台達集團
DELTA GROUP

| | |
|---|---|
| Document Name: | Personal Data Protection and Incident Response Management Regulation |
| Document No.: | DEI-PIMS-ST02 |
| Version: | 001 (Approved by the PIMS convener on August 27, 2024)<br>002 (Approved by the PIMS convener on July 22, 2025) |

# Table of Contents

## 1. Purpose

Delta Group has considered the “Delta Group Information Security and Personal Information Protection Policy” and “Information Security Management Standards” in formulating the ”Personal Data Protection and Incident Response Management Regulation”. The Group has also implemented a PDCA (Plan-Do-Check-Act) management model to ensure the continuous and effective operation of the personal data protection management system. This system is designed to maintain the confidentiality, integrity, availability, and legality of personal data (including private information) while preventing deliberate or accidental threats from both internal and external sources.

## 2. Scope

2.1. This regulation applies to the Delta group.

2.2. Delta Group personal information management system is based on the framework of ISO27701 international standard, and it covers the critical business of Delta Group.

## 3. Definition

3.1. “Delta Group” includes Delta Electronics and its subsidiaries, affiliated companies, and its affiliates that have direct or indirect substantial control over the world.

3.2. “Delta Members” is the collective name for all directors (including independent directors), managers, and employees of all companies within the Group.

## 4. Rights and Responsibilities

4.1. All Personnel

Employees of the Delta Group (including full-time staff, secondees, and contracted staff), as well as outsourced vendors, must understand and comply with the Group’s information security and personal data protection management system.

4.2. Management level shall conduct the following points in order to show the support of implementing personal information management system.

4.2.1. Communicate with stakeholders and comply with the regulation requirements in order to enhance the personal information management objectives.

4.2.2. Authorize the Personal Information Management Execution Team to manage personal

information management process.

4.2.3. Comply with “Delta Group Information Security and Personal Information Protection Policy” in order to establish personal information management objectives and strategies.

4.2.4. Approve personal information audit plan and result.

4.2.5. Approve the acceptable risk level within the group.

4.2.6. Provide necessary resource that support the personal information management system.

4.3. The Group has established an Information Security and Personal Data Protection Organization (hereinafter referred to as the "Information Security and Data Protection Organization") to carry out related operations according to its responsibilities. For detailed information on the organizational structure and responsibilities, please refer to the ”Information Security and Personal Information Management Organization Charter”.

4.3.1. Personal Data Management Team: Responsible for conducting Delta Group personal information protection measures.

4.3.2. Information Security Management Team: Responsible for conducting Delta Group information security protection measures.

## 5. Identifying Personal Data and Privacy Requirements

5.1. Personal information management system mechanism

5.1.1. The Group has established an Information Security and Personal Data Protection Organization and issued a Personal Data Management Policy to explain the direction, objectives, and implementation measures.

5.1.2. Conduct risk assessments, evaluate risk levels, consolidate the findings into a risk assessment report, and track them regularly. For detailed implementation, please refer to clause 6.1 of this regulation on Personal Data (including Privacy) Risk Assessment.

5.1.3. Choose the personal data control objectives and measures that are suitable for the Delta Group to implement, and regularly review and confirm their feasibility and effectiveness. For detailed implementation, please refer to clause 9 of this regulation on Check.

5.1.4. After the personal information management system documents are issued, conduct

internal audits of personal information management to confirm the effectiveness of implementation.

5.2. Personal information management system- PDCA cycle

5.2.1. Plan: Based on the strategy and objectives of the Delta Group, a personal information management system was established by forming a personal information management organization, controlling potential threats and vulnerabilities, conducting risk assessment and security control measures.

5.2.2. Do: Implement the mechanism for controlling personal information management.

5.2.3. Check: Conduct regular checks on personal information management to ensure the implementation and effectiveness of personal data management.

5.2.4. Act: Based on the results of the check, implement corrective and preventive measures to improve the management system.

