Business Codes of Conduct

SiS Distribution (Thailand) Public Company Limited

Effective from January 1st, 2026

Codes of Conduct

SiS Distribution (Thailand) Public Company Limited (the Company) recognizes the importance of conducting business with integrity, transparency, and accountability under good corporate governance practices to build trust among all stakeholders, including shareholders, employees, customers, partners, government agencies, the community, and society at large.

The Company is committed to conducting its business based on the principles of ethics and business conduct to ensure that all decisions and operations are carried out honestly, transparently, fairly, and responsibly towards society. This is to ensure that the business operates sustainably and in alignment with international standards.

This Codes of Conduct has been established as a guideline for the conduct of the directors, management, and all employees of the Company, as well as individuals involved in the Company's business activities, to ensure that operations are conducted in accordance with the principles of business ethics.

To ensure that the Codes of Conduct remains relevant and aligned with changes in the business environment, laws, and governance standards, the Company mandates an annual review and update of the Codes of Conduct. The updated version will be presented to the Board of Directors for approval to ensure that the Codes of Conduct continues to align with the organization's values and good governance practices at an international level.

This Codes of Conduct has been approved by the Board of Directors in the Board of Directors' meeting of No. 6/2025 held on December 12th, 2025, and shall be effective from January 1st, 2026, onwards.

Table of Contents

Definition and Meaning

Definition	Meaning
Ethics	Embracing virtuous practices that should be followed and upheld to the point of becoming ingrained habits—qualities or behaviors that are considered beautiful and accepted as morally right.
Code of Conduct	Appropriate principles of conduct in practicing a specific profession, which are established by professionals in each field. These principles serve as a foundation for adherence and behavior, emphasizing the cultivation and reinforcement of awareness regarding correct conduct. The goal is to instill a commitment to maintain the reputation and promote the honor of both one and the organization.
The Company	SiS Distribution (Thailand) Public Company Limited and its subsidiaries.
Directors	Directors of SiS Distribution (Thailand) Public Company Limited and its subsidiaries.
SIS Directors	Directors of SiS Distribution (Thailand) Public Company Limited.
Management	Management of SiS Distribution (Thailand) Public Company Limited and its subsidiaries
SIS Management	The Management as defined by the Securities and Exchange Commission, Thailand (SEC) (Document No. SorJor. 14/40), refer to individuals holding managerial positions, with the first four positions counted from the Managing Director, including those holding positions equivalent to the fourth-level managerial positions. This also includes individuals holding managerial positions in the Accounting and Finance Department at the level of Department Manager or above, consisting of; 1. Executive Directors 2. General Manager 3. Operation Director 4. Financial Controller
Employees	Employees of SiS Distribution (Thailand) Public Company Limited and is subsidiaries, including both permanent and temporary staffs.
Related Transactions	Transactions between a listed company and subsidiaries with its related person.
Related Person	A person who may have led to the conflict of interests of the company's directors or executives, causing a conflicting situation to make a decision based on personal or corporate benefits. This includes; 1. The directors, management, major shareholders, controlling person, person to be nominated for directors, executive, or controlling person position, as well as their related persons and close relatives. 2. Any juristic person with major shareholders or controlling persons in (1). 3. Any person whose actions can be identified as proxy or under the influence of (1) and (2). 4. The director of a juristic person with controlling power. 5. The spouse, underage offspring or adopted child of the director in (4). 6. A juristic person under the controlling power of the person in (4) or (5). 7. Any individual acting with the understanding or agreement that, if the company conducts a transaction providing financial benefits to such an individual, the following persons will also receive financial benefits. 7.1 The company's director. 7.2 The company's executive. 7.3 The company's controlling person. 7.4 The director of the person with controlling power over the company. 7.5 The spouse, underage offspring or adopted child of the person described in 7.1 to 7.4.

Definition	Meaning
Corruption	Abuse of power, bribery or any actions which may or may not be illegal but are carried out with the intent to gain undeserved benefit to the organization, themselves, or others. Corruption encompasses the receiving, offering, and giving of the money (including donations, collection and any benefits which can be converted into currency), gifts, services, articles, entertainment, and any other benefits both direct and indirect to individuals, juristic person, or government entities to persuade those parties to proceed or omit their duties in order to achieve in any benefits to individuals, family, friends, acquaintances or business operations.
Political Support	Providing financial assistance, assets, items, or other benefits to support political activities, both directly and indirectly, to political parties, politicians, individuals with political responsibilities, and organizations closely associated with political parties at various levels, including local, regional, national, and international levels.

Section 1
Codes of Conduct

This Codes of Conduct is applicable to the directors, management, and all employees at every level of SiS Distribution (Thailand) Public Company Limited (the Company) and its subsidiaries, ensuring that operations are conducted in accordance with business ethics principles, transparency, accountability, and in alignment with the organization's values.

Stakeholders Involved in the Codes of Conduct

1. Persons who are obligated to adhere to this Codes of Conducts are.
   - 1.1 Directors
   - 1.2 Management
   - 1.3 Employees

2. Stakeholders whom the directors, Management, and employees have a responsibility to be accountable are.
   - 2.1 The Company.
   - 2.2 Shareholders.
   - 2.3 Employees.
   - 2.4 Business Partners.
   - 2.5 Customers.
   - 2.6 Consumers.
   - 2.7 Business Competitors.
   - 2.8 Trade Payables.
   - 2.9 Financial Institution Creditors.
   - 2.10 Regulators.
   - 2.11 Community and Society
   - 2.12 Environmental

The director, Management, and employees are obligated to strictly adhere to the Codes of Conduct and the related policies established by the Company. This is to demonstrate their responsibility towards the stakeholders associated with the Company. The Codes of Conduct applies to those with duties to comply and their responsibilities towards the stakeholders, as outlined in the table below.

Codes of Conduct to be adhered	Persons with responsibilities to adhere to Codes of Conduct		
	Directors	Management	Employees
Codes of Conduct regarding responsibility to the Company	✔	✔	✔
Codes of Conduct regarding responsibility to Shareholders.	✔	✔	✔
Codes of Conduct regarding responsibility to Employees.	✔	✔	
Codes of Conduct regarding responsibility to Business Partners.	✔	✔	✔
Codes of Conduct regarding responsibility to Customers.	✔	✔	✔
Codes of Conduct regarding responsibility to Consumers	✔	✔	✔
Codes of Conduct regarding responsibility to Business Competitors.	✔	✔	✔
Codes of Conduct regarding responsibility to Trade Payables.	✔	✔	✔
Codes of Conduct responsibility to Financial Institution Creditors.	✔	✔	✔
Codes of Conduct regarding responsibility to Regulators.	✔	✔	✔
Codes of Conduct regarding responsibility to Society and Community.	✔	✔	✔
Codes of Conduct regarding responsibility to Environment.	✔	✔	✔

1. Codes of Conduct regarding responsibility to the Company

1.1 Perform duties with responsibility, always considering the best interests of the Company as a priority.

1.2 Refrain from engaging in business activities or taking actions that directly or indirectly create competition with the Company's operations.

1.3 Perform duties with honesty, integrity, transparency, and a strong sense of ethics.

1.4 Utilize and manage the Company's assets to achieve maximum benefit, ensuring they are not used for personal gain or for others unrelated to the Company's business.

1.5 Perform work to the best of one's knowledge, skills, and experience for the Company's ultimate benefit.

1.6 Adhere strictly to the Company's rules, regulations, and policies in all actions.

1.7 Avoid using one's authority improperly, whether directly or indirectly, for personal gain or for giving others unjust benefits.

1.8 Avoid accepting gifts, entertainment, or benefits from business partners in any form that may exceed reasonable limits.

1.9 Refrain from providing information or opinions to external parties that may harm the Company's reputation or operations.

1.10 Do not use confidential Company information for personal gain, either directly or indirectly, and maintain confidentiality as strictly as possible in accordance with the Company's Confidential Information Protection and Controlling the Use of Inside Information Policy and Information Disclosure Policy stated in Section 2 of this Codes of Conduct.

1.11 Report any suspected violations of the law, the Codes of Conduct, or unethical behavior within the organization, including inaccurate financial reporting or inadequate internal controls, for the benefit of the Company. This must be done in accordance with the Company's whistleblower policy, which is outlined in Section 3 of this Code of Conduct.

2. Codes of Conduct regarding responsibility to Shareholders.

2.1 Perform duties with honesty, transparency, and within the framework of the laws and the Company's requirements, adhering to this Codes of Conduct in all business transactions and decision-making activities to ensure that the business operates with integrity, clarity, transparency, and accountability.

2.2 Utilize knowledge, skills, and experience to the fullest to create fair and sustainable returns for shareholders.

2.3 Protect shareholder information and data with the utmost care and maintain shareholder trust.

2.4 Disclose the Company's information accurately, completely, and in a timely manner, in accordance with the guidelines set by the Securities and Exchange Commission (SEC) and the Stock Exchange of Thailand (SET).

3. Codes of Conduct regarding responsibility to Employees.

3.1 Provide fair and appropriate compensation and benefits, aligned with the circumstances and in accordance with applicable laws and regulations.

3.2 Ensure a safe working environment that protects the lives and property of employees.

3.3 Make appointments, transfers, rewards, and disciplinary actions in a fair, honest, and equitable manner, based on knowledge, capability, and appropriateness.

3.4 Manage personnel transparently, from recruitment and performance evaluations to compensation and promotions, with Anti-Bribery and Corruption Policy being a key consideration in all processes, ensuring fairness and transparency in human resource management.

3.5 Promote continuous development and knowledge transfer for employees.

3.6 Provide regular training and seminars to enhance employees' knowledge and skills.

3.7 Provide equal and secure channels for employees to offer feedback or file complaints in accordance with the Company's grievance procedures, as outlined in Section 3 of this Codes of Conduct.

4. Codes of Conduct regarding responsibility to Business Partners.

4.1 Treat partners fairly and equitably, based on mutual benefits, with a focus on building sustainable and transparent business relationships.

4.2 Adhere strictly to agreements and terms that have been agreed upon with partners. If any terms cannot be met, inform the partner immediately and work together to find a solution.

4.3 Collaborate with business partners in the development and improvement of products or services to achieve mutual benefits and provide the highest customer satisfaction.

4.4 Respect intellectual property and information received from business partners, including maintaining the confidentiality of trade-related information.

4.5 Promote transparency in business operations by disclosing necessary information completely and honestly, ensuring clear understanding and preventing misunderstandings.

5. Codes of Conduct regarding responsibility to Customers.

5.1 Treat customers fairly by providing high-quality products and services that meet customer expectations.

5.2 Disclose information about products and services fully, accurately, and transparently, allowing customers to make informed decisions and use the information effectively in managing products and services.

5.3 Maintain the confidentiality of customer data and personal information strictly, in compliance with relevant laws and personal data protection standards.

5.4 Continuously improve products and services, including providing necessary knowledge and support to customers, enabling them to present and manage products and services effectively

5.5 Provide accessible and convenient channels for communication and complaints, with the Company addressing complaints promptly and transparently.

5.6 Focus on building long-term relationships with customers by offering sales support, training, and high-quality after-sales services, along with seriously addressing customer feedback.

6. Codes of Conduct regarding responsibility to Consumers.

6.1 Provide complete, accurate, and transparent information about products and services to consumers through electronic channels such as websites, applications, or online media, including product labels displaying important information such as ingredients, precautions, and usage instructions.

6.2 Take responsibility for selecting products that meet quality and safety standards, ensuring consumers receive safe and high-quality products.

6.3 Encourage customers, who are the Company's distributors, to provide quality service to end consumers and support the collection of consumer complaints regarding products for prompt and effective resolution.

6.4 Provide accessible and convenient channels for complaints from consumers, such as through websites, electronic channels, or telephone numbers, to enable quick and transparent reporting of issues or concerns.

6.5 Comply with personal data protection policies for consumers and maintain the confidentiality of customer information, ensuring it is secure and not disclosed without consumer consent.

6.6 Encourage consumer participation in providing feedback and suggestions about products and services to help improve and develop them in response to market demands.

7. Codes of Conduct regarding responsibility to Business Competitors.

7.1 Conduct business under fair competition principles, adhering to relevant laws and regulations regarding commercial competition.

7.2 Do not seek confidential information from competitors through dishonest or inappropriate methods.

7.3 Do not damage the reputation of competitors by spreading false information or making defamatory accusations.

7.4 Promote constructive competition in the market by focusing on developing high-quality products and services that meet customer needs, without engaging in inappropriate actions towards competitors.

7.5 Respect the intellectual property of competitors and do not use or disclose copyrighted materials or trademarks of competitors without permission.

7.6 Do not use dishonest or inappropriate methods to attract customers or convince them to switch partners or suppliers.

8. Codes of Conduct regarding responsibility to Trade Payables.

8.1 Treat trade payables equally and fairly, adhering to transparency and respecting the rights of creditors.

8.2 Comply strictly with agreements and conditions as agreed, including making payments on time and in accordance with the terms.

8.3 Notify creditors immediately if unable to meet the terms or pay debts as scheduled, and work together to find a solution and corrective measures.

8.4 Maintain a positive relationship with trade creditors, providing necessary information to ensure transparent and smooth operations.

8.5 Prioritize compliance with laws and regulations related to debt repayment and financial transactions.

9. Codes of Conduct responsibility to Financial Institutions Creditors.

9.1 Comply strictly with the terms and conditions in the financial agreements made with financial institution creditors, including the purpose of the funds, debt repayment, and other specified conditions.

9.2 Treat all financial institution creditors equally, without discrimination, while emphasizing the importance of maintaining transparency in financial transactions.

9.3 Report the Company's financial status accurately, completely, and on time to financial institution creditors, as per the terms outlined in the agreement, ensuring transparency in the review process.

9.4 Comply with all relevant laws and regulations related to financial transactions, including responsible debt management.

9.5 Notify financial institution creditors immediately if the Company is unable to meet the terms of repayment or any agreement and cooperate in finding transparent solutions to resolve the issue.

10. Codes of Conduct regarding responsibility to Regulators.

10.1 Strictly comply with laws, regulations, rules, and orders issued by regulatory authorities overseeing the Company, ensuring no actions are taken that contradict such laws or regulations.

10.2 Fully cooperate with regulatory authorities in the review and inspection of information related to the Company’s business operations.

10.3 Report any violations of laws or regulations, or any non-compliance with the requirements set by regulatory authorities, promptly and accurately.

10.4 Follow the practices and guidelines established by regulatory authorities to ensure the Company’s operations are transparent and subject to review.

10.5 Prioritize maintaining governance standards and relevant reporting practices to build trust with regulatory authorities and stakeholders.

