(Translation)

Information Security Guideline Policy

Saha Pathana Inter-Holding Public Company Limited

September 19, 2025

Content

Information Security Guideline Policy
Saha Pathana Inter-Holding Public Company Limited
(3rd Revised Edition)

1. Introduction

The Company's information and communication technology system is critical to providing services to the Company's directors, executives, employees, and authorized external parties. Therefore, to ensure that electronic transactions, operations, and management are conducted appropriately, efficiently, securely, reliably, and on a continuous basis, the Company has established an Information Technology Security Policy and Information Technology Security Practices as guidelines for the use of information technology.

2. Objective

2.1 To ensure that the company's information and communication technology systems operate with stability, security, continuous availability, and efficiency, so that business transactions are conducted accurately and reliably in accordance with the security standards for electronic transactions.

2.2 To establish operational guidelines for executives, system administrators, and system users to recognize the importance of maintaining security in the use of the company's information and communication technology systems.

2.3 To protect staff users and related parties from committing offenses under the Computer Crime Act and other laws related to information technology.

3. Definitions

The definitions used in these guidelines consist of the following:

"The Company" means Saha Pattana Inter-Holding Public Company Limited.

"User" means a person who is authorized to access, manage, or maintain the Company's information and communication technology systems, with rights and responsibilities as defined by the Company.

"Executive" means an executive of the Company.

"System Administrator" means the Information Technology Department Manager or a person assigned to control, oversee, and manage the Company's information and communication technology systems.

"Staff" means personnel under the Company's organization.

"Assets" means computer data, computer systems, and information and communication technology property of the Company, such as network equipment and software legally purchased by the Company for authorized use, etc.

"Information Access or Access Control" means the control and restriction of rights to use the Company's information and communication technology systems with respect to services and data as necessary for operational use, including protection against unauthorized access to the system by both internal and external parties.

"Information Security" means the preservation of confidentiality, integrity, and availability of data within the Company's information and communication technology systems.

"Security Incidents" means events that occur within the Company's information and communication technology systems, or events suspected of being vulnerabilities or capable of ultimately causing damage, which result in a violation of the Company's information technology security policy. Examples include allowing others to access the system on one's behalf, failing to set a password or using an insecure password to access the system, disclosing important documents to external parties, installing or using unwanted programs, being subject to network intrusion or attack, or unauthorized disclosure of sensitive information, etc.

"Undesirable or Unforeseen Security Situations" refers to situations that the system administrator does not wish to occur or that cause damage to the Company's information and communication technology systems in ways that were not anticipated by the system administrator. Examples include unwanted programs, program errors or malfunctions, network intrusion into the system, alteration or loss of important data, website defacement, unauthorized disclosure of sensitive information, system attacks rendering services unavailable, disruption of computer and network systems, or other events that constitute a violation of the information technology security policy.

"Information Technology Department" means the unit and/or responsible party whose duties involve managing information technology systems and computer systems, and serving as the central information network hub of the Company including studying and analyzing in order to develop the Company's information technology and computer systems, as well as collaborating with or supporting the operations of other related departments.

"Computer Data" means data, messages, instructions, sets of instructions, or anything else stored within a computer system in a state that the computer system can process, and shall also include electronic data as defined under the law on electronic transactions.

"Information Center" means the Server Room, Backup Room, Control Room, Network Room, and air conditioning system areas.

"Computer System" means a device or set of computer devices connected to work together, in which instructions, sets of instructions, or other items and operational guidelines have been defined to enable the device or set of devices to process data automatically.

"Communication Network System" means a system that can be used for communication, interconnection, or transmission of information between the Company's various information technology systems, where connectivity may be in both wired and wireless forms. Communication network systems include Local Area Network (LAN), Wide Area Network (WAN), Intranet, and Internet systems.

"Local Area Network (LAN)" means a network that interconnects devices within a close or confined area.

"Wide Area Network (WAN)" means a network that interconnects devices over long distances.

"Intranet System" means an internal communication network system that connects various computer systems within the organization, serving as a network intended for internal communication and the exchange of data and information within the Company.

"Internet System" means a communication network system that connects the Company's various computer systems to the worldwide internet communication network.

"Information" means data that has been processed and organized, which may appear in the form of numbers, text, or graphics, into a system that users can easily understand and utilize for management, planning, decision-making, and other purposes.

"Information and Communication Technology System" means the Company's operational system comprising computer systems, database systems, communication network systems, system users, system developers, system administrators, and the Company's executives, working together to define objectives, collect and store data, process data, and deliver resulting outputs or information to system users and the Company's executives for use in planning, operational support, decision-making, management, analysis, and monitoring of performance across various levels of the Company's organization.

"Password" means letters, characters, or numbers used as a tool for identity verification and authentication, in order to control access to data and information systems for the purpose of maintaining the security of data and information and communication technology systems.

"Information Security" means the implementation of security measures for the Company's information and communication technology systems, comprising three fundamental properties as follows:

(1) Confidentiality; the preservation of data as confidential, whereby only authorized persons shall be able to access such data.

(2) Integrity; the assurance that data will not be subjected to any action resulting in alteration or modification by unauthorized persons, whether such action is intentional or not.

