Cybersecurity management

(I) Describe the cyber security risk management architecture, cyber security policy, specific management solution and resources invested in cyber security management.

1. Cybersecurity risk management architecture

   The Information Department is responsible for managing and implementing information security policy, promoting information security information, increasing employee information security awareness, collecting and improving organization information security management system performance and effectiveness of technologies, products or procedures, etc. The Auditing Office performs cyber security audit on the internal control system - information cycle, and evaluates the effectiveness of the information operation internal control of the Company.

2. Cybersecurity policy:

   To implement information security management, the Company has established the internal control system - information cycle and information machine room management regulations, cyber security inspection control. Accordingly, through the joint effort of all employees, the following policy objectives are expected to be achieved:

   - Ensure the confidentiality and integrity of information assets.
   - Ensure that specification data can be accessed according to the department function.
   - Ensure the continuous operation of information system.
   - Prevent unauthorized modification or use of data and system.
   - Perform information security audit operation periodically, and ensure through execution of information security.

3. Specific management program
   - Internet network information security control.
     - Construction of firewalls
     - Perform virus scan on the computer system and data storage medium periodically
     - Review the system log of each network service item periodically, and track abnormal conditions
   - Data access control.
     - Computer equipment shall be under the custody of dedicated personnel, and account and password shall be set up
     - Different access authorities are granted according to job functions
     - Cancel original authorities of transferred or resigned personnel
     - Prior to scrap of equipment, confidential and sensitive data and licensed software shall be removed or overwritten
     - Remote login management information system shall be approved appropriately
   - Response and recovery mechanism.
     - Inspect emergency response plan periodically
     - Perform periodic system recovery drill annually
     - Establish system backup mechanism, and implement remote backup
     - Periodically review computer network security control measures
   - Promotion and inspection.
     - Promote and educate information security information at all time, in order to increase employees' information security awareness
     - Perform cyber security inspection irregularly on an annual basis

4. Resources for cyber security management

   The Company values cyber security and continues to increase the investment in information security related infrastructure construction and security protection architecture related software and hardware.

   The Company's total investment in information security related software and hardware expenses in 2024 is approximately NTD 223,257, demonstrating the Company's emphasis on cybersecurity.

(II) For the most recent year and up to the printing date of the annual report, the loss due to major cyber security events, possible impacts and countermeasures:

Presently, the Company has no occurrence of major cyber security events leading to operating loss. The Company will continue to implement information security management policy goals and implement recovery plan drill periodically, in order to protect important system and data security of the Company.