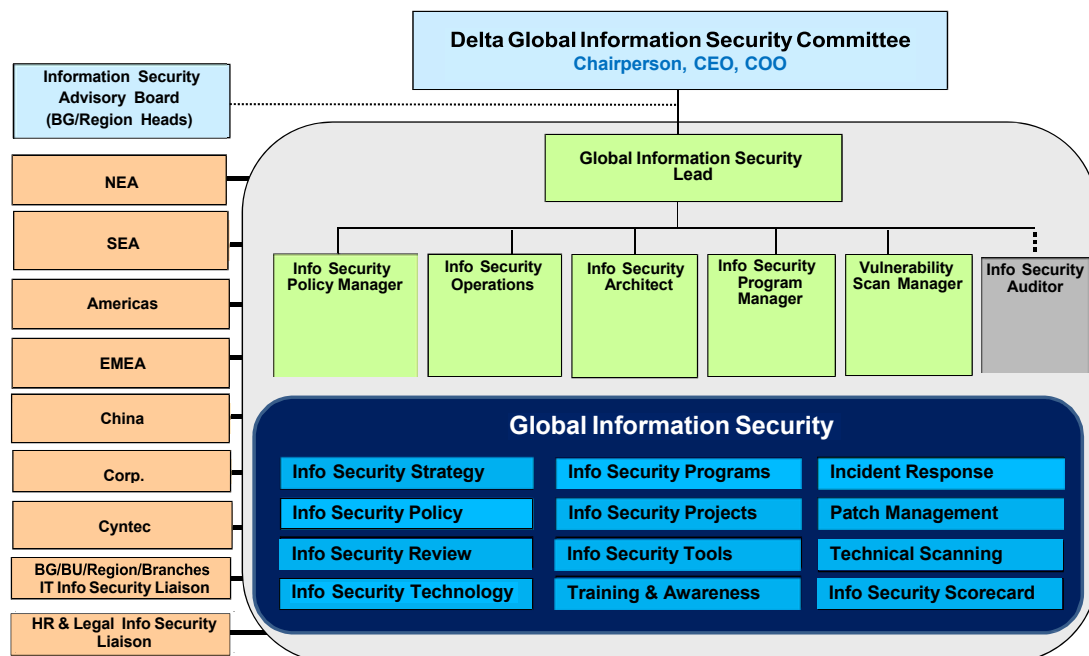




Implementation of Delta Information Security

Delta Group established Delta Global Information Security 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 (2020), Delta Chief Information Officer reported implementation status and future planning in terms of Cybersecurity & Information Security Threats, Information Security Strategies, Personnel Awareness & Process Enhancement and Security & Infrastructure Evolution to the Board of Directors on July 29.

A. Organizational Chart of Delta Information Security



B. Delta Information Security Policy

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

- Internet user policy
- Corporate E-mail user policy
- Computer user policy
- Anti-virus/DLP arrangement and user policy

- Process and security principle of storage media
- Password principle
- Information backup and recovery policy
- Event management policy
- Acceptable use of mobile devices
- Encryption and its policy
- The use of device and countermeasures
- Mobile computation and remote work policy
- Remote access policy

C. Construction and Risk Assessment for Delta Information Security Management System

- In response to increasing demands on the outsourcing market for customers' information, Delta implemented the Information Security Management System in 2018 to identify, manage and continue improving the security needs of customers' information, which may be encountered internally and externally, based on information security management regulations set forth in ISO 27001:2013 published by the International Organization for Standardization (ISO) in order to ensure the confidentiality, integrity and availability of customers' information asset. The international independent certification company conducted external audit activities in Delta sites on July 7th and July 8th 2020, Delta passed the verification and successfully maintain ISO 27001:2013 information security certification again.
- Delta has stipulated assessment policy on information security risk, requesting all aspects of information security, including but not limited to physical objects, network, environment and constant operation to be in compliance with international security standards. Besides, Delta also has set up an emergency response plan, including quick response to potential events, crisis process and disaster recovery, constant improvement, and high-risk event measures.

D. Implementation of Delta Information Security Management

Delta Corporate IT revised the Global Information Security Policy from time to time in order to correspond the company's policies, and keep associates worldwide again noticed of the importance to information security. Delta adopts the following 3 strategies (**PPT**) to implement Delta information security management:



P (PEOPLE): Personnel Awareness

- Worldwide Employees Re-sign Security Policy Annually
- Conduct Phishing Simulation and Training
- Security Topics with Monthly IT Newsletter
- Personal Security Compliance
- Security Awareness Training

P (PROCESS): Process Enhancement

- Data Control & Use Guidelines
- ISO 27001 Certificate Maintenance
- Business Continuity Plan
- Automate Incident Investigation
- Implement Personal Data / Privacy
- Refine InfoSec Evaluation & Implementation Processes

T (TECHNOLOGY): InfoSec Infrastructure

- Data Leakage Prevention
- Next Generation Firewall
- Intrusion Detection System
- Intrusion Prevention System
- Enterprise Mobility Management
- Vulnerability Management & Penetration Test

E. Delta Electronics (Jiangsu) Ltd., Delta Electronics Power (Dongguan) Co., Ltd., Delta Video Display System (Wujiang) Ltd., and Delta Electronics Components (Wujiang) Ltd. obtained the Authorized Economic Operator status in China on Jun. 20, July 18, Sept. 3, and Nov. 19 of 2019.

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

- No severe information security events occurred in 2019 and as of the day of publication of 2019 annual report.