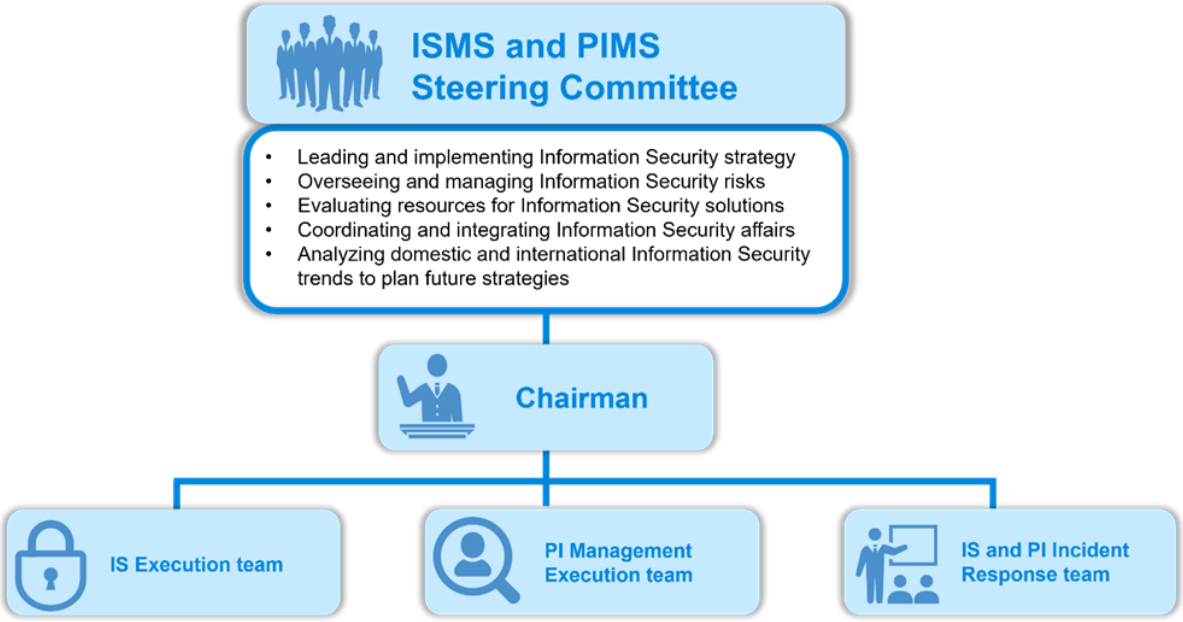
Implementation of Delta Information Security

1. Organizational Chart of Delta Information Security

The Company has set up an Information Security Steering Committee, chaired by the CEO and with its Chief Information Officer as the Chief Information Security Officer and senior executives from all global business groups and regions as Committee members. The Information Security Department has also been established to oversee Delta's information security and physical security planning and related audits, and to facilitate the operation of this Committee. Through quarterly management review meetings, the Information Security Committee reviews the results of information security risk analysis and the corresponding protective measures and policies adopted by the Company to ensure the suitability, appropriateness and effectiveness of the ongoing operation of the information security management system. The Chief Information Security Officer reports annually to the Board of Directors on the effectiveness of information security management and the direction of the information security strategy to ensure that information security policies and controls are implemented in Delta's business units around the world. On April 30, 2024, the Chief Information Security Officer reported to the Board of Directors on the status of information security governance.

2. Delta Information Security Policy

Delta continues to refine the information security system and enhance the protection capabilities. It promotes overall information security governance, establishes a consistent information security policy, and plans Delta Group's information security management system by forming the Information Security Steering Committee. Delta's Board of Directors is responsible for approving the Group's information security and personal information protection policies, as well as making decisions on major information security-related issues. All information security management regulations comply with domestic and international information security laws and regulations. Delta actively seeks to apply international information security standards and certification to a wider range of areas to integrate information security practices into the daily operations. This policy is reviewed annually in light of changes in government laws and regulations, the environment, and business and technology. Any revisions must be approved by the Board of Directors and announced for implementation. Information security policies and awareness campaigns are conducted annually for the Group's employees to enhance information security awareness.



