Personal Data Protection Policy

SiS Distribution (Thailand) Public Company Limited (the Company) is committed to protecting the personal data of all individuals. This Personal Data Protection Policy has been established to outline the principles, methods, and purposes for the collection, use, and disclosure of personal data, as well as to inform data subjects of their rights as stipulated by law. The Policy aims to ensure that the Company's operations comply with the Personal Data Protection Act B.E. 2562 (2019) and relevant international standards.

The Company will review this Policy periodically to ensure its continued alignment with legal, technological, or business practice developments. Any updates or revisions to this Policy will be published on the Company's official website.

1. Personal Data

"Personal Data" means any information that identifies, or can be used to identify, an individual either directly or indirectly, but does not include information of deceased persons.

2. Restricted Personal Data Collection

The Company will collect, use, disclose, share, transfer, and store personal data for specific and legitimate purposes, within a defined scope, and by lawful and fair means. The collection of personal data will be limited to what is necessary and relevant to the Company's purposes, such as product sales, service provision, or other electronic services, in accordance with the objectives stated in this Policy only.

Prior to collecting personal data, the Company will ensure that data subjects are informed and have provided their consent through appropriate channels such as written documents, electronic media, or short messages, as determined by the Company, to enable the effective use of data in accordance with the intended purposes.

The Company will obtain consent from data subjects before collecting their personal data only when processing cannot rely on other lawful bases, unless such collection is carried out for the following purposes.

2.1 **Compliance with Laws:** Including, but not limited to, the Personal Data Protection Act, the Electronic Transactions Act, the Telecommunications Business Act, the Anti-Money Laundering Act, the Civil and Commercial Code, the Criminal Code, and the Civil and Criminal Procedure Codes.

2.2 **Investigation or Legal Proceedings:** disclosure of personal data for the purpose of an official investigation by competent authorities or for judicial proceedings and court rulings.

2.3 **For the Benefit of the Data Subject:** Disclosure of personal data for the benefit of the data subject in cases where consent cannot be obtained at that time or where the processing is necessary to protect the data subject's interests.

2.4 **For Legitimate Interests of the Company or Others:** Disclosure of personal data as necessary for the legitimate interests of the Company or another individual or legal entity, provided such interests do not override the rights of the data subject.

2.5 **Prevention or Mitigation of Harm:** Disclosure of personal data as necessary to prevent or mitigate danger to a person's life, body, or health.

2.6 **Performance of a Contract:** Disclosure of personal data as necessary for the performance of a contract to which the data subject is a party, or to take steps at the request of the data subject prior to entering into such a contract.

2.7 **Public Interest in Research or Statistics:** Disclosure of personal data as necessary for achieving purposes relating to historical or archival documentation, public interest, research, or statistical studies, provided that appropriate safeguards are in place.

In the event that the data subject does not wish the Company to continue collecting or using their personal data, they have the right to withdraw their consent previously given to the Company. Such withdrawal can be made by contacting the Company's Data Protection Officer (DPO) through the communication channels specified in this policy.

For personal data collected by the Company before the Personal Data Protection Act B.E. 2562 (2019) came into effect, the Company shall continue to collect, use, or disclose such data for original purposes, with appropriate data protection measures in accordance with the applicable law. The data subject may, however, withdraw consent at any time by contacting the DPO.

3. Data Security and Quality Protective Measure

3.1 The Company recognizes the importance of maintaining the security of personal data and has established appropriate measures in accordance with Technical Measures, Organizational Measures, and Physical Measures to ensure the secure processing of personal data and to prevent personal data breaches. These measures are designed to maintain the confidentiality, integrity, availability, and accuracy of personal data, as well as to prevent unauthorized or unlawful loss, access, alteration, destruction, use, or disclosure of such data. The measures include, but are not limited to, the following:

- 3.1.1 Implementation of data encryption technologies and access controls restricted to authorized personnel only.
- 3.1.2 Regular review, monitoring, and maintenance of information security systems.
- 3.1.3 Strict compliance with the Company's Information Technology Security Policy.
- 3.1.4 Secure data storage in high-security systems with reliable data backup mechanisms.
- 3.1.5 Retention of personal data only for the necessary duration and for the specific purposes defined.
- 3.1.6 Provision for data subjects to access, correct, or delete their personal data in accordance with their legal rights.

