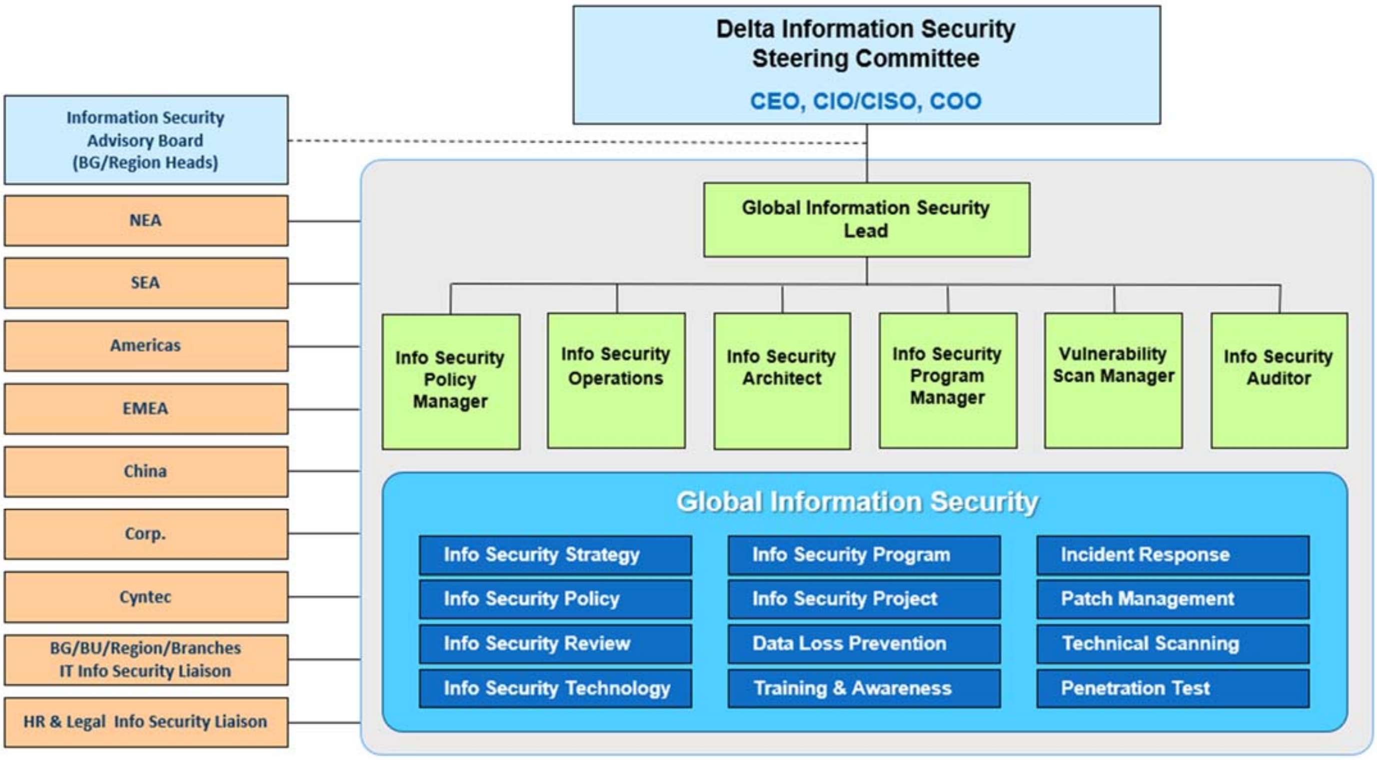
Implementation of Delta Information Security

Delta Group established Delta Information Security Steering Committee to implement strict information security in a global scale and a comprehensive information security management process. Delta Chief Information Officer regularly reports the achievement and strategies of information security implementation to the Board of Directors every year. This year (2022), Delta Chief Information Officer reported overall Delta Information Security governance to the Board of Directors on February 24. The topics include cyberattack incident and the plan for information security governance

1. Organizational Chart of Delta Information Security

Delta Group has set up an Information Security Steering Committee, wherein the CEO, CIO/CISO, COO are in charge of supervision and review, direct the Information Division's Information Security Department to coordinate and facilitate information security compliance, information security operations, security architecture, vulnerability management& scanning and information security risk management. It also organizes information security managers in different parts of the world to ensure implementation of information security policy, management and control across business units globally. Delta Information Security Steering Committee is held on quarterly base, to discuss the effectiveness of information security management, information security-related issues and developments.