11. Codes of Conduct regarding responsibility to Community and Society.

11.1 Conduct business with consideration for the impact on society and the community, ensuring that no actions are taken that could harm the environment or the community.

11.2 Encourage employee and stakeholder participation in social and community activities, particularly in areas such as education, public health, and improving the quality of life within the community.

11.3 Promote activities that contribute to social development in various areas, with a focus on projects that positively impact the well-being and quality of life of the community.

11.4 Support education or public activities that foster a sustainable and stable society.

11.5 Maintain social responsibility standards by conducting business under the principles of transparency and accountability.

12. Codes of Conduct regarding responsibility to Environment.

12.1 Conduct business with consideration for the environmental impact at every stage, focusing on minimizing negative environmental effects.

12.2 Comply strictly with laws and regulations related to environmental protection and disclose information about the environmental impact of the Company's operations to stakeholders.

12.3 Support efficient resource use, promote recycling, the use of biodegradable materials, and the adoption of environmentally friendly products.

12.4 Provide training and raise awareness about environmental conservation for employees at all levels, encouraging active participation in protecting the environment.

Section 2
Related policies

To ensure that the operations of the directors, management, and employees are conducted within the legal framework and in alignment with the Codes of Conduct, the Company has established policies for all levels of directors, management, and employees to follow strictly. The objective is to promote transparency, fairness, and accountability. The details are as follows:

Related Policies as below:

1. Anti-Bribery and Corruption Policy.
2. Anti-Money Laundering and Terrorist Financing Policy
3. Receiving or Giving of Gifts, Assets or Other Benefits Policy.
4. Donation and Funding Policy.
5. Political Policy.
6. Conflicts of Interests Management Policy.
7. Reports Stating the Interests and Security Holding Policy.
8. Handling Confidential Information and Controlling the Use of Inside Information Policy.
9. Information Disclosure Policy.
10. Protecting and Using of the Assets of the Company Policy.
11. Human Rights Policy.
12. Personal Data Protection Policy.
13. IT Security Policy.
14. Facilitation Payment Policy.
15. Revolving Door Policy.
16. Trade Compliance Policy.
17. Occupational Health, Safety, and Environment Policy.
18. Environmental Policy.
19. Social Policy.

The coverage of these policies is according to the table below:

Policy	Responsible Parties		
	Directors	Management	Employee
Anti-Corruption Policy.	✔	✔	✔
Anti-Money Laundering and Terrorist Financing Policy	✔	✔	✔
Receiving or giving of Gifts, Assets or Other Benefits Policy.	✔	✔	✔
Donation and Funding Policy.	✔	✔	✔
Political Policy.	✔	✔	✔
Conflicts of Interests Management Policy.	✔	✔	✔
Reports Stating the Interests and Security Holding Policy.	✔	✔	-
Handling Confidential Information and Controlling the Use of Inside Information Policy.	✔	✔	✔
Information Disclosure Policy.	✔	✔	✔
Protecting and Using of the assets of the Company Policy.	✔	✔	✔
Human Rights Policy.	✔	✔	✔
Personal Data Protection Policy.	✔	✔	✔
IT Security Policy.	✔	✔	✔
Facilitation Payment Policy.	✔	✔	✔
Revolving Door Policy.	✔	✔	-
Trade Compliance Policy	✔	✔	✔
Occupational Health, Safety, and Environment Policy.	✔	✔	✔
Social Policy	✔	✔	✔
Environmental Policy.	✔	✔	✔

Related Policies

Anti-Bribery and Corruption Policy

Definition

Bribery means offering, giving, receiving, or soliciting of any item of value or advantage to influence the actions or decisions of an individual in a position of trust or authority, whether in the public or private sector, to obtain or retain business or secure an improper business or personal advantage. Bribery can involve cash payments, gifts, entertainment, favors, or any other form of inducement intended to corrupt the judgment or actions of the recipient.

Corruption means abuse of power, bribery, kickbacks, extortion, fraud, deception, collusion, cartels, embezzlement, or any actions which may or may not be illegal but are carried out with the intent to gain undeserved benefit to the organization, themselves, or others. Corruption encompasses the receiving, offering, and giving of the money (including donations, collection and any benefits which can be converted into currency), gifts, services, articles, entertainment, and any other benefits both direct and indirect to individuals, juristic person, or government entities to persuade those parties to proceed or omit their duties in order to achieve in any benefits to individuals, family, friends, acquaintances or business operations.

Anti-Bribery and Corruption Policy

SiS Distribution (Thailand) Public Company Limited (the Company) commits and intends to operate business with transparency, integrity, and accountability for all stakeholders to provide the sustainable growth of the company. This commitment is upheld by adhering to corporate governance principles and ethical business conduct. The Company consistently conducts audits to ensure compliance, providing confidence that the Anti-Bribery and Corruption Policy is effectively implemented as follows.

The Company acknowledges the profound impact of corruption within Thai society and on an international scale. Corruption poses significant risks to business operations and is a major barrier to sustainable growth. In response, the Company is committed to full compliance with laws related to anti-bribery and corruption. The Company has established an Anti-Bribery and Corruption Policy that applies to all Company activities.

In addition to complying with the requirements of the Thai Private Sector Collective Action Against Corruption (CAC) as a member, this policy is also aligned with the guidelines set by the U.S. Foreign Corrupt Practices Act (FCPA), and the UK Bribery Act 2010. It reflects our commitment to maintaining the highest ethical standards and ensuring full compliance with both domestic and international anti-corruption regulations.

The Company promotes strict adherence to the Anti-Bribery and Corruption Policy for all directors, management and employees of the Company, its subsidiaries, as well as all business representatives. The policy aims to be guidelines for preventing bribery, and corruption as outlined below:

1. Directors, management, and employees of the Company and its subsidiaries are strictly prohibited from direct and indirect involving or accepting any forms of bribery, or corruption to generate inappropriate benefit to themselves, their family, friends and business from individuals, juristic persons, or the entities that having business with the Company and its subsidiaries. The Company intends to cultivate and promote a corporate culture entirely free from corruption, emphasizing that any form of corruption is unacceptable within the Company.

2. The Company requires the assessment and management of corruption and fraud risks to be conducted annually, or whenever there are changes in relevant laws, standards, or the business environment. The Company also reviews compliance with internal controls related to anti-corruption as part of the annual internal audit plan. In addition, the Company ensures that anti-corruption measures, practices, and requirements are regularly reviewed, evaluated, and improved on an annual basis to ensure alignment with both internal and external environments and to address any emerging risks.
3. Directors, management, and employees of the Company and its subsidiaries are required to adhere to the Anti-Bribery and Corruption Policy, the Codes of Conduct and other instructions relating to the Anti-Bribery and Corruption Policy that is defined by the Company.
4. Directors, management, and employees of the Company and its subsidiaries shall not be involved in any direct and indirect bribery or corruption. Also, it is prohibited to ignore or neglect when notice the corruption and clues of corruption that relate to the Company and its subsidiaries.
5. The Anti-Bribery and Corruption Policy emphasizes the importance of awareness and avoidance of channels that could generate corruption. It outlines the following key principles for all parties to follow:
    5.1 Directors, managements, and employees of the Company and its subsidiaries are prohibited from receiving monetary, gifts, or assets that can be converted into currency or other benefits from individuals, juristic persons or entities that have business with the Company and its subsidiaries for gaining inappropriate benefits to themselves, their family, friends, businesses, except during internationally recognized New Year holidays or customary practices widely accepted.
    5.2 Directors, managements and employees of the Company and its subsidiaries are strictly prohibited from offering gifts, assets, or any other benefits, or excessively extravagant entertainment to external parties with the intent to improperly influence their actions or decisions.
    5.3 Donation or sponsorship for charitable purposes shall comply with the Company's requirement, transparent and traceable. The intent behind donations or support shall not be related to any bribes.
    5.4 All procurement and contracting activities related to the Company's and its subsidiaries' business operations, whether with public or private sectors, must be conducted with transparency, fairness, and auditable, and must comply with business ethics and applicable laws.
    5.5 The Company has a neutral political stance and will not engage any activities to support any political parties. The Company emphasizes democracy and respect in the right of liberty, especially the election of the directors, all levels of the managements and the employees of the Company.
6. The Company establishes a good internal audit and control system to ensure that management of corruption risks is appropriate and sufficient, covering all the following details: The Company has established an effective internal control and audit system to ensure that corruption and fraud risk management is appropriate, adequate, and auditable. This system covers all areas of the organization's operations, including finance, accounting, procurement, sales, and contracting.

7. The Company has defined the scope and responsibilities of the Quality Assurance Department in relation to anti-corruption efforts. Management is responsible for ensuring adequate resource allocation to support effective implementation of control and prevention measures against bribery and corruption, in alignment with the Company's Anti-Bribery and Corruption Policy.

8. The Company establishes a continuous communication strategy to ensure that directors, managements and employees of the Company, its subsidiaries, and business representatives acknowledge, comprehend, and implement the policies, measures, and guidelines for anti-corruption. This communication strategy encompasses the Company's expectations and channels for reporting to the Audit Committee. It includes penalties for non-compliance and safeguards for whistleblowers and reporters. Communication channels may include employee and new director orientations, meetings, electronic training, publication on the Company's website, and other electronic media etc.
9. The Company establishes a communication strategy to inform business partners about the Company's Codes of Conduct, Anti-Corruption, and related policies through various channels such as the Company's website and electronic media etc.
10. The Company assigns the Audit Committee to oversee the risks and internal control system relating to corruption including the Anti-Bribery and Corruption Policy implementation. The Audit Committee shall continuously report the audit result to the Board of Directors.
11. The Board of Directors and management have duties and responsibilities to support and implement the Anti-Bribery and Corruption Policy by indicating the system to encourage and support Anti-Bribery and Corruption Policy. They are also responsible for continually reviewing and developing policies, systems, and measures as appropriate.
12. If any form of corruption or clues of corruption relating to the Company and its subsidiaries is discovered or disclosed, it shall be reported to the person responsible for anti-corruption immediately, using the specified reporting channels.
13. Directors, management and employees of the Company and its subsidiaries shall cooperate in investigating and examining the facts related to corruption according to the indicated corruption investigation procedures.
14. The Company has protection measures in place to ensure fairness to informants or those who report corruption related to the Company and its subsidiaries, and such individuals will be treated in accordance with the indicated protection measures.
15. Directors, management, and employees of the Company who are involved in corruption or engaged in any activities that violate the Company's Codes of Conduct and policies, both directly and indirectly, will be subject to disciplinary actions as defined by the Company. If such corruption is illegal, legal penalties will also be applied.
16. The Management and the employees of the Company and its subsidiaries shall get all information and undergo training relating to the Anti-Corruption as determined by the Company.
17. Directors, managements and employees of the Company and its subsidiaries shall be aware of the importance of Anti-Corruption and the Codes of Conduct in order to enhance the sustainable growth of the Company as well as to be the good citizens of Thai society.
18. The Anti-Corruption working group has authority to examine and investigate in all circumstances that are direct and indirect related to the corruption.

Operating Requirements

1. To comply with the Anti-Bribery and Corruption Policy, it is essential to adhere to the good corporate governance principles, Codes of Conduct and any related operational instructions defined by the Company to promote the ethics and corporate governance of the Company and its employees.

2. The Anti-Bribery and Corruption Policy applies to all aspects of the Company's business operations, including human resources processes. This encompasses recruitment, training, performance evaluation, promotion, and the provision of employee benefits and welfare. Compliance with the Anti-Corruption Policy is a key consideration in these processes. The Company consistently emphasizes that all employees must conduct their duties in strict accordance with this policy.

Anti-Bribery and Corruption Guidelines

To ensure the effective implementation of the above policy, the Company has established the following guidelines:

1. The Company shall conduct an assessment of corruption risk at least once a year and additionally whenever there are changes that may affect the organization's risk level.
2. The Company shall conduct a review and evaluate the effectiveness of internal controls related to anti-corruption, integrated into the annual internal audit plan. Any findings from the internal audit concerning corruption or suspicious behavior shall be urgently reported to senior management, the Audit Committee, and the Board of Directors.
3. The Company shall regularly review, examine, and improve anti-corruption measures, practices, and relevant requirements, and report the results to the Board of Directors annually to ensure comprehensive coverage of both existing and emerging risks.
4. The Company strictly prohibits all personnel from offering, giving, receiving, or soliciting any form of benefit that may influence business decisions or create a conflict of interest, whether directly or indirectly.
5. In the event that any act or indication of corruption is witnessed or suspected, employees are required to immediately report it to their supervisor, the Quality Assurance Department, or through the Company's established whistleblowing channels. The Company has implemented a whistleblowing system and protection measures for whistleblowers to encourage personnel to report information in good faith.
6. Employees are required to report to their supervisor upon receiving gifts given in customary practice. Gifts that cannot be declined must be handed over to the Company's designated central department for safekeeping. In cases where travel rewards are received, employees must notify the Company for appropriate handling. Business entertainment must have a clear and legitimate business purpose and must be conducted in accordance with the Company's Code of Conduct, relevant policies, and employee handbook.
7. The giving of gifts or business entertainment to business partners or external parties must receive prior approval and be supported by proper documentation of the approval and payment for audit purposes. The Company strictly prohibits giving any items that are excessively luxurious or could be interpreted as a bribe.
8. All donations and sponsorships must be approved by the authorized person in accordance with the Company's regulations, with proper supporting documentation maintained. The Quality Assurance Department must be able to verify the legitimacy and appropriateness of the purposes at all times.
9. The Company stipulates that all procurement processes must be conducted in writing, with clear segregation of duties between approvers and reviewers. The selection criteria must be fair and transparent, and vendors with a history of fraudulent or corrupt practices shall be avoided.
10. Charitable donations or sponsorships shall comply with the Company's regulations, ensuring transparency and auditability. Such contributions must not be intended as, or perceived to be, a form of bribery.