In addition, the Company regularly verifies the accuracy of personal data to ensure that it remains correct, up to date, and effectively used for the intended purposes within an appropriate scope.

3.2 **Retention of Personal Data:** The Company will retain personal data only for as long as necessary to fulfill the purposes for which it was collected, taking into consideration the nature of the data and applicable legal requirements. Once the retention period has expired or the data becomes irrelevant or excessive, the Company will review and handle such personal data appropriately in accordance with applicable standards.

3.3 **Discontinuation of Use or Removal of Personal Data:** Upon fulfillment of the intended purpose or when personal data is no longer required, the Company will discontinue the use or remove such data from its storage systems using appropriate and lawful methods to prevent unauthorized access or use.

3.4 **Irreversible Data Deletion:** In cases where the Company deletes or destroys personal data, such data will be permanently deleted and rendered irretrievable. The deletion process will be carried out in accordance with data security standards to ensure that deleted data cannot be recovered or reused. The Company will also maintain the confidentiality and security of deleted or destroyed data at all times.

3.5 **Audit:** The Company will conduct periodic reviews to delete, destroy, or anonymize personal data on a permanent basis to limit or discontinue its retention once the defined retention period has lapsed, or when the data becomes irrelevant or excessive for its processing purposes. This also applies in cases where the Company receives a data deletion request from the data subject.

4. Objectives for Personal Data Collection, Storage, and Usage

The Company collects, retains, and uses personal data of relevant individuals for the following purposes. All collection, use, and disclosure of personal data are carried out only for lawful and necessary purposes relating to the Company's business operations, internal management, corporate governance, and compliance with applicable legal and regulatory requirements.

The Company may also use cookies or other tracking technologies to enhance service efficiency and user experience, as specified in the Company's Cookie Policy.

4.1 **For the Company's Core Business Operations:** The Company may collect, use, and disclose personal data for sales and distribution management, the provision of related products and services, customer and partner relationship management, billing, payment collection, product delivery, and after-sales service, as well as for communication, coordination, and technical support with customers and business partners.

4.2 **For Customer, Partner, and Business Relationship Management:** The Company may collect, use, and disclose personal data for data collection and analysis to better understand customer needs, marketing communications, dissemination of news, promotions, and sales activities, as well as for the development and maintenance of business relationships, and for monitoring service quality and performance.

4.3 **For Procurement and Resource Management:** The Company may collect, use, and disclose personal data for communication, coordination, and contract execution with relevant parties, contract administration, logistics planning, warehousing, and quality inspection, as well as for data transfer and disclosure to contractual and business partners in accordance with business agreements.

4.4 **For Recruitment and Human Resource Management:** The Company may collect, use, and disclose personal data for recruitment purposes, whether directly or through recruitment agencies, including qualification review, employment history verification, and suitability assessment. This also includes personnel management such as recordkeeping, payroll, training and development, compensation and benefits administration, occupational health and safety management, and employee welfare. Personal data may also be retained for internal management and legal compliance purposes.

4.5 **For Internal Management and Corporate Governance:** The Company may collect, use, and disclose personal data for accounting, finance, procurement, internal audit, risk management, internal control, and data accuracy verification. This also includes access control management, information system and data security, as well as legal, contractual, and dispute management.

4.6 **For Compliance with Legal and Regulatory Requirements:** The Company may collect, use, and disclose personal data to comply with applicable laws and regulations, including disclosure to regulatory authorities such as the Securities and Exchange Commission, government agencies, tax authorities, and security agencies. This may include preparing statutory reports, undergoing external audits, retaining information for evidentiary purposes, and exercising the Company's legal rights and obligations.

4.7 **For Investor and Stakeholder Communications:** The Company may collect, use, and disclose personal data for communication and dissemination of material business information, shareholder meetings, and disclosures required by the Stock Exchange, as well as for coordination with investors, analysts, external organizations, and the media.

4.8 **For Security and Data Protection:** The Company may collect, use, and disclose personal data to record and monitor entry and exit within Company premises, ensure the safety and security of personnel, assets, and information systems, and conduct inspections or record evidence to mitigate security risks.

4.9 **For Sustainability and Corporate Social Responsibility Initiatives:** The Company may collect, use, and disclose personal data for the implementation of sustainability projects, collaboration with external organizations, and communication and coordination with project participants.

