Personal Data Protection Policy and Implementation

The Company places great importance on the protection of privacy. In compliance with the **Personal Data Protection Act (PDPA)**, the Company has established the *Personal Data Protection Management Regulations* and implemented rigorous personal data privacy and security management and protection measures. These measures are incorporated into the internal control system and are subject to regular annual audits to ensure that data access and sharing are properly governed and protected, and that data availability, integrity, and confidentiality are maintained.

The scope of application covers all branches, operating locations, subsidiaries, customers, and suppliers. With respect to the collection, processing, use, and protection of personal data involved in business operations, the Company strictly complies with relevant government laws and regulations and uses personal data only within the scope permitted by law. The Company does not provide, lease, or otherwise disclose personal data to third parties in any disguised manner. All practices are implemented in accordance with the Company's *Personal Data Protection Management Regulations*, with a commitment to safeguarding data security and privacy rights.

The Company's privacy protection policy is as follows:

To regulate and implement the collection, processing, and use of personal data, prevent infringement of personal rights, and promote the reasonable use, protection, and management of personal data, the Company has established these management regulations in accordance with the *Personal Data Protection Act* promulgated by the competent authority, the Personal Data Protection Commission (hereinafter referred to as the "PDPA").

Personal Data Protection Task Force

To ensure effective protection and management of personal data, the Company has established a **Personal Data Protection Task Force** (hereinafter referred to as the "Task Force"), which consists of a management representative appointed by top management, a management team, and an internal assessment team.

The responsibilities of the Task Force include:

1. Proposing the Company's personal data protection policies.
2. Promoting the Company's personal data management system.
3. Assessing and managing personal data privacy risks.
4. Proposing awareness enhancement and education and training programs on personal data protection for employees of all departments.
5. Evaluating the infrastructure of the Company's personal data management system.
6. Reviewing, examining, and assessing the legality and appropriateness of the personal data management system.
7. Responding to, handling, reporting, and conducting drills for personal data security incidents.
8. Planning and executing other matters related to personal data protection and management.

Meetings of the Task Force are convened on an as-needed basis to support business operations and are chaired by the management representative. If the management representative is unable to chair a meeting, a member of the management team may be designated to act on their behalf.

Responsibilities of Each Department

Each department shall designate a responsible person to handle the following matters:

1. Review requests made by data subjects pursuant to Articles 10 and 11, Paragraphs 1 to 4 of the PDPA.
2. Review notifications required under Article 11, Paragraph 5 and Article 12 of the PDPA.
3. Provide consultation on personal data protection laws and regulations.
4. Coordinate and liaise on matters related to personal data protection.
5. Report incidents related to personal data damage prevention and crisis response within the department.
6. Implement the Company's personal data protection policies and conduct self-audits within the department.
7. Plan and execute other personal data protection and management matters within the department.

Personal Data Protection Contact Window

The Company shall establish a personal data protection contact window to handle the following matters:

1. Coordination, liaison, and emergency reporting related to personal data protection among government agencies.
2. Reporting of non-information-technology-related personal data security incidents.
3. Serving as the single point of contact for the public in the event of major personal data breach incidents.
4. Preparation and updating of the roster of personnel responsible for personal data protection.
5. Compilation of education and training rosters and records for personnel and employees involved in personal data protection.

Principles for Collection and Use of Personal Data

Each department shall ensure that the collection, processing, use, or international transmission of personal data is conducted in good faith, limited to the minimum scope necessary for specific purposes, and reasonably related to the purpose of collection.

When collecting personal data directly from a data subject, each department shall clearly inform the data subject of the following matters, unless one of the exceptions under Article 8 of the PDPA applies:

1. Name of the agency or department.
2. Purpose of collection.
3. Categories of personal data.
4. Duration, region, recipients, and methods of use of personal data.
5. Rights exercisable by the data subject under Article 3 of the PDPA and the methods for exercising such rights.
6. The impact on the data subject's rights and interests if the data subject chooses not to provide personal data.

When collecting personal data not directly provided by the data subject, the department shall, prior to processing or use, inform the data subject of the source of the personal data and the matters listed in Article 8, Paragraph 1, Subparagraphs 1 to 5 of the PDPA, unless an exception under Article 9, Paragraph 2 applies. Such notification may be made concurrently with the first use of the personal data. For personal data collected prior to the amendment and implementation of the PDPA,

notification shall be provided in accordance with the PDPA unless an exemption under Article 9, Paragraph 2 applies.