5.3. Stakeholder Requirements

The Group actively engages with relevant stakeholders (such as employees, regulatory authorities, associations, clients, expert groups, or vendors) to proactively communicate and gather their requirements regarding information security and personal data (including privacy). This includes understanding obligations and responsibilities outlined in laws, regulations, or contracts.

5.4. Unit Requirements within the Group

Under the Group's information security and personal data protection policies, each unit establishes operational procedures for personal data management within their respective security responsibilities to fulfill the general personal data protection policy requirements of the Group.

5.5. Determining the Scope of Personal Data Management System Implementation

The scope of the Group's implementation of the personal data management system should encompass all security and personal data management activities related to its responsible business operations.

5.5.1. The ISMS and PIMS steering Committee is required to determine the scope of the personal data management system, including its operational limitations and extent of operation.

5.5.2. When deciding on the scope of the personal data management system, consideration

should be given to:

(1) Identifying the impact of internal and external issues on the personal data management system.

(2) Understanding the requirements and expectations of relevant stakeholders.

(3) Operational activities within the Group and those provided by other organizations.

## 6. Plan

6.1. Personal Data (Including Privacy) Risk Assessment

The Group regularly conducts risk identification and management for personal data (including privacy) to recognize risks, assess their impacts, utilize appropriate measures to mitigate or compensate for risks, and understand residual risks. This process is essential to provide necessary control measures for ensuring a secure operational environment within the Group, enabling the provision of secure and reliable services while conducting business operations. For detailed risk management procedures, please refer to the “Information Security Risk Management Policy”.

6.2. Personal Data (Including Privacy) Goals and Achievement Plan

Please refer to the goals set in the Group's " Delta Group Information Security and Personal Information Protection Policy".

6.2.1. Goals should meet the following criteria:

(1) Consistency with the Information Security and Personal Information Protection Policy

(2) Measurable (if feasible)

(3) Consideration of applicable information security and personal information protection requirements, as well as the results of risk assessments and risk management.

(4) Monitored

(5) Communicated

(6) Updated as necessary

(7) Documented information to be provided

6.2.2. When planning how to achieve personal information protection goals, determine the following:

(1) Tasks to be completed

(2) Required resources

(3) Responsible personnel

(4) Completion timeline

(5) Method of evaluating outcomes.

6.3. Change Planning

When the Group determines a need to change the personal data management system, changes should be executed in a planned manner.

## 7. Support

7.1. Resource Management

The Group's “Personal Data Management Team” is responsible for planning manpower, scheduling work effectively, and facilitating internal and external communications to support the Group's units in aligning with the ISO 27701 international standard requirements for PDCA management cycle and continuous improvement.

7.1.1. Build Establish and maintain a personal information management system.

7.1.2. Establish and deploy personal information management and control mechanisms.

7.1.3. Confirm that the personal information management procedures can support the needs of operations.

7.1.4. Identify and discover regulations and related contract requirements.

7.1.5. Maintain an appropriate and effective control mechanism, and use relevant technical solutions for control when necessary.

7.1.6. Conduct regular personal information management reviews and implement an appropriate action plan.

7.1.7. Improve the operational process measures of personal information management as needed.

7.2. Enhancing Security Awareness

7.2.1. To enhance information security and privacy awareness among employees and external vendors of the Group, the Personal Data Management Team should collect relevant information on personal data protection and communicate this information promptly through various channels.

7.2.2. Educational training content should include topics related to personal data protection

and privacy, such as implementation regulations of the personal data management system, legal requirements concerning personal data protection, operational procedures for personal data, incidents or cases of personal data breaches, issues related to personal data protection, and other relevant knowledge.

7.3. Personnel Management and Education Training

Please refer to clause 11, “Personnel Management, Education, and Training”, in this regulation.

7.4. Continuous Communication

The Group should determine the need for internal and external communication or dissemination related to the information security and privacy management system and update issues in the “List of Interested Parties for Information Security and Personal Information Management” including the following:

(1) Topics for communication or dissemination

(2) Timing of communication or dissemination

(3) Audience for communication or dissemination

(4) Method of communication or dissemination

7.5. Document Management

For detailed document management, please refer to the “Personal Data Document and Record Management Regulation”.

