RH 匯僑設計 Rich Honour Design Group

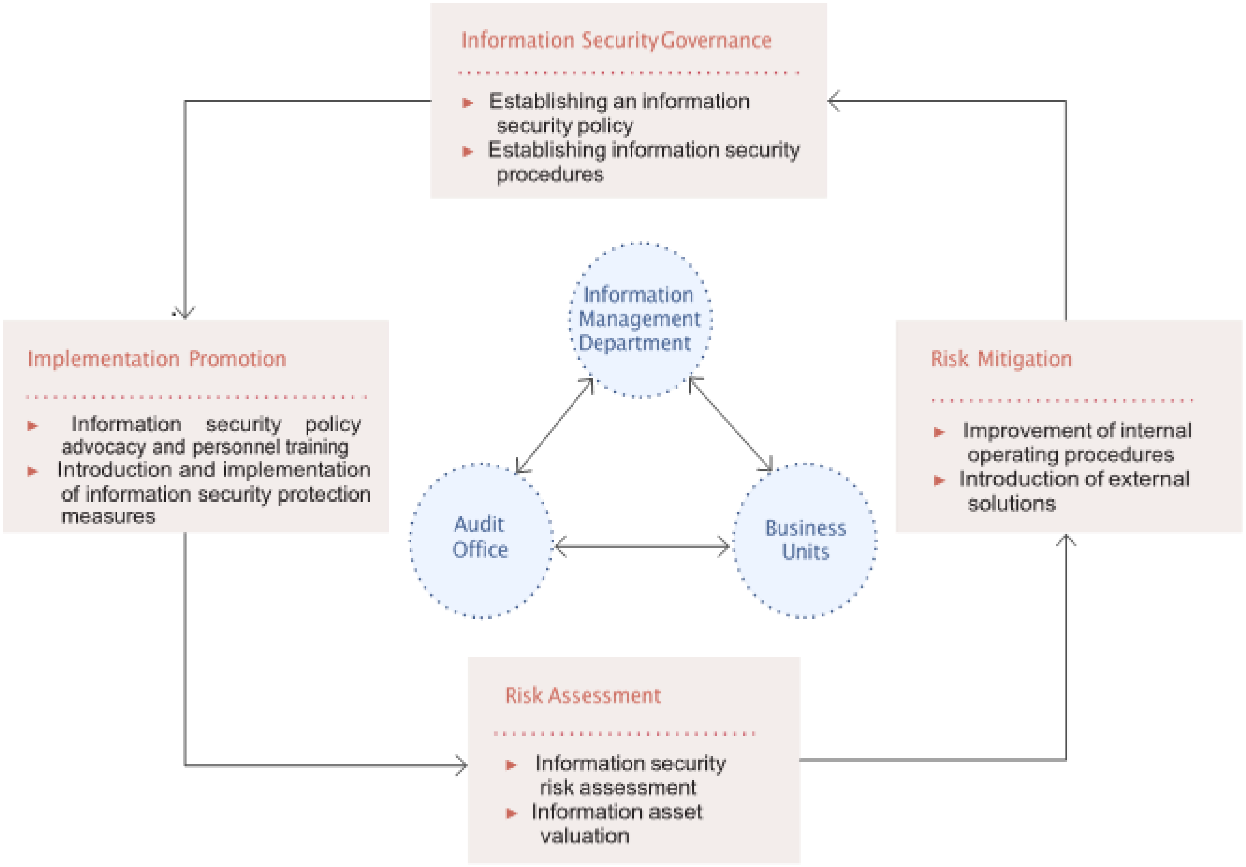
Information Security Policy

A. Information Security Management Framework

(1) The Information Management Department is the responsible unit for the cybersecurity of the Company. The department has an information security supervisor and a professional information security personnel responsible for formulating the internal cybersecurity policies of the Company and planning and implementing cybersecurity protection and information security policy promotion. The department holds bi-weekly information security meetings and makes announcements about the Company's overall information security governance.

(2) The Company's Audit Office is the unit responsible for instructing the supervision of information security. The office has an audit supervisor and dedicated auditors to instruct the implementation of internal information security. If any deficiency is found in an audit, the office will immediately ask the audited unit to propose relevant improvement plans and specific actions to be taken, and regularly track the improvement results, in order to reduce internal information security risks.

(3) We adopt regular audits and PDCA (Plan-Do-Check-Act) cycle management in our organizational operating model to ensure the achievement of reliability targets and continuous improvement.