3. Specific management solutions

In order to achieve the information security policy and objectives and to establish a comprehensive information security protection, the management issues and specific management plan are as follows:

(1) Organizational Control

- Delta has established the “Delta Group Information Security and Personal Data Protection Policy”, which serves as a guideline for defining the division of authority and responsibilities within the information security and personal data management organization, promoting staff education and training, as well as managing computer hardware and software, networks, and physical environments.
- Delta’s major information systems had been certified with ISO/IEC 27001 since December 3, 2018. To continuously ensure the implementation of information security and the maintenance of certificate validity, we annually conduct control measures, including asset inventory, risk assessment and treatment, critical information system business continuity drills, and internal audits. The external verification firm conducted an assessment on July 12, 2024, and passed the verification based on the ISO/IEC 27001:2022 international standard. The certificate’s validity has been extended until August 8, 2027. We will continue to promote and implement the information security system across the Delta Group’s global regions and business units to minimize potential security threats and build a secure and reliable information environment that protects the interests of the Group and its customers.
- To ensure that information security management documents align with the actual operation of the organization and adapt to the ever-changing landscape of information technology, Delta has added 1 new management regulations in response to the trend and demand for using cloud solutions, a new cloud service management policy has been established. Furthermore, to optimize and strengthen existing processes, and to meet customer and external audit requirements, we also revised 20 procedural documents in 2024. This unwavering commitment to continuous improvement of Delta’s information security management ensures that the information systems and data are properly protected.
- Collaborating with large international information security companies to conduct comprehensive information security inspections, using their professional services so as to enhance advanced information security based on the objective results from third-party verification.
- Delta’s cybersecurity service provider supplies cyber threat intelligence to enhance the existing threat detection solutions. Additionally, we have joined to the Taiwan Computer Emergency Response Team / Coordination Center (TWCERT/CC), receiving cyber threat intelligence periodically. This information is analyzed and integrated with existing intelligence to improve defense efficiency and to take appropriate preventive measures to reduce potential risks to the Compan.

(2) Personal Control

In today’s digital and informatization world, information security education and training are highly essential. Employees can better understand the importance of information security and learn how to prevent and respond to various information security threats through adequate information security awareness training. This includes learning how to avoid common human errors and ensuring compliance with relevant regulations and standards. By cultivating a culture of information security awareness, employees can significantly reduce the organization’s exposure to security risks as well as increase the protection level of data and system, thus ensuring a safe and secure environment for the Group’s business operations.

- In addition to providing cybersecurity education training to newly hired employees ,and technical and management personnel are also required to complete annual information security education training and pass the test. In 2024, a total of 39,562 people completed annual cybersecurity training, both online and physical, with a coverage rate of 99%. The Information Security Department also periodically issues information security newsletters to inform

employees about the latest information security risks and things employees should be aware of. Additionally, the IT department has a dedicated email address for reporting cybersecurity issues promptly.

- To strengthen employees' awareness of information security, we also conduct phishing email drills and phishing email recognition awareness training for employees in global, and analyze the results of the drills to improve the effectiveness. In 2024, a total of 48 phishing email drills were conducted, with 234,440 emails sent out. The average click-through rates for all employees were lower than the target.

(3) Technical Control

- Maintained and operated antivirus and endpoint protection system, coupled with multi-layered cybersecurity monitoring mechanisms, to prevent the risk of computer viruses and malicious software intrusions.
- Deployed Security Information and Event Management (SIEM) system and planned to deploy Endpoint Detection and Response tools for enhancing the efficiency of cybersecurity threat detection and response.
- Built next-generation firewall to achieve network protection and segmentation to strengthen security control measures for critical infrastructure services.
- Deployed a Secure Email Gateway (SEG) to block phishing emails containing malicious programs or links sent by hackers.
- Monitor outbound data transmissions in real time to identify and manage potential data leakage risks.
- For applications deployed within the Company, vulnerability assessment and management are conducted. In response to digital transformation and cloud security, more automated integration solutions are being promoted to enhance cyber resilience.

4. Information security management resources invested

Information security has become an important issue in the Company's operation, and the information security management issues and resources invested are as follows:

- Dedicated manpower: We have 1 dedicated information security manager and 14 people in the "Information Security Department", which are responsible for our information security planning, information security system operation, technology introduction and related audits to maintain and continuously strengthen information security.
- Delta has established the "Information Security Steering Committee", chaired by the CEO, the Chief Information Security Officer serving as the convener, the Chief Operating Officer and senior executives from various global business group and regions are members of the committee. Regular quarterly meetings are held to discuss information security issues and business requirements faced by different regions, and to decide on necessary resources and implementation plans.
- In 2023, Delta has also established the "Information Security Promotion Committee", with executives assigned by various business group to serve as information security promotion seeds. During regular bimonthly meetings, in addition to discussing information security issues, the committee also promotes information security activities being advocated by the headquarters, aiming to enhance colleagues' awareness of information security.

5. The impact of historically severe information security incidents and countermeasures

Delta has established clear procedures for reporting and handling information security incidents. Information security incidents are recorded and graded by the information security maintenance management team. The other relevant units are required to resolve information security incidents within the target response time and conduct root cause analysis and corrective actions after the incident is resolved to prevent recurrence. In 2024, the Company had no information security incidents that caused losses to the Company and customers.