台達電子工業股份有限公司

DELTA ELECTRONICS, INC.

Information Security Management Standards

Document Number: DEI-DIS-ST02 / Version: 1.0

Last Reviewed Date: 2023/11/30

Confidential Level: Internal Public

Document Summary – Information Security Management Standards			
Document Number	DEI-DIS-ST02		
Version	1.0		
Description	Delta Group has established this document to ensure confidentiality, integrity, availability, and regulatory compliance of Delta Group′ s information and information processing facilities (including software, hardware, data, documents, employee, etc.) and protect Delta Group′ s information assets from internal and external threats and incidents (both intentionally and unintentionally) . Per requirements of ISO27001, Delta Group′ s business requirement, and Delta Group's information security policy, this document has established a PDCA management model		
Document Owner	Information Security Department		
Last Revision Date	2023/11/30	Approval Date	
Approval Records	Name: LF Tseng Title: CISO		

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

Countersign Record	
Countersign Department	
Signature	

Table of Content

1 Purpose

Delta Electronics Inc. (hereinafter referred to as "Delta Group" or "Delta") has established this document to ensure confidentiality, integrity, availability, and regulatory compliance of Delta Group's information and information processing facilities (including software, hardware, data, documents, employee, etc.) and protect Delta Group's information assets from internal and external threats and incidents (both intentionally and unintentionally). Per requirements of ISO27001, Delta Group's business requirement, and Delta Group's information security policy, this document has established a PDCA management model.

2 Scope

All Delta Group information system operation procedures and environments.

3 Definition

3.1 Delta Group: Delta Electronics ("Delta") and its subsidiaries, affiliates, and companies with direct or indirect substantive control of Delta.

3.2 Delta Personnel: Delta Group's directors (including independent directors), supervisors, managers, and all employees.

4 Roles and Responsibilities

4.1 All Personnel

Employees (including regular, temporary and contract employees) and outsourced vendors should understand and comply with Delta's information security and privacy information management system.

4.2 Management

Support the implementation and improvement of Information Security Management Systems ("ISMS") and Privacy Information Management Systems ("PIMS"), provide resources required for ISMS operation, and

ensure all Delta ISMS and PIMS personnel are competent to perform their duties.

4.3 Information Security Management Team

Responsible for conducting information security management related operations of Delta Group.

4.4 Personal Data Management Team

Responsible for conducting personal information management related operations of Delta Group.

5 Identify Information Security Requirements

5.1 Operation of ISMS and PIMS

Per ISO 27001 Standard, Delta Group has established ISMS and PIMS based on the Plan-Do-Check-Act (“PDCA”) model to ensure the effectiveness and continual improvement of the management system. The details of the model are listed as followings:

5.1.1 Plan: Per *DEI-DIS-PL01-Delta Group Information Security and Personal Data Protection Management Policy*, an information security and personal information protection organization shall be established to control potential information security threats and vulnerabilities, plan risk assessments, and develop and deploy control measures for the implementation of ISMS and PIMS.

5.1.2 Do: Perform ISMS and PIMS control measures.

5.1.3 Check: Monitor the implementation of ISMS and PIMS control measures and review the effectiveness of ISMS and PIMS.

5.1.4 Act: Establish and perform corrective actions based on the ISMS and PIMS review findings and recommendations to ensure the continual operation of ISMS and PIMS.

5.2 Needs and Expectations of Interested Parties

Delta Group shall proactively communicate with interested parties (including employees, authorities, unions, customers, experts, vendors, etc.) and collect interested parties' ISMS and PIMS requirements (For example, information security duties or obligations in laws, regulations, or contracts).

5.3 Needs and Expectations of Delta Group Departments

In compliance with Delta Group's ISMS and PIMS policies and procedures, each individual department shall establish information security and privacy protection operating procedure for its own security roles and responsibilities to meet Delta Group's information security and privacy protection requirements.

5.4 Determining the scope of ISMS and PIMS

Delta Group's ISMS and PIMS scope shall be the security and privacy management of all business activities that Delta Group handles.

5.4.1 ISMS and PIMS Steering Committee Meeting shall determine the boundaries and applicability of the ISMS and PIMS when establishing the scope.

