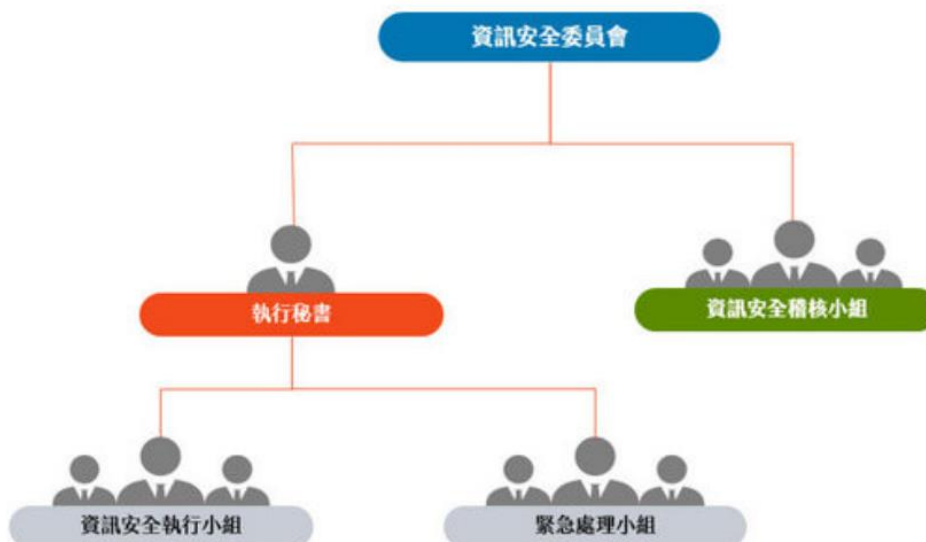# Information Security

Information processing is an important part of the company's daily operations. Silitech is committed to safeguarding the security of the company's information assets such as information, equipment, employees, and networks, and to prevent internal and external threats, damages, deliberate or accidental. Therefore, The scope of information security at the company formulates Information Security Policy encompasses employees, clients, suppliers, and shareholders and all IT software and hardware associated with its business activities that is not only for the IT department's reference in planning, implementing and evaluating information business, but also should be followed by all employees.

The Silitech's Information Security Policy is based on the Information Security Regulations established by the Executive Yuan and its affiliated agencies, and refers to various rules of standard operating procedures and work instructions issued by the Silitech. The abstracts are the following:

1. **To establish the「Information Security Committee」**

    「Information Security Committee」has the supreme authority on the company's information security. The general manager is the chairman of the committee, the third-level directors of the company are the members of the committee, and the director of the IT department is the convener. The information security meeting will be hosted as needed.

    Its missions are to formulate and evaluate the company's information security policies or information incidents review and supervision of security matters.

2. **To organize Information Security Team**

    It is composed of the company's IT department team members. It's responsible for information security monitoring and to ensure company's information systems running

normally include software and hardware, and equipment maintenance.

3. **To establish information security guidelines**

Based on the Silitech's Information Security Policy, to prepare standard operating procedures and work instructions as a basis for daily information security operations.

4. **To training and publish information security propaganda regular**

The Information Security Team should host information security training to improve employees' knowledge of information security and provide the best practice of their working which related to information security.

To make information security announcements regular, let all employees know about the latest information security threats and what they should be noticed.

Information Security Training Course :

Course Title	Date	Hours
Information Security Training Course	2020/11/19	10:00-11:00 (1 hr)
Information Security Training Course & Prevention of Insider Trading	2021/10/26	13:30-15:30 (2 hr)

Implementation of Information Security Management Blueprint

Organization & system
Establish the Information Security Committee.
Organize Information Security Team.
Establish information security guidelines.
Prepare information operating specification.

Information security operations
Information security promotion and training.
Establish information classification and management.
Information Operations Security Control Disaster Prevention Exercise.
Security incident evidence preservation.

Information security audit
Record daily security inspections and reviews.
Audit information security indicators(KPI).
Internal audit.
External audit.

Analysis & inspect
Analysis of information security incidents.
Analyze the reasons for the lack of information security.
Improved tracking of security incidents.
Security threat warning.

Implementation in daily work.
Internalized in organizational culture.