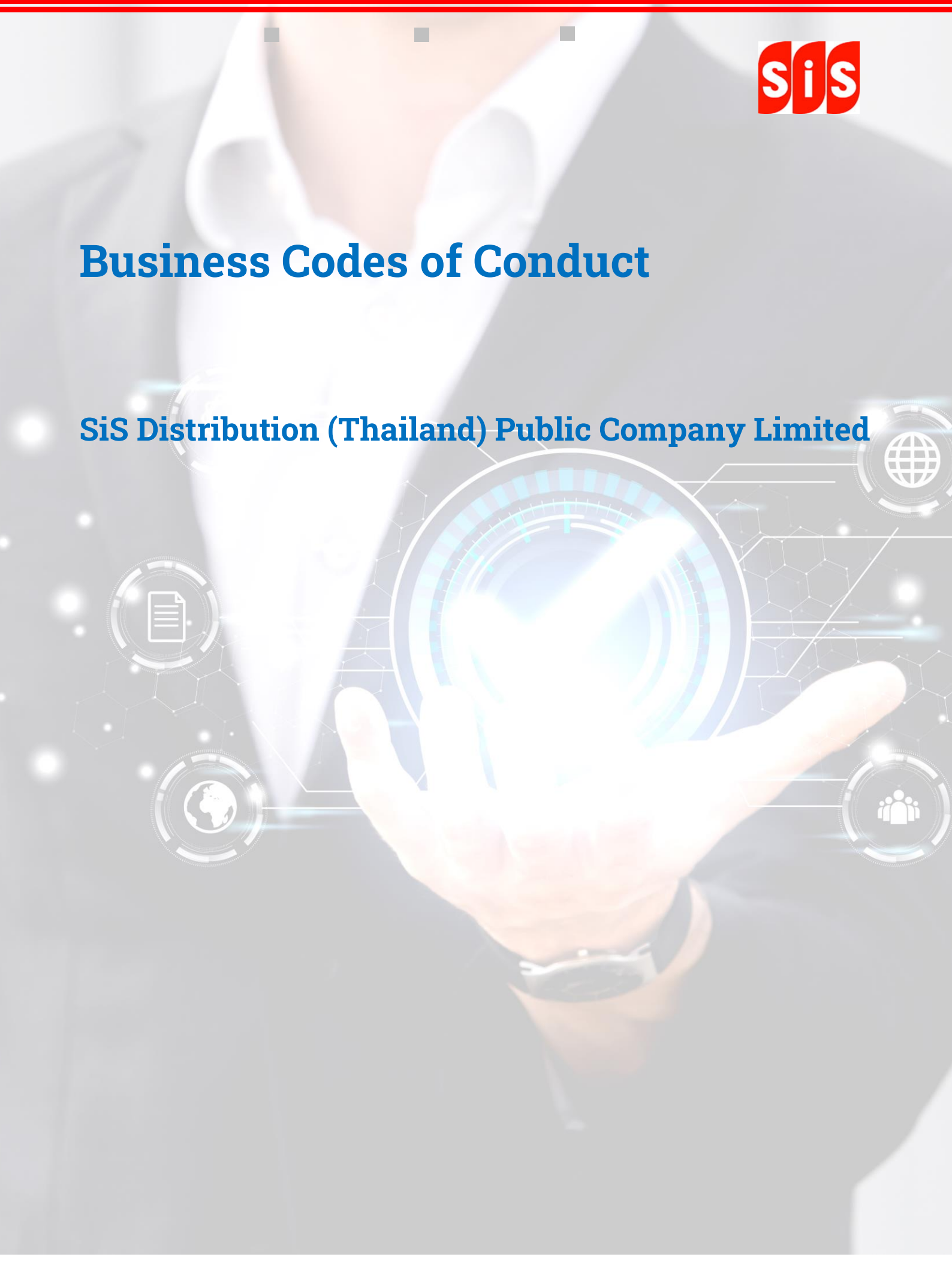
Business Codes of Conduct

SiS Distribution (Thailand) Public Company Limited



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, executives, 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 person taking action under the perception or agreement that if such action is to bring the financial benefit to the person, the following person will also gain similar benefit:gain benefits along with the actions of that individual. 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.
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

Persons affiliated with this Codes of Conduct include the following;

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 Customers.
   - 2.5 Business Partners.
   - 2.6 Business Competitors.
   - 2.7 Trade Payables.
   - 2.8 Creditors.
   - 2.9 Regulators.
   - 2.10 Society, Community and Environmental.

The director, Management, and employees are required to adhere strictly to the Codes of Conduct and related policies established by the Company. This is to demonstrate responsibility to stakeholders associated with the Company. The outlined Codes of Conduct cover the roles that must adhere to and the responsibilities towards stakeholders, as shown in the table below;

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

1. Codes of Conduct regarding responsibility towards the Company

1.1 Performing duties with a sense of responsibility, prioritizing the interests of the Company as paramount.

1.2 Not engaging in or undertaking any activities that may compete or potentially lead to competition with the Company's business.

1.3 Fulfilling duties with honesty and integrity.

1.4 Taking responsibility for using and preserving the Company's assets for maximum benefit, avoiding personal use or use for the benefit of others outside the scope of the Company's business.