5.4.2 When determining the scope, Delta Group shall consider the followings:

(1) External and internal issues and their impacts on ISMS.

(2) Needs and Expectations of Interested Parties.

(3) Interfaces and dependencies between activities performed by Delta Group and those that are performed by other organizations.

5.5 Information Security Policy Acknowledgment

All Delta personnel shall read over the Delta Group's Information Security Policy Acknowledgement, to understand Delta Group's security requirements. When necessary (such as changes in laws and regulations),

Delta Group personnel shall sign the Acknowledgement.

6 Establishment of ISMS Roles and Responsibilities

Delta Group has established Information Security and Personal Information management organization to perform relevant activities in accordance with their assigned roles and authorities. Refer to *DEI-DIS-ST04-Information Security and Personal Information Management Organization Charter* for further details.

7 Plan

7.1 Information Risk Assessment

To establish controls for a secured operation environment and enable Delta Group to provide secured and reliable services, Delta Group shall perform information security and privacy risk assessments at planned intervals, including risk identification, impact analysis, remediation and risk mitigation controls, and residual risks. Refer to *DEI-DIS-ST05-Information Security Risk Management Policy*.

7.2 Information Security Objective and Planning to Achieve Them

Please refer to objective established in the Delta Group's *DEI-DIS-PL01 Delta Group Information Security and Personal Information Protection Policy*.

7.2.1 The Information security objectives shall:

(1) Be consistent with the Information Security Policy.

(2) Be measurable (if practicable).

(3) Take into account applicable information security requirements, and the results from risk assessment and risk treatment.

(4) Be monitored.

(5) Be communicated.

(6) Be updated as appropriate.

(7) Be available as documented information.

7.2.2 When planning how to achieve the information security objectives, Delta Group shall determine:

(1) What will be done.

(2) What resources will be required.

(3) Who will be responsible.

(4) When it will be completed.

(5) How the results will be evaluated.

7.3 Planning for Changes

When Delta Group determines the need for changes to the ISMS, the changes shall be carried out in a planned manner.

8 Support

Delta Group supports ISMS implementation via the following methods:

8.1 Resource Allocation

Delta Group's ISMS Team and Personal Data Management Team are responsible for ensuring an effective internal and external communication and the recourse allocation planning to support all Delta Group departments' ISMS and PIMS system are in compliance with ISO 27001 requirements and ISO 27701 requirements, to conduct the PDCA management cycle and continuous improvement.

8.2 Ensuring the Competence of Operation

8.2.1 All Delta Group departments shall conduct training to ensure all information security relevant personnel are competent. Personnel responsible for information security shall receive at least 3 hours of training annually.

8.2.2 To ensure the competence or improvement of employees who perform information operations, where applicable, take actions to

acquire the necessary competence, and evaluate the effectiveness of the actions taken.

8.2.3 Retain appropriate documented information as evidence of competence.

8.3 Enhancing Security Awareness

8.3.1 To ensure Delta Group's employees and outsourced providers are aware of security risk and enhance information security and personal data protection awareness, ISMS Team and Personal Data Management Team shall collect and communicate relevant topics via various channel.

8.3.2 Information security and privacy information protection training shall include information operations topics, such as ISMS and PIMS policies and procedures, information security and personal data protection laws and regulations, information security incidents and case study, information security technology and other related knowledge. etc. Besides internal training, Delta Group can assign employees to attend relevant external training and conference.

8.3.3 Information security and privacy information protection awareness notification shall be conducted in the following events:

(1) On-boarding of new employees: All new joiners shall be aware of Delta Group's ISMS and PIMS requirements that are relevant to their duties. All new joiners shall be notified on the ISMS and PIMS policies and procedures of Delta Group.

(2) Change in roles, equipment, operation procedures: In the event that there is a change in role, equipment, or operating procedures, relevant personnel shall be made aware of ISMS policies and procedures to prevent potential incident and data

leakage from happening.

(3) After engaged an outsourcing service provider, project owner shall notify the outsourcing service provider on the ISMS and PIMS policies and procedures that they are required to follow. Relevant access controls policies and procedures shall be communicated in accordance with Delta Group's *DEI-DIS-ST03-Information Security Control Standards*.