(3) Availability; the assurance that data or all information and communication technology systems are ready to provide service at the time they are needed.

"Malware" means a set of instructions that cause damage to, destruction of, modification or alteration of, addition to, malfunction of, or improper operation of the information and communication technology system contrary to its defined commands.

"Electronic Mail (E-Mail)" means a system used by individuals to send and receive messages between one another via computers and interconnected communication networks. The data transmitted may include text, photographs, graphics, animations, and audio. A sender may send messages to one or multiple recipients. Standards used for this type of data transmission include SMTP, POP3, and IMAP.

"Highest Privilege Users" means system users or user accounts that have the highest level of access rights within an information technology system, network, or application, and are capable of performing critical actions that significantly impact the security, availability, and confidentiality of the system.

"Help Desk System" means an information technology system used to receive reports, problem notifications, requests for assistance, or requests for information services from users within the Company, with systematic management of status tracking, task assignment, responses, and job closure, in order to provide users with efficient, transparent, and auditable service.

"Artificial Intelligence (AI)" means technology capable of simulating human thought processes, such as learning, decision-making, and content generation, etc.

"Public AI Tools" means AI systems made available for use by the public, such as ChatGPT, Google Gemini, and Copilot, etc.

"Sensitive Data" means data that constitutes business secrets, customer data, personal data, etc.

"Personally Identifiable Information (PII)" means data that can be used to identify a specific individual, including information that can identify a person whether used alone or in combination with other data. Examples include name, address, telephone number, email address, social security number, passport number, driver's license number, government-issued identification (tax identification number), date of birth, nationality, place of birth, etc.

"Information and Communication Technology Risk Assessment" means the process of analyzing, examining, and evaluating risks that may arise within the Company's information technology systems — such as risks from cyber attacks, network system failures, data breaches, or disruptions to information technology services in order to identify approaches for managing and mitigating potential impacts.

"Internet Protocol Address (IP Address)" means a unique number assigned to a device within a network system, used to identify and facilitate communication between various devices both inside and outside the organization, under the control of the Information Technology Department.

4. Information Technology Security Structure

To establish a management and governance framework for the Company's information security from the outset, including controls and operational practices to ensure security, the Company has defined the parties involved and their responsibilities in managing the Company's information security as follows:

4.1 Information Technology Department

(1) Define plans, goals, and operational procedures for maintaining the Company's information technology security, covering budget and personnel numbers, in alignment with the Company's strategic plan.

(2) Manage the development of information technology security operational procedures, including policies, standards, guidelines, and manuals, for operations relating to data Confidentiality, data Integrity, and system availability.

(3) Manage risk and analyze risks that may cause system problems affecting the Company's business operations.

(4) Oversee the information technology system to ensure that established measures can be implemented effectively, monitor system attacks and potential threats, and develop business continuity plans for emergency system recovery.

(5) Maintain readiness and regularly learn new techniques in information technology security.

(6) Assess information technology resource requirements and cost effectiveness and procure and develop information technology systems in alignment with the Company's strategy.

(7) Maintain the Company's information technology resources to effectively support internal operations.

4.2 Internal Units means all employees of the Company who are involved with information in any capacity.

(1) Strictly comply with information security operational procedures.

(2) Maintain the confidentiality of the Company's data and information and not disclose their own system access passwords.

(3) Report information security breach incidents and security problems when such events occur to the Information Technology Department.

(4) Use the Company's data and information assets responsibly and use data only for work they are responsible for or have been authorized to access.

4.3 External Units means external parties who come to work at or perform work for the Company and are involved in the use of the Company's data or other information assets, such as service providers, vendors, contractual counterparties, or authorized parties, by:

(1) Strictly complying with information technology security operational procedures.

(2) Maintaining the confidentiality of the Company's data and information and not disclosing their own system access passwords.

(3) Reporting information security breach incidents and security problems when such events occur to the Information Technology Department.

(4) Using the Company's data and information assets responsibly and using data only for work they are responsible for or have been authorized to access.

5. Information Technology Security Guidelines

The information technology security guidelines are divided into 11 sections as follows:

Section 1: Access and Control of Information and Information and Communication Technology System Usage

To prevent unauthorized persons from accessing data, systems, or technology resources, covering both technical and administrative aspects.

1.1 **User Access Rights Control**

(1) User access rights to systems are defined based on the responsibilities for accessing and using data of each user group.

(2) Users must submit a request in the Help Desk system and make a written request for access rights to the Information Technology Department or the assigned unit.

(3) The Information Technology Department Manager or assigned person is the approving authority, in accordance with the Standard Operating Procedure on Requesting Services from the Information Technology Department (SOP-IT-01).

1.2 User Rights Management

(1) The information technology system administrator shall define access rights to the relevant information and communication technology system appropriate to the user's service needs and responsibilities in accordance with the Company's regulations, and shall review rights regularly at least once a year, or when the Human Resources Department notifies of a transfer, change of position, resignation, or retirement, or when the user's home department submits a request to the Information Technology Department to grant or revoke usage rights, in accordance with SOP-IT-01.

(2) The system administrator must set up a new user account and password for first-time use, for the purpose of verifying the true identity of the information and communication technology system user.

(3) When a staff member resigns or changes responsibilities in a system for