Where written consent of the data subject is required pursuant to Article 19, Subparagraph 5, or the proviso of Article 20, Subparagraph 6 of the PDPA, each department shall obtain a written consent form from the data subject.

When collecting, processing, or using personal data pursuant to Articles 19 or 20 of the PDPA, each department shall conduct a thorough review and obtain approval before proceeding. Where personal data is used beyond the scope of the specific purpose pursuant to the proviso of Article 19, records of the data usage history shall be maintained. Personal data shall not be arbitrarily linked across databases or misused.

Correction, Deletion, and Record-Keeping

If personal data held by the Company is inaccurate or incomplete, the data-collecting unit shall obtain approval and request the data-holding unit to correct or supplement the data, with relevant records retained. Where the processing or use of personal data has been suspended, the data-holding unit shall duly record such actions.

When the specific purpose for which personal data was collected ceases to exist or the retention period expires, the data-collecting unit shall obtain approval and request the data-holding unit to delete and cease processing or use of the personal data, unless an exception under Article 11, Paragraph 3 of the PDPA applies. All deletion, suspension of processing, or cessation of use shall be properly recorded.

Where deletion, suspension of collection, processing, or use of personal data is required proactively or upon request of the data subject pursuant to Article 11, Paragraph 4 of the PDPA, approval shall be obtained and the data-holding unit shall carry out the action and maintain records accordingly. In the event of theft, leakage, alteration, or other infringement of personal data as stipulated in Article 12 of the PDPA, incidents shall be reported in accordance with reporting procedures. Upon investigation, the unit responsible for the data breach shall release information pursuant to the Company's information disclosure procedures and promptly notify the affected data subjects by appropriate means.

Data Subject Requests

When a data subject requests inquiries, access, review, copies, or actions pursuant to Articles 10 or 11, Paragraphs 1 to 3 of the PDPA, the data subject shall complete a *Personal Data Application Form* and provide relevant supporting documents.

If the application documents are incomplete or deficient, the applicant shall be notified to make corrections within a specified period. Applications shall be rejected in writing under any of the following circumstances:

1. Failure to correct deficiencies within the specified period.
2. Any circumstance specified in the proviso of Article 10 of the PDPA.
3. Any circumstance specified in the proviso of Article 11, Paragraph 2 or Paragraph 3 of the PDPA.
4. Non-compliance with applicable laws or regulations.

Approval, rejection, or extension of requests submitted pursuant to Articles 10 and 11 of the PDPA shall be handled within the time limits prescribed in Article 13 of the PDPA, and the reasons shall be provided to the applicant in writing.

When a data subject reviews their personal data, such review shall be accompanied by the departmental personal data protection contact window and conducted in accordance with the Company's document access procedures. Where personal data files are of a special nature or where disclosure of file names is restricted by law, access may be limited or denied in accordance with the Freedom of Government Information Law or other applicable laws.

Personal Data Security Management

To prevent theft, alteration, damage, loss, or leakage of personal data, all departments shall implement security maintenance measures in accordance with these regulations and relevant laws. Personal data files shall be subject to a management system with classified and graded controls, and security management rules shall be established for personnel with access to such data.

In the event of security incidents such as malicious damage, operational negligence, or illegal intrusion (including hacker attacks), emergency response measures shall be implemented immediately and personal data security incidents shall be reported accordingly.

Personal data file security maintenance shall also comply with applicable laws, regulations of competent authorities, and the Company's internal policies on personal data protection, information security, and confidentiality.

Zero Tolerance Policy

The Company adopts a **zero-tolerance policy** toward personal data incidents. In the event of any personal data infringement, responsible units—including information security, legal, procurement, and business departments—shall investigate and handle the matter in accordance with the PDPA and the Company's incident reporting and handling procedures. Any violation of confidentiality obligations shall be subject to applicable legal liabilities and internal disciplinary actions, including but not limited to termination of cooperation.

Quantitative Indicators and Management Metrics for FY 2025 (ROC Year 114)

The Company's quantitative data and management indicators related to the personal data protection policy for FY 2025 are as follows:

- **Personal Data Collection, Processing, and Use Notice Forms**
  All new employees and job applicants are required to complete a Personal Data Collection, Processing, and Use Notice Form. A total of **120 forms** were completed during FY 2025, accounting for **100% of all interviewees**.
- **Internal Audits**
  One internal audit is conducted annually.
- **Incident Response and Risk Management**
  Zero (0) violations of the Personal Data Protection Act occurred during the year.