11. All procurement and contracting activities related to the Company's and its subsidiaries' business operations, whether with public or private entities, shall be carried out transparently and in compliance with business ethics and applicable laws. All personnel must adhere to the Company's Codes of Conduct and operational practices.
12. The Company maintains a position of political neutrality and shall not engage in or support any particular political party. The Company values democracy and respects the political rights and freedoms of its directors, executives, and employees, especially the right to participate in elections.
13. The Company requires the establishment and implementation of an annual audit plan that comprehensively covers the review of operational procedures related to accounting practices, financial record entries, record retention, financial documentation, and Company data. The audit shall also include the examination of sales, marketing, procurement, contracting processes, and the identification and resolution of potential errors, as well as any other processes that may pose a risk of corruption. Such audits must be carried out effectively, regularly, and sufficiently to ensure that accounting and financial recording are accurate, complete, reliable, and reflect actual transactions.
14. The Company requires appropriate and rigorous audits of the procedures for retaining financial records, documents, evidence, and information of the Company and its subsidiaries. In addition, the Company shall maintain a sound and sufficient internal control system to ensure that financial transaction data can be promptly verified.
15. The Company mandates audits of sales, marketing, procurement, and contracting processes, particularly those areas prone to corruption risks. The Company shall also identify appropriate corrective measures and regularly review and improve operational procedures and practices.
16. The Company requires clear segregation of duties in each stage of operations to ensure compliance with good internal control principles. Furthermore, the Company shall design work systems that promote checks and balances among all departments.
17. The Company has established measures and operational procedures for processes that pose a risk of corruption, in accordance with sound internal control principles. Adequate supporting documentation is required for all transactions, with proper record retention. In addition, the procedures and methods of operation are regularly reviewed and improved to ensure their continued effectiveness.
18. The Company requires joint discussions with risk owners or relevant departments for activities involving corruption risks to design, review, and improve internal control systems and operational procedures to minimize such risks.
19. The Company has established a monitoring process to ensure that the anti-bribery and anti-corruption measures are effectively implemented. This is to ensure that the Board of Directors, management, and employees consistently comply with the Company's anti-bribery and corruption policies and requirements.
20. The Company instills a strong sense of integrity and anti-corruption values among its directors, management, and employees. To ensure their full awareness and adherence to these practices, the Company has incorporated anti-corruption guidelines into the orientation programs for new directors and employees. In addition, the Company continuously reinforces these principles among executives and employees through electronic media and conducts annual e-Learning training sessions to promote awareness and strengthen a culture of transparency and zero tolerance toward corruption.

21. The Company has established communication channels for stakeholders to report any incidents of fraud or corruption. These include a direct communication channel with management via complain@sisthai.com, as announced on the Company's website. The Company maintains a secure database system to record all reports received. In addition, stakeholders may directly contact the Audit Committee through independentdirector@sisthai.com.
22. The Company strictly prohibits any form of exploitation or abuse of authority over others, including offering or promising valuable items to gain an improper advantage.
23. The Company has established clear and appropriate policies regarding employee expense reimbursement to prevent fraud and corruption. All expense claims are subject to review and approval by both the employee's immediate supervisor and the General Affairs Department, which oversees cost control. Employees are informed from the outset that reimbursements are made only for actual expenses incurred and must not be treated as personal income.
24. The Company considers fraud and corruption to be serious offenses. In the event of such misconduct, a committee will be appointed to determine appropriate disciplinary actions, which may include reprimand, compensation for damages, termination of employment, or legal action against the involved employee(s). The Company will also conduct a thorough investigation to identify root causes, implement preventive and corrective measures, and improve internal systems to prevent recurrence.
25. The Company will not demote, penalize, or take any adverse action against employees who refuse to engage in or support acts of fraud or corruption, even if such refusal may result in a loss of business opportunity for the Company.

Consulting and Reporting Non-Compliance relating to the Anti-Bribery and Corruption Policy

The Company provides an opportunity for all stakeholders to report the clues and complaints of non-compliance relating to the Anti-Bribery and Corruption Policy. The stakeholders can report the clues and complaints directly to the Audit Committees through established channels for the purpose of conducting a thorough investigation and assessment of the reported complaints, with the following details:

1. The Quality Assurance Department, under the oversight of the Audit Committee, is responsible for managing and conducting investigations when disclosures or complaints related to non-compliance with the Anti-Bribery and Corruption Policy are received. The Audit Committee shall arrange the investigation when there is evidence to support the claims.
2. For external stakeholders, the Company provides a channel for receiving complaints regarding non-compliance with the Anti-Bribery and Corruption Policy. This channel is also dedicated to providing consultation and guidance about the Anti-Bribery and Corruption Policy, as follows:

   The Audit Committee
   Address: 9 Pakin Building, 9th Floor, Room No. 901, Ratchadaphisek Road,
   Din Daeng, Bangkok 10400
   Tel: 020-020-3000 Ext. 3291
   Email: independentdirector@sisthai.com

3. For internal stakeholders, the Company provides a channel for receiving complaints about non-compliance with the Anti-Bribery and Corruption Policy. These channels are also dedicated to providing consultation and guidance about the Anti-Bribery and Corruption Policy, as follows:
   - 3.1 Supervisors, executives, and the Management who are entrusted by the complainant or the whistleblower.
   - 3.2 Human Resources Manager
   - 3.3 Quality Assurance Department
   - 3.4 Company Secretary
   - 3.5 Lotus Notes Database named: Secret Suggestion Box
   - 3.6 The Audit Committees as per communication channel stated in item 2.

Complaints Managing Procedure

The Company designates the Audit Committee as responsible for managing complaints related to non-compliance with the Anti-Bribery and Corruption Policy. A specific committee will be appointed to assess and handle complaints and clues on a case-by-case basis. The appointment of this committee will prioritize independence and appropriateness in addressing the specific complaints.

The procedures for managing clues and complaints related to corruption are as follows:

1. The person receiving the clues or complaints shall report such information to the Quality Assurance Department for an initial assessment prior to further report to the Audit Committee.
2. If the preliminary assessment reveals the validity of the complaint or disclosure, the Audit Committee will appoint a specific committee to gather facts, evidence, and conduct a thorough investigation.
3. The specific committee will present details of clues or complaints, along with the facts and evidence, to the Audit Committee for evaluation and consideration. This process typically takes approximately 30-60 days (depending on the complexity of facts-finding).
4. The Audit Committee reviews and assesses the clues and complaints to develop a plan for taking punitive action against the wrongdoers, in accordance with the established penalty outlined.
5. The Audit Committee evaluates and considers the damage incurred by both the affected parties and the complainants to develop measures for mitigating the impact on those affected and implementing protective measures for the complainants.
6. In cases that fall under the criteria that must be reported to the Board of Directors, the Audit Committee shall present the investigation report, the punishment and mitigation guidelines, including its implementation to the Board of Directors.
7. In case the whistleblowers or the complainants reveal themselves, the specific committee will inform them of the results within 7 business days after the case is concluded.

Complainants and Whistleblower Protection Measures

1. The Company will not disclose the names and information of the whistleblowers or complainants.
2. The Company will treat information related to clues and complaints as confidential, only disclosing it as necessary for processing and assessing the clues and complaints, with a primary focus on the safety and protection of the whistleblowers, complainants, and affected parties.
3. In cases where the Audit Committee assesses the situation and finds that there is an impact on the whistleblowers or complainants, the committee will take fair and appropriate measures to protect the whistleblowers or complainants, tailored to specific circumstances.

4. In situations where the whistleblowers or complainants are in circumstances that are not safe or where they may be at risk of harm because of their disclosures and complaints, they are encouraged to request the company to establish appropriate protective measures.
5. The Company will not consider degrading, punishing, or having negative impact on the employees who refuse the fraud and corruption even such refusion may cause the Company business opportunity lost.

Penalty

This Anti-Bribery and Corruption Policy is considered a strict discipline that must be adhered to diligently. Any persons who violate or fail to comply with it are deemed to be acting against the Company's policies and the Codes of Conduct, and any such actions that cause harm or result in business opportunities loss for the Company may lead to disciplinary action in accordance with the Company's employment regulations, and may also be subject to legal penalties as per the Securities and Exchange Act (No. 4) B.E. 2551.

This Anti-Bribery and Corruption 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.

Somchai Sittichaisrichart
Managing Director
SiS Distribution (Thailand) Public Company Limited

Anti-Money Laundering and Terrorist Financing Policy

Definition

Money Laundering means the process of converting money or assets obtained through unlawful activities into money or assets that appear legitimate or cannot be easily traced to their illicit origins.

Terrorism means acts of terrorism as defined under the Criminal Code or offenses as stipulated in international conventions and protocols on terrorism to which the company's operating country is a signatory or adheres, regardless of whether such acts occur domestically or internationally.

Anti-Money Laundering and Terrorist Financing Policy

SiS Distribution (Thailand) Public Company Limited (the Company) recognizes the importance of complying with laws and regulations concerning anti-money laundering (AML) and counter-terrorist financing (CFT). The Company is committed to promoting transparency and integrity across all business operations. This policy has been established to guide the Company's efforts in managing risks related to money laundering and terrorist financing, as outlined below:

1. Directors, management, and employees of the Company and its subsidiaries must strictly adhere to this policy and must not, under any circumstances, engage in or facilitate money laundering or terrorist financing activities, directly or indirectly.
2. The Company will designate appropriate personnel to oversee AML/CFT compliance and implement internal control measures to manage risks associated with money laundering and terrorist financing.
3. The Company will not engage in transactions or relationships with individuals or entities suspected of involvement in money laundering or terrorist financing.
4. The Company will promote awareness and understanding of the importance of AML/CFT compliance among directors, executives, and employees.
5. It is the duty of all persons to report any suspicious activities or information regarding potential money laundering or terrorist financing involving the Company or its subsidiaries to the Company.

Anti-Money Laundering and Terrorist Financing Guidelines

To ensure the effective implementation of the above policy, the Company has established the following guidelines:

1. The Company will follow customer due diligence process, as outlined in the Trade Compliance Policy, to avoid business relationships with individuals or entities suspected of money laundering or terrorist financing.
2. Customer information will be periodically reviewed or reassessed when suspicious transactions or circumstances arise.
3. Reports on potential money laundering or terrorist financing activities will be reviewed by the Quality Assurance Department. Initial findings will be presented to the Audit Committee, which will appoint a task force to investigate further. Findings will then be escalated to the Board of Directors and relevant regulatory authorities as required by law.
4. This Anti-Money Laundering and Terrorist Financing Policy is considered a strict discipline that must be adhered to diligently. Any person who violates or fails to comply with it is deemed to be acting against the Company's policies and the Codes of Conduct may lead to disciplinary action in accordance with the Company's employment regulations and may also be subject to legal penalties.

Consulting and Reporting Non-Compliance relating to the Anti-Money Laundering and Terrorist Financing Policy

The Company provides an opportunity for all stakeholders to report the clues and complaints of non-compliance relating to the Anti-Money Laundering and Terrorist Financing Policy. The stakeholders can report the clues and complaints through established channels for the purpose of conducting a thorough investigation and assessment of the reported complaints, with the following details:

1. The Quality Assurance Department, under the oversight of the Audit Committee, is responsible for managing and conducting investigations when disclosures or complaints related to non-compliance with the Anti-Money Laundering and Terrorist Financing Policy are received.
2. For external stakeholders, the Company provides a channel for receiving complaints regarding non-compliance with the Anti-Money Laundering and Terrorist Financing Policy. This channel is also dedicated to providing consultation and guidance about the Anti-Money Laundering and Terrorist Financing Policy, as follows:

   The Audit Committee
   Address: 9 Pakin Building, 9th Floor, Room No. 901, Ratchadaphisek Road,
   Din Daeng, Bangkok 10400
   Tel: 020-020-3000 Ext. 3291
   Email: independentdirector@sisthai.com
3. For internal stakeholders, the Company provides a channel for receiving complaints about non-compliance with the Anti-Money Laundering and Terrorist Financing Policy. These channels are also dedicated to providing consultation and guidance about the Anti-Money Laundering and Terrorist Financing Policy, as follows:
   - 3.1 Supervisors, executives, and the Management who are entrusted by the complainant or the whistleblower.
   - 3.2 Human Resources Manager
   - 3.3 Quality Assurance Department
   - 3.4 Company Secretary
   - 3.5 Lotus Notes Database named: Secret Suggestion Box
   - 3.6 The Audit Committees as per communication channel stated in item 2.

This Anti-Money Laundering and Terrorist Financing 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.

Receiving or Giving of Gifts, Assets, or Other Benefits Policy

Definition

Receiving or Giving of Gifts means receiving or giving monetary gifts to the outsider consisting of vendors, customers, service providers, bank or financial institute personnel, officer of the government, state enterprises and private sectors including ordinary people.

Entertainment and Hospitality mean expenditure on business entertainment, such as food and beverage entertainment, sport entertainment and any expenditure relating directly to business operations or trade customs. This may also include providing business-related knowledge and understanding.

Receiving or Giving of Gifts, Assets, or Other Benefits Policy

SiS Distribution (Thailand) Public Company Limited (the Company) is well aware that receiving or giving gifts, assets, or other benefits as well as engaging in various forms of hospitality can be avenues for potential corruption. Therefore, the Company has established the Receiving or Giving of Gifts, Assets, or Other Benefits Policy to align with its Anti-Corruption and related policies, as follows.

1. Directors, management, and employees of the Company and its subsidiaries are strictly prohibited from receiving money, gifts, assets, or any other benefits that may result in an improper advantage for themselves, their families, friends, or businesses from any external party related to the Company.
2. Directors, management, and employees of the Company and its subsidiaries are strictly prohibited from offering gifts, assets, or any other benefits to external parties with the intent to improperly influence or induce any action or omission in the performance of duties.
3. The Company has a policy not to host or entertain external parties, whether from the public or private sector, for business advantages, except for appropriate social occasions conducted in accordance with proper etiquette.
4. The Company requires the Quality Assurance Department to closely monitor, review, and report compliance with this policy.
5. The Company communicates this policy and related practices to directors, management, employees, representatives, and business partners through various channels, such as meetings and electronic communications, to ensure thorough understanding and awareness.

Receiving or Giving of Gifts, Assets, or Other Benefits Guidelines

To ensure the effective implementation of the above policy, the Company has established the following guidelines:

1. Directors, Management and employees of the Company and its subsidiaries are prohibited from accepting cash, gifts, convertible assets, or any other benefits that may result in inappropriate advantages for themselves, their families, friends, or businesses from individuals, entities, or organizations conducting business with the Company or its subsidiaries.
   Exceptions are permitted for gifts given during the international New Year or in accordance with widely accepted customs and traditions. In such cases:
   - For gifts with a value exceeding 3,000 Baht or uncertain value: the recipient must hand them over to the General Affairs department for further consideration and appropriate action by the Company.
   - In cases where the recipient receives a travel reward or trip: the recipient must notify the Company so that appropriate handling or arrangements can be determined.
2. Acceptance of entertainment or hospitality from external parties must be reasonable, align with business ethics, and comply with relevant policies and the employee handbook.