## 8. Do

8.1. Risk Assessment

8.1.1. Each unit shall carry out a risk assessment at least once a year.

8.1.2. The risk assessment shall include the assessment of known risks and potential risks:

(1) The risk assessment of known risks should include the re-evaluation of the value of personal information groups, the weight of weaknesses and the weight of threats. When considering the weight of weakness and the weight of threat, the existing management system and the current status of control should be fully considered.

(2) The risk assessment of potential risks should include factors such as potential impacts, potential weaknesses, and potential threats. Consider and quantify the level of potential risks faced by personal information as the basis for selecting control measures.

8.1.3. Internal and external issues and requirements of stakeholders shall be identified, and risk assessment shall be carried out. For details, please refer to the “List of Interested Parties for Information Security and Personal Information Management”.

8.1.4. Units with risk values exceeding the acceptable threshold determined by the ISMS and PIMS steering Committee are required to develop and formulate risk treatment plans. The outcomes of each execution should be documented incrementally for future reference, and reports should be submitted to the Personal Data Management Team within the improvement period.

8.1.5. In response to changes in information security and privacy data protection requirements identified by the Information Security Management Team within the Group, the Personal Data Management Team should conduct risk assessments on the affected areas.

8.2. Tracking of Risk Treatment

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

## 9. Check

9.1. Monitor ISMS and PIMS Performance Measurements

9.1.1. ISMS and PIMS performance measurements shall be established based on the objectives of Delta Group Information Security and Personal Information Protection Policy. The measurement should be measurable, objective, and cover confidentiality, integrity, and availability.

9.1.2. 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 Personal Data Management Team.

9.1.3. 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.

9.2. Measure the ISMS and PIMS performance measurements

9.2.1. Each department shall complete the “Information Security and Privacy Management Performance Measurement Statistical Table” according to the measurement cycle

specified in the ISMS and PIMS effectiveness measurements. This table should be submitted regularly to the ISMS Team and the Personal Data Management Team for summarization. Departments are also required to retain the monitoring data to prepare for the verification of measurement results for accuracy.

9.2.2. 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.

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

9.3. Analysis and Evaluation of ISMS and PIMS Performance Measurements

9.3.1. 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 the calculation and confirm whether the relevant department has failed to achieve the target measurements.

9.3.2. ISMS Team and Personal Data Management Team shall examine the results of the measurements every year, analyze, evaluate the results, and report the results to ISMS and PIMS Steering Committee.

9.4. Personal Information Management System Internal Audit

9.4.1. Requirements for Internal audit

Delta Group should continue to improve the effectiveness of the personal information management system by formulating personal information management policies, establishing personal information management goals, conducting self-checking results based on personal information management, implementing corrective and preventive measures, and reviewing management. Management should ensure the implementation of regular audits, at least once a year.

9.4.2. General requirement

Delta Group shall conduct internal audits at planned intervals to provide information on the Personal Information Management System.

(1) Conforms to the organization's own requirements for its information security and personal information management system.

(2) Is effectively implemented and maintained.

9.4.3. Procedure for Audit

(1) Internal audit shall be carried out at least once a year as scheduled by each unit. The execution method can be carried out by the company's internal personnel or external experts.

(2) Preparatory Work for Personal Information Management Internal Audit

A. The leader of the Personal Data Internal Audit Team shall notify the inspected unit before the audit.

B. During the audit process, if the audit tools need to be used, the implementation method and possible risks should be discussed with the supervisor of the audit unit in advance. The consideration should include:

I. Avoid peak hours or omit unnecessary audit items.

II. During the audit process, relevant personnel should be assigned to monitor from the side to ensure that problems can be dealt with in time.

C. The designated internal auditor should fully understand the purpose, scope, implementation method and possible risks of audit before performing the internal audit, and should fully understand the “ISMS and PIMS Internal Audit Checklist”.

