Information Technology (IT) Security Policy

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

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

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

1. Definitions in this policy

1.1 The Department means Information Support Department (IS)

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

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

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

1.5 Employee means staff of the IS Department.

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

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

2. General

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

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

3. Responsibilities of the Department Management

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

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

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

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

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

4. Security of the Infrastructure of the Department

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

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

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

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

5. Management of the Department's properties.

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

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

6. Security of departments concerning the Employee.

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

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

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

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

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

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

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

7. Security of Physical and Environment.

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

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

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

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

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

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

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

8. Computer Network System Management

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

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

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

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

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

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

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

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

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

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

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

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

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

8.12.3 Internet data from File Transfer Protocol (FTP) servers

8.12.4 Internet data from web servers

8.12.5 Type of data in User Network (Usenet)

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

9. Control of IT Assets Accessibility

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

11. IT System Risk Management

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

11.1.1 Improper use of IT system violates the policies, announcement, and regulations.

11.1.2 Threats from computer viruses, computer warms and malware.

11.1.3 Threats from malicious attacks on the system by unauthorized individuals, which may affect IT information and communications.

11.1.4 Limitations in the provision of IT system services which may result in unavailability or inability to use the service.

11.1.5 Physical or natural disaster.

11.1.6 Other aspects may occur.

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

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

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

12. The Departments' Operations Continuity Management

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

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

13. Compliance with the IT Security Policy

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

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

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

14. Service Agreement for Computer Network Systems and Information Systems

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

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

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

14.1.3.1 For SAP System

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

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

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

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

14.2 Connection for SiS network system via LAN line.

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

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

14.3 Connection for SiS network system via wireless.

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

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

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

14.4 Data retrieval services via internet and intranet networks.

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

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

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

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

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

14.5 Data retrieval services via online database.

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

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

14.6 E-mail communication services for the employees.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

14.9.3 The requester shall request in writing to the Operations Director for each request. The following technical details shall be identified:

14.9.3.1Number of port which required for opening.

14.9.3.2Number of destination IP address.

14.9.3.3Purpose or name of application which shall use such port.

14.9.3.4Start and end date of services.

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

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

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

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

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

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

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

Guidelines for IT Security

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

This Information Technology (IT) Security Policy has been approved by the Board of Directors in the Board of Directors' meeting of No. 6/2025 held on December 12th, 2025.

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

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