2. Delta Information Security Policy

Delta Group implemented ISO27001 Information Security Management System (ISMS) in 2017 and obtained the certification. In order to maintain the validity of the certificate, Delta Group passes the third-party external audit every year. The current certificate is valid from August 8, 2021 to August 8, 2024 which covers year 2022. In order to ensure the effectiveness and appropriateness of this management system, the information security policies are reviewed on yearly base. Also, Delta Group has joined the Taiwan Information Security Alliance and High-Tech Information Security Alliance, etc. to obtain the latest information or updates regarding information security.

Delta Group’s global employees and contracted personnel shall observe the Delta Information Security Policy as follows:

1. Guidelines for Information Equipment User
2. Guidelines for Mobile Device User
3. Guidelines for Password User
4. Guidelines for Corporate E-mail User
5. Guidelines for Internet User
6. Guidelines for Information Handling
7. Guidelines for Software Usage and Authorization
8. Guidelines for User of Removable Media Devices
9. Guidelines for Visitor Security
10. Guidelines for Deployment of Anti-virus and Information Leakage Protection Software
11. Guidelines for Remote Access
12. Guidelines for Information Security Event Management
13. Information Security Requirement for External Network Application Services
14. Guidelines for Corporate Resource User

3. Information and communication security management resources

I. Global information & communication security management
A total of 9 specialists in charge of IT information security organize the monthly Information Security Representatives Meeting to review global information & communication security issues, and more than 40 information security representatives appointed by every major unit hold monthly Data Loss Prevention (DLP) Plan Execution & Review Meetings.

II. Security Operating Center (SOC)
SOC Team is responsible for real-time monitoring and identifying information security incidents to enhance the responding mechanism to information security incidents.
Delta Electronics (Wuhu) Co., Ltd., Delta Electronics (Dongguan) Co., Ltd., Delta Networks (Dongguan) Ltd. and Delta Electronics (Chenzhou) Co., Ltd. have been received advanced level certification from the Customs of China (General Administration of Customs of China (GACC)) in 2020.

III. Vulnerability Scan and Penetration Testing
A vulnerability scan was conducted regularly on Delta Group's network equipment, applied system and products, as well as a penetration test on the website and system.

IV. Annual information & communication security trainings, anti-phishing email training exercises
Information & communication security trainings were organized for Delta Group employees globally along with effective use of language; anti-phishing email training exercises, identifying phishing emails, evaluation of training exercise results were also held across regions to improve maintain efficiency.

4. Information security and privacy management system introduction and verification

In response to the emphasis on protection of personal data all over the world, the ability to protect and manage personal data privacy is becoming more important. However, if personal data is to be properly protected, the cybersecurity capability must be indispensable. ISO27701 is an international standard for security of personal data. In order to strengthen Delta Group’s management of information security and privacy protection in various countries, Delta Group has expanded the scope of the ISO 27001 certification to European such as the Netherlands and Switzerland from 2021, and also has introduced the privacy information management system (PIMS) to continuously enhance the protection of information assets and personal data and reduce the risks faced based on the ISO27701 standards and the PDCA cycle.

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

In January 2022, some of Delta’s information systems were compromised due to a cyberattack, causing inaccessibility of the Company’s website, Office Automation for office works and relevant systems. Upon detecting the incident, the IT department promptly notified relevant departments to activate the emergency response mechanism and sought the assistance of external experts to resolve the problem by protecting relevant programs, analyzing and investigating the cyber breach, and recovering affected systems. The incident, however, did not significantly affect overall operations and was already reported to the government's law enforcement agencies. The Company has likewise issued a statement regarding the incident pursuant to laws and regulations.

According to the preliminary investigation and analytical review, it was found that there was a data breach on the Company’s employee accounts via social media or through the internet. In view of this, Delta's Information & Security Unit has planned for more intense trainings and social media training exercises for Delta employees globally, and the IT Team will improve the Company’s email filtering mechanism, surveillance and network/system security controls to reduce risks and avoid similar incidents in the future.