(3) Drafting the Internal Audit Plan

A. The audit scope includes the standard requirements related to PIMS, such as management policies, organizational structure, information asset classification and control, education and training, risk assessment, data retention and processing, data security issues, data transmission, third-party information disclosure, outsourced processing, management review, and corrective and preventive measures, among others.

B. Audit basis: “Delta Group Information Security and Personal Information Protection Policy” and the “ISO27701 International Standard”.

C. 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.

D. 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.

9.4.4. Conduct Internal Audits

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 “ISMS and PIMS Internal Audit Checklist”. Evidence shall be retained. Internal audit results shall be submitted to 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 Personal Data Management Team for review. The result shall be consolidated into an internal audit report for the auditee’s confirmation and submitted to the ISMS and PIMS Steering Committee.

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

9.4.5. Audit Result

| | |
|---|---|
| Conformity | (1) Actual operations fit written regulations; the records and sign-offs are handled in accordance with the regulations.<br>(2) Written regulations have been established, but there is no actual operational requirement yet. |
| Non-conformity | (1) Violation of established management regulations.<br>(2) Violation of the requirements of the ISO 27701 standard.<br>(3) Although the personnel performed operations in accordance with the regulations, errors occurred in the process.<br>(4) Operations have achieved the purpose of personal information protection, but complete written procedures or records have not yet been established. |

| | |
|---|---|
| Not applicable | The inspected unit did not have the operation content mentioned in the inspection question. |

9.4.6. Retention of Internal Audit Records

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

## 10. Improvement

10.1. Continual Improvement

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

10.2. Nonconformity and Corrective Action

10.2.1. Nonconformity may be raised based on the following activities:

(1) Internal Audit Results

A. Auditee shall issue a “Corrective and Preventive Measure Form” within two weeks of receipt of the internal audit report for the nonconformity items. The corrective action form shall be approved by the head of the auditee department and submitted to the Personal Data Management Team for review.

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

(2) Evaluation of Measurements

The Personal Data Management Team shall issue “Corrective and Preventive Measure Form” to the relevant department. The relevant department shall reply to “Corrective and Preventive Measure Form” and submit the document to the Personal Data Management Team for the following non-conformity items. The nonconformity items shall be included in the next internal audit. The Personal Data Management Team shall consolidate the results of measurements and submit them to the ISMS and PIMS Steering Committee.

(3) External Audit Results

A. In response to non-conformities identified during external audits, the relevant

responsible units should complete the “Corrective and Preventive Measure Form” and submit it to the Personal Data Management Team for record-keeping.

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

10.2.2. Nonconformity items shall be monitored until corrective actions have been completed, based on the following requirements:

(1) The Personal Data Management Team shall monitor the progress of corrective action items based on the approved timeline in the “Corrective and Preventive Measure Form”. If an action item has been completed, it is required to record the completion and review date in “Corrective and Preventive Measure Form”.

(2) If 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. If a corrective action cannot be completed within the original and revised timeline, the 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 the Personal Data Management Team before the corrective action timeline specified in the “Corrective and Preventive Measure Form”. Relevant evidence and records shall be submitted to the Personal Data Management Team for review and approval.

(4) If 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, the Personal Data Management Team shall dispute the “Corrective and Preventive Measure Form”.

## 11. Personnel Management, Education, and Training

11.1. Safety review of pre-employment personnel: Relevant regulations are handled in accordance with the relevant regulations of Delta’s personnel safety review.

11.2. Promotional safety of employees

11.2.1. Personnel promotion shall be handled in accordance with the relevant regulations of

Delta's personnel safety review.

11.2.2. All new recruits must sign the employment contract that contains personal information clauses before they can start processing or receiving personal data.

11.3. Resignation and transfer: Personnel resignation or transfer shall follow Delta Group's relevant resignation and transfer procedures to handle transfer and removal of account authorization.

11.4. Personal responsibility for password protection

11.4.1. All employees of the Delta Group should consider passwords as personal confidential information, select and use them carefully, and not share them with others. If there is a need for substitution at work, the password should be updated immediately after the end of the proxy/substitution.

