台達電子工業股份有限公司

DELTA ELECTRONICS, INC.

Delta Group Information Security and Personal Information Protection Policy

Document Number: DEI-DIS-PL01 / Version: 1.0
Last Approval Date: 2023/04/27
Confidential Level: Public

Document Summary – Delta Group Information Security and Personal Data Protection Policy			
Document Number	DEI-DIS-PL01		
Version	1.0		
Description	A policy for establishing an information security management and personal information management system to ensure the confidentiality, integrity and availability of Delta Group's information assets.		
Document Owner	IT Information Security Department		
Last Revision Date	2023/03/31	Last Reviewed Date	2023/03/31
Approved Date	2023/04/27		
Approval Records	Approved by the Board on 2023/04/27		

Document Release/ Revision/ Deletion Approval Record (e-Form)	
Form Number	

Table of Content

1 Purpose

To strengthen information security management and protect the rights of personal data subjects, Delta Group (hereinafter referred to as “the Group”) intends to establish an information security management and personal information management system to ensure the confidentiality, integrity and availability of the Group's information assets and meet the requirements of relevant laws and regulations, so that it is protected from internal and external threats. Based on ISO 27001, ISO 27701, the Personal Data Protection Act and the relevant laws and regulations on personal data protection in the regions where the Group is located, and considering the business needs of the Group, this Policy is formulated as the Group's highest guidelines for information security management and personal data protection.

2 Scope

2.1 This policy is applicable to the Group, which includes board of directors (including independent directors), managers and all employees of the Group (including staffed personnel, contracted personnel, and others), as well as customers, vendors or third-party personnel.

2.2 The Group shall base on the requirement of local laws or regulations to establish information security and personal data protection policy with the reference and compliance of this policy. This policy shall prevail in the event that local regulatory requirements are less stringent than the requirements in this policy.

3 Definition

3.1 Delta Group

This refers to Delta Electronics Inc. (in short, Delta Electronics) and its subsidiaries, affiliates and companies which Delta Electronics has direct or indirect substantive control worldwide.

4 Information Security and Personal Data Protection Responsibilities

4.1 All the Group personnel are responsible for implementing and maintaining the Group's information security and personal data protection management systems. To implement and execute information security and personal data protection controls, the Group shall establish a relevant Committee. Chairman of the committee shall be CEO/President of the organization, or assigned by the organization's CEO/President.

4.2 Management shall support and participate in the implementation of Information Security and Personal Data Protection Management Systems.

4.3 The Group shall establish a personal data protection management system in accordance with personal data protection regulations to ensure the proper controls over personal data protection and maintain the Group's reputation.

4.4 The Group personnel and outsourced service providers shall notify the Group in a timely manner if any information security incident or personal data leakage occur, or if they are made aware of any information security breach.

4.5 The Group shall undertake measures to ensure that the Group meets its obligations under the personal data protection regulations for personal data collection, use, and disclosure. The Group is responsible for demonstrating that personal data is properly managed and protected. This includes adapting legal requirements into policies and practices, data protection by design, and using monitoring mechanisms and controls to ensure that policies and processes are effectively implemented.

4.6 The Group shall notify the individual of the purpose of collecting personal data. The notification shall include how the personal data will be used and to whom it may be shared.

4.7 The Group shall not collect, use, disclose personal data unless the individual gives, or is deemed to have given, the individual's consent to the collection, use or disclosure, as the case may be; or the collection, use or disclosure (as the case may be) without the individual's consent is required or authorized under any written law.

4.8 The Group shall conduct disciplinary actions in accordance with the Group's Human Resource policies if any personnel has violated the Group's Information Security and Personal Data Protection policies and procedures.

4.9 When the outsourced service is related to information security and personal data protection, the Group's outsourced service providers shall sign a non-disclosure agreement that requires outsourced service providers to comply with the Group's information security and personal data protection policies and procedures. Any personnel shall not use the Group's information assets and personal data without authorization.

5 Information Security Objectives

5.1 Information security is a critical component of regulatory compliance. To ensure the confidentiality, availability and integrity of the group's information assets, implementing a proper level of information security control in the Group is required.

5.2 The Group shall ensure the consistency of operating environment's security while sharing the information internally or externally.

5.3 The Group's information Security policies and procedures shall be established in compliance with applicable information security laws and regulations.

5.4 The Group's information technology operations shall ensure information security and protect confidential and sensitive information from data leakage and loss.

5.5 The Group's information assets (including software, hardware, network devices, database, and others) shall be properly protected to prevent any unauthorized or accidental modification and destruction. Backup plans and disaster recovery programs shall be established and tested regularly.

5.6 The Group’s information technology projects shall consider information security-related issues.

5.7 The Group shall ensure information security awareness training is conducted regularly to enhance employees’ awareness.

6 Personal Data Protection Objectives

6.1 The Group shall establish personal data protection management system in compliance with data protection legislation to ensure the personal data entrusted to the Group is processed in accordance with data subjects’ rights.

6.2 The procedures regarding the collection, processing and handling of personal information within the Group shall prevent it from being stolen, altered, damaged, destroyed, disclosed or from other unreasonable use of personal information, and exercise the duty of good managers to establish the foundation of trust for personal data providers and protect the rights and interests of the parties.

6.3 The Group shall notify the affected individual about the personal data breach to the data subject and conduct remediation action.

6.4 The Group shall ensure the correctness of personal data and update it where necessary.

6.5 The Group shall ensure only the minimum necessary personal data is collected for legitimate purposes and will not process excess personal data.

6.6 The Group shall ensure personal data protection awareness training is conducted regularly to enhance employees’ awareness.

7 Exception Management

Everyone should comply with the Group's information security policies. However, due to legal issues, technical capabilities or cost considerations anyone that needs an exemption from the policies should submit a request for approval. This will help maintain flexibility and completeness of information security and ensure personal data protection management.

8 Authorization and Updates

This policy shall be maintained, updated, and reviewed annually to meet the ongoing legal, regulatory, environmental, business, and technical developments. Changes to this policy shall be approved by the Board of Directors and announced to all Delta personnel.

9 Revision History

Version	Description	Author	Approver	Date
1.0	First release	IT Information Security Dept.	Board of Directors	2023/04/27