3. Directors, Management, and employees of the Company and its subsidiaries are prohibited from offering items, assets, or any other benefits to external parties as an incentive to perform or omit duties inappropriately, to gain an unfair business advantage, or for personal gain. Any giving of gifts as part of cultural or traditional practices must receive prior approval from the supervisor. Additionally, hospitality or entertainment must not be excessively extravagant.
4. The employees who contact vendors and receive the demo with a value given by the vendor for testing or any other purpose shall inform the General Affairs Department for recording and keeping such goods in the Company's system prior to use. The employees are responsible for returning the items or tracking their return to the Company.
5. Providing, offering, or giving money, gifts, or any other benefits to the outsider or those related to conducting business with the Company and its subsidiaries shall be carried out in accordance with the procedures, guidelines, and approvals established by the Company.
6. The Company does not have a policy of entertaining the outsider who conducts business or interacts with the Company, both in private and government sectors, to avoid engaging in practices that may be considered as bribery. However, entertainment may be provided on special occasions, in accordance with social norms, budget allocations, or when deemed appropriate. This is to maintain good business relationships without expecting anything in return.
7. The Quality Assurance Department is responsible for ensuring strict compliance with the policy and ensuring that there is no use in gift-giving, entertainment, or hospitality as a means of corruption. They are also responsible for promptly reporting any issues or suspicious behavior to senior management, the Audit Committee, and the Board of Directors.
8. The Company ensures that directors, Managements and employees of the Company, its subsidiaries, business representatives, and business partners are aware of the Receiving or Giving of Gifts, Assets, or Other Benefits Policy and guidelines through various communication channels, such as meetings and electronic communication. Everyone can access this policy on the Company's website.

This Receiving or Giving of Gifts, Assets, or Other Benefits 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.

Donation and Funding Policy

Definition

Provision/receipt of support means giving/receiving financial support, products, or services with the aim of creating public benefit or promoting the Company's business and positive image.

Provision/receipt of donations means giving/receiving money, goods, or any other benefits for charitable purposes to individuals or other juristic persons. It is done with the intention of creating public benefit or promoting the Company's business and positive image.

Donation and Funding Policy

SIS Distribution (Thailand) Public Company Limited (the Company) is committed to conducting its business with transparency, integrity, and good corporate governance, while upholding the principles of anti-corruption in all forms. The Company recognizes that donations and sponsorships could potentially be misused as a means or pretext for obtaining undue or illegal benefits, or for favoring certain individuals, which could harm the Company's reputation, credibility, and interests.

Accordingly, the Company has established this Donation and Funding Policy to ensure that all donations and funding activities are carried out with honesty, transparency, accountability, and for genuine public benefit without the intention of receiving inappropriate business advantages or returns.

The Company encourages donations and fundings that align with its sustainability approach, with particular emphasis on education and environmental initiatives that create shared value between the business and society. All activities shall adhere to the following Company's ethical framework1. Transparency: All donations and funding must be approved by authorized personnel in accordance with prescribed procedures, supported by complete documentation, and subject to audit and review.

2. Accountability: The purpose, outcomes, and beneficiaries of each donation or sponsorship must be clearly identified and justifiable, ensuring that no conflict of interest arises.
3. Appropriateness and Alignment with Corporate Objectives: Donations and funding must align with the Company's vision, mission, and values, and must comply with applicable laws and government regulations.
4. Anti-Corruption Principle: The Company shall not make or support any donation or fund that is intended or could be construed as an improper inducement to influence a decision in favor of the Company or any related individual.

Donation and Funding Guidelines

To ensure the effective implementation of the above policy, the Company has established the following guidelines:

1. Donations and support must be contributed to education and the environment and should be given to an organization that has been vetted by the relevant authorities. Furthermore, these donations should be clearly demonstrated as selfless acts without expecting any personal benefits, whether for oneself, family, friends, or acquaintances, and should not create an unfair advantage or perception of benefiting the Company's business unfairly.
2. Donations for charitable purposes and the provision of various forms of support shall be carried out in accordance with the procedures and expense regulations established by the Company.
3. The Company's donations for charitable purposes and the provision of various forms of support must be carried out in accordance with this policy, whether it involves financial contributions or company assets.
4. A plan shall be established specifying the objectives, the donated amount, and the organizations to be recipients. This plan will be presented to the Management for approval prior to any donations on behalf of the Company.

5. The Quality Assurance Department shall be responsible for ensuring that the policy is strictly adhered to, and that donations and support are not used as a means of facilitating corruption. Any concerns or suspicious behaviors shall be reported urgently to the senior management, the Audit Committee, and the Board of Directors.
6. The Company ensures that directors, Managements and employees of the Company, its subsidiaries, business representatives, and business partners are aware of the Donation and Funding Policy and guidelines through various communication channels, such as meetings and electronic communication. Everyone can access this policy on the Company's website.

This Donation and Funding 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.

Political Policy

Definition

Political contribution means providing financial assistance, assets, items, or other benefits to support political activities, both directly and indirectly, to political parties, politicians, individuals with political responsibilities, and organizations closely associated with political parties at various levels, including local, regional, national, and international levels.

Political Policy

SIS Distribution (Thailand) Public Company Limited (the Company) is committed to maintaining political neutrality and will not engage in any political activities, either directly or indirectly. This is to prevent the Company's resources from being used in ways that could result in conflicts of interest or be perceived as political support, which may affect the Company's reputation, credibility, and independence.

The Company's has established the Political Policy in alignment with its intention to conduct business with political impartiality, while respecting democratic principles and the legal rights and freedoms of individuals, as follows:

1. The Company shall not provide any political support or assistance to political parties, politicians, or politically affiliated organizations.
2. The Company shall not use its resources, assets, or reputation to express political opinions or affiliations.
3. The Company shall encourage directors, executives, and employees to exercise their political rights as responsible and independent citizens, without compromising the Company's neutrality.

Political Guidelines

To ensure the effective implementation of the above policy, the Company has established the following guidelines:

1. The Company requires all directors, management, and employees to refrain from engaging in any political activities that could lead others to believe that the Company supports any political party, politician, or political group. No statements or actions shall be made on behalf of the Company that could be interpreted as taking a political stance.
2. The Company prohibits providing any form of financial assistance, including money, assets, goods, or other benefits, whether directly or indirectly, to support or promote any political party, politician, or organization affiliated with a political party. This includes donations, provision of goods, purchase of products or services for fundraising purposes, or any other actions that could be perceived as undertaken by the Company to gain improper advantages or benefits.
3. The Company requires all personnel to avoid wearing clothing, displaying symbols, or expressing messages during work that could be interpreted as representing or supporting any political party, as well as any actions that might cause others to perceive the Company as politically biased.
4. The Company assigned the Quality Assurance Department to ensure strict compliance with this policy and to verify that no political assistance is used as a means for corruption. Any suspicious behavior must be promptly reported to senior management, the Audit Committee, and the Board of Directors.
5. The Company shall communicate this policy and related guidelines to all directors, management, employees, subsidiaries, business partners, and relevant stakeholders through various channels, such as meetings and electronic communications. The policy shall also be made publicly accessible on the Company's website.

6. The Company respects the personal rights of directors, management, and employees to hold political opinions or participate in political activities in their personal capacity. However, such activities must not be conducted in the name of the Company, must not utilize Company resources, and must not create the impression that the Company is politically involved.

7. The Company encourages employees and stakeholders to report any suspected violations of this policy through the Company's whistleblowing channels. All reports will be handled fairly and confidentially. Proven violations will result in disciplinary actions and, where appropriate, legal measures.

This Political 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.

Conflicts of Interests Management Policy

Definition

Conflict of Interest means engaging in any activities that require personal interests or those involving individuals related by blood or other connections to influence decision-making, which may hinder or obstruct the Company's best interests, both directly and indirectly.

Related Persons means to individuals who may cause directors or managements of a listed company to face a conflict of interest in making business decisions, whether to prioritize the benefit of such persons or the best interests of the company. These include:

1. Directors, management, major shareholders, controlling persons of the listed company, persons nominated to be directors, management, or controlling persons, as well as their related persons and close relatives.
2. Any juristic person in which a major shareholder or controlling person is a person as specified in Item 1.
3. Any person whose circumstances indicate that they act on behalf of, or are under the influence of, persons specified in Items 1 or 2.
4. Directors of a juristic person that controls the company's business.
5. The spouse, minor children, or adopted minor children of directors as specified in Item 4.
6. Any juristic person in which the persons specified in Items 4 or 5 have controlling power.
7. Any person acting with the understanding or agreement that if the company enters into a transaction that provides financial benefits to such person, the following persons will also receive financial benefits:
   - 7.1 Directors of the company
   - 7.2 Management of the company
   - 7.3 Controlling persons of the company
   - 7.4 Directors of the company's controlling persons
   - 7.5 Spouses, minor children, or adopted minor children of the persons specified in Items 7.1 to 7.4

Major Shareholder means to a shareholder who directly or indirectly holds more than 10 percent of the total voting shares of any juristic person, including the shares held by their related persons.

Management means to the top four management positions immediately below the Managing Director and all equivalent positions, including those in accounting or finance functions at the level of Department Manager or higher, or equivalent positions.

Controlling Person means to a person who has control over a juristic person's management or policies, meaning one who holds more than 50 percent of the total voting rights of that juristic person, or who directly or indirectly controls the majority of voting rights at the shareholders' meeting, or has the power, directly or indirectly, to appoint or remove at least half of the directors of that juristic person.

Connected Transaction means to any transaction conducted between a listed company or its subsidiaries and any related person of the listed company.

Conflicts of Interests Management Policy

SiS Distribution (Thailand) Public Company Limited (the Company) recognizes the importance of conducting its business with transparency, good corporate governance, and accountability in order to build trust among shareholders, investors, customers, business partners, and all stakeholders. To this end, the Company has established this Conflict of Interest Management Policy to define the principles and guidelines for preventing, controlling, and managing conflicts of interest in accordance with the principles of good governance and sound corporate oversight, as follows:

1. Directors, management, and employees shall perform their duties with honesty, transparency, and fairness. They must not use their positions, authority, or internal information to seek personal gain or benefits for related parties.
2. Must avoid any actions that may conflict with the Company's interests, including interactions with the Company's business counterparts—such as suppliers, customers, and competitors—or the exploitation of the Company's business opportunities, as well as engaging in external employment or activities that could affect the Company's interests.
3. Related persons shall avoid entering into transactions with the Company unless such transactions are necessary and in the Company's best interest. In such cases, the related person must notify the relevant supervisory unit or the Company Secretary in advance. The transaction must be conducted on an arm's length basis as if with an independent third party. Directors, management, or employees with an interest in the transaction must not participate in the decision-making process and must disclose relevant information accurately and completely in accordance with applicable laws, regulations, and internal procedures.
4. All related-party transactions shall be subject to review or consideration by the Audit Committee. In the event that any Audit Committee member has an interest in such a transaction, that member shall not take part in the review or consideration of the matter.

Conflicts of Interests Management Guidelines

To ensure the effective implementation of the above policy, the Company has established the following guidelines:

1. The Board of Directors has been informed of and reviewed transactions that may pose a conflict of interest and Relate Party Transactions. Furthermore, the Company adheres to the criteria set by the SET by pricing and conducting these transactions as if they were with external parties. Details of these transactions are disclosed in the Annual Report.
2. During the Board of Directors' meetings, if a director has a conflict of interest or is involved in a matter that could affect their impartiality, such director will be excused from the meeting to allow the remaining directors to deliberate freely and openly.

3. The Company has established controls regarding the use of internal information by requiring the directors and the Managements to report changes in shareholding to the Securities and Exchange Commission, Thailand (SEC) in accordance with the Securities and Exchange Act. The Managements and the employees are prohibited from disclosing internal information to external individuals or those not related to the Company. Moreover, as the Company operates in a manner that provides transparency and shares information with all employees, so all directors, Managements and employees are prohibited from trading the Company's shares during the blackout period, which is during the end of each quarter until the Company submitted the Financial Statement to the SET. Furthermore, since 2014, there is an additional requirement for the directors and the Managements to notify the Board of Directors through the Company Secretary at least 1 working day in advance prior to trading the Company's share.
4. To ensure that employees are aware of these practices, the Company includes guidelines for managing conflicts of interest in its orientation program for new employees and directors. Additionally, there is continuous emphasis on these guidelines through electronic media to ensure that the directors, the Managements, and all employees are well-informed about the practices for preventing conflicts of interest on a quarterly basis.
5. The Quality Assurance Department shall be responsible for ensuring that the policy is strictly adhered to, and there is no conflict of interest in the Company. Any concerns or suspicious behaviors shall be reported urgently to the senior management, the Audit Committee, and the Board of Directors.
6. The Company ensures that directors, Managements and employees of the Company, its subsidiaries, business representatives, and business partners are aware of the Conflicts of Interests Management Policy and guidelines through various communication channels, such as meetings and electronic communication. Everyone can access this policy on the Company's website.

This Conflicts of Interests Management 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.

Reports Stating the Interests and Security Holding Policy

Definition

Management means the first four levels of management positions below the Managing Director, including all positions equivalent to the fourth level. This also includes positions within the accounting or finance functions at the level of Department Manager or equivalent and above.

Related Person means a spouse, minor child, and any person as defined under Section 258 of the Securities and Exchange Act B.E. 2535 (1992).

Trading Blackout Period means the period specified by the Company during which directors, executives, and employees are prohibited from trading the Company's securities. This period commences from the end of each financial quarter until the date the company discloses its financial statements or other significant information to the public.

Reports Stating the Interests and Security Holding Policy

SiS Distribution (Thailand) Public Company Limited (the Company) recognizes the importance of good corporate governance, transparency, and accountability toward shareholders, investors, and all stakeholders. To ensure that directors, management, and employees comply with the laws and regulations of the Securities and Exchange Commission (SEC), the Stock Exchange of Thailand (SET), as well as the Securities and Exchange Act B.E. 2535 (1992) and its amendments, the Company has established this Reports Stating the Interests and Security Holding Policy. The objective of this policy is to promote accurate, transparent, and verifiable disclosure of information, prevent the use of insider information for personal gain, and build confidence among shareholders, investors, and the public.

1. Directors and management shall prepare and submit reports stating the interests on their own interests and those of related persons to the Company Secretary on an annual basis, and whenever there are any changes to such information.
2. Directors, management, and employees are prohibited from trading the Company's securities during trading blackout periods, in which material information has not yet been disclosed to the public.
3. Directors and management are required to report any changes in their securities holdings to the SEC in accordance with applicable laws and regulations.
4. The Company assigned the Company Secretary to monitor, collect, and regularly report relevant information to the Board of Directors to ensure continuous oversight and compliance.