11.4.2. If employees need to use a shared account due to business needs, the audit trail of the shared account shall be kept in an appropriate manner.

11.5. Proxy system

11.5.1. Each unit of the Delta Group shall appropriately assign various personal information affairs to employees, and prevent unauthorized access to prevent personal information from being stolen, altered, damaged, lost, leaked or other unreasonable use.

11.5.2. All important personnel of the personal information management system should have a proxy, and confirm that the proxy is familiar with the business content and responsibilities; and ensure that the proxy can carry out personal information related business operations, and event notifications.

11.6. Compliance with relevant laws and internal regulations

11.6.1. Besides the laws and regulations of Delta Group, other laws and regulations such as: Trade Secrets Law, Personal Data Protection Law, Copyright Law, Criminal Law, etc., shall be followed and abide by.

11.6.2. Education and training or other publicity methods should be used to educate relevant personnel to understand external laws and regulations as well as various regulations set by Delta Group.

11.6.3. Law compliance shall be followed in accordance with the relevant regulations of Delta Group.

11.6.4. All Delta members who violate laws or internal regulations shall be punished in accordance with relevant regulations and laws of Delta Group.

11.7. Personal Information Management Education and Training Plan: The Personal Data Management Team shall plan and implement the personal information management education and training program. These programs should be designed based on the roles and functions of personnel involved in information operations or to enhance the work abilities of colleagues. Relevant personal information management training should be provided to employees at different levels.

11.8. The targets and timing of personal information management education and training

11.8.1. New employees: New employees of Delta should receive appropriate personal information management related education and training to understand the personal information management policy and the individual duties.

11.8.2. General regular education and training

(1) According to the personal information management education training plan in clause 11.7.

(2) Conduct personal data incident drills at least once a year.

11.8.3. Change of position, equipment or workflow: When job transfers, equipment changes, or operating procedures are updated, new departments should provide relevant operators with appropriate training. A list of handover tasks can be established to facilitate the transition of work.

11.8.4. External contractor: The relevant regulations shall be based on “Information Operation Outsourcing Instruction”.

11.8.5. In addition to the education and training organized by Delta, and if necessary, send personnel to participate in related training or seminars organized by external parties.

11.9. Personal information management training evaluation and record

11.9.1. Personal information management education training should include evaluation system, such as in-class quizzes or discussions, as the basis for evaluating the effectiveness of trainings.

11.9.2. Personal information management education training plans, learning assessment results, check-in records, and other related records should be kept for tracking

management.

## 12. Personal Data Incident Response Management

12.1. Definition

12.1.1. Personal data incident: refers to any permanent or temporary incident, tampering, damage or loss of personal information, or unauthorized access or disclosure caused by Delta Group or outsourced third-parties while transmitting, storing or processing personal data.

12.1.2. Stakeholders: refer to people or groups involved in activities such as the collection, processing, or utilization of personal data, including but not limited to parties, employees, manufacturers, competent authorities of Delta Group, mass media, etc.

12.1.3. All personnel: all Delta Group employees, contracted personnel, manpower dispatch, or partners (customers, third parties, consultants, etc.) working with the Delta Group.

12.1.4. Contact Person for customers: refers to the external contact person designated by the Personal Data Management Team when a personal data incident occurs or may affect the rights and interests of customers.

12.2. Rights and Responsibilities

12.2.1. The Personal Data Management Team is responsible for the following matters:

(1) When a personal data incident occurs, receive the information of the incident and make decisions, and supervise the implementation of this regulation.

(2) According to the severity of the incident, decide alongside with Personal Data Management Team whether to activate the Personal Information Incident Response Team.

(3) Coordinate and designate the person responsible for contacting data subjects (customers, employees, suppliers, etc.).

(4) Coordinate and designate the person responsible for contacting the media.

(5) Coordinate with Delta Group's Personal Information Management Execution Team members to jointly formulate a strategy and responses for personal data incidents, and revise the plan as appropriate.

(6) Be the main contact for relevant government authority of Delta Group, and provide necessary information according to the instructions of the authority.

