台達電子工業股份有限公司

DELTA ELECTRONICS, INC.

Information Security and Personal Information Management Organization Charter

Document Number: DEI-DIS-ST04 / Version: 1.0

Last Review Date: 2023/06/23

Confidential Level: Internal Public

Document Summary– Information Security and Personal Information Management Organization Charter			
Document Number	DEI-DIS-ST04		
Version	1.0		
Description	The purpose of this document is to reinforce Information Security Management Systems and Personal Information Management System in Delta Electronics Inc.; to establish management structure that is responsible for reviewing ISMS and PIMS policies and procedures and coordinating the implementation of controls; and to ensure the continual operations of ISMS and PIMS.		
Document Owner	Information Security Department		
Last Revision Date	2023/06/23	Approved Date	2023/08/19
Approval Records	Chairman of ISMS & PIMA steering committee		

Document Release/ Revision/ Deletion Approval Record (e-signature)	
E-form Number	2023080160796
Application Date	2023/08/18

Table of Content

1 Purpose

To effectively promote and implement the Delta Group's (hereinafter referred to as "the Group") information security (hereinafter referred to as "IS") and personal information (hereinafter referred "PI") management system. By establish an appropriate management framework to review information and personal data management policies and procedures, allocate security responsibilities, and coordinate the implementation of various information security measures within the Group, in order to facilitate the sustainable and robust operation of the IS Management System and PI Management System(hereinafter referred "ISMS and PIMS ").

2 Scope

All business activities that are relating to ISMS and PIMS within Delta Group.

3 Definition

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

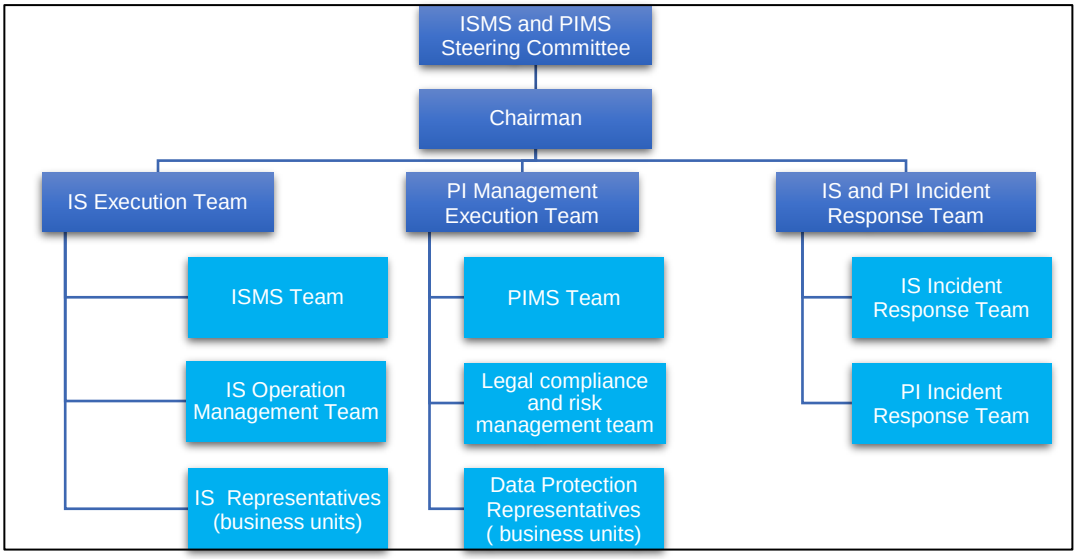
3.2 External Experts: competent authorities, judicial and police units, information security consultants, information service consultants, and other organizations, institutions, or individuals that provide professional advice and consultation or information exchange.

4 Policy

4.1 Information Security and Personal Information Management Organization Structure

In order to ensure the implementation of ISMS and PIMS, Delta has established an ISMS and PIMS organization. The organization structure is shown in the figure below. Members of this organization should be listed in

the "Information Security Management Organization Member List" and "Personal Data Protection Team Organization List" respectively. In case of personnel changes, they should be updated accordingly.



4.2 ISMS and PIMS Steering Committee Responsibility

The roles and responsibilities of ISMS and ISMS steering committee are listed as below. Overseas branches and manufacturing sites may modify the structure of this steering committee to adapt to the specific organization structure and local legal and regulatory requirements.

4.2.1 Chairman

The chairman shall be CEO of the organization or be the representative who is assigned by the chairman.

(1) Host annual committee meeting, review ISMS, PIMS and information security governance implementation status.

(2) Responsible for the major decision-making and supervision of information security management, personal data protection, and cybersecurity governance.

(3) Host cross-functional meeting for resource allocation to implement ISMS and ISMS measures. (if required)

4.2.2 Convener

The convener shall be assigned by the chairman.

(1) ISMS convener is responsible for overseeing the implementation and operation of ISMS of the Group.

(2) PIMS convener is responsible for overseeing the implementation and operation of PIMS of the Group.

4.2.3 Committee Members

Each business group, business units, and corporate function department shall assign one to two representatives to be the committee members.