1.5 Performing tasks with full knowledge and experience to maximize benefits for the Company.

1.6 Adhering strictly to the rules, regulations, and various policies of the Company.

1.7 Avoiding the use of authority for personal gain or allowing others to rely on one's authority, directly or indirectly, for personal or others' benefits.

1.8 Avoiding acceptance of favors beyond normal relationships from persons with business affiliations with the Company.

1.9 Avoiding making comments about external parties on matters that may negatively impact the Company's reputation and operations.

1.10 Not using critical information about the Company for profit or other benefits, directly or indirectly, and maintaining the confidentiality of the Company's information by being cautious and ensuring that confidential documents or information are not disclosed to external parties. This includes adhering to the Company's Handling Confidential Information and Controlling the Use of Inside Information Policy and Information Disclosure Policy, as outlined in Section 2 of this Codes of Conduct.

1.11 Reporting or complaining when encountering illegal, unethical, or misconduct actions within the organization, including employees and other stakeholders. This includes reporting inaccurate financial reports or internal control deficiencies for the benefit of the Company, following the Company's complaint handling policy as outlined in Section 2 of this Codes of Conduct.

2. Codes of Conduct regarding responsibility towards Shareholders.

2.1 Performing duties with honesty and integrity within the legal framework and regulations of the Company, adhering to this Codes of Conduct in all transactions and decision-making activities. This is to ensure that business operations are conducted with integrity, clarity, transparency, and are auditable.

2.2 Fulfilling responsibilities with full knowledge and capability according to professional principles, utilizing knowledge and experience to perform duties to the best of one's ability.

2.3 Dedication to treating shareholder information and data with confidentiality and trust, similar to how one would treat their own information.

2.4 Disclosing the Company's information accurately, sufficiently, and timely, following the criteria set by the Securities and Exchange Commission, Thailand (SEC) and the Stock Exchange of Thailand (SET).

3. Codes of Conduct regarding responsibility towards Employees.

3.1 Providing fair and appropriate returns and ensuring that employees have sufficient and suitable benefits that align with their circumstances.

3.2 Taking care to maintain a safe working environment for the lives and property of employees at all times.

3.3 Employee appointments, promotions, transfers, rewards, and penalties must be carried out fairly, honestly, and based on knowledge, skills, and suitability.

3.4 Emphasizing the development and knowledge transfer of employees by providing equal and consistent opportunities for all employees.

3.5 Conducting regular training seminars to continuously develop the knowledge and skills of employees.

3.6 Actively listening to feedback and suggestions from employees at all levels, ensuring equality, and providing channels for employees to express concerns or complaints about any misconduct, events, or situations that impact their work or decisions. This should be done in accordance with the company's complaint handling guidance, as outlined in Section 2 of this Codes of Conduct.

4. Codes of Conduct regarding responsibility towards Customers.

4.1 Interacting with customers fairly regarding products and services.

4.2 Providing accurate and complete information about products and services.

4.3 Safeguarding the confidentiality of customer data and information.

4.4 Offering knowledge to customers for the development of products and services.

4.5 Establishing channels for customers to voice complaints about products and services, following the company's complaint handling policy as outlined in section 2 of this Codes of Conduct.

5. Codes of Conduct regarding responsibility towards Business Partners.

5.1 Treating business partners fairly and equally, based on a foundation of mutually fair compensation.

5.2 Adhering to agreements, contracts, or conditions that have been mutually established. In cases where compliance with conditions is not possible, promptly inform business partners to collaboratively find solutions.

6. Codes of Conduct regarding responsibility towards Business Competitors.

6.1 Operating within the framework of good competition rules.

6.2 Not seeking confidential information from business competitors through unethical or inappropriate means.

6.3 Not tarnishing the reputation of business competitors through malicious accusations.

7. Codes of Conduct regarding responsibility towards Trade Payables.

7.1 Dealing with trade payables fairly and maintaining a balanced relationship, based on fair compensation for both parties.

7.2 Adhering to agreements or conditions that have been mutually agreed upon. In cases where compliance with conditions is not possible, promptly inform the trade payable to find a solution together.

8. Codes of Conduct responsibility towards Financial Institutions

8.1 Complying strictly with the terms and conditions specified in agreements, covering aspects such as the purpose of fund usage, repayment, and any other agreed-upon terms.

8.2 Treating all financial institutions equally and fairly.

8.3 Reporting the Company's financial status and information accurately and consistently.

9. Codes of Conduct regarding responsibility towards Regulators

9.1 Fulfilling duties strictly in accordance with laws and regulations established by the regulatory authorities overseeing the Company.

9.2 Cooperating with regulatory authorities and providing information related to any violations or non-compliance with laws, rules, and regulations to those authorities.