(7) If a personal data incident is also applicable to personal information protection laws of other countries, it is necessary to assist in reporting to the local government authority or/and relevant parties in accordance with relevant local regulations.

12.2.2. The Information Security Execution Team is responsible for the following matters:

(1) Ensure and maintain the information equipment related to the personal information of Delta Group to avoid the occurrence of personal information protection loopholes.

(2) Coordinate related information equipment to cooperate with each other in the identification, collection, retrieval, sealing and transportation of digital evidence.

(3) Coordinate with the members of the emergency response team and the unit where the incident occurred to assist personnel with digital evidence preservation.

(4) Handle or assist in preventive or response measures for personal data incidents undertaken by Delta Group.

12.2.3. Shall set up the Legal Compliance and Risk Management Team that is responsible for the following matters:

(1) Provide applicable analysis and legal advice of the laws and regulations related to the protection of personal data to which Delta Group should apply, and adjust this procedure in accordance with the requirements of the laws and regulations.

(2) Continue to pay attention to external information or news related to violations and penalties of personal information.

(3) Review the applicable personal information protection laws and regulations periodically, and confirm the requirements of the relevant government authority for contact, consultation, registration or violation notification channels.

(4) Provide legal opinions on handling personal data incidents.

(5) Assist in handling compensation matters for personal data incidents.

(6) Discuss what needs to be notified to the government authority and parties involved.

(7) Consult or confirm with relevant external units whether the associated procedures should be initiated.

12.2.4. Data Protection Representative / Contact Persons of Each Unit:

(1) Each unit shall appoint a personal data representative /contact person to be the contact between the unit and the Personal Data Management Team.

(2) Supervise each unit, implement personal information management and respond to

personal data incidents.

(3) Participate the meeting held by Personal Data Management Team to track and report on the personal data protection related tracking items of each unit. For the flexibility of meetings, tracking items and contents for meetings can be proposed or presented in written forms.

(4) When a personal data incident occurs, the data protection representative/contact person of the responsible unit for the incident should decide the communication means along with the designated contact window for clients.

12.2.5. The responsibilities above may vary differently for branches abroad due to different organizational structures. However, appropriate procedures should be established for confirmation and revised in accordance with the requirements of this regulation.

12.3. Operating Procedures and Instruction

12.3.1. The handling process when a personal data incident occurs includes: incident discovery phase, incident notification and response handling phase, and review operations.

12.3.2. Incident discovery stage: When the following situations occur, the personal data incident response procedure should be initiated immediately.

(1) According to the internal report of Delta Group, it is possible that the personal data of customers, employees, etc. have been infringed;

(2) Received a notification from an outsourcing vendor of a personal data incident;

(3) Received notification from the party that the personal data has been infringed, and there is a clear sign of the infringement;

(4) Received a media report or an incident is reported by the media;

(5) Received a notification from a consumer protection agency that there is an incident;

(6) Received a notification from the government agency, law enforcement agencies, or other government agencies that there is an incident;

(7) The paper, digital data or computer equipment of Delta Group's personal data is stolen or lost;

(8) Any party or client claims to reveal an information incident or has filed a lawsuit;

(9) There are other specific evidence, and the unit supervisor judges that there is a possibility of a personal data incident.

12.3.3. Incident Notification and Response and Handling Stages

(1) When personnel of each unit discover that a personal data incident has occurred, they should notify the manager and data protection representative of the incident unit according to the “Personal Data Incident Handling Process”, and fill in the "Personal Data Incident Record and Notification Form" for notification. After receiving the notification, the Personal Data Management Team should decide whether to activate the Incident Response Team, make public statements, and decide which level of manager should be notified, based on the severity of the incident. Personal Data Management Team should complete the preliminary investigation of the incident, assess the impact, and be responsible for follow-ups.

(2) If the personal data incident involves information technology technical related matters, the Information Security Execution Team should coordinate and review the abnormal state of the internal technological environment (such as network equipment, server status, terminal status, etc.), and seek external support (such as digital forensics).