8.3.4 Awareness Evaluation and Record

(1) Evaluation methods shall be considered to evaluate the effectiveness of the training. For example, conducting exam and discussion, etc.

(2) Awareness training programs, training assessment results, and attendance records shall be retained for tracking purposes.

8.4 Continuous Communication

Delta Group shall determine the internal and external communication or dissemination needs related to the ISMS and PIMS, and update the topics in *DEI-DIS-ST04-F02-List of Interested Parties for Information Security and Personal Data Management*, including the following:

(1) On what to communicate.

(2) When to communicate.

(3) With whom to communicate.

(4) How to communicate.

8.5 Documentation Control

The ISMS policies and procedures of each department of Delta Group shall comply with the following document management requirements, please refer to *DEI-DIS-ST01-ISMS Document and Numbering Standards* for detailed document management. If a Delta Group company has its own

documentation control methods, the company may follow its own methods.

9 Do

Delta Group implement the following information security control requirements:

9.1 Information Security Risk Assessment

9.1.1 The relevant department shall perform the information asset inventory at least annually, and shall update the risk assessment results based on the information asset inventory results.

9.1.2 ISMS Team shall compile the risk assessment results of each department. Based on the previous acceptance risk values defined by ISMS and PIMS Steering Committee, ISMS Team shall request the departments with risk values greater than the acceptance risk value to plan and prepare the risk treatment plan.

9.1.3 After the establishment of the risk treatment plan, relevant authority is responsible for executing its risk treatment plan and report the result to ISMS Team within the remediation timeline.

9.1.4 When there is any change in ISMS and PIMS requirements, risk assessment shall be performed for the impacted scope.

9.2 Tracking of Risk Treatment

ISMS Team shall proactively monitor the effectiveness of the implementation of risk treatment plans and report to ISMS and PIMS Steering Committee.

10 Check

10.1 Monitor ISMS and PIMS Performance Measurements

10.1.1 ISMS and PIMS performance measurements shall be established based on the objectives of ISMS and PIMS policy. The measurement should be measurable, objective, and cover confidentiality, integrity, and availability.

10.1.2 Each department shall evaluate the ISMS and PIMS performance measurements on a yearly basis. If there is any modification or introduction of the measurements, each department shall notify ISMS Team.

10.1.3 ISMS Team and Personal Data Management Team are responsible for collecting and compiling the performance measurements on a regular basis and reporting to the ISMS and PIMS Steering Committee on an annual basis to review the effectiveness of the management system.

10.2 Measure the ISMS and PIMS performance measurements

10.2.1 Each department shall fill in the *DEI-DIS-ST04-F04 Information Security and Privacy Management Performance Measurement Statistical Table* according to the measurement cycle of each performance measurement in the document ISMS and PIMS effectiveness measurements results in the *DEI-DIS-ST04-F04 Information Security and Privacy Management Performance Measurement Statistical Table,* regularly submit it to the ISMS Team and Personal Data Management Team for summarization, and keep the monitoring data to prepare the measurement results for verification of accuracy.

10.2.2 ISMS Team and Personal Data Management Team are responsible for confirming that all relevant performance measurements are measured according to the measurement cycles and retaining the records of measurements.

10.2.3 ISMS Team and Personal Data Management Team shall conduct sample testing to verify the accuracy of the measurements submitted by each department.

10.3 Analysis and Evaluation of ISMS and PIMS Performance Measurements

10.3.1 If a certain measurement did not meet the measurement target, ISMS Team and Personal Data Management Team shall verify whether there was an error in calculation and confirm whether the relevant department has failed to achieve the target measurements.

10.3.2 ISMS Team and Personal Data Management Team shall examine the result of the measurements on a yearly basis, analyze, evaluate the results, and report the results to ISMS and PIMS Steering Committee.

10.4 Conduct Information Security and Privacy Information Management Internal Audit

10.4.1 General requirement

Delta Group shall conduct internal audits at planned intervals to provide information on whether the ISMS and PIMS:

(1) Conforms to

i. The organization's own requirements for its information security management system.

ii. The requirements of this document.

(2) Is effectively implemented and maintained.