10. Codes of Conduct regarding responsibility towards Society, Community and Environment

10.1 Avoiding actions that may have an impact on environmental and social damage.

10.2 Instilling a sense of responsibility for society and the environment among all levels of employees.

10.3 Promoting efficient use of energy and energy conservation.

10.4 Promoting the development of societal quality, with a focus on education and the environment.

Section 2
Related policies

To ensure clarity and convenience for the directors, Managements, and employees in carrying out their duties within the framework of the law, including various regulations and in alignment with the Codes of Conduct, the Company has established the policies. These policies are designed for the directors, Managements, and employees to adhere to, promoting transparency, fairness, clarity, and accountability in their work. The details are outlined as follows:

Related Policies as below:

1. Anti-Corruption Policy.
2. Receiving or Giving of Gifts, Assets or Other Benefits Policy.
3. Donation and Funding Policy.
4. Political Policy.
5. Conflicts of Interests Management Policy.
6. Reports Stating the Interests and Security Holding Policy.
7. Handling Confidential Information and Controlling the Use of Inside Information Policy.
8. Information Disclosure Policy.
9. Protecting and Using of the Assets of the Company Policy.
10. Human Rights Policy.
11. Personal Data Protection Policy.
12. IT Security Policy.
13. Facilitation Payment Policy.
14. Revolving Door Policy.

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

Policy	Responsible Parties				
	Directors	**SIS Directors**	**Management**	**SIS Management**	**Employee**
Anti-Corruption	✔	✔	✔	✔	✔
Receiving or giving of Gifts, Assets or Other Benefits	✔	✔	✔	✔	✔
Donation and Funding	✔	✔	✔	✔	✔
Political	✔	✔	✔	✔	✔
Conflicts of Interests Management	✔	✔	✔	✔	✔
Reports Stating the Interests and Security Holding	✔	✔	✔	✔	-
Handling Confidential Information and Controlling the Use of Inside Information	✔	✔	✔	✔	✔
Information Disclosure	✔	✔	✔	✔	✔
Protecting and Using of the assets of the Company	✔	✔	✔	✔	✔
Human Rights	✔	✔	✔	✔	✔
Personal Data Protection	✔	✔	✔	✔	✔
IT Security	✔	✔	✔	✔	✔
Facilitation Payment	✔	✔	✔	✔	✔
Revolving Door	✔	✔	✔	✔	-

Anti-Corruption Policy

Definition

Fraud means intentional action taken to obtain illegal advantage to themselves or the others.

Corruption means 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.

Anti-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-Corruption Policy is effectively implemented as follows.

The Company recognizes the vital of corruption in Thai society, as well as international contexts This also generates risks to business operations and is significant obstacle to the business sustainable growth. Therefore, the Company is committing to adhering to Thai laws in countering corruption and establishes the Anti-Corruption Policy which covers all activities of the Company. The Company promotes strict adherence to the Anti-Corruption Policy for all directors, Managements and employees of the Company, its subsidiaries, as well as all business representatives. The policy is aimed at preventing corporate fraud and corruption and is outlined as follows:

1. Directors, Management, and employees of the Company and its subsidiaries are strictly prohibited from direct and indirect involving or accepting any forms of 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 mandates the annual assessment and management of corruption risks. This includes the examination of internal controls related to anti-corruption measures, which is an integral part of the annual internal audit plan. Additionally, the Company requires annual reviews, audits, and updates of measures, practices, and requirements related to anti-corruption to ensure their alignment and suitability with both the internal and external organizational context. This process extends to encompass emerging risks that may arise.
3. The Board of Directors, the Managements, and the employees of the Company and its subsidiaries are required to adhere to the Anti-Corruption Policy, the Codes of Conduct and other instructions relating to the Anti-Corruption Policy that is defined by the Company.

4. The Board of Directors, the Managements, and the employees of the Company and its subsidiaries shall not be involved in any direct and indirect 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-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 The Directors, the Managements, and the 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 having business with the Company and its subsidiaries for gaining inappropriate benefits to themselves, their family, friends, businesses, excepting during internationally recognized New Year holidays or customary practices widely accepted. In this case, such benefits would not exceed the value of 3,000 Baht. Furthermore, any form of hospitality and entertainment should be reasonable and in accordance with the Codes of Conduct, relevant policies, and the employee guidelines.
    5.2 The Directors, the Managements and the employees of the Company and its subsidiaries are prohibited from offering gifts, assets, or any other benefits to external individuals to incentivize them to perform non-permissible duties or omit their duties in order to gain the business or private benefits.
    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 The procurement and contracting processes relate to the Company and its subsidiaries' businesses, with the government or private sectors shall be executed legally, transparently, and consistent with the Codes of Conduct and guidelines determined by the Company.
    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 respects 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:
    6.1 Examines working procedures to ensure the accuracy, completeness, and integrity of financial accounting and record-keeping, confirming that they reflect actual transactions.
    6.2 Examines the process of retaining and maintaining financial records, evidence, and the Company and subsidiaries data to ensure appropriateness, integrity, and adequate control systems that allow for timely and effective auditing of financial transactions.
    6.3 Examines the sales, marketing, procurement, and contracting processes, with a focus on areas with corruption risks. Additionally, identifying and implementing suitable resolutions for discrepancies correction, and consistently reviewing and refining work processes and procedures.
    6.4 Segregating duties at each working stage to ensure compliance with good internal control principles.