4.10 **For Complaint and Whistleblowing Management:** The Company may collect, use, and disclose personal data for the receipt and investigation of complaints or whistleblowing reports, internal investigations, or relevant legal proceedings.

5. Restrictions on Usage and/or Disclosure of Personal Data

5.1 **Use and Disclosure of Personal Data:** The Company may use and disclose personal data in accordance with the consent obtained and within the scope authorized by the data subject. Such use shall be limited to the purposes specified in this Personal Data Protection Policy regarding the collection, retention, and use of personal data by the Company. The Company shall supervise and ensure that its employees or any other persons acting on its behalf do not use and/or disclose personal data beyond the authorized scope. However, the Company may disclose personal data without obtaining consent from the data subject in cases falling under the exceptions specified in Clause 2 of this Policy.

5.2 **Use of External Service Providers:** The Company may engage external information service providers to store or process personal data. Such providers must implement appropriate security measures to protect personal data and are prohibited from collecting, using, or disclosing personal data other than as specified in the agreement with the Company.

5.3 **Disclosure upon Request by Government Authorities:** In the event that the Company receives a request from a government agency requiring disclosure or delivery of personal data, the Company will notify the data subject in advance unless prohibited by law or an order from a competent authority. This is to allow the data subject to exercise their legal rights as prescribed by applicable laws.

5.4 **Cross-Border Data Transfer:** The Company may need to transfer personal data to foreign countries for the purposes stated in this Policy. Such data transfer shall be carried out only to destinations with adequate personal data protection measures, as prescribed under the Notification of the Personal Data Protection Committee B.E. 2566 (2023).

6. Data Subject Rights

6.1 Data subjects are entitled to exercise their rights to manage their personal data as permitted by law and in accordance with applicable requirements, as follows:

6.1.1 **Right to Withdraw Consent:** Data subjects have the right to withdraw the consent previously given to the Company for the collection, use, or disclosure of their personal data if they no longer wish for the Company to continue processing it.

6.1.2 **Right to Access and Disclosure of Data Sources:** Data subjects have the right to access their personal data collected by the Company and to request a copy of such data. They may also request the Company to disclose how it obtained their personal data if it was collected without their consent.

6.1.3 **Right to Data Portability:** Data subjects have the right to request the Company to transmit or transfer their personal data to another data controller, provided it does not contravene any legal obligations, contractual requirements, or the rights and freedoms of others.

6.1.4 **Right to Object:** Data subjects have the right to object to the collection, use, or disclosure of their personal data at any time, particularly in cases where such data is processed for direct marketing purposes or for scientific or statistical research.

6.1.5 **Right to Erasure:** Data subjects have the right to request the deletion, destruction, or anonymization of their personal data if they believe it has been collected, used, or disclosed unlawfully, or if the Company no longer needs to retain it.

6.1.6 **Right to Restrict Processing:** Data subjects have the right to request a temporary suspension of the processing of their personal data while the Company is verifying a request for data rectification.

6.1.7 **Right to Rectification:** Data subjects have the right to request the Company to correct their personal data to ensure it is accurate, complete, and not misleading, provided such corrections do not contravene legal requirements.

6.1.8 **Right to Lodge a Complaint:** Data subjects have the right to file a complaint in the event of a personal data breach or any damage caused to their personal data with the Office of the Personal Data Protection Committee.

6.2 Data subjects may exercise their rights by completing the "Personal Data Subject Rights Request Form (PDPA/F2025/010)," which can be downloaded from the Company's website, and submitting it through the channels specified in the form or via designated electronic channels.

6.3 The Company reserves the right to review and consider requests made by data subjects. The Company may contact the data subject or an authorized representative to request additional information or documentation necessary for verification and processing. The Company will handle the request appropriately within the legally prescribed timeframe and notify the applicant of the outcome.

7. Respect for Data Subject Privacy

The Company places great importance on and respects the privacy rights of all personnel. The Company will collect, use, and disclose personal data only as necessary for purposes related to human resource management and legitimate business operations. The Company will not use or disclose personal data for any other purposes unless consent has been obtained from the data subject or as required by law.

Personnel have the right to manage their personal data as outlined in Clause 6 of this Policy. The Company will handle the exercise of these rights with due care and within an appropriate timeframe.

