# Information Security Management

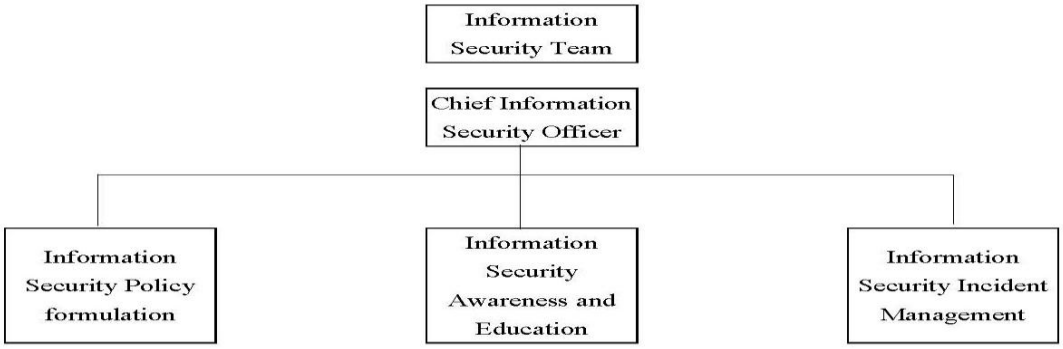
**Regulations on implementing information security protection, actual implementation, and response measures:**

- **Information Security Risk Management Group**

**Through the establishment of an information security management system and a dedicated unit (Information Division), the scope of application covers the Company, its subsidiaries, clients, and suppliers. This unit focuses on the implementation of improvement of information security protection, detection, promotion, and education. In compliance with relevant government regulations and in accordance with company policies, we are committed to safeguarding data security and privacy rights. Efforts are made to strengthen information security protection, to conduct security testing, to promote awareness, and to provide education on information and communication security. By regularly reporting the information management status in the monthly internal operation meetings and quarterly board meetings, the Group assigned dedicated personnel to carry out management and organization to ensure the normal operation of information systems. To reduce security incidents and assure information preservation, the Group also regularly upgrades software and hardware to safeguard the confidentiality, integrity, and availability of the Group's data and personal information.**

- **To ensure the protection and management of personal data, the Group stipulated the "Personal Data Protection Act" (simplified as PDPA) on August 12, 2024.**

**The main powers and responsibilities of this group are as follows:**




**Information Security Policy Setting Group: Responsible for the formulation of various security policies, and continues to make adjustments to relevant policies according to information technology and the law and regulations.**

**Information Security Promotion Education Group: Responsible for educating and training employees on the company's information security policy, and conducting tests to assess their understanding of relevant information security concepts.**

**Information Security Event Handling Group: Responsible for handling the company's information security incidents and emergency repair during zero-time difference attacks.**

- **Information Security Policy**

**(1) Network connection policy measures:**

**The company's external connection, open host, wireless network services, VPN connection policy, and vulnerability detection.**

**(2) Data backup policy measures:**

**The backup mode adopts three modes: local backup, remote backup, and offline backup.**

**(3) Data backup verification measures:**
**Local backup, same factory backup in different places, remote backup in different places, and offline backup.**

**(4) E-Mail information security policy measures:**
**Set relevant email processing policies, company filtering email policies, information security promotion, and email information security usage guidelines**

**(5) Confidentiality device disposal measures:**
**In order to ensure that the data is not leaked when the company stores important data due to failure or replacement of the equipment, this method is specially formulated to provide a basis for handling various information products when selling various information products.**

- **Information Security Specific Management Plan, Implementation and Goals**
- **Palo Alto Network Firewall**

  **All kinds of abnormal network uses are prevented to safeguard the security and smoothness of the Group's external network and reasonably manage employees' online access, thereby improving the use in line with the Control of Information Security Inspection.**
- **Chunghwa Telecom hinet Enterprise Information Services**