Reports Stating the Interests and Security Holding Guidelines

To ensure the effective implementation of the above policy, the Company has established the following guidelines:

1. The Company requires directors and management to prepare report stating the interests on their personal interests and those of their related persons at least once a year and whenever there are any changes. Such reports must be submitted to the Company Secretary, who will compile and present them to the Chairman of the Board of Directors and the Chairman of the Audit Committee to ensure transparency, accountability, and to minimize potential conflicts of interest.
2. The Company prohibits directors, management, and employees from trading the Company's securities from the end of each financial quarter until the date the Company discloses its financial statements or material information to the public (Trading Blackout Period). If it is necessary to trade during this period, prior approval must be obtained from the responsible compliance unit. Directors and executives must also notify the Company Secretary at least one business day in advance before buying or selling the Company's securities.

3. Directors and management are required to report the purchase, sale, transfer, or receipt of the Company's securities to the Office of the SE) in accordance with Section 59 of the Securities and Exchange Act B.E. 2535 (1992) and its amendments.
4. The purchase of securities under the Employee Joint Investment Program (EJIP) is exempt from the reporting requirements under Section 59. However, any subsequent sale or transfer of securities acquired through the EJIP must still be reported in compliance with Section 59.
5. The Company Secretary is responsible for compiling and reporting information on the interests and securities holdings of directors and executives to the Board of Directors on a quarterly basis to ensure continuous, transparent, and lawful governance.

This Reports Stating the Interests and Security Holding 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.

Confidential Information Protection and Controlling of Inside Information Usage Policy

Definition

Trading Blackout Period means the period specified by the Company during which directors, executives, and employees are prohibited from trading the Company's securities. This period commences from the end of each financial quarter until the date the company discloses its financial statements or other significant information to the public.

Management means the first four levels of management positions below the Managing Director, including all positions equivalent to the fourth level. This also includes positions within the accounting or finance functions at the level of Department Manager or equivalent and above.

Related Person means a spouse, minor child, and any person as defined under Section 258 of the Securities and Exchange Act B.E. 2535 (1992).

Confidential Information Protection and Controlling of Inside Information Usage Policy

SiS Distribution (Thailand) Public Company Limited (the Company) recognizes that its internal and confidential information is a valuable asset that could affect the Company's securities price, investor confidence, and competitive advantage. Accordingly, the Company has established this Confidential Information and Controlling of Insider Information Usage Policy to set forth principles and guidelines for controlling, safeguarding, managing, and using insider information in compliance with applicable laws and good corporate governance practices.

This policy applies to all directors, management, employees, as well as external service providers or consultants who may have access to such information. The general requirements are as follows:

1. Directors, management, employees, authorized persons with access to the Company's information, and related persons are prohibited from using the Company's information, directly or indirectly, for personal benefit or for the benefit of others before such information has been publicly disclosed by the Company.
2. Directors, management, employees, and authorized persons with access to the Company's information must not disclose the Company's information such as financial data, customer information, contracts, business plans, human resources data, marketing strategies, products, operational performance, or any confidential business information—to the public or any third party, unless authorized by Compliance Department.
3. Directors, management, employees, and authorized persons with access to the Company's information are prohibited from giving advice or inducing any third party to buy or sell the Company's securities based on insider information.

Confidential Information Protection and Controlling of Inside Information Usage Guidelines

To ensure the effective implementation of the above policy, the Company has established the following guidelines:

1. Directors, management, and employees are strictly prohibited from using any non-public information regarding the Company's financial status or operating results for the purpose of trading the Company's securities, or for obtaining personal benefit or advantage for others.
2. Directors and management must comply with their reporting obligations concerning the holding of securities. The Company has informed directors and executives of their responsibilities to report on their own, their spouse's, and their minor children's holdings or changes in holdings of the Company's securities, as well as those of related persons as defined under Section 258 of the Securities and Exchange Act B.E. 2535 (1992). Such reports must be submitted to the Office of the Securities and Exchange Commission (SEC) in accordance with Section 59, with penalties stipulated under Section 275 of the same Act.
3. The Company requires directors and management to report all transactions involving the Company's securities to the Company Secretary, who shall record such changes, maintain an updated summary of individual shareholdings, and present this information to the Board of Directors on a quarterly basis. This information shall also be disclosed in the Company's annual report.
4. The Company prohibits directors, management, and employees from trading the Company's securities during the trading blackout period, which begins from the end of each financial quarter until the date on which the Company publicly discloses its financial statements or any significant information. In cases where trading during the blackout period is deemed necessary, prior approval must be obtained from the Compliance Department with a valid justification before any transaction can be executed.
5. To ensure awareness and compliance, the Company provides periodic reminders to all directors, management, and employees regarding the prohibition of trading the Company's securities during the designated blackout period each quarter. This guideline has been reviewed and approved by the Board of Directors.

This Confidential Information Protection and Controlling of Inside Information Usage 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.

Information Disclosure Policy

Information Disclosure Policy

SiS Distribution (Thailand) Public Company Limited (the Company), as a listed company on the Stock Exchange of Thailand (SET), recognizes the importance of transparent, accurate, complete, and timely disclosure of information. The Company is committed to ensuring that shareholders, investors, and all stakeholders have equal access to relevant information. Accordingly, the Company has established the following information disclosure policy:

1. The Company shall disclose all material information related to its operations, financial position, and significant events in compliance with the laws, regulations, and notifications of the Securities and Exchange Commission (SEC) and the SET, as well as any other information that may affect investment decisions in the Company's securities.
2. The Company shall refrain from providing undisclosed internal or privileged information to any external party such as journalists, analysts, or specific investors, to prevent unequal access to information.
3. The Company shall disclose information only through official and authorized channels, as approved by the responsible units, to ensure the accuracy, completeness, and consistency of the disclosed information in accordance with regulatory requirements.

Information Disclosure Guidelines

To ensure the effective implementation of the above policy, the Company has established the following guidelines:

1. In addition to periodic disclosure of important information to provide investors and shareholders with essential data for investment decisions, the Company also has a policy for disclosing information when significant events occur that are necessary for investment decisions in the Company's securities. This is to ensure that all stakeholders shall receive information on an equal basis. The disclosure of information shall be according to the criteria set by the Securities and Exchange Commission, Thailand (SEC) and the SET.
2. The Company has a policy to avoid providing non-public information to the public, journalists, analysts, or others. Therefore, all non-public information that has not been disclosed to the public shall be approved by the Compliance Department prior to dissemination. The Investor Relations or relevant persons are authorized to provide such information. Additionally, for information concerning other the joint ventures, approval from the joint venture investors as per the conditions specified in the agreement is required. This policy shall be under the scope of responsibilities as defined by the SEC.
3. In the case where shareholders or investors inquire about information from the Company, it is the responsibility of the Investor Relations, the Company Secretary, or other designated person appointed by the Compliance Department to respond to these queries. The information provided shall be data that has already been disclosed to the public, within the boundaries set by the SEC and the SET. For non-public information, it is necessary to obtain permission from the Compliance Department prior to disseminating such information.

This Information Disclosure 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.

Protecting and Using the Assets of the Company Policy

Protecting and Using the Assets of the Company Policy

SiS Distribution (Thailand) Public Company Limited (the Company) has established a policy requiring all directors, management, and employees to recognize the importance of the Company's assets, both tangible and intangible. They are responsible for safeguarding, maintaining, and utilizing such assets efficiently for the maximum benefit of the Company, and must not use the Company's assets for personal gain or for the benefit of others.

Protecting and Using the Assets of the Company Guidelines

To ensure the effective implementation of the above policy, the Company has established the following guidelines:

1. Directors, management, and employees are responsible for safeguarding the Company's assets to prevent deterioration, damage, loss, or misuse. They must ensure the efficient and effective use of the Company's assets for the best interests of the Company's business operations.
2. The Company's assets include both tangible and intangible assets, such as:
   - Tangible assets – buildings, premises, equipment, office tools, vehicles, and any other physical property owned by the Company.
   - Intangible assets – technology, information systems, technical know-how, intellectual property rights, patents, copyrights, trademarks, commercial data, and the Company's confidential information, including business plans, financial forecasts, and human resources data.
3. The Company's assets must not be used for personal purposes or for the benefit of external parties without proper authorization.
4. Any improper or unauthorized use of the Company's assets, or actions inconsistent with this policy, must be reported to the supervisor immediately.

This Protecting and Using the Assets of the Company 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.

Human Rights Policy

Human Rights Policy

SiS Distribution (Thailand) Public Company Limited (the Company) emphasized on human rights of all stakeholders and has established the Human Rights Policy. This policy aims to ensure that all directors, management and employees are aware of the significance of respecting and upholding human rights in all aspects for every individual, as well as in society and communities, in compliance with the laws of each country and the treaty each country is committed to. The Company is committed to the following principles:

1. Support and respect for the protection of human rights and avoid actions that violate human rights.
2. Treat others fairly, equally, and indiscriminately.
3. Monitor and oversee to ensure that the Company's business operations do not become involved in human rights violations.
4. Recognize and respect employees' rights to freedom of association and collective bargaining.
5. Ensure all employees are treated in accordance with applicable health and safety regulations, as well as labor and anti-human trafficking laws.
6. Refrain from access to resources that have an impact on the traditional way of life and well-being of the community.
7. Resist human rights violations and the infringement of all stakeholders' privacy throughout the supply chain.
8. Communicate, disseminate, provide knowledge, and understanding, as well as setting guidelines, monitoring, and encouraging stakeholders in the business value chain to engage them in conducting business ethically, respecting human rights, and treating everyone in accordance with human rights principles.

Human Rights Guidelines

1. Respect human rights by treating everyone with dignity and courtesy, honoring each individual, and interacting with all stakeholders equitably. This includes protecting the rights of individuals who may be unable to defend themselves. Discrimination based on physical or mental condition, race, nationality, place of origin, religion, gender, sexual orientation, age, disability, social status, culture, citizenship status when legally entitled to work, HIV status, language, skin color, education, traditions, veteran status, or any other characteristic protected by law is strictly prohibited.
2. Perform duties carefully to prevent the risks of human rights violation in business and committed to preventing all forms of harassment. The Company strictly adheres to the policy and guidelines for non-discrimination, not support forced, debt-bonded and indentured labor, anti-child labor, anti-harassment, and not accept all forms of harassment. All complaints received by the Company shall be considered and kept confidential. If the allegations are confirmed, remedial action, disciplinary measures, dismissal, or legal action will be taken.
3. Provide a safe and healthy workplace for all employees, which includes, but is not limited to, a safety-designed work environment, workplace adjustment for employees with disability or health condition, access to safety and sanitation equipment, and necessary resources. Additionally, offering annual health checkups, medical expenses sharing, and ensuring appropriate working hours and environment.

4. Communicate and disseminate the policy to provide knowledge, understanding, guidelines, and support to the employees, vendors, and partners in the business value chain. This is to ensure participation in business operation with ethics, respecting and treating everyone under human rights, and adhering.
5. Oversee the respect for human rights, do not ignore when finding any actions that potentially violate human rights in connection with the Company. Reports shall be made to the supervisor or responsible person. The reporter shall give cooperation to any inquiry or investigation of facts. In case of any doubt or question, such person shall consult his/ her supervisor or responsible person via the established communication channels.
6. Establish a channel for whistleblowing and complaint, ensuring fairness and safeguarding the individuals who make such reports or complaints. through the following means:
   6.1 The external stakeholders can report directly to the Audit Committee through
   Address: 9 Pakin Building, 9th Floor, Room No. 901, Ratchadaphisek Road,
   Din Daeng, Bangkok 10400
   Tel: 020-020-3000 Ext. 3291
   Email: independentdirector@sisthai.com
   6.2 The internal stakeholders can report to
   - Supervisors, executives, and the Management who are entrusted by the complainant or the whistleblower.
   - Human Resources Manager
   - Quality Assurance Department
   - Company Secretary
   - Lotus Notes Database named: Secret Suggestion Box
   - The Audit Committee as stated in item 6.1
7. Ensure that any instances of harassment, abuse, corporal punishment, or other inhumane treatment within the organization are thoroughly investigated through whistleblowing mechanisms, interviews, surveys, or other appropriate means.
8. To uphold our commitment to human rights, the Company has instituted a comprehensive Human Rights Due Diligence process. This includes regular risk assessments to identify potential human rights risks within our operations, supply chain, and business relationships. The Company also ensures ongoing monitoring of human rights' performance, with transparent reporting on our progress through regular updates and reports.
9. Regularly review human rights policy, taking into consideration significant changes that may affect the organization.

This Human Rights 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.

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.

Information Technology (IT) Security Policy

In today's digital era, information systems play a vital role in both business operations and everyday life. The use of digital technology has become an integral part of organizational processes and service delivery. This is particularly true for SiS Distribution (Thailand) Public Company Limited (the Company), which operates in the technology sector.

Recognizing the importance of safeguarding its information assets, the Company views information security as essential to protecting its data, system resources, and digital assets from cyber threats and unauthorized access.

Accordingly, the Company has established this Information Technology Security Policy, along with corresponding management guidelines, to ensure that all operations are conducted efficiently, transparently, and in full compliance with applicable laws, international standards, and industry best practices in information security management.

1. Definitions in this policy

1.1 The Department means Information Support Department (IS)

1.2 Property means hardware, software, and information technology of the Company.

1.3 Network system means the computer network of the Company under governance of Information Technology Department.

1.4 **Information System** refers to the Company's information systems that are under the supervision and management of the Information Technology Department.

1.5 Employee means staff of the IS Department.

1.6 Network system administrator means staff who are responsible for providing services for computer network system.

1.7 IT developer means staff of the IS Department who are responsible for developing IT for the Department or other departments in the Company.

2. General

2.1 This IT Security Policy has been developed by the IT Security Committee. This policy will be reviewed and updated on an annual basis (if applicable).

2.2 The IT Security Policy shall be documented in writing and approved by the Operations Director. It shall be disclosed to all employees for acknowledge.

3. Responsibilities of the Department Management

3.1 The Operations Director shall be the signatory for approval on the IT Security Policy.

3.2 The Operations Director shall review and update the policy on an annual basis (if applicable).

3.3 The Operations Director shall advocate for ensuring that all employees in the Department are aware of the importance of safeguarding the information assets of the Department.

3.4 The Operations Director shall advocate for all employees in the Department to adhere to the IT Security Policy and relevant laws.

3.5 The Operations Director shall support resources to ensure that computer network system management and services shall be secured and complied with this policy.

4. Security of the Infrastructure of the Department

4.1 The Department shall establish the IT Security Committee to draft guidelines on information security for computer network systems and present it to the Operations Director for endorsement. This Committee has a primary role in drafting IT security requirements and overseeing employees including external parties to comply with this IT Security Policy.

4.2 The Human Resources Department shall arrange a written commitment between employees and the Department that they will not disclose confidential information of the Department and the Company to external parties without written approval from the Operations Director.