Information Security Governance
- Establishing an information security policy
- Establishing information security procedures

Implementation Promotion
- Information security policy advocacy and personnel training
- Introduction and implementation of information security protection measures

Risk Mitigation
- Improvement of internal operating procedures
- Introduction of external solutions

Risk Assessment
- Information security risk assessment
- Information asset valuation

B. Information Security Policy

Cybersecurity management covers the following aspects:

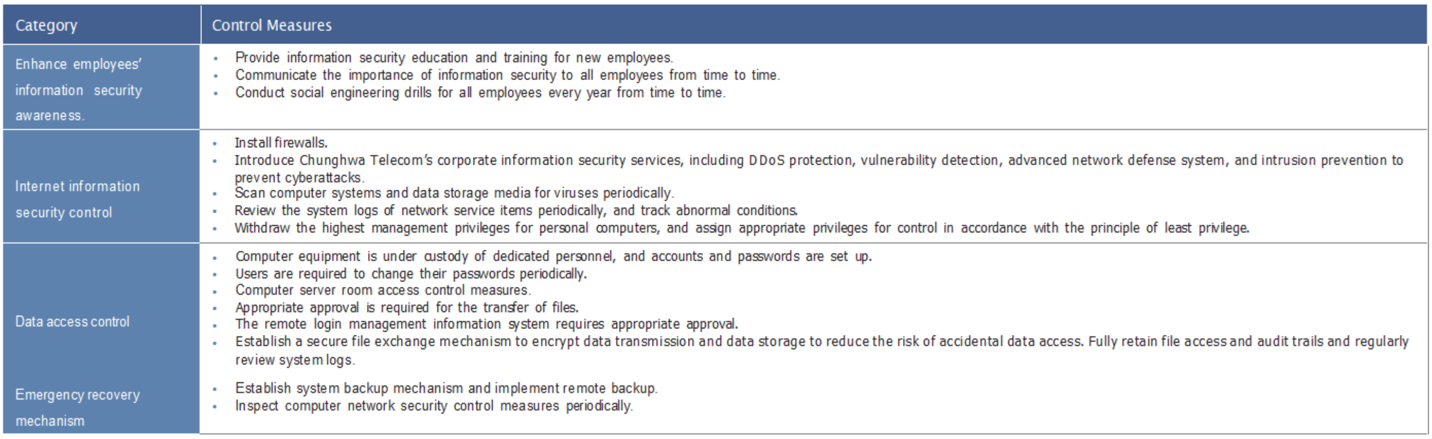
(1) Systems and regulations: Formulate a cybersecurity management system for the Company to regulate personnel behavior.

(2) System protection: Establish a cybersecurity management system and implement information security protection management measures.

(3) Personnel training: Conduct cybersecurity education and training to enhance the information security awareness of all employees.

(4) External audits: Carry out risk assessments on information security and network risks, and propose control points as appropriate to control and manage information security risks.

C. Information Security Management Plan



Category	Control Measures
Enhance employees' information security awareness.	• Provide information security education and training for new employees. • Communicate the importance of information security to all employees from time to time. • Conduct social engineering drills for all employees every year from time to time.
Internet information security control	• Install firewalls. • Introduce Chunghwa Telecom's corporate information security services, including DDoS protection, vulnerability detection, advanced network defense system, and intrusion prevention to prevent cyberattacks. • Scan computer systems and data storage media for viruses periodically. • Review the system logs of network service items periodically, and track abnormal conditions. • Withdraw the highest management privileges for personal computers, and assign appropriate privileges for control in accordance with the principle of least privilege.
Data access control	• Computer equipment is under custody of dedicated personnel, and accounts and passwords are set up. • Users are required to change their passwords periodically. • Computer server room access control measures. • Appropriate approval is required for the transfer of files. • The remote login management information system requires appropriate approval. • Establish a secure file exchange mechanism to encrypt data transmission and data storage to reduce the risk of accidental data access. Fully retain file access and audit trails and regularly review system logs.
Emergency recovery mechanism	• Establish system backup mechanism and implement remote backup. • Inspect computer network security control measures periodically.

D. Resources Invested in Cybersecurity Management

(1) Implementation of preventive drills: Local and off-site backup and recovery drills are conducted regularly every year. An automatic backup and redundancy mechanism is established for the important server system environment and data to ensure that personnel can successfully restore system operations in the event of a disaster.

(2) Management based on the principle of least privilege: We adjust the maximum management privileges for personal computers, and assign appropriate privileges for control in accordance with the principle of least privilege.