7. The Company defines the scope and authorities of the Quality Assurance Department relating to anti-corruption as follows:
   7.1 Examines and develops an annual audit plan that covers accounting, financial transaction recording, document retention, and financial data of the Company. This plan should also include sales, marketing, procurement, and contracting processes. This includes effectively, continuously, and adequately establishing resolutions for discrepancy correction and other procedures that may have risk relating to corruption.
   7.2 Develops measures and working procedures for processes with a risk of corruption that adhere to good internal control principles, to have sufficient support evidence and appropriate evidence retention, including regularly review and refine work processes to ensure suitability and consistency.
   7.3 Collaborates with the relevant risk owners or departments to design and develop internal control systems or working procedures to mitigate corruption risks with certain activities.
   7.4 Promptly reports findings from internal audits related to corruption or other suspicious behaviors to senior management, the Audit Committee, and the Board of Directors.
   7.5 Monitors the implementation of anti-corruption measures to ensure that the Board of Directors, Management, and the employees consistently adhere to the Anti-Corruption Policy and its requirements.
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-Corruption Policy implementation. The Audit Committee shall continuously report the audit result to the Board of Directors.
11. The Board of Directors and the Managements have duties and responsibilities to support and implement the Anti-Corruption Policy by indicating the system to encourage and support Anti-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. The Board of Directors, the Managements, the 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. The Board of Directors, the Managements, the employees of the Company who 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 Managements 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. The Board of Directors, the Managements and the 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 direct and indirect related to the corruption.

Operating Requirements

1. To comply with the Anti-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-Corruption Policy covers all business processes of the Company including the human resource management process, ranging from recruiting, training, evaluating, promoting, and provision of employee benefits and perks. All employees are required to execute their operations under this Anti-Corruption Policy.

Guidelines for Anti-Corruption

1. The workflow is designed to provide cross-functional checks and a counterbalance with mutual oversight and authority among related departments.
2. Instills the employees for the consciousness and value of anti-fraud and corruption.
3. There are channels available for stakeholders to report fraud and corruption, both through direct contact with the management via complain@sisthai.com, as specified on the Company's website. The Company has a database system to store all incoming reports. Additionally, there is a direct channel to contact the independent directors through independentdirector@sisthai.com.
4. It is prohibited for the Management and the employees from receiving any gifts, excepting during internationally recognized New Year holidays or customary practices widely accepted. In this case, such benefits would not exceed the value of 3,000 Baht. The acceptance of gift with value exceeding 3,000 Baht shall be reported to the supervisor and forwarded to the General Affair Department for further action. In case of travelling package receiving, it shall be informed to the Company to further allocate such gift.
5. It is prohibited for inappropriate seeking of authority over others, such as promising to provide valuable items in order to gain inappropriate advantage.

6. The company has established a clear and appropriate expense reimbursement policy for employees to prevent fraud and corruption. There is an expense audit team responsible for reviewing every expense request, both direct from supervisors and from the General Affairs department, which oversees expense control. Additionally, all employees are informed from the outset that the Company strictly follows the policy of reimbursing actual expenses and does not allow them to be considered as income.
7. The company views fraud and corruption as serious offenses, and when such misconduct occurs, a joint committee is convened to consider appropriate punitive measures. These measures may include verbal warnings, compensating for damages, terminating employment, or pursuing legal action against the individuals involved in fraud and corruption. Additionally, a thorough investigation of the issues is conducted to identify ways to prevent and rectify them, and systems are adjusted to minimize the recurrence of fraud and corruption.
8. To ensure that the Board of Directors, the Managements, and the employees are aware of these practices, the Company has incorporated them into the orientation program for new employees and directors. Additionally, there is continuous emphasis on these principles to the Board of Directors, the Managements, and employees through electronic media on a quarterly basis.
9. The Company will not consider demoting, penalizing, or delivering negative consequences to the employees who refuse to engage in fraud or corruption, even if such actions result in a business opportunity loss for the Company.

Consulting and Reporting Non-Compliance relating to the Codes of Conduct and Related Policies

The Company provides an opportunity for all stakeholders to report the clues and complaints of non-compliance relating to the Codes of Conduct, Anti-Corruption, and other policies. 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 Codes of Conduct, Anti-Corruption, Human Rights, and other relevant 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, Anti-Corruption, Human Rights and other relevant policies. This channel is also dedicated to providing consultation and guidance about 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, Anti-Corruption, Human Rights and other relevant 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 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 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 Codes of Conduct, Anti-Corruption, and other policies. 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 putting the negative impact to the employees who refuse the fraud and corruption even such refusion may cause the Company business opportunity lost.

Penalty

This Anti-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-Corruption Policy has been approved by the Board of Directors in the Board of Directors' meeting of No. 7/2023 held on November 21st, 2023.

This policy shall be effective from January 1st, 2024, onwards.

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

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. Receiving money, gifts, assets that can be converted into currency, or any other benefits that result in undue personal, family, friend, or business advantage from individuals, juristic person, or the entity that having business with the Company and its subsidiaries are strictly prohibited. However, there is an exception during the internationally recognized New Year holidays or customary practices widely accepted, in which the value should not exceed 3,000 Baht. Entertainment and hospitality should be appropriate and in line with the Codes of Conduct, relevant policies, and employee guidelines.2. The employees are prohibited from accepting gifts on occasions following customary practices with a value exceeding 3,000 Baht from business associates with the Company. When offered gifts by any other individuals, the employees are required to report this to their superiors and forward it to the General Affairs Department for further action.
3. 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.
4. 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.
5. 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.
6. 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.

7. 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. 7/2023 held on November 21st, 2023.