4.3 To expedite the resolution of security violations, the supervisor of Computer Network System Services should maintain a list of contact persons for coordinating about information security such as internet service providers, IT security coordination centers etc.

4.4 The supervisor of the computer network system services assesses the risks associated with external access to the computer network system and establishes clear and periodic support or mitigation measures, which may be taken every 6 months.4.5 The computer network system administrator shall notify the policy about computer network system access and procedures to access network system control room to the external parties prior to granting for usage.

5. Management of the Department's properties.

5.1 The Department shall maintain an inventory of the computer network system of the Department with clearly designating responsibility for each asset. Its assets should be categorized based on their level of importance, confidentiality, and value to determine the appropriate management method.

5.2 The computer network system administrator shall manage the assets categorized and stored to prevent damage, unserviceability or loss.

6. Security of departments concerning the Employee.

6.1 The supervisor of the computer network system services and Human Resources Department shall determine duties and responsibilities for IT security in writing for the employees and/ or the external service providers.

6.2 The Human Resources Department and relevant internal departments shall examine in detail the qualifications of the new applicant such as their employment history, education background, and their level of risk in accessing information etc.

6.3 The Human Resources Department and relevant departments shall determine the hiring conditions, including roles and responsibility for IT security. New employees shall agree and sign off to consent their hiring conditions.

6.4 The Department shall encourage awareness among employees and external service providers about the security-related aspects of their own responsible work.

6.5 The employees and external service entering to perform their duties shall adhere to the security policy of the Department.

6.6 The employees who violate or breach the IT Security Policy of the Department will be subject to disciplinary action.

6.7 The resigned or terminated employees shall return the Department's assets within their possession and any access rights to the assets and information shall be cancelled.

7. Security of Physical and Environment.

7.1 The computer network system services, IT system development, and General Affair departments are responsible for creating secure areas and controlling access to authorized persons. Furthermore, the areas for external parties' access shall be identified to prevent unauthorized physical access, damage, interference, or intrusion into the assets and information of the department.

7.2 The Department shall prepare crisis preventive plans, such as fire, flooding, earthquakes, or any other damage caused by human and natural factors to encounter the crisis and recover the system as soon as possible.

7.3 The employees shall place and protect the Department's properties from environmental threats, dangerous and unauthorized access.

7.4 To reduce the risk of system failures in supporting network services, the Department shall maintain and ensure the continuous operability of public infrastructure systems such as the electrical system, air-conditioning system etc. Additionally, contingency systems should be in place in case of events that render the primary public infrastructure systems unusable.

7.5 Equipment of the computer network system used outside the Department, such as power cables, communication cables, and other cables, shall be protected against unauthorized access to mitigate risks to signal lines or the computer network system equipment itself.

7.6 The computer network system administrator shall inspect devices with data storage to ensure the important media and copyrighted software in the devices have been deleted or overwritten prior to discarding such equipment to prevent its re-use.

7.7 The employees are prohibited from taking departmental assets and information outside the Department unless the authorization is obtained. This practice must align with the regulations governing the removal of materials from the building with strict adherence.

8. Computer Network System Management

8.1 The computer network system services section shall establish the operational guidelines for providing computer network services and ensure that these guidelines are documented in writing. These guidelines should also be made accessible to the employees and relevant stakeholders for their awareness and adherence.

8.2 The computer network system administrator shall control the services provided by external service providers to ensure compliance with the security agreement between the Department and external service providers.

8.3 The Department shall plan for IT resources demand to determine the required IT resources in the future to ensure the appropriate and adequately effective of the system.

8.4 Newly upgraded or newly installed IT systems must undergo a thorough examination prior to launch to ensure that there is no impact on the overall computer network system.

8.5 The computer network system administrator shall detect, prevent, and recover the IT assets from the malwares or mobility programs (the program capable of self-transferring from one computer's memory to anther). This includes creating awareness of the dangers posed by these malwares and disclosing safe computer network system usage guidelines to users.

8.6 The computer network system administrator shall regularly back up data and test the recorded data according to data backup procedures.

8.7 The supervisor of the computer network system shall manage the computer network system, manage service level, determine measures to prevent network system threats and look after security system for network and network application including all IT information sent in the network.

8.8 The computer network system services section shall establish a media management process for handling data storage media to prevent unauthorized disclosure, alteration, deletion, or destruction of information assets.8.9 All employees in the Department shall adhere to the regulations regarding document control.

8.10 The Department shall establish procedures and supportive measures for IT and software exchange within the Department or with the other departments.

8.11 Prior to public disclosure, the person responsible for information dissemination shall verify the accuracy of the information to ensure its accuracy and prevent misunderstanding. Furthermore, once the information has been released, there should be mechanisms in place to prevent unauthorized modifications to the information.

8.12 The computer network system administrator shall store computer traffic data in accordance with the Computer-Related Crime Act, as follows:

8.12.1 Internet data from Network Access Systems. (Dial up services)

8.12.2 Internet data from electronic mail (e-mail) servers.

8.12.3 Internet data from File Transfer Protocol (FTP) servers

8.12.4 Internet data from web servers

8.12.5 Type of data in User Network (Usenet)

8.12.6 Computer network system and IT network according to authorized scope.

9. Control of IT Assets Accessibility

9.1 The supervisor of the computer network system services and relevant supervisors shall control and limit access rights to the system as necessary.

9.2 The computer network system administrator is responsible for managing users' accounts and passwords to enable users to access the computer network and IT systems according to their permission.

9.3 The users shall have measures to prevent unauthorized persons from accessing IT assets within their responsibility, especially when there is no staff supervision such as locking computer screen when not in use or locking the door when left the operating room etc.

9.4 Critical IT assets included but not limited to documents or recorded media, shall not be located in unsafe places, such as free physical accessibility or in public places, easy to detect etc.

9.5 Prior to using the computer network system or network devices, every user shall identify themselves each time to determine who is requesting access and what level of privileges they have for system usage.

9.6 The computer network system administrator shall protect the access to ports for system monitoring and configuration, whether it is physical access or access over the network.

9.7 The computer network system administrator shall segregate the network into user groups and network infrastructure groups responsible for providing information services. This includes highly critical information systems. This is being done to facilitate access control and network security management.

9.8 The computer network system administrator shall define the network connectivity pathway to restrict access to IT information in network from users.

9.9 The computer network system administrator shall implement user authentication, password control, and access time limitations for the operating system such as cutting off the system when users do not use for a specific period of time etc.

9.10 The computer network system administrator shall control portable communication devices such as notebooks, PDAs etc. and find ways to reduce the risks associated with these devices when they are introduced into the Company's computer network.

10. Procurement, Development, and Preventive Maintenance of IT systems

10.1 The IT developer who developed or improved the existing system shall determine the security requirements of the new system prior to launch for the users. This is essential to prevent users from disrupting the system or interfering with the overall computer network system.

10.2 The IT developer shall examine the data correctness prior to inputting them into the evaluation process and shall have the inspection system during evaluation to detect its error (if any). This also included the inspection post-evaluate to ensure IT information correctness prior to release for usage.

10.3 The IT developer shall control the installation of software into the service-providing system to reduce risk of service disruption, abnormal behavior, or system unavailability. For instance, when installing hardware or developing any system that could affect the overall system, it is crucial to isolate it from the production environment beforehand or conduct testing in the demonstration system prior to deploying it to the real system.

10.4 The IT developer shall avoid using actual data in the system for system tests. In case of necessary, it shall be carefully controlled, such as removing personal data or confidential information prior to use etc.

10.5 The supervisor of the IT system development shall have a system in place to restrict access to the source code for the system being provided to prevent unauthorized or unintentional changes.

10.6 The computer network administrator shall have procedures in place to control or modify the IT system. A technical review of the system is also needed to ensure that the system continues to function properly after any changes or modifications have been made.

10.7 Avoid the modification of software from manufacturers unless it is necessary. In case of necessary, the modification shall be strictly controlled.

10.8 The supervisor of IT system development shall protect against IT data leakage or minimize the possibility of IT data being disclosed to unauthorized parties to prevent others from using the information without permission.

10.9 The computer network administrator shall plan for system risk assessment, conduct testing, and establish measures to mitigate system vulnerabilities.

11. IT System Risk Management

11.1 The computer network administrator shall prepare a risk assessment report with recommendations for risk mitigation for the Management considerations every 6 months. The risk factors shall at least cover the following issues:

- 11.1.1 Improper use of IT system violates the policies, announcement, and regulations.
- 11.1.2 Threats from computer viruses, computer warms and malware.
- 11.1.3 Threats from malicious attacks on the system by unauthorized individuals, which may affect IT information and communications.
- 11.1.4 Limitations in the provision of IT system services which may result in unavailability or inability to use the service.
- 11.1.5 Physical or natural disaster.
- 11.1.6 Other aspects may occur.

11.2 The computer network system administrator shall establish operational procedures for encountering the event relating to security of the Department's computer network system including identify roles and responsible person clearly.

11.3 The computer network system administrator shall record the security violation event considering on type, quantity and expense from such damage for learning and prevent its reoccurrence.

11.4 The computer network system administrator shall collect and maintain evidence for reference in case the events are related to legal actions.

12. The Departments' Operations Continuity Management

12.1 The Department shall establish requirements for computer network system management to ensure continuous services and emergency respond plan to recover the system in case of damage.

12.2 The supervisor of the computer network system shall test and update the emergency respond plan regularly to ensure that it is always up to date and can be used in case of real emergencies.

13. Compliance with the IT Security Policy

13.1 The Department shall determine laws and policy for computer network systems usage in writing clearly and update on an annual basis.

13.2 The Department shall ensure that all network users adhere to the IT Security Policy, computer network system accessibility policy and refrain from violating any laws related to the Computer-Related Crime Act.

13.3 The Department shall have a plan assessing the Department's IT security system. This assessment shall be performed by responsible person in the Department or external party. The tools or software used for assessment shall be controlled to prevent unauthorized or malicious use of these assessment tools.

14. Service Agreement for Computer Network Systems and Information Systems

14.1 Provision of personal user accounts and passwords for accessing SiS computer network and information systems

- 14.1.1 When the user is a new employee, they shall go through the step for account request, acknowledge for using policy, and accepting the Non-Disclosure Agreement of the Company.

14.1.2 The users must change their passwords immediately after receiving them from the system administrator, in accordance with the requirements specified in Clause 15.14.1.3 The Company has measures to prevent repeated incorrect password attempts in order to protect against unauthorized system access and ensure the security of user accounts. Details are as follows:

14.1.3.1 For SAP System

- If a user enters an incorrect password three (3) times, the system will automatically close the active session window.
- If a user enters an incorrect password six (6) consecutive times, the system will lock the SAP user account.
- If an SAP user account is locked, the user may unlock it through the "Unlock User DB" in Lotus Notes. For employees who do not have a Lotus Notes user account, their supervisor shall perform the unlock procedure on their behalf.
- If the user has already performed an unlock once in a day but is still unable to access the system, the user must contact the IS Department to unlock the account and request a new password.

14.1.4 The users are required to change their passwords for SAP system at least once every 90 days by creating a new password in accordance with the requirements specified in Clause15.

14.1.5 The users are responsible for storing and maintaining their own password confidentially. They cannot deny responsibility in case the other persons get unauthorized access to this confidential information and misuse it unless an investigation by the Company's representative or law enforcement can prove that it is not the user's fault.

14.1. 6 The system will automatically log out after 3,900 seconds (65 minutes) of inactivity, and it will immediately close the workspace.

14.2 Connection for SiS network system via LAN line.

14.2.1 The proxy setting as specified by the Company requirement is needed for the connection for SiS network system via LAN line.

14.2.2 The users shall have the Company's account to authenticate themselves prior to access to SiS network system.

14.3 Connection for SiS network system via wireless.

14.3.1 The users shall possess the Company's account prior to gaining access to this wireless network system.

14.3.2 The Company's wireless network is named "SIS" which required user authentication prior to access.

14.3.3 The users of the wireless network shall strictly adhere to the Company's computer network system usage policies.

14.4 Data retrieval services via internet and intranet networks.

14.4.1 The users accessing data through the internet and intranet networks shall authenticate each time they access the system.

14.4.2 The users shall carefully use and avoid accessing information from unsecured sources.

14.4.3 The users shall follow the instructions from the safety computer network system using guidance.

14.4.4 The users shall strictly adhere to the computer network usage policies.

14.4.5 The users shall not violate the Computer-Related Crime Act.

14.5 Data retrieval services via online database.

14.5.1 The user shall connect to the internet prior to retrieving data in the Company's online database.

14.5.2 In the event that the Company's internet service provider is unable to provide services, this has an impact on the ability to access the online database.

14.6 E-mail communication services for the employees.

14.6.1 The Company provides and facilitates the use of e-mail through Microsoft 365 to support its operations.

14.6.2 The users shall adhere to the regulations and shall not use them in a way that causes harm to others or the Company. The users are responsible for all usage unless they can prove that they are not the actor.

14.6.3 The users are prohibited from sharing or distributing their e-mail account with others or providing access to their e-mail account to the others.

14.6.4 Once the users have successfully set up their accounts, their mailbox will have a minimum size of 50 GB, and the size of each e-mail together with its attachment sent shall not exceed 35 MB.

14.6.5 The Department may access or disclose communication information of the users to comply with the laws, respond to legal requests or legal processes, or protect the rights and property of the Company or the other users.

14.6.6 The Department may temporarily suspend services to enhance security systems or halt disruptions to the service.

14.6.7 The Company does not guarantee the security or preservation of data stored in the system.

14.6.8 The IS Department reserves the right to modify or alter any aspect of the services at any time and may terminate or suspend a user's service without prior notice if they are found to be in violation of the Company's email usage agreement.

14.6.9 The agreement for e-mail usage is in electronic format so the service provider reserves the right to send information about additional services to the users via e-mail or the Company's website.

14.7 Download services for copyright software, free software or open-source software which are available in SiS network system.

14.7.1 This service has been established to provide convenience to the community. The Company uses copyrighted software in compliance with the law. The government has established measures to prevent software copyright infringement, and the Company collaborates with various government agencies to procure legally compliant software for continued usage.

14.7.2 The use of copyrighted software can be installed for the Company-owned computer only.

14.7.3 In case the users take and use copyrighted software on personal computers, the Company will not be responsible for any consequences arising from such actions.

14.7.4 These software offerings can be downloaded exclusively through the SiS network system, and there is no duplicate services or copy on the other media for distribution.

14.8 Computer network server hosting services for departments in the Company.

14.8.1 The department who own the network server hosting equipment shall accept and strictly adhere to the security policies.