(1) Responsible for decision making of ISMS, PIMS, and issues relating to information security governance

(2) Responsible for organizing the operation of ISMS and PIMS activities

(3) Responsible for overseeing, examining, and evaluating ISMS and PIMS policies and procedures.

(4) Responsible for attending the steering committee meetings and examining the effectiveness and appropriateness of ISMS and PIMS policies and procedures.

4.3 Information Security Execution Team

This team shall be led by the head of information security department and is responsible for planning and executing tasks relating to ISMS. This execution team includes three functional teams, which are ISMS operation team, Business IS representative team, and DLP management team.

4.3.1 ISMS Team Responsibility

(1) Provide information security management measures.

(2) Identify external documents/requirements related to

information security.

(3) Promote ISMS related activities.

(4) Conduct ISMS related awareness training.

(5) Consolidate internal and external information security issues and interested parties' information security requirements, and update the "ISMS&PIMS Interested Party List" on regular base.

(6) Evaluate internal and external information security issues and conduct risk assessment when is required.

(7) Establish a risk management framework and conduct risk management practices.

(8) Analyze and discuss new information security product and technology.

(9) Consolidate and analyze ISMS Measurement Indicator.

(10) Follow-up findings and correction action items identified based on internal or external audit.

(11) Consolidate applicable laws and regulations regarding information security.

4.3.2 IS Operation Management Team Responsibility

(1) Collection of Cybersecurity Intelligence

(2) Assistance in Managing Cybersecurity Incidents

(3) SIEM Operation and Management

(4) DLP System and Policy Maintenance

(5) Data Leakage issues reporting and follow-up.

4.3.3 Business IS Representative Team Responsibility

Each business group, business units, and corporate function department shall assign one to two ISMS enforcement

representative. The representatives are responsible for the implementation and reinforcement of ISMS and collect information security issues and requirements from his/her own department.

4.4 Personal Information Protect Execution Team

This team includes three functional teams, which are personal data management team, business data protection representative team, and legal compliance and risk management team.

4.4.1 Personal Data Management Team Responsibility

(1) Responsible for managing the overall operation of the Group's PIMS policies and procedures.

(2) Organizing personal data risk assessment practices

(3) Establish personal data related awareness training program.

(4) Evaluate the appropriateness of outsourcing the operation activities relating to personal data.

(5) Consolidate PIMS related issues to be discuss in the ISMS and PIMS steering committee meetings.

4.4.2 Legal Compliance and Risk Management Team Responsibility

(1) Provide legal advice and interpretation on the applicable PI related laws and regulations on the collection, processing, and use of personal data.

(2) Consolidate a list of applicable PDP laws and regulations and document the list in "Personal Data Protection Legal Compliance List". For changes in laws and regulations, the team shall update the "Personal Data Protection Legal Compliance List" and this policy with the PDP Governance Team.

4.4.3 Business Data Protection Representatives Team Responsibility

Each business group, business units, and corporate function department shall assign one to two PIMS representative to assist in implementing the Group's policies and procedures regarding PIMS. The representatives are responsible for the following items:

(1) Confirm the reasonableness, objectives, methods of handling, and retention period of personal data prior to the collection, processing, and use of personal data.

(2) Ensure the processing of personal data is limited to what is necessary in relation to the purposes for which the personal data is collected.

(3) Inquire regulatory and compliance issues regarding the collection, use, and process of personal data with the local legal department or relevant authorities.

(4) In the event that the collection, process, and use of personal data involves transfer of personal data to a third country or to an international organization via network connection from the Group's information systems or database, it is mandatory to inquire regulatory, compliance, and technical issues regarding the collection, use, and process of personal data with the local legal department, IT department, or relevant authorities.

(5) The Group's business groups, business units, and corporate functions shall ensure the security of personal data by complying with the following requirements:

   i. The collection, use, and processing of personal data shall be fairly, reasonable, and limited to what is necessary in relation to the purposes for which the personal data is processed.

ii. The Group shall protect personal data in its possession or under its control by making reasonable security arrangements.

iii. The Group shall make the business contact information available to the public for the data subjects to exercise their rights regarding personal data or submit related complaints and consultations or arrange appropriate responses or measures in compliance with local laws and regulations.

iv. The representative shall establish personal data breach incident response plan that covers such incidents as theft, alteration, damage, loss, or leakage of personal data.

v. When engaging an outsourced personal data processor to act on behalf of the Group to collect, process, and use of personal data, the Group shall monitor the processor to ensure reasonable security arrangements are performed.

vi. The representative shall ensure its compliance with the Group's PIMS policies and procedures (including those that are published locally based on local applicable laws and regulations or the business requirements) for the protection of personal data.

vii. If the business group/ unit/ corporate function collects, processes, and uses personal data, the representative shall ensure that the department performs its business activities in accordance with the Group's PDP policies and procedures, applicable laws and regulations, and international standards. PIMS controls shall be

established based on the nature of the duties of each department. The controls shall be announced to all personnel within each department electrically, written notice, or other means. The representative shall continuously respond to the security maintenance requirements of personal data protection, and propose improvement plans after audits.