This policy shall be effective from January 1st, 2024, 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

1. SiS Distribution (Thailand) Public Company Limited ("the Company") recognizes that donations and support could be used as a pretext for corruption. Therefore, the Company gives priority on making charity donations, especially in the fields of education and the environment. The Company will not donate to exert the influence of the authorized persons or to cause unfair advantages as follows:1. Donations and support must be contributed to education and the environment and should be given to an organizations that have 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. 7/2023 held on November 21st, 2023.

This policy shall be effective from January 1st, 2024, 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 political neutrality and will refrain from engaging in any activities that provide political assistance or support any political parties. The Company upholds to the principle of democracy and respects the freedom to participate in political activities, especially in the election of directors, all levels of the Managements and the employees. Therefore, the Company has established the political policy as follows:

1. Avoid engaging in any political activities that could lead others to believe that the Company supports any particular political party.
2. Avoid providing financial assistance, which includes giving assets, money, goods, or any other benefits such as money or goods donation, goods and services purchase, to directly or indirectly support, promote, or advocate for any political party, politician, or organization closely associated with a political party that could lead others to believe that these actions are performed on behalf of the Company and intended to benefit the Company or yield other unauthorized gains.
3. Avoid dressing during work in a manner that displays political party symbols or adorning oneself with attire and accessories that might lead others to believe that the Company is taking a political stance.
4. Assign the Quality Assurance Department to ensure strict compliance with the policy and none of use political assistant for corruption purposes. This includes urgently reporting of any suspicious issues or behaviors to senior management, the Audit committee, and the Board of Directors.
5. The Company ensures that directors, Managements and employees of the Company, its subsidiaries, business representatives, and business partners are aware of the Political Policy and guidelines through various communication channels, such as meetings and electronic communication. Everyone can access this policy on the Company's website.

This Political Policy has been approved by the Board of Directors in the Board of Directors' meeting of No. 7/2023 held on November 21st, 2023.

This policy shall be effective from January 1st, 2024, 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.

Conflicts of Interests Management Policy

SiS Distribution (Thailand) Public Company Limited ("the Company") is a listed company in the Stock Exchange of Thailand (SET) who aware of the importance of conflicts of interest management so the Company has established the Conflicts of Interests Management Policy as follows:

1. Avoid engaging in any activities that conflict with the interests of the Company, whether through interactions with business-related parties of the Company, such as vendors, customers, competitors, or by utilizing opportunities or information gained from holding positions as a director, Management, or the employee to seek personal gain. This extends to engaging in competitive business with the Company or performing work outside the scope of the Company's responsibilities that may adversely impact on the duties.
2. Avoid engaging Related Party Transactions unless it is necessary for the benefit of the Company. In such cases, the parties involved shall notify the Compliance Department or Company Secretary in advance. Such transaction shall be performed as the same as it were with an external party. The Board of Directors, the Management, or the employees who have a vested interest in such transactions shall not participate in the decision-making process and shall disclose information accurately and in accordance with the legal and regulatory processes established by the supervisory authorities.
3. The Related Party Transactions shall undergo examination or assessment by the Audit Committee. In cases where a member of the Audit Committee has a vested interest in a related transaction, that committee member shall not participate in the assessment of the transaction.

Guidelines for Conflicts of Interests Management

1. The Board of Directors has been informed 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. 7/2023 held on November 21st, 2023.

This policy shall be effective from January 1st, 2024, onwards.

Reports Stating the Interests and Security Holding Policy

SiS Distribution (Thailand) Public Company Limited ("the Company") is a listed company in the Stock Exchange of Thailand (SET) who aware of the importance of the reports stating the interests according to Section 89/14 and security holding according to Section 59 of the Securities and Exchange Act, so the Company has established the Reports Stating the Interests and Security Holding Policy as follows:

1. The directors and the Management are responsible for preparing the reports stating their and their related persons' interests at least once a year and when there is change. These reports shall be submitted to the Company Secretary to compilation of the report stating the interest and reports on changes in the Company's shareholdings for the Board of Directors. This is to ensure that shareholders and general investors have confidence that the Board of Directors and the Management can manage and conduct business with honesty, integrity, transparency, and accountability.
2. The directors, the Managements, and the employees of the Company are prohibited from trading the Company's securities during the end of the quarter until the Company has disclosed its Financial Statements publicly. During such period, if an employee has a necessity to trade the Company's securities, they must notify and obtain approval from the Compliance Department prior to engaging in any transactions.
3. In cases where the directors and the Managements trade, transfer, or receive the Company's securities, they shall report such transactions to the Securities and Exchange Commission, Thailand (SEC) within 3 business days from the date of the transaction, as required by Section 59. This reporting is essential for disclosing the changes to the shareholders.

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. 7/2023 held on November 21st, 2023.

This policy shall be effective from January 1st, 2024, onwards.

