Information Security Management

■ Information Security Management Risk management framework

(1) The company established the position of Information Security Manager on December 4, 2023, and appointed Mr. Chen, Jung-Kuei, Vice President of the CEO Office, to the role. Information security is the responsibility of the information department to promote the planning, execution, audit, and communication coordination of related matters, and to conduct relevant education and training and advocacy to ensure that personnel are familiar with the security responsibilities of business operations. The information department regularly reviews cybersecurity policies and annually reports cybersecurity issues to the board of directors.

(2) 2025 Cybersecurity Report: The Chief Information Security Officer of the Company reported the implementation status of the 2025 cybersecurity initiatives to the Board of Directors on November 7, 2025.

■ Policies of information security

(1) Document Security Policy:

Through the document encryption system, provide encrypted outgoing documents to suppliers, limiting the number of times the file can be opened, printed, modified, and the document's validity period.

(2) Host Security Policy:

A. Regular backup of the host and offsite backup of files.
B. The host regularly updates virus codes and automatically scans to prevent viruses.
C. Regular automatic updates of the operating system patches are performed on the host.

(3) Internet Security Policy:

A. All external computers and information devices must be reviewed by the information unit before they can connect to the internal network.
B. Introduce a malicious website and ad blocking system to block and restrict suspicious websites.
C. Firewalls only open specific network ports to provide specific services.

(4) Customer Security Policy:

A. Computer automatically updates patches to the latest version and system regularly forces updates.
B. Users are restricted from installing software on their own and must have the software reviewed and installed by the IT department.

C. The external design personnel have introduced terminal operation cloud desktop, and relevant engineering data is stored in the machine room.

■ **Specific plan for internet security risk management**

(1) Through the firewall, internal and external networks are separated, and each unit is isolated through virtual networks.

(2) Implement intrusion defense systems and regularly report cybersecurity reports to management.

(3) Regularly promote awareness of information security and provide education and training to colleagues, in conjunction with annual internal audits of information security policies and risk assessments.

■ **Resources for investing in information and communication security management**

(1) Business disaster recovery management; regularly perform local backups, remote backups, and off-site backups based on the system backup cycle. Conduct annual server backup file restoration drills and data verification.

(2) Joining TWCERT/CC Taiwan Cybersecurity Alliance can enhance the company's cybersecurity intelligence analysis and acquisition, as well as strengthen cybersecurity resilience.

(3) The company went public in November 2023 and established an "Information Security Unit" in December of the same year, which is managed by the Information Department. This unit is responsible for planning, monitoring, and implementing information security management operations. The unit is led by the Information Security Vice President, Mr. Chen, Jung-Kuei, who is responsible for promoting information security policies and resource allocation. Additionally, the unit is staffed with one Information Security Supervisor and two Information Security personnel to promote information and communication security strategies.

(4) A monthly report is submitted to senior management on the implementation of information security, including the assessment and identification of relevant cybersecurity risks and the mitigation of potential security threats.

(5) The Company has regularly conducted social engineering drills by simulating phishing emails and social scam scenarios to enhance employees' awareness of cybersecurity threats and their ability to identify hacking techniques, thereby strengthening the human aspect of the Company's cybersecurity defense.

(6) The Company achieved a SecurityScorecard external defense rating of over 90 points. The Information Department regularly monitors and reviews the

evaluation results as a basis for continuous improvement of cybersecurity measures.

(7) The Company plans to implement ISO 27001 in the fourth quarter of 2025 to ensure the confidentiality, integrity, and availability of information assets, thereby enhancing the overall maturity of information security management.

(8) The Company plans to establish an ERC (Emergency Response Center) organization by the end of 2025 to strengthen its ability to respond to cybersecurity threats and emergencies, as well as to enhance business continuity and operational resilience.