(3) When the unit contact person or outsourced manufacturer handles the personal data incident, the process and results should be reported to the manager or data protection representative of the relevant business unit continuously. The manager or representative shall be responsible for reporting the incident status to the Personal Data Management team or/and the Incident Response Team.

(4) The unit that causes the incident should find out the cause of the incident, confirm the scope of influence with related units, and complete the preliminary incident analysis as soon as possible.

(5) If the personal data incident applies to the personal information protection laws of other countries, the relevant unit shall notify the local government authority or/and the relevant parties in accordance with the relevant local regulations.

12.3.4. Review work

After handling the severe personal data incident, the Personal Data Management Team shall convene an incident review meeting. Related personnel and units should cooperate and participate in the meeting. The content of the meeting shall include the following:

(1) Explain the whole incident.

(2) Review of the responsiveness of relevant personnel involved in the process of personal data incidents.

(3) Make suggestions and plans on how to prevent the incident from recurring.

(4) If additional tools or resources are needed, please propose them at the meeting.

(5) According to the conclusions of the meeting, if there is a need to modify this regulation, a revision of this regulation should be proposed.

12.4. Incident Response Team

When a personal data incident occurs and the circumstances are serious, the Incident Response Team should be activated. Its organization and responsibilities are as follows:

12.4.1. Organization

The Incident Response Team is composed of members of the Personal Information Management Execution Team and related personnel for the handling of personal data incidents. The convener of the Incident Response Team is selected by the convener after a resolution, and will work and lead the incident response operations and other matters jointly with the contact person of the unit where the incident occurs.

12.4.2. Responsibilities

(1) After the responsible unit provides a complete record of the incident occurrence, organize, summarize the incident and report to the Personal Data Management Team, and report to the highest level according to the personal information incident notification level standard, referring to "Personal Data Incident Level and Notification Level".

(2) Investigate the cause and authenticity of the incident, and take necessary measures to prevent the incident from expanding, controlling or reducing damage.

(3) The unit responsible for the incident shall put forward suggestions and improvement measures to internal and external stakeholders, and provide contact methods such as telephone number and email that can handle personal data incident inquiries.

(4) Investigate the quantity and scope of data related to personal data incidents, and evaluate the degree of damage.

(5) The Personal Information Incident Response Team confirms that the incident has been properly handled, and the case can be closed after reporting to the highest-level manager.

12.5. Classification and notification of personal data incidents

The Personal Data Management Team should determine the level of the incident based on the scope and impact of the personal data incident, referring to the “Personal Data Incident Level and Notification Level”. Assess whether it should be notified to senior supervisors, competent authorities, or data subjects.

12.6. Key Points of Handling Personal Incidents

12.6.1. Direct, decide and designate the handling of incidents (The Personal Data Management Team will coordinate these matters and report to the highest-level supervisor in accordance with the “Personal Data Incident Level and Notification Level”)

(1) Approve necessary responses to control the impact of the incident.

(2) Publish the external written statement and the internal staff description.

(3) Designate the speaker as the only external spokesperson.

12.6.2. Incident handling, review and improvement (Responsible Unit/ Personal Data Management Team / Incident Response Team)

(1) It is necessary to fully record the process of an information incident, such as the cause, time, location, related personnel, quantity and scope of the incident or impact, and the estimated degree of damage, and report to the chairman.

(2) Participate in the incident review meeting, provide a complete record of the incident process, and make suggestions and improvement measures in response to internal and external stakeholders.

(3) Relevant personnel should be assigned to confirm whether there is a risk of another incident.

(4) If it is found that the incident involves a third-party violation of laws, regulations and requirements, it can be reported to the police for assistance if necessary.

12.6.3. Coordination and Communication between the Parties (request and appeal handling team)

(1) Continuously monitor the flow of incident-related information and report internal

information received.

(2) The parties shall be notified in accordance with the law to explain the progress of the incident and the impact on the rights and interests of the parties, and to ensure that the parties understand the handling status of the Delta Group and the protection of their rights and interests.