Confidential Information Protection and Controlling of Inside Information Usage Policy

SiS Distribution (Thailand) Public Company Limited ("the Company") is a listed company in the Stock Exchange of Thailand (SET) who aware of the importance of the handling confidential information and controlling the use of inside information so the Company has established the Confidential Information Protection and Controlling of Inside Information Usage Policy as follows:

1. The directors, the Managements, and the employees are strictly prohibited from using information of the Company for personal gain or for the benefit of others in securities trading prior to the Company discloses it to the public.
2. To do not disclose the Company information such as financial information, customer information, contracts, business plans, human resources information, marketing data, products, operating results or any other confidential information or the information that can affect the business operations to the public if it has not been approved by senior managements or the Compliance Department.
3. The Management and the employees shall refrain from using personal information, which includes income and benefits-related data, for personal gain or disclose to others.

Guidelines for protection of confidential information and preventing internal information usage for personal gain

1. The directors, the Managements, and all employees are prohibited from using the internal information about financial status and operating results of the Company, which has not been publicly disclosed for securities trading or for personal gain.
2. The Company has informed the directors and the Managements about their responsibilities in reporting securities holding and any changes in the Company's securities holding, including those held by themselves, their spouses and child who have not yet reached the age of majority, and their related parties as per Section 258 of the Securities and Exchange Act B.E. 2535. Individuals mentioned in this context shall report this information to the SEC within 3 business days from the date of trading, transferring, or receiving of the Company's securities, in accordance with Section 59. The Company also has informed the directors and the Managements about penalties as per Section 275 of the Securities and Exchange Act B.E. 2535.
3. The company requires the directors and the Managements to report their securities trading to the Company Secretary for the purpose of recording changes and summarizing the number of securities held by each person. This information shall be presented to the Board of Directors during quarterly meetings and be disclosed in the Annual Report.
4. The Company establishes a policy that the employees, other than the Management, are to follow the same guidelines as the Management regarding refraining from the Company's securities trading during the end of each quarter, until the Company publicly discloses its Financial Statement. During such period, if the employees need to trade their Company's securities, they must notify and obtain approval from the Compliance Department prior to engaging in any transactions.
5. To ensure that the directors, the Managements, and the employees are aware of these guidelines, the Company has provided notifications to all directors, Managements, and employees to aware of refraining from the Company's securities trading during the specified periods on quarterly basis. This guideline has been accepted 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. 7/2023 held on November 21st, 2023.

This policy shall be effective from January 1st, 2024, onwards.

Information Disclosure Policy

SiS Distribution (Thailand) Public Company Limited ("the Company") is a listed company in the Stock Exchange of Thailand (SET) who aware of the importance of the information disclosure so the Company has established the Information Disclosure Policy as follows:

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 the 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 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. 7/2023 held on November 21st, 2023.

This policy shall be effective from January 1st, 2024, onwards.

Protecting and Using the Assets of the Company Policy

1. The directors, the Managements, and the employees have the responsibility and duty to oversee the assets of the Company to prevent deterioration, damage, or loss. They should efficiently utilize Company assets for the full benefit of the Company and refrain from using Company assets for personal gain or the gain of others.
2. The mentioned assets refer to both tangible and intangible assets, such as chattel, real estate, technology, academic knowledge, official papers, patent rights, copyright, and confidential information that has not disclosed to the public including the business plans, financial projections, and information about human resources.

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. 7/2023 held on November 21st, 2023.

This policy shall be effective from January 1st, 2024, onwards.

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 the all directors, Managements and employees aware of 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. This includes:

1. Supporting and respecting the protection of human rights and avoiding actions that violate human rights.
2. Treating others fairly, equally, and indiscriminately.
3. Monitoring and overseeing to ensure that the Company's business operations do not become involved in human rights violations.
4. Refraining access to resources that have an impact on the traditional way of life and well-being of the community.
5. Resisting human rights violations and the infringement of all stakeholders' privacy throughout the supply chain.
6. Communicating, disseminating, providing 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.

Guidelines for Human Rights

1. Respect human rights, treating each other with respect, dignity and equality to all stakeholders including the persons who lack the ability to protect their own rights and benefits, without discrimination based on physical or mental differences, race, nationality, place of origin, , ethnicity, religion, gender, language, age, skin color, education, social status, culture, tradition, or any other status.
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 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. 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.
4. 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.

5. Establish a channel for whistleblowing and complaint, ensuring fairness and safeguarding the individuals who make such reports or complaints. through the following means:

5.1 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

5.2 The internal stakeholders can report to

- Supervisors, executives, and the Management who are entrusted by the complainant or the whistleblower.
- Human Resources Manager

6. 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. 7/2023 held on November 21st, 2023.

This policy shall be effective from January 1st, 2024, onwards.

Personal Data Protection Policy

SiS Distribution (Thailand) Public Company Limited ("the Company") is acutely aware of the importance of effectively personal data protection to grant the data owner to protect their own personal data. Therefore, the Company has established this Personal Data Protection Policy to outline the procedures and practices that the Company adheres to regarding the personal data of relevant parties, ensuring the security, stability, and transparency of the data such as data collection, storage, usage, disclosure including the rights of personal data owners. This policy encompasses the handling of both existing data and any data that the Company may develop or acquire in the future as described below.

1. Personal Data

"Personal Data" means data that can identify an individual, whether through direct or indirect means.