14.8.2 The network server hosting equipment that is brought in for hosting must undergo an examination by the network system administrator to ensure that it will not disturb the operation of other systems and will not pose a security risk. If a risk is identified during the assessment, it will not be allowed to be hosted in the networking control room until the issue has been resolved by the department responsible for the network server equipment.

14.18.3 In case the network server hosting equipment causes disruption to other systems, resulting in abnormal operation or the inability to provide services, the network system administrator reserves the right to disconnect such network server equipment from the network immediately, without prior notice, to maintain security measures.

14.9 Request for other special services which require the Company's Port Firewall opening for the Company's employees.

14.9.1 The requester shall accept and strictly adhere to the security policies.

14.9.2 The purpose of usage shall not violate the Company's policies, announcements and it shall be in compliance with the laws.

14.9.3 The requester shall request in writing to the Operations Director for each request. The following technical details shall be identified:
14.9.3.1 Number of port which required for opening.
14.9.3.2 Number of destination IP address.
14.9.3.3 Purpose or name of application which shall use such port.
14.9.3.4 Start and end date of services.

14.9.4 The Department will not approve u if considering found that the request violates the Company's policies, announcements, requirements or the laws, or if it may introduce security vulnerabilities to the information system.

14.9.5 The Department has the right to immediately terminate the services if found after approval that there is violation of the Company's policies, announcements, requirements, or if it may introduce security vulnerabilities to the information system or cause damage to the Company's information system.

15. User Account and Password Control Policy for Information System Access

15.1 For accessing the SAP system, an Identification and Authentication mechanism must be in place to verify user identity and access rights before entering the information system, including access to critical and personal data. The control must be sufficiently stringent — for example, by requiring complex passwords that are difficult to guess. Each user must be assigned an individual user account. The overall adequacy of password complexity and control measures should be assessed based on the following factors.

- Passwords should have a minimum length of eight (8) characters.
- Passwords should contain at least three (3) of the following four (4) elements: special characters, numbers, uppercase letters, and lowercase letters.
- Users should change their passwords at least once every 90 days.
- The system shall lock or temporarily disable a user account after six (6) consecutive incorrect password attempts.
- For systems that allow user access via the Internet, multi-factor authentication (MFA) should be implemented to enhance security.
- The IS Development team is responsible for conducting an annual review of user access rights to the SAP system.
- Modification or deletion of User IDs shall follow these rules:
  - In the event of resignation or termination of employment, the User ID must be disabled or deleted within three (3) days after the effective date of the announcement.
  - In the event of a department transfer where the new department has no requirement to access the system, the User ID must be deleted within three (3) days after the effective date of the announcement.

15.2 If any information system cannot technically enforce the password policy as specified above due to technological limitations, access to such a system shall be restricted exclusively to the internal network (Intranet).

15.3 All users are responsible for safeguarding their own user accounts and passwords. Disclosure, sharing, or allowing others to use one's account or password is strictly prohibited, in order to prevent unauthorized access to the information systems and mitigate the risk of personal data breaches.

Guidelines for IT Security

1. All management and employees are required to be aware of and strictly adhere to the Company's IT Security Policy.
2. All Management and employees shall strictly adhere to the Company's computer service agreement
3. In case that IT utilization is found to violate the Company's policies, announcements, or regulations, or the law, or if it poses a security risk to the information system or causes damage to the Company's IT system, the Department shall have the right to terminate such services immediately.

This Information Technology (IT) Security 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.

Wareeporn Sittichaisrichart
Operations Director
SiS Distribution (Thailand) Public Company Limited

Facilitation Payment Policy

Definition

Facilitation Payment means the payment of allowance to government officials unofficially to ensure that they carry out or expedite the process promptly. This process should not rely on the discretion of government officials and should be an action within their official duties. It should be a right that legal entities already possess, such as requesting licenses, letters of certification, and receiving public services etc.

Facilitation Payment Policy

SiS Distribution (Thailand) Company Limited ("the Company") is committed to conducting our business with the highest standards of integrity, transparency, and ethical behavior. This Facilitation Payment Policy outlines the Company's stance on facilitation payments, as well as the legal obligations and best practices required under the Thai Private Sector Collective Action Against Corruption (CAC), the U.S. Foreign Corrupt Practices Act (FCPA) and the UK Bribery Act 2010.

The Company has a strict policy of not paying any form of facilitation payment, whether directly or indirectly. The Company will not engage in any activities or accept any actions in exchange for business convenience.

Facilitation Payment Guidelines

To ensure the effective implementation of the above policy, the Company has established the following guidelines:

1. Directors, management, and employees of the Company and its subsidiaries are strictly prohibited from making or authorizing any facilitation payment under any circumstances, whether directly or indirectly through third parties.
2. If an employee encounters a situation in which a facilitation payment is requested, the employee must politely refuse and immediately report the incident to their supervisor or the Compliance Department.
3. The Company shall provide regular communication and training to employees regarding the proper procedures for refusing facilitation payments, to ensure understanding and effective compliance.
4. Any violation of this policy and its guidelines shall result in disciplinary action in accordance with the Company's internal regulations. If the act constitutes a breach of law, the offender shall also be subject to legal action under applicable laws.

This Facilitation Payment 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.

Revolving Door Policy

Definition

Government employees mean individuals holding political positions, civil servants or local government employees with permanent positions or regular salaries, employees or personnel working in state enterprises or government agencies, local administrators, and members of local councils who are not in political positions. It also includes officials as defined under laws governing local administration and extends to include directors, subcommittee members, employees of government agencies, state enterprises, or government entities, as well as individuals or groups authorized or delegated to exercise administrative authority on behalf of the state in performing certain actions under the law, whether established within the bureaucracy, state enterprises, or other state-related operations.

Hiring of government employee means the engagement of individuals who are or were formerly state employees to work within the company. This may involve the use of insider information or relationships to benefit the company, potentially leading to conflicts of interest between the company and government organizations. Such actions are aimed at gaining unfair business advantages or influencing policy decisions to favor private entities associated with the former state employee.

Revolving Door Policy

SIS Distribution (Thailand) Company Limited ("the Company") recognizes the importance of conducting business with transparency and integrity, particularly in preventing any actions that may lead to fraud, corruption, or conflicts of interest. Accordingly, the Company has established this Revolving Door Policy to regulate the employment of individuals from government agencies, or those who have previously held positions in agencies directly or indirectly responsible for supervising the Company. This policy aims to ensure that all employment practices are appropriate, transparent, and not used as a means to grant undue benefits or exert improper influence on the Company's business operations.

Guidelines on the Employment of Government Official

To ensure the effective implementation of the above policy, the Company has established the following guidelines:

1. The Company shall not hire or appoint any individual who is currently serving in a government agency to any position within the Company. This is to prevent conflicts of interest and to avoid any undue influence arising from the person's official duties in the public sector.
2. Individuals who previously held positions in government agencies or in regulatory bodies that directly supervise or are related to the Company may be hired or appointed only after a minimum cooling-off period of two (2) years from the date they left such public office.
3. The Company shall disclose the names and professional backgrounds of directors, executives, or advisors who formerly held positions in government organizations directly related to the Company. The reasons for their appointments shall also be clearly stated in the Company's Annual Report to promote transparency to all stakeholders.
4. The Company shall conduct thorough background checks on all individuals proposed for appointments as directors, executives, or advisors to ensure that there are no potential conflicts of interest or connections with government agencies that could compromise the independence of the Company's operations.

This Revolving Door 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.

Trade Compliance Policy

Definition

Contracted agent means any individual, entity, or organization that has entered into a binding agreement with the company to provide services or perform any obligations as stipulated in the contract on behalf of the Company.

Trade Compliance Policy

SiS Distribution (Thailand) Public Company Limited ("the Company") is committed to transparency and upholding good corporate governance in business operations. To further support this commitment, the Company has established this Trade Compliance Policy as a guideline to ensure full compliance with applicable trade and export control laws, and regulations.

This policy applies to all directors, management, employees, and contracted agents of the Company, and governs interactions with customers, vendors, and other business partners to maintain integrity and compliance across all business activities. All employees are required to familiarize themselves with and strictly adhere to this Trade Compliance Policy. It is imperative that everyone understands the legal obligations related to the export of products, services, technology, and information, as well as the potential consequences of non-compliance.

1. Laws and Ethics Compliance

The Company is dedicated to upholding all applicable laws, regulations, and ethical standards. To ensure compliance, the Company commits to the following:

1.1 Licenses and Authorizations: The Company will secure all required licenses or governmental authorizations prior to the use, transfer, import, export, or sale of any products, software, technology, or services. License requirements will be evaluated based on factors such as the nature of the product, its destination, the end user, and the intended end use. Compliance with these licensing obligations is essential to ensure lawful and secure business operations.

1.2 Anti-Bribery and Corruption Compliance: The Company will adhere to all requirements relevant anti-bribery, anti-kickback, and anti-corruption laws, including the U.S. Foreign Corrupt Practices Act, the UK Bribery Act, and local regulations in all jurisdictions where it operates.

1.3 Assistance to Business Partners: The Company agrees to provide reasonable assistance to business partners to ensure compliance with the applicable Codes of Conduct and laws, and to support inquiries into suspected legal violations.

1.4 Notification of Legal Actions: If required and relevant to business partners, the Company will notify them of any investigation, inquiry, or enforcement action initiated by a governmental, administrative, or regulatory body concerning offenses or alleged offenses such as fraud, bribery, corruption, trade violations, anti-trust issues, or any other business misconduct or legal violations.

1.5 Prohibited Relationships: The Company will not engage with any individual or entity involved in, or suspected of, bribery, kickbacks, fraud, or other improper activities.

1.6 Proper Use of Funds: The Company will ensure that funds provided by business partners are utilized in compliance with the terms and conditions set by the business partner.

1.7 Accurate Record Retention: The Company will prepare, maintain and provide, upon request, proper, accurate, and complete financial and business records to business partners, ensuring transparency and avoiding improper or false accounting practices such as fund parking or the creation of slush funds.

1.8 Competition Law Compliance: The Company's employees and contracted agents will not engage in activities that unlawfully restrict competition, including but not limited to:

- **Price Manipulation**: Refraining from unlawfully fixing, adjusting, or controlling prices in coordination with competitors or third parties.
- **Bid Rigging**: Avoiding bid structuring or orchestration to direct business to a specific competitor, and not engaging in bid rotation or collusive bidding practices.
- **Boycotts**: Not participating in or supporting any restrictive trade practices or boycotts prohibited under applicable laws.
- **Market Allocation**: Not dividing or allocating markets, customers, or territories among suppliers or competitors.
- **Restrain competition**: Avoiding activities that unfairly restrain competition, such as limiting the production or sale of certain products or product lines.
- **Exclusive Dealing**: Not forcing customers to purchase only specific vendors' products.

1.9 Responsible to Customers: The Company emphasizes the importance of customers, so the Company has the following directions:

- **Customer Equivalent Treatment:** Treating every customer equally and fairly, without any form of discrimination.
- **Safe and Beneficial Products:** Ensuring that all sourced products are safe for use and effectively meet customers' operational needs.
- **Innovative Products and Services:** Sourcing and providing innovative products and services to meet the evolving demands of our customers.
- **Transparent and Accurate Information:** Providing transparent, accurate, complete, and sufficient information about our products and services via multiple accessible channels, such as websites, product labels, and user manuals.
- **Review of Publicized Content:** Maintaining a thorough review process for all publicized content on websites and/or leaflets before release to ensure accuracy and compliance.

2. Trade Secrets and Intellectual Property

The Company considers trade secrets and intellectual property to be of importance in its business operations. Therefore, employees and contracted agents of the Company are required to adhere to the following guidelines:

2.1 Proper Use of Information: It is strictly prohibited to acquire or use the trade secrets or intellectual property of third parties illegally.

2.2 Protection of Business Partners' Information: Confidential information or trade secrets of business partners must not be disclosed without authorization. This includes prohibiting the transfer, dissemination, use, or disclosure of such information, except as necessary for regular business operations or with written consent from the business partner.

2.3 Protection of Copyright and Intellectual Property Infringement: It is strictly prohibited to purchase products that infringe on copyrights or intellectual property, as well as engaging in transactions with or supporting business partners involved in the trade of such infringing products.

3. Conflict of Interest Managing

To ensure transparency and uphold good governance in business operations, the Company does not only manage its own conflicts of interest under the Conflict of Interest Management Policy but also prioritizes the management of conflicts of interest involving business partners. Therefore, employees and contracted agents of the Company are required to report any conflicts of interest related to business partners or their employees through the channels specified by the business partners.

4. Customer Due Diligence

A robust customer due diligence is essential to ensure compliance with legal requirements, mitigate risks, and maintain a good business reputation. The following process shall be applied to ensure the effective customer due diligence process.

4.1 Information Gathering: Gather basic information, including the company name, address, contact details, and business registration documents. Physical address and contact information verification may be needed in some cases.

4.2 Business Purpose Verification: Verify the customer's business purpose to understand the intended use of purchased products and ensure that the product shall not be misused to violate the basic human rights of others. This helps identify potential risks, especially if the customer operates in sensitive regions or industries.

4.3 Business Reputation Verification: Perform thorough due diligence on the customer's business reputation by utilizing online searches and consulting industry references. This process ensures that customers adhere to applicable regulations and refrain from engaging in corrupt or unethical business practices.

4.4 Creditworthiness Risk Assessment: Assess the financial stability of the customer by reviewing credit reports, financial statements, and payment histories.

4.5 Ownership and Beneficiaries Verification: Verify the identity of the ultimate beneficial owners to ensure they are not associated with any prohibited entities or individuals.

4.6 Screening Against Watchlists: In case of required by business partner for applicable products, check to ensure that the customer is not on a restricted party list which includes, but not limited to,

- Sanctions Lists and Sanctions List Service (SLS) indicated by the Office of Foreign Assets Control (OFAC).
- Consolidated Screening List (CSL) indicated by the International Trade Administration.
- EU Sanction Map.
- UK Sanction List.

4.7 Spotting Against Red Flag: In case of required by business partner for applicable products, check to ensure the products will not be destined for a restricted end-use, end-user, or to a restricted destination considering 4 indicators:

- **Place -** Companies headquartered in a prohibited country as required by partner, delivery dates are vague, shipping routes are circuitous, or a freight forwarder is listed as the product's final destination. When engaging in business in countries ranked lower on the Corruption Perceptions Index (CPI), additional due diligence measures may be necessary. This includes enhanced scrutiny of third-party relationships, greater monitoring of financial transactions, and ensuring compliance with anti-corruption laws.
- **Purpose** - Customer is reluctant to offer information about the end-use of the item, the product's capabilities do not fit the buyer's line of business, the customer is unfamiliar with the product's performance characteristics but still requires the product.
- **Product** - The item ordered is incompatible with the technical level of the country to which it is being shipped, such as semiconductor manufacturing equipment being shipped to a country that has no electronics industry.
- **People –** Any association with individuals or entities on a government denied party list, from a prohibited country, or associated with a bank in a prohibited country is restricted. This includes individuals attempting to use a government bank from a prohibited country, customers preferring to pay cash for high-value items, customers requesting omissions or changes to invoice details, or those seeking anonymity or refusing to provide identity verification documents. Prohibited parties also include, but are not limited to, end users involved in nuclear technology, missile technology (including space exploration and UAV/drone activities), chemical or biological weapons, maritime nuclear propulsion, military end uses, weapons of mass destruction, or specific activities related to oil and gas exploration and production (Russian transaction related).