  **Chunghwa Telecom Network Security Service is introduced to prevent more than 99% of outbound cyberattacks to ensure the safety of the company's information environment and compliance with the Control of Information Security Inspection.**

- **Tahsin ERP Backup System**

  **The Group has established an information management backup system to ensure the security and sustainable development of corporation operation system. Recovery procedures are rehearsed regularly every year to ensure personnel's technical implementation and experience inheritance of personnel as well as the compliance with the Control of System Recovery Plan and Test Program.**

- **ArmorX Email Protection System**

  **Spam management mechanism has been established to block outbound spams and defense against malicious email, prevent and reduce various information security risks and ensure the compliance with the Control of Information Security Inspection.**

- **The Group’s Email Backup System**

  **The Group has established an online backup system for the Group's e-mail system, so as to ensure the security of the e-mail system and consistent compliance with e-mail- related regulations, and store historical e-mails for ten years for the sake of inquiry and reference of transaction information. The backup system is in line with the Control of System Recovery Plan and Test Program.**

- **Anti-virus System**

  **Internal computer anti-virus treatment mechanism and intrusion detection have been established to prevent hacker attacks and ensure the effective access to computer resources and compliance with the Control of Information Security Inspection.**

- **The Group's File Backup Mechanism**

  **The Group carried out on-site backup, remote backup in the same plant, remote backup in different plants, and offline backup. The Group utilized online drives and external hard drives to regularly backup and verify data everyday, to ensure the access control of data and the security of account/password management.**

- **Resources, Implementation, and Objectives for Information Security Management**

  **(1) Dedicated Personnel**

  **A dedicated information security unit (Information Division) has been established. The information security task force consists of four members responsible for the planning of information security strategies, the implementation of security technologies, and the auditing of information security internal control systems, aiming to maintain and continuously enhance cybersecurity.**

  **(2) Information Security Meetings**

  **Internal information security review meetings are held weekly. Execution results are reported during monthly management meetings, and a comprehensive information security governance report is submitted to the Board of Directors on a quarterly basis.**

  **(3) Customer Satisfaction**

  **No major information security incidents have occurred, and there have been no complaints related to customer data loss.**

**(4) Security Announcements**

**Important information security regulations and reminders are communicated on an ad-hoc basis through the company's internal email platform and the Tahsin Web Portal.**

**(5) Information security education, promotion and implementation:**

**2024**

| Education and promotion (video conference) | Hours | Number of people |
|---|---|---|
| Social engineering and network camera cybersecurity | 1.5H | 167 |
| Social engineering and generative AI | 1.0H | 75 |

**Until the end of March, 2025**

| Education and promotion (video conference) | Hours | Number of people |
|---|---|---|
| Social engineering and personal information security | 1.0H | 176 |

| Social engineering drill test results | | Employees tested | | |
|---|---|---|---|---|
| Execution date | Content | Total number | Number | Percentage |
| 2024/03/18 | Clicking links | 248 | 24 | 9.6% |
| | Entering data | | 9 | 3.6% |
| 2024/10/16 | Clicking links | 221 | 7 | 3.1% |

| | | | | |
|---|---|---|---|---|
| | **Entering data** | | **4** | **1.8%** |
| **2025/03/10** | **Clicking links** | **221** | **12** | **5.4%** |
| | **Entering data** | | **2** | **0.9%** |
| **2025/03/17** | **Clicking links** | **221** | **4** | **1.8%** |
| | **Entering data** | | **2** | **0.9%** |

- **2025 Information Security Implementation Objectives:**

  **1. Continuously monitor information security status and follow up on the handling of information security cases.**

  **2. Regularly assess information security systems and adjust strategies to ensure effectiveness and protection.**

  **3. Enhance employee information security awareness by arranging two training sessions annually, and ensure compliance with relevant regulations during daily operations and business executions to maintain system stability and security.**

  **4. Strengthen the protection of potential operational risks by establishing access control and encryption measures to safeguard information systems and related assets, and prevent the leakage of the Group's sensitive data.**