(3) Questions and answers (Q&A) and consultation channels should be established for handling personal data incidents, so as to adopt a unified and convenient channel to help the parties understand the handling of personal data incidents.

(4) After the incident occurs, the parties should be notified individually, including the fact that their personal data has been infringed, the corresponding measures taken by Delta Group, the contact information of Delta Group's contact person, the possible impact of the incident, and the expected actions taken by Delta Group.

(5) The method of notification related to personal data incidents refers to the immediate implementation of words, writing, telephone, text message, email, fax, electronic document or other methods sufficient to make the parties aware of the incident.

(6) If an individual notification is too expensive, the scope of the notification is too large, or individual parties cannot be notified, the announcement can be made through the internet, news media or other methods that are sufficient for the public to get notified. A summary of the occurrence of a personal data incident, and a toll-free number shall be set up when necessary, so that the parties involved can quickly know about the incident and its handling status.

(7) When notifying data subjects about the incident, relevant records, including the notification method, time, object, execution unit, and notification content, should be recorded.

12.6.4. Notify the relevant government authority (Personal Data Management Team/ Incident Response Team are responsible for it)

(1) After receiving a notification that a personal data incident has occurred, notify the relevant government authority about the scope and details of the incident within the statutory time limit to avoid expansion of the damage.

(2) After the incident, there should be procedures drawn up to prevent similar incidents from recurring. A proper follow-up plan should be done.

(3) The notification to the relevant government authority shall include the facts and possible outcome of the incident, types and quantity of data involved, appropriate contingency plans that reduce negative effects, and preventive measures to avoid recurrence of similar accidents.

(4) When notifying the government authority about the incident, relevant records, including the notification method, time, object, execution unit, and notification content, should be recorded.

12.6.5. Media responses (According to the “Personal Data Incident Level and Notification Level” the highest level manager or other designated person who should be notified)

(1) Continuously monitor whether the incident escalates and cause media attention, and report any external information immediately.

(2) If the media reports on the incident, various control measures for personal information management should be reported, including how the incident happened and current processing status, and make a unified announcement externally or internally through the spokesperson.

(3) If a personal data incident occurs within the units, the units, Personal Information Incident Response Team or/and the Personal Data Management Team shall prepare press release once the incident happened, and be ready to release it to the public anytime.

## 13. Announcement and Implementation

13.1. If necessary to make or amend this bylaw, the Personal Information Management Execution should draw up the draft, and it will take effect after receiving approval from the Information Security and Personal Information Management System convener.

13.2. If any local applicable laws for Delta Group's regional offices and this bylaw are inconsistent, relevant documents shall be drawn up separately to ensure compliance with local laws and regulations.

## 14. References

14.1. Delta Group Information Security and Personal Information Protection Policy (DEI-DIS-PL01)

14.2. Personal Data Document and Record Management Regulation (DEI-PIMS-ST03)

14.3. Personal Data Incident Handling Process (DEI-PIMS-PR01)

14.4. Personal Data Incident Level and Notification Level (DEI-PIMS-PR02)
14.5. Information Security Management Standards (DEI-DIS-ST02)
14.6. Information Security and Personal Information Management Organization Charter (DEI-DIS-ST04)
14.7. Information Security Risk Management Policy (DEI-DIS-ST05)
14.8. Information Operation Outsourcing Instruction (DEI-DIS-ST06)

## 15. Attachments

15.1. ISMS and PIMS Measurement Result (DEI-PIMS-ST02-F01)
15.2. Corrective and Preventive Measure Form (DEI-PIMS-ST02-F02)
15.3. Personal Data Incident Record and Notification Form (DEI-PIMS-ST02-F03)
15.4. ISMS and PIMS Internal Audit Checklist (DEI-DIS-ST02-F01)

## 16. Edition History

| Version | Effective Date | Summary of Document Additions, Revisions, or Deletions. |
|---|---|---|
| 1.0 | 2024/08/27 | The first edition was in 2024 August. |
| 2.0 | 2025/07/22 | 12.2.3 Revised the review frequency of applicable personal information protection laws and regulations from “every six months” to “periodically.” |