2. Restricted Personal Data Collection

The collection and storage of personal data collection by the Company will be performed with specific purposes and scopes, and by methods that comply with legal and ethical standards. The collection and storage will be limited to the extent necessary for product sales, services provision or any other electronic services for the Company's purposes. The Company shall seek for acknowledgment and consent from the data owner via an electronic means, short message or any alternate means specified by the Company for the benefits of product or service sales and purchase. Prior to performing the aforementioned actions, the Company shall request the consent from data owner unless:

2.1 It is required by applicable laws, such as the Personal Data Protection Act, the Electronic Transaction Act, the Telecommunications Business Act, the Anti-Money Laundering Act, the Civil and Criminal Code, the Civil and Criminal Procedure Code, etc.

2.2 It is carried out for the benefit of facilitating investigations by investigating officers or for the court's consideration and judgment.

2.3 It is carried out for the benefit of the personal data owner and requesting consent cannot be done at that time.

2.4 It is necessary for the Company's lawful benefits or the benefits of other individuals or legal entities other than the Company.

2.5 It is necessary for the prevention or avoidance of any events harmful to an individual's life, body, or health.

2.6 It is necessary to comply with any agreement to which the personal data owner is a party or respond to any requests of personal data the owner prior to entering into such agreement.

2.7 It is carried out to achieve the objectives related to the compilation of historical documents or annotations, for the public benefit, or for educational, research, and statistical purposes, provided that appropriate safeguards are in place.

3. Data Security and Quality Protective Measure

3.1 The Company realizes the importance of maintaining the security of personal data of all stakeholders. Therefore, appropriate measures have been established to ensure the security of personal data and to comply with data confidentiality in order to prevent loss, unauthorized access, destruction, use, alteration, or disclosure of personal data without legal rights or consent, as outlined in the Information Technology (IT) Security Policy.

3.2 Personal data that can identify an individual, such as name, age, address, phone number, ID Card number, and financial information etc. which the Company has obtained and are accurate, and up-to-date shall only be used for the purpose of the Company's operations. The Company shall implement the appropriate measures to protect the rights of the personal data owners.

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

The Company collects, stores, and uses personal data from stakeholders for the following purposes.

4.1 For the benefit of buying or providing goods and services to the data subject, including services that the data owner may be interested in, such as sales promotion activities, payment channel services, digital services, market research etc.

4.2 For the purpose of establishing databases and utilizing information to offer benefits based on the interests of the data owner.

4.3 For the benefit of analyzing and presenting services or products of the service provider and/or individuals who are distributors, dealers, or have affiliations with the service provider and/or other individuals.

4.4 For any other lawful purposes and/or to comply with laws or regulations applicable to the service provider, or to enhance efficiency in providing various services, both currently and in the future.

4.5 To grant permission for the Company to transmit, transfer, and/or disclose personal information to the business group of the Company, business partners, external service providers, data processors, interested parties for rights transfer, transferees, any entity/ organization/ juristic person having a contract with the Company or a relevant relationship, and/or Cloud computing service providers. The consent allows the Company to transmit, transfer, and/or disclose such information both domestically and internationally. The Company will retain the aforementioned information only for the duration necessary for the purposes stated.

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

5.1 The Company shall use and disclose personal data in accordance with the consent of the data owner, strictly for the purposes of data collection, storage, and usage by the Company only. The Company shall oversee its employees, officers, or operators to not use and/or disclose personal data for any purposes other than the collection of personal data and disclosure thereof to third parties unless.

a) It is required by applicable laws, such as the Personal Data Protection Act, the Electronic Transaction Act, the Telecommunications Business Act, the Anti-Money Laundering Act, the Civil and Criminal Code, Civil and the Criminal Procedure Code, etc.

b) It is carried out for the benefit of facilitating investigations by investigating officers or for the court's consideration and judgment.

c) It is carried out for the benefit of the personal data owner and requesting consent cannot be done at that time.

d) it is necessary for the Company's lawful benefits or the benefits of other individuals or legal entities other than the Company.

e) It is necessary for the prevention or avoidance of any event harmful to an individual's life, body, or health.

f) It is necessary to comply with any agreement to which the personal data owner is a party or respond to any requests of the personal data owner prior to entering into such agreement.

g) It is carried out to achieve objectives related to the compilation of historical documents or annotations, for the public benefit, or for educational, research, and statistical purposes, provided that appropriate safeguards are in place.

5.2 The Company may use the information services of external third-party providers to manage and store personal data, provided that those service providers shall have adequate security measures in place and are prohibited from collecting, using, or disclosing personal data for any purposes not stipulated by the Company.

6. Rights Concerning Personal Data of the Data Owner

6.1 Personal data owners are entitled to request access and copy of their personal data based on the criteria and methods prescribed by the Company or may request the Company to disclose how their personal data is acquired. However, the Company may refuse the request in accordance with the applicable laws or court orders.

6.2 Personal data owners are entitled to request the correction or modification of their personal data if it is inaccurate or incomplete and to update their own data.

6.3 Personal data owners are entitled to request the deletion or destruction of their personal data, except in cases where the Company is required to comply with the law applicable to such data storage.

7. Respecting the Privacy of the Data Owner

The Company places great importance on respecting privacy. The data owners are entitled to refuse to receive any marketing or public relations information from the Company through various communication channels. Upon such refusal, the customer shall remain to receive the information concerning services.

8. Disclosures Concerning Operations, Practices, and Policies Related to Personal Data

The Company has policy to adhere to the laws and announcements on telecommunication service client right protection concerning personal data, privacy rights, and freedom to communicate with others via telecommunication, including the laws regarding personal data. The Company has also established client data protective measures on the Company's website.