4.5 Information Security and Personal Information Incident Response Team

4.5.1 Information Security Incident Response Team Responsibility

4.5.2 IS Incident Team's roles and responsibilities are listed as followings:

(1) Team Lead

Team Lead shall be assigned by CIO.

i. If a major information security incident occurred, assemble an emergency response team and contact the relevant team members.

ii. Coordinate the resource allocation and supervise the ISMS representatives' operations.

iii. Based on the evaluation of the incident, provide a recommendation to CIO to determine whether a Business Continuity Plan shall be activated.

iv. If a disaster has occurred, work with disaster recovery personnel to take charge of the disaster recovery process and relevant activities, such as evacuation of personnel and equipment.

v. Manage post-disaster recovery processes including post-disaster communication, coordinating activities with emergency response team, and planning out the

recovery activities for the original site.

(2) Team Member

Team members shall include representatives from core business functions. Roles and responsibilities are listed as followings:

i. Contact relevant personnel to perform disaster recovery activities, including development, maintenance, update, and execution.

ii. Organize relevant personnel to perform semi-annual business continuity plan testing and drill.

iii. Collect evidence on the disaster site for prospective claims and legal remedies.

iv. Evaluate damage on the disaster site and perform recovery actions.

4.5.3 PI Incident Response Team

The team is responsible for organizing the emergency response team if a personal data related incident has occurred. The emergency response team shall perform incident response activities and notify internal/ external parties regarding the incident. Refer to the Person Data Incident Response Procedure for the detailed process.

4.6 ISMS and PIMS Steering Committee Meeting

4.6.1 Facilitate the Meeting

(1) The meeting shall be conducted regularly (at least annually) to ensure the effectiveness of ISMS and PIMS management systems. If an unplanned meeting is required, the chairman of ISMS and PIMS Steering Committee may organize an ad-hoc

meeting.

(2) The meeting may be conducted in the method of documentation review.

(3) Unless advice otherwise, the meeting shall be organized and facilitated by the ISMS Operation Team and PIMS Operation Team.

4.6.2 Deputy Mechanism

If the chairman could not host the meeting, the chairman shall assign a deputy chairman to perform his/ her duties. If the committee members or the attendees could not attend the meeting, the person shall assign a deputy to undertake his/ her duties.

4.6.3 Attendees

When required, internal or external expert may be invited to attend the meeting and participate in the discussion.

4.6.4 Meeting Minutes

(1) Conversation and decision shall be recorded in a written format. Meeting minutes shall be distributed to the attendee.

(2) Meeting minutes shall be maintained based on its confidential and security level, and proper security controls shall be conducted.

4.6.5 Meeting Agenda

(1) Recommended topics of review in the meeting are listed as followings:

i. ISMS and PIMS audit findings and corrective actions.

ii. Recommendation from internal personnel, external parties, authorities, interested parties.

iii. Review of the introduction of new product and

technology.

iv. Review of corrective and preventative plans.

v. Review of risk assessment results.

vi. Status of implementation of action items raised in the previous meeting.

vii. Any items that may impact ISMS and PIMS management system.

viii. Recommendation from ISMS and PIMS relevant personnel.

ix. KPI report of ISMS and PIMS.

x. Review information security and personal data incident.

(2) Recommended decisions to be made in the meeting are listed as followings:

i. Areas of improvement for ISMS and PIMS management system.

ii. Update on risk assessment and risk treatment plan.

iii. Revise policies and procedures based on potential internal/ external incidents, including:

1) Changes in the operational requirements.

2) Changes in the security requirements.

3) Changes in the procedures due to changes in the operational requirements.

4) Changes in management and regulatory requirements.

5) Changes in contractual requirements; and

6) Changes in the risk tolerance.

iv. Coordinate resources required for ISMS and PIMS operation.

v. Areas of improvement for control effectiveness matrix.

vi. On a yearly basis, review ISMS KPI and PIMS KPI measurements, evaluate whether these KPIs shall be updated, and draft action plans for the modification of KPI indicators.

4.7 Internal and External Communications

ISMS Operation Team and PIMS Operation Team shall decide whether an internal and external communications relevant to the information security management system including:

(1) on what to communicate.

(2) when to communicate.

(3) with whom to communicate.

(4) who shall communicate; and

(5) the processes by which communication shall be affected.

5 Reference

5.1 Reference Documents

PIMS-CHT-02-03-002 Personal Data Incident Response Management Procedure

5.2 Reference Forms

(1) DEI-DIS-ST04-FO01 ISMS Organization Member List

(2) DEI-DIS-ST04-FO02 ISMS&PIMS Interested Party List

(3) DEI-DIS-ST04-FO03 List of Applicable Laws

(4) DEI-DIS-ST04-FO04 ISMS Measurement Indicator List

(5) PIMS-CHT-04-04-001 Personal Data Protection Team Organization

List

(6) PIMS-CHT-04-05-001 Personal Data Protection Measurement Indicator List

Revision History

Version	Description	Author	Manager	Date
1.0	Combine Information Security and Data Protection Function	Jenny Tsen	LF Tseng	2023/08/XX