Information Security Management

(I) Describe the cyber security risk management framework, the cyber security policy, the specific management plan and the resources invested in the cyber security management, etc.

1. Cyber security risk management framework:
   (1) The Company has appointed an information security officer, established an information security office, and assigned an information security manager and personnel (see the company organization chart).
   (2) The Information Security Office is responsible for the planning and promotion of the Group's information security system, technical evaluation, education and training, supervision and auditing to strengthen information security risk control.
   (3) Cyber security management task: The Information Security Office is responsible for promoting cyber security management to implement cyber security management control measures.
2. Cyber Security Policy:
   (1) To improve employee awareness, prevent data leakage, and implement daily maintenance to ensure the confidentiality, integrity, availability, and compliance of the core system management business.
3. Specific management plan
   (1) The Information Security Office shall organize regular information security risk assessments, set priorities based on the magnitude of the risk impact and the cost required to reduce the risk, adopt the Plan-Do-Check-Act (PDCA)

approach to structure multi-layer information security defense, and establish information security key performance indicators.

(2) By joining the Joint Security Organization, we can obtain external information sharing and information security incident assistance channels in a timely manner.

A. Taiwan Information Security Officers Consortium (CISO)

B. Taiwan Computer Emergency Response Team / Coordination Center (TWCERT/CC)

C. Science Park Information Sharing and Analysis Center (SPISAC)

4. Resources invested in the cyber security management

(1) Regular server and PC-related vulnerability patching is performed to reduce the risk of equipment exposure.

(2) Vulnerability scanning and penetration testing

A. We conduct annual vulnerability scanning and penetration testing of the Group's network equipment, applications and products.

(3) Annual cyber security education training, and anti phishing drills

A. The Group conducts education and training on cyber security, educates employees on the identification of phishing emails, conducts phishing drills, and analyzes the results of the drills to develop improvement measures to continuously raise the awareness of all employees on information security.

B. Every year, senior management will receive cyber security education training to integrate the awareness of information security into daily management.