10.4.2 Drafting the Internal Audit Plan

The internal audit plan shall include:

(1) Internal Audit Scope

i. The ISMS and PIMS internal audit shall cover processes and controls related to the scope of the ISMS and PIMS implementation.

ii. The scope can be modified based on the result of the previous internal audit and shall cover the level of control implementation, effectiveness and the level of compliance of ISMS and PIMS performance measurements.

(2) Appointment of Internal Auditor

i. It is recommended to appoint the internal auditor who has completed ISO 27001 Lead Auditor training or attended relevant training for at least two hours to perform the internal audit.

ii. Conflict of interests shall be avoided when appointing the internal auditor to ensure the independency and the impartiality.

iii. When required, an internal or external expert may be appointed.

10.4.3 Internal Audit Preparation

(1) The leader of the internal audit team shall notify the auditee prior to performing the audit.

(2) Prior to the ISMS & PIMS internal audit, the appointed internal auditor shall understand the purpose, scope, audit methods, potential risk of the audit, and the content of the *DEI-DIS-ST02-F01-ISMS and PIMS Internal Audit Checklist*.

10.5 Conduct Internal Audits

10.5.1 When conducting internal audits, the followings shall be aware of:

(1) Internal auditor shall be impartial and objective. Audit scope, audit areas, non-conformity findings shall be documented in *DEI-DIS-ST02-F01-ISMS and PIMS Internal Audit Checklist*. Evidence shall be retained. Internal audit results shall be

submitted to the Head of Department of the auditee for confirmation. The confirmed checklist shall be submitted to ISMS Team and Personal Data Management Team for review.

(2) Internal auditor is responsible for the confidentiality of information that was collected during the audit.

(3) An internal audit report shall be submitted to the lead of ISMS and PIMS internal audit team for review. The result shall be consolidated into internal audit report for the auditee's confirmation and submit to ISMS and PIMS Steering Committee.

(4) ISMS Team or Personal Data Management Team may propose a modification of audit areas based on the recommendation of authorities and the result of internal audits.

10.5.2 In the event that using an audit tool is required, it is mandatory to discuss with the auditee on how the tool would be used and what the potential risk would be. The discussion shall cover the followings to determine how business continuity can be ensure:

(1) Avoid peak periods and unnecessary audit items.

(2) During the audit, it is required to assign a person to monitor the audit to ensure an immediate response if an unplanned issue has occurred.

(3) Access control of the audit record generated by the audit tool shall be implemented to prevent unauthorized data access.

(4) The auditor shall document the tools being used for the audit and the result in *DEI-DIS-ST02-F01-ISMS and PIMS Internal Audit Checklist*.

(5) Appropriate personnel shall be assigned to be in charge for the audit tool's installation, safekeeping, removal, and access

controls to prevent unauthorized data access.

10.5.3 If using a computer-assisted audit techniques is required, it is mandatory to consider the followings for the examination:

(1) Discuss the scope of audit with the system owner and the system custodian prior to the audit.

(2) Audit testing shall be conducted by the system owner of the auditee.

10.6 Retention of Internal Audit Records

ISMS Team and Personal Data Management Team are responsible for the record-keeping for a minimum of three years for the ISMS and PIMS internal audit documentation and records. Records shall be stored in a centralized storage location based on the security level of the document.

11 Improvement

The Delta Group requirements of continual improvement are as follow:

11.1 Continual Improvement

Delta Group shall continually improve the suitability, adequacy and effectiveness of the ISMS and PIMS.

11.2 Nonconformity and Corrective Action

11.2.1 Nonconformity may be raised based on the following activities:

(1) Internal Audit Results

i. Auditee shall issue a *DEI-DIS-ST02-F02-Corrective Action Form* within two weeks of receipt of internal audit report for the nonconformity items. The corrective action form shall be approved by the head of the auditee department and submitted to ISMS Team and Personal Data Management Team for review.

ii. ISMS Team and Personal Data Management Team shall consolidate the result of internal audit to the ISMS and PIMS Steering Committee.