4.8 Ongoing Monitoring: Upon satisfaction of customer due diligence, customer name will be updated and retained in the Company's database. Continuously monitor the transactions for unusual patterns that may indicate illicit activity.

5. Contracted Agent Due Diligence

Prior to engaging in any contracted agent, the Company will assess the necessity of such an engagement. This includes evaluating whether the Company possesses the internal resources and expertise required to achieve the intended objectives without external assistance. Contracted agent services will be utilized only when deemed essential to the success and effectiveness of the operations. In cases where it is necessary to engage contracted agents, the following process will be implemented to ensure efficient operations.

5.1 Initial Risk Assessment: Consider the nature of the work, the reputation of the potential contracted agent, and any potential compliance or legal risks associated with the engagement.

5.2 Selection Criteria and Evaluation: Selected the contracted agent based on strict criteria, including their industry reputation, compliance with legal and ethical standards, financial stability, and the quality of their services. The evaluation process will involve a thorough review of references, past performance, and certifications as applicable.

5.3 Due Diligence Review: Verify the contracted agent's compliance with applicable laws, regulations, and company policies. This review may include background checks, financial audits, and the evaluation of any potential conflicts of interest. When contracted agents operate in countries with lower rankings on the CPI, additional due diligence measures may be necessary.

5.4 Contractual Agreements: Once a contracted agent has passed the due diligence review, the Company will enter into a formal agreement that clearly defines the scope of work, performance expectations, compliance requirements, and confidentiality obligations. The contract will also include clauses that allow for monitoring and audits.

5.5 Compliance Program and Codes of Conduct Training: The contracted agents will be required to participate in the Company's compliance program, which includes acknowledging on the Company's Codes of Conduct for Business Partners.

5.6 Ongoing Monitoring and Audits: Throughout the engagement, the Company will monitor the contracted agent's performance and adherence to the agreed-upon terms. Regular audits may be conducted to ensure continued compliance and to identify and prevent any emerging risks.

5.7 Termination of Engagement: If at any point the contracted agent fails to meet the Company's mutually agreed standards, the Company reserves the right to terminate the engagement. This decision will be based on an evaluation of ongoing risks, performance, and the continued need for the contracted agent's services.

6. Person In Charge of Trade Compliance Policy

For any questions or guidance regarding this Trade Compliance Policy, all stakeholders are encouraged to contact the following person:

Compliance Department
Address: 9 Pakin Building, 9th Floor, Room No. 901, Ratchadaphisek Road,
Din Daeng, Bangkok 10400
Tel: 020-020-3000 Ext.3060
Email: Compliance@sisthai.com

This Trade Compliance 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.

Occupational Health, Safety, and Environment Policy

Occupational Health, Safety, and Environment Policy

SiS Distribution (Thailand) Public Company Limited (the Company) recognizes that human resources are the foundation of sustainable organizational growth. Therefore, the Company places great importance on occupational health, safety, and the working environment to ensure a safe workplace, prevent accidents and occupational illnesses, and minimize environmental impacts arising from the Company's activities.

The Company is committed to continuously developing, improving, and implementing an occupational health, safety, and environmental management system that complies with all applicable laws, regulations, and relevant standards to ensure the highest level of safety for employees, business partners, communities, and the environment.

Occupational Health, Safety, and Environment Guidelines

To ensure the effective implementation of the above policy, the Company has established the following guidelines:

1. Develop and continuously improve occupational health, safety, and environmental management systems in compliance with labor laws, health and safety regulations, and relevant international standards.
2. Provide adequate resources to support the implementation of the management system, including personal protective equipment, first-aid kits, fire prevention systems, and regular fire evacuation and firefighting training to ensure readiness and workplace safety.
3. Conduct appropriate risk assessments for all work processes to identify hazards, evaluate risk levels, and establish preventive and control measures to reduce or eliminate workplace risks.
4. Promote awareness among management and employees on the importance of occupational health, safety, and environmental practices through regular training, including specialized courses for employees performing high-risk tasks such as forklift operations in warehouses.
5. Provide annual health check-ups and appropriate medical benefits to promote employee well-being and quality of life.
6. Record and analyze accident and incident data to identify causes, develop preventive and corrective measures, and reduce risks to prevent recurrence.
7. Ensure management drives, supports, and monitors the implementation of this policy, while all employees comply with occupational health, safety, and environmental measures and maintain standards consistent with applicable laws, regulations, and international practices.

This Occupational Health, Safety, and Workplace Environment 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.

Environmental Policy

SiS Distribution (Thailand) Public Company Limited (the Company) recognizes the importance of environmental protection, natural resource conservation, and minimizing the environmental impact of its business operations. The Company is committed to conducting its business responsibly and in compliance with all applicable environmental laws, regulations, and requirements, with the belief that environmental stewardship is a fundamental foundation of sustainable success.

Accordingly, the Company has established this Environmental Policy to serve as a framework for sustainable environmental management in alignment with the principles of Environmental, Social, and Governance (ESG) as follows:

1. Environmentally Responsible Business Operations

The Company is committed to managing its business responsibly by considering environmental impacts across every stage of its value chain. All business units are encouraged to implement measures and best practices that minimize adverse environmental effects and continuously improve performance in this area.

2. Efficient Use of Energy and Natural Resources

The Company emphasizes the efficient use of energy, water, and natural resources by minimizing waste and promoting the adoption of renewable energy. These efforts aim to enhance operational efficiency while reducing greenhouse gas emissions.

3. Waste and Pollution Management

The Company recognizes that the growing volume of waste contributes to greenhouse gas emissions. Therefore, the Company implements systematic waste management practices starting from waste separation to enable recycling and reuse, and to select qualified service providers for special waste disposal in accordance with environmental standards to minimize pollution arising from business operations.

4. Environmentally Friendly Procurement and Products

The Company is dedicated to offering safe and environmentally friendly products and services, including IT equipment, cloud solutions, and renewable energy technologies that meet environmental standards and support a sustainable future. The Company's specialized team actively studies emerging technologies and engineering practices to ensure that all distributed products meet safety, quality, and eco-friendly criteria.

5. Green Logistics

The Company is committed to reducing air pollution and improving quality of life by adopting modern technologies to optimize transportation routes, minimize fuel consumption, and lower pollution emissions.

6. Employee Awareness and Participation

The Company encourages all employees to develop awareness, understanding, and a sense of responsibility for environmental conservation through continuous training, internal communications, and participation in environmental initiatives.

7. Legal Compliance and Continuous Improvement

The Company strictly adheres to all applicable environmental laws, regulations, and standards. Furthermore, it regularly reviews and updates this policy to ensure ongoing compliance, relevance, and alignment with best practices and international benchmarks.

8. Greenhouse Gas Emission Reduction

The Company is committed to reducing greenhouse gas emissions through comprehensive management identifying emission sources, utilizing modern technologies to enhance energy efficiency, and adopting renewable energy sources. Beyond its own operations, the Company strives to extend these practices to its value chain by continuously sourcing and promoting environmentally friendly products.

This Environmental 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.

Social Policy

SiS Distribution (Thailand) Public Company Limited ("the Company") is committed to conducting its business responsibly toward society, with respect for human rights and adherence to the principles of equality, transparency, and fairness. This commitment extends to all stakeholder groups, including shareholders, employees, customers, business partners, communities, and the broader society.

The Company operates under the principles of Environmental, Social, and Governance (ESG), as well as in alignment with the guidelines of the Stock Exchange of Thailand (SET) and the Securities and Exchange Commission (SEC). The Company also upholds international human rights standards as a framework for policy formulation, operations, and continuous review.

Accordingly, the Company has established this Social Policy as a guideline for conducting business responsibly and sustainably.

1. Environmentally Responsible Business Operations

- Respect human rights by avoiding all forms of human rights violations and discrimination based on gender, age, race, religion, political opinion, disability, or any other status.
- Ensure fair employment through equitable compensation and benefits in compliance with labor laws and competitiveness within the industry.
- Prohibit the use of child labor, forced labor, and all forms of human trafficking.
- Promote equal opportunity and inclusion by supporting underprivileged individuals, the elderly, and persons with disabilities under the principle of non-discrimination.
- Maintain occupational health and safety by providing a safe and suitable working environment with preventive and responsive measures for health and safety risks.
- Support continuous learning, training, and career development to enhance skills and promote professional growth.

2. Responsibility to Consumers and Customers

- Ensure product and service quality and safety by selecting and delivering high-quality, safe, and environmentally friendly products and services.
- Provide transparent and sufficient information through accurate, complete, and non-misleading communication, with accessible channels for feedback and complaints.
- Protect personal data by strictly complying with personal data protection laws and information security standards.

3. Sustainable Partnership and Supply Chain Collaboration

- Conduct business ethically and fairly with transparency, integrity, and respect for intellectual property rights.
- Uphold labor and human rights standards by encouraging and expecting business partners to follow fair labor practices and respect human rights.
- Establish a Codes of Conduct for Business Partners as a guideline for responsible and sustainable business collaboration.

4. Community Development and Social Investment

- Support community development initiatives that align with the Company's strategic direction and local needs, such as education, healthcare, local employment, and environmental protection.
- Avoid the use of resources that may negatively affect the existing livelihoods of local communities.
- Encourage employee and partner participation in social responsibility activities based on transparency and accountability.

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

5. Human Rights Review and Grievance Mechanisms

- Conduct human rights due diligence covering the identification, assessment, prevention, mitigation, and monitoring of human rights risks related to the Company's operations and supply chain.
- Provide appropriate remediation measures when violations occur and communicate the outcomes to relevant stakeholders.
- Establish confidential, accessible, and secure grievance channels that ensure non-discrimination and protection for complainants.

6. Stakeholder Engagement and Communication

- Communicate policies and performance to shareholders, employees, customers, business partners, investors, government agencies, and communities regularly through appropriate channels, and gather feedback for continuous improvement.

7. Governance, Monitoring, and Evaluation

- Operate with transparency, honesty, and fairness in accordance with business ethics and a strict Anti-Bribery and Corruption Policy.
- Establish appropriate key performance indicators (KPIs) to ensure effective governance, monitoring, and evaluation.
- Disclose company reports and information through appropriate corporate communication channels in a transparent and timely manner.

This Social 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.

Section 3
Consulting and Reporting

The Company provides an opportunity for stakeholders to report any misconduct or complaints regarding violations of the Codes of Conduct and related policies. Stakeholders can report these issues to the Audit Committee through designated channels for investigation and resolution. The details are as follows:

1. The Quality Assurance Department, under the oversight of the Audit Committee, is responsible for managing and conducting investigations when disclosures or complaints related to non-compliance with the Codes of Conduct and related policies are received. The Audit Committee shall arrange the investigation when there is evidence to support the claims.
2. For external stakeholders, the Company provides a channel for receiving complaints regarding non-compliance with the Codes of Conduct and related policies. This channel is also dedicated to providing consultation and guidance about the Codes of Conduct and related policies, as follows:

   The Audit Committee
   Address: 9 Pakin Building, 9th Floor, Room No. 901, Ratchadaphisek Road,
   Din Daeng, Bangkok 10400
   Tel: 020-020-3000 Ext. 3291
   Email: independentdirector@sisthai.com
3. For internal stakeholders, the Company provides a channel for receiving complaints about non-compliance with the Codes of Conduct and related policies. These channels are also dedicated to providing consultation and guidance about Codes of Conduct and related policies, as follows:
   3.1 Supervisors, executives, and Management who are entrusted by the complainant or the whistleblower.
   3.2 Human Resources Manager
   3.3 Quality Assurance Department
   3.4 Company Secretary
   3.5 Lotus Notes Database named: Secret Suggestion Box
   3.6 The Audit Committees as per communication channel stated in item 2.

Report Managing Procedure

The Company designates the Audit Committee as the party responsible for handling complaints. The Audit Committee may appoint a special task force to review and address complaints and whistleblowing cases as appropriate, taking into account independence and suitability.

The process for handling complaints and whistleblowing related to the Codes of Conduct and related policies is as follows:

1. The recipient of the complaint will forward the information to Quality Assurance Department for initial review before reporting it to the Audit Committee.
2. If the initial review finds that the complaint or whistleblowing has merit, the Audit Committee will appoint a special task force to collect facts and conduct a thorough investigation.
3. The special task force will present the findings to the Audit Committee within 30-60 days, depending on the complexity of the case.
4. The Audit Committee will make a decision on the complaint and prepare a course of action, including any disciplinary measures, in line with the defined penalty guidelines.
5. The Audit Committee will assess the damage caused by the incident and prepare a plan to mitigate the impact on the affected parties. This will include implementing the necessary measures to protect the whistleblower, and reporting the plan to the Board of Directors for approval.
6. If the whistleblower or complainant has disclosed their identity, the special task force will inform the whistleblower or complainant of the results within 7 business days from the conclusion of the investigation.

Complainants and Whistleblower Protection Measures

1. The Company will not disclose the names and information of the whistleblowers or complainants.
2. The Company will treat information related to clues and complaints as confidential, only disclosing it as necessary for processing and assessing the clues and complaints, with a primary focus on the safety and protection of the whistleblowers, complainants, and affected parties.
3. In cases where the Audit Committee assesses the situation and finds that there is an impact on the whistleblowers or complainants, the committee will take fair and appropriate measures to protect the whistleblowers or complainants, tailored to specific circumstances.
4. In situations where the whistleblowers or complainants are in circumstances that are not safe or where they may be at risk of harm because of their disclosures and complaints, they are encouraged to request the company to establish appropriate protective measures.

Penalty

The Codes of Conduct and the related policies are considered mandatory and must be strictly followed. Any violation or failure to comply is considered a breach of the Company's policies and Codes of Conduct. Such violations that result in damage or loss of business opportunities for the Company will lead to disciplinary action in accordance with the Company's internal regulations on disciplinary measures. Additionally, violations may be subject to legal consequences under the Securities and Exchange Act (No. 4) B.E. 2551.