A.Information and Communication Security Management:

- ●Information and communication security risk management framework:
  The responsible unit for information and communication security is the information center. It is responsible for planning, implementing, and promoting information and communication security management and communicating awareness of information and communication security to our people from time to time.
- ●The Audit Office is the unit for auditing information security governance. It performs audits periodically to find out implementation deficiencies and asks the auditee to come up with related correction plans and submits them to the Board of Directors as well as follows up on the improvement status periodically in order to minimize internal information and communication security risks.
- ●For the operational model, annual PDCA management is adopted to ensure fulfillment of reliable information and communication and constant reflection and improvement.

B. Information security management solution:

Information security management solution		
Category	Description	Related measures
Access control	User account, access control, and system operation	1. User account access control and review 2. Periodic inventory check of user account permissions
Access control	Control over access by staff to internal and external systems and data transmission channels	1. Internal/external accessible scope-defined control measures 2. Operational track record
External threat	Internal potential weaknesses, virus attack channels, and protective measures	1. Host/computer weakness detection and update measures 2. File and mail virus protection and malware detection 3. Firewall protection and malware detection
System usability	System usable status and management in case of discontinued service	1. System/network usable status monitoring and reporting mechanism 2. Information backup measures, local/remote backup mechanism 3. Periodic disaster recovery drill
Educational training and communication	Communication of information security risk cases from time to time	1. Communication of information security risk cases from time to time

C.Information and communication security policy:

Our company upholds the principle of maintaining information security. We ensure comprehensive protection and preventive measures for data stored or transmitted by the company to eliminate incidents such as damage, computer viruses, leakage, misuse, and infringement. Our information security policy is as follows:

1. Information and communication security measures shall meet the requirements of government laws and applicable requirements of the Company's information security policy and internal control regulations. All information security control or procedures shall be developed, revised, and established in compliance with internal information control regulations.

2. All staff and suppliers and customers of the Company, should they need information to be provided by the Company, must follow the required procedure and designated regulations in honor of this policy.

3. Information and asset managers at respective departments of the Company shall be responsible for the information or assets within their field or held by them and have a monitoring procedure in place for the use status so that potential risks of system or unit information abuse may be uncovered at any time; it reinforces the confidentiality, usability, and integrity of the data.

4. All staff shall report safety events, safety weaknesses, and violations of safety policies and procedures through appropriate reporting channels.

5. Work assignment shall take into consideration division of labor; functions and scope of responsibilities shall be separated in order to prevent against unauthorized modification or misuse of information or service.

6. It is strictly prohibited that people install, use, or download illegal or unauthorized software in Company's information equipment.

7. The Company will revise its information security policy periodically and enforce it in order to enhance operational safety of respective information systems.

8. Anyone that jeopardize information security shall be sought after for his/her civil, criminal, and administrative liabilities and be punished accordingly, depending on the circumstances.

<table>
<tr><th colspan="2">Input of information security management resources</th></tr>
<tr><td>Item</td><td>Description</td></tr>
<tr><td>Information Security Specialist</td><td>Two information security specialists are in place</td></tr>
<tr><td>External Firewall</td><td>Reinforce the security of external gateways. For the network gateway, the new-generation Layer 7 firewall is adopted.</td></tr>
<tr><td>External Network Access Line</td><td>To strengthen line security, we have applied to Chunghwa Telecom for information security services for a total of 13 lines based on their service differences and importance. These lines will be used in conjunction with the new generation firewall to achieve an external double-layer defense effect.</td></tr>
<tr><td>Anti-virus System</td><td>The latest ApexONE anti-virus system of Trend Micro is configured; it can detect and remove general system viruses and also reinforce website credit rating, detect and keep off suspicious connections, monitor behavior, and control access of surrounding equipment, among others.</td></tr>
<tr><td>Terminal computer (PC, NB)</td><td>Reinforce terminal computer safety management and gradually eliminate early-stage operating systems; at present, more than 99% of the terminal computers are of Windows 11 or higher-level operating systems.</td></tr>
<tr><td>Information Security Solutions</td><td>The additional setup of a second physical backup and Chunghwa Telecom’s offline cloud backup mechanism—based on the 3-2-1 disaster recovery architecture—has been completed and put into operation.</td></tr>
<tr><td>Information Security Planning</td><td>Conducted a social engineering drill simulating hacker techniques, sending a total of 690 mock phishing emails to 138 employees. The exercise tested and educated staff on identifying phishing, scams, and other attack methods, enhancing employees’ awareness and defensive capability against social engineering attacks.</td></tr>
<tr><td>Education and Training</td><td>n accordance with the Information Security Guidelines for Listed and OTC Companies, annual information security awareness training and social engineering drill training courses were conducted for employees who use information systems.
<table>
<tr><th>Courses</th><th>Sessions</th><th>Participants</th><th>Training Hours</th></tr>
<tr><td>Information Security Awareness Training</td><td>1 session</td><td>57 participants</td><td>2 hours/perperson</td></tr>
<tr><td>Social Engineering Drill Training</td><td>1 session</td><td>63 participants</td><td>40 mins/pweperson</td></tr>
</table>
</td></tr>
</table>