9. Personal Data Protection Officer

The Company has complied with the Personal Data Protection Act B.E. 2562 by appointing the Data Protection Officer (DPO) to oversee the Company's operations related to personal data collection, usage, and disclosure to be consistent with the Personal Data Protection Act B.E. 2562 including any laws relevant to personal data protection. Additionally, the Company has established the rules and orders for the relevant parties to perform consistently to enable the smooth operations of the personal data protection policy. This is in alignment with the Company's IT Security policy.

10. The Company's Communication Channel

SiS Distribution (Thailand) Public Company Limited
9 Pakin Building, 9th Floor, Room No. 901, Ratchadaphisek Road, Din Daeng, Bangkok 10400
Tel: 02-020-3000
Data Protection Officer Email: dpo@sisthai.com

11. Enforcement

To ensure compliance with this policy, the Company has established the Personal Data and IT Security Committee ("the Committee"). This Committee is responsible for the management and protection of personal data by setting guidelines, procedures, as well as amending, and improving data management practices, with approval from the Management Director, to define the data protection guidelines between the Company and all stakeholders.

This Personal Data Protection Policy has been approved by the Board of Directors in the Board of Directors' meeting of No. 7/2023 held on November 21st, 2023.

This policy shall be effective from January 1st, 2024, onwards.

Information Technology (IT) Security Policy

Nowadays that information technology (IT) are widely used in working and daily life, especially for SiS Distribution (Thailand) Public Company Limited ("the Company") which operates the business as importer and distributor for IT equipment. The Company has established the Information Technology (IT) Security Policy and guidelines as follows:

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 Employee means staff of the IS Department.
   - 1.5 Network system administrator means staff who are responsible for providing services for computer network system.
   - 1.6 IT developers 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 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 shall assess the risks associated with external access to the computer network system and establish clear and periodic support or mitigation measures, which may be done 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. it's the 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, unserviceable 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 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 input 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

14.1 Services for user and personal password for using SiS network system.

14.1.1 When the user is 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 shall change their password immediately upon receiving the password from the system administrator. The length of the new password shall not be less than 8 characters.

14.1.3 The system will be automatically locked in case of wrong password has been entered for 6 times and will immediately disable access to that user's workspace. The account owner shall contact directly to the Department to request a password reset.

14.1.4 The users are required to change their password at least every 90 days. The length of the new password shall not be less than 8 characters.

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 for 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 gain 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 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 use the 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.

Guidelines for IT Security

1. All Managements 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. 7/2023 held on November 21st, 2023.

This policy shall be effective from January 1st, 2024, 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

Due to the high risk that facilitation payment to government officials might lead to bribe, fraud and corruption, SIS Distribution (Thailand) Company Limited ("the Company") places great importance on anti-corruption and supporting transparent operations and fair business competition. Therefore, 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.

Guidelines for Facilitation Payment

1. The directors, Managements, and employees of the Company and its subsidiaries are strictly prohibited from providing Facilitation Payment which may lead to corruption.
2. Violations of the Facilitation Payment policy and guidelines will be subject to disciplinary actions as determined by the Company. Legal actions may also be pursued if the violation constitutes a breach of the law.

This Facilitation Payment Policy has been approved by the Board of Directors in the Board of Directors' meeting of No. 7/2023 held on November 21st, 2023.

This policy shall be effective from January 1st, 2024, onwards.

Revolving Door Policy

Definition

Government employees means individuals holding political positions, civil servants, or local government officials with regular positions or salaries. They also include employees or personnel working within state-owned enterprises or government agencies. This term encompasses local authorities and members of local councils who are not political officeholders but serve in governance capacities. Government officers, as defined by relevant laws, include directors and its sub-committees, government and state enterprise employees, or individuals working in state agencies, including both natural persons and legal entities or associations, that exercise authority or are delegated authority by the state to perform government functions, whether established within the government system, state-owned enterprises, or other state-related activities.

Revolving Door Policy

SIS Distribution (Thailand) Company Limited ("the Company") emphasizes the importance of anti-activities that may lead to fraud and corruption and supports transparent information disclosure for all stakeholders. To ensure that such actions do not lead to any undue benefits, the Company has established the Revolving Door Policy to prevent any potential conflicts of interest as follows:

1. The Company does not have a policy to hire government employees who are currently in positions. In cases where a former government employee who has left their government position or individuals who have previously worked for a relevant government oversight entity directly related to the Company's activities wish to assume a position within the Company, there must be a cooling-off period of 2 years from the day they leave their government position until they can assume a role within the Company.
2. The Company will disclose the names and backgrounds of the directors, the Management, and advisors who have previously held positions in state organizations directly related to the Company. This will be disclosed in the Annual Report, along with an explanation for their appointments, to ensure transparency.
3. The Company has the process of examining the background of the individuals that the Company intends to nominate as the directors, advisors, and Managements to prevent potential conflicts of interest prior to the appointment.

This Revolving Door Policy has been approved by the Board of Directors in the Board of Directors' meeting of No. 7/2023 held on November 21st, 2023.

This policy shall be effective from January 1st, 2024, onwards.