8. Disclosures of Personal Data Practices, Procedures, and Policies

The Company has established a clear policy to comply with personal data protection laws and other relevant regulations, including the Personal Data Protection Act, measures for protecting the rights of telecommunications service users related to personal data, privacy rights, and freedom of communication. The Company is committed to safeguarding personal data in accordance with legal principles to ensure that your information is protected from unauthorized or inappropriate use.

The Company has implemented various measures to ensure the protection of personal data, including strict compliance with its Personal Data Protection Policy. This policy covers the collection, use, and disclosure of personal data, outlines procedures for maintaining data security, controls access to personal data, and prevents data leakage. In addition, the Company has established a Personal Data Protection Policy that informs data subjects of their rights, the types of personal data collected, and how such data is used.

9. Personal Data Protection Officer

The Company has complied with the Personal Data Protection Act B.E. 2562 by appointing a DPO to oversee and ensure that the Company's personal data processing activities are carried out in accordance with applicable laws and relevant policies.

The roles and responsibilities of the DPO are as follows:

9.1 Provide advice and guidance on key legal requirements related to personal data protection to data controllers, data processors, and relevant employees in accordance with the Personal Data Protection Act B.E. 2562 and other applicable data protection laws.

9.2 Collaborate with the Personal Data Protection working group (PDPA working group) to prepare and update relevant documentation such as the Personal Data Protection Policy, Privacy Notices, manuals, and personal data management procedures to ensure compliance with applicable laws and standards.

9.3 Monitor and ensure that the Company's operations comply with the Personal Data Protection Act and the Company's internal policies.

9.4 Assess and determine the purposes for which personal data is used or disclosed, explain data subjects' rights, and clarify the protective measures implemented by the Company.

9.5 Report matters related to personal data protection to the PDPA working group and the management team.

9.6 Monitor access to, use of, and disclosure of personal data to ensure compliance with legal requirements.

9.7 Provide consultation and support in maintaining the Record of Processing Activities (RoPA) and preparing personal data breach reports.

9.8 Coordinate with the Personal Data Protection Committee (PDPC) in cases of complaints or legal issues.

9.9 Coordinate with data subjects in cases of complaints or rights requests and may delegate coordination to relevant personnel as appropriate.

9.10 Oversee the collection, use, disclosure, and storage of personal data to ensure legal compliance.

9.11 Be responsible for notifying relevant authorities of personal data breach incidents within the legally required timeframe and informing data subjects when the breach may pose a high risk to their rights and freedoms.

9.12 Provide advice and support on conducting Data Protection Impact Assessments (DPIAs).

9.13 Promote awareness, understanding, and a strong culture of personal data protection among employees.

10. The Company's Communication Channel

If you have any inquiries regarding the collection of personal data, exercising your rights concerning personal data, or filing a complaint about a personal data breach, you can contact the DPO at:

- **Data Protection Officer**
  1. Ms. Varapa Intakorn-Udom Tel: 02-020-3291
  2. Mr. Apisak Polsen Tel: 02-020-3090
  3. Mr. Pichit Polpinit Tel: 02-020-3299
  4. Ms. Areerat Khuanpadung Tel: 02-020-3060
  5. Ms. Sirinun Leelapeeraphun Tel: 02-020-3316
  6. Ms. Nittaya Srivaranon Tel: 02-020-3552
- E-mail: DPO@sisthai.com
- Address: SiS Distribution (Thailand) Public Company Limited
- 9 Pakin Building, 9th Floor, Room No.901, Ratchadaphisek Road, Din Daeng, Bangkok 10400
- Working Hours: 09:00 a.m. – 06:00 p.m.

11. Enforcement

To ensure the effective implementation of this policy in compliance with the Personal Data Protection Act B.E. 2562 (2019), the Company has appointed a PDPA Working team. This committee serves as the governance mechanism to oversee the Company's personal data protection operations, with the authority and responsibility to plan, coordinate, supervise, and monitor personal data protection activities in collaboration with the DPO and relevant management.

This Personal Data Protection Policy has been approved by the Board of Directors in the Board of Directors' meeting of No. 6/2025 held on December 12th, 2025.

This policy shall be effective from January 1st, 2026, onwards.