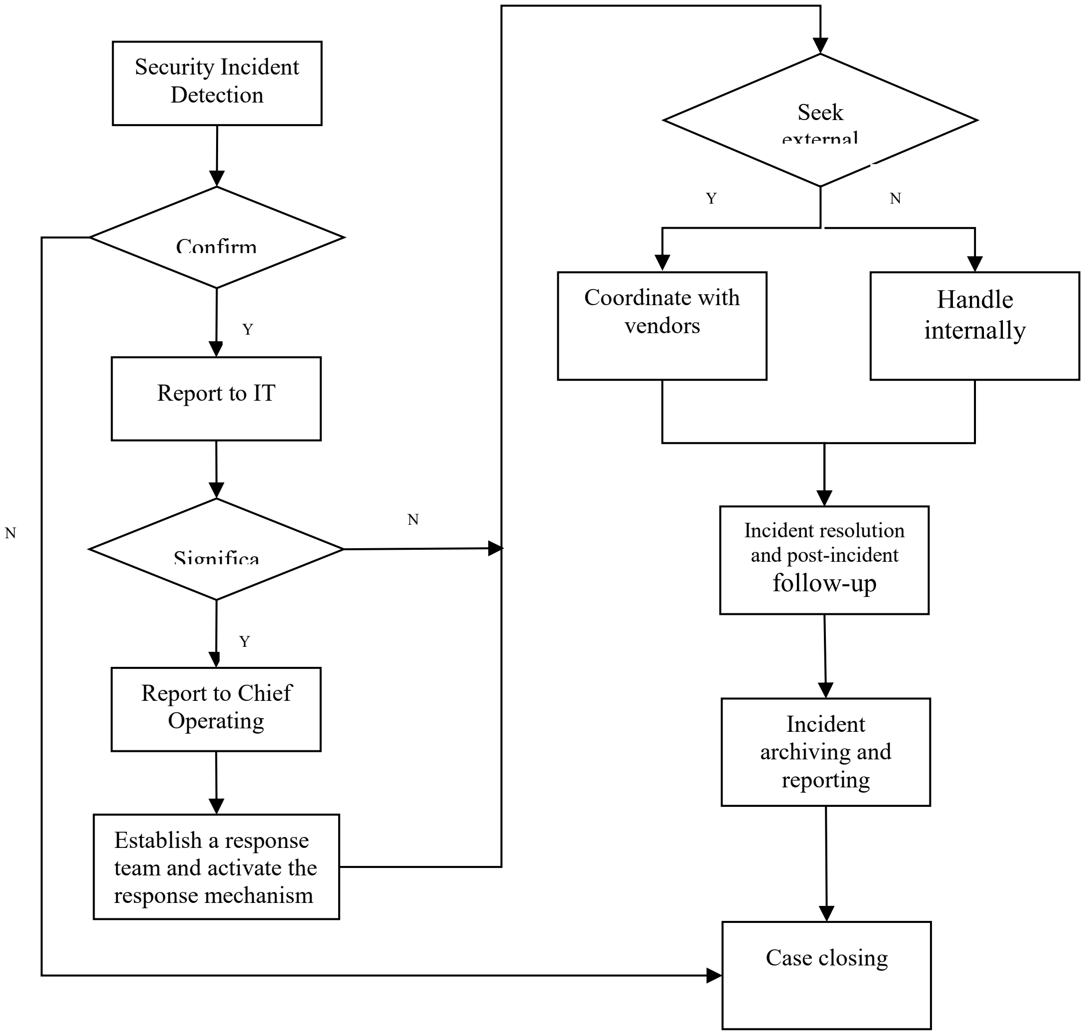
(3) Social engineering drills: Social engineering drills are conducted from time to time every year to simulate phishing emails from hackers in order to test employees' awareness of information security risks, supplemented by information security advocacy and education and training, avoiding information security risks caused by inappropriate email behavior.

(4) Network security protection: Implement next-generation firewalls, including web activity management, URL filtering, and an intrusion prevention system. Regularly review protection reports and adjust security strategies as needed to prevent users from accessing malicious websites

and to reduce the risk of external cyberattacks on the company.

(5) Establishment of a secure file exchange mechanism: An enterprise-grade cloud-based file exchange platform has been introduced to encrypt data transmission and data storage to reduce the risk of accidental data access. We fully retain file access and audit trails and regularly review system logs.

E. Incident Reporting Procedure for Information Security


Security Incident Detection
Confirm
Y
N
Report to IT
Significa
N
Y
Report to Chief Operating
Establish a response team and activate the response mechanism
Seek external
Y
N
Coordinate with vendors
Handle internally
Incident resolution and post-incident follow-up
Incident archiving and reporting
Case closing