(2) Evaluation of Measurements

ISMS Team and Personal Data Management Team shall issue *DEI-DIS-ST02-F02-Corrective Action Form* to the relevant department. The relevant department shall reply to *DEI-DIS-ST02-F02-Corrective Action Form* and submit the document to ISMS Team and Personal Data Management Team for the following non-conformity items. The nonconformity items shall be included in the next internal audit.

The nonconformity items:

i. For monthly indicator, an indicator has recorded as not meeting target for two consecutive months.

ii. For quarter, semi-annual, annual indicator, an indicator has recorded as not meeting target.

ISMS Team and Personal Data Management Team shall consolidate the result of measurements and submit it to the ISMS and PIMS Steering Committee.

(3) Information security and privacy information leakage incident

i. The root cause of the incident should be analyzed by the department where the information security incident or data breach occurred. The department shall issue *DEI-DIS-ST02-F02-Corrective Action Form* within two weeks. The department shall complete the *DEI-DIS-ST02-F02-Corrective Action Form* and submit it to ISMS Team and Personal Data Management Team for review.

ii. ISMS Team and Personal Data Management Team are responsible for consolidating the result of incident response and report to ISMS and PIMS Steering Committee.

(4) External Audit Results

i. ISMS Team and Personal Data Management Team shall issue *DEI-DIS-ST02-F02-Corrective Action Form* for the nonconformity items within two weeks of external audit. The relevant responsible department shall complete the *DEI-DIS-ST02-F02-Corrective Action Form* and submit it to ISMS Team and Personal Data Management Team for review.

ii. ISMS Team and Personal Data Management Team is responsible for submitting the consolidated nonconformity corrective action result of external audit to the ISMS and PIMS Steering Committee.

11.2.2 Nonconformity items shall be monitored until the corrective action has been completed. The monitoring and tracking shall be based on the following requirements:

(1) ISMS Team and Personal Data Management Team shall monitor the progress of corrective action items based on the approved timeline in *DEI-DIS-ST02-F02-Corrective Action Form*. If an action item has been completed, it is required to record the completion and review date in *DEI-DIS-ST02-F02-Corrective Action Form*.

(2) In the event that a corrective action cannot be completed within the approved timeline, it is mandatory to record the root cause of the delay and establish a revised timeline. In the event that a

corrective action cannot be completed within the original and revised timeline, ISMS Team and Personal Data Management Team shall report the issue to the ISMS and PIMS Steering Committee.

(3) The action owner shall report the status of the action item to ISMS Team and Personal Data Management Team before the corrective action timeline defined in *DEI-DIS-ST02-F02-Corrective Action Form*. Relevant evidence and records shall be submitted to the lead of ISMS Team and Personal Data Management Team for review and approval.

(4) If the ISMS Team and the Personal Data Management Team have determined that the evidence of corrective actions is not sufficient, it is mandatory to notify the auditee to make corrections and provide a revised schedule. If the auditee fails to update the evidence, ISMS Team and Personal Data Management Team shall dispute the *DEI-DIS-ST02-F02-Corrective Action Form*.

12 Policy Update and Revision

This document shall be approved by the CISO and announced. On a yearly basis, this document shall be reviewed based on the change in legal, regulation, environment, business, and technology requirements. In the event that this document is revised, the revised document shall be announced to all Delta employees via an email notification, a post on Delta Group's public forum, or a briefing in a meeting.

13 Reference

13.1 Reference Documents

(1) DEI-DIS-PL01-Information Security and Personal Data Protection

Management Policy

(2) DEI-DIS-ST01-ISMS Document and Numbering Standards

(3) DEI-DIS-ST03-Information Security Control Standards

(4) DEI-DIS-ST04-Information Security and Personal Information Management Organization Charter

(5) DEI-DIS-ST05-Information Security Risk Management Policy

13.2 Reference Forms

(1) DEI-DIS-ST02-F01-ISMS and PIMS Internal Audit Checklist

(2) DEI-DIS-ST02-F02-Corrective Action Form

(3) DEI-DIS-ST04-F02-List of Interested Parties for Information Security and Personal Information Management

(4) DEI-DIS-ST04-F04-ISMS and PIMS Measurement Result

14 Revision History

Version	Revision Date	Author	Approver	Description
1.0	Initial Publication	Jenny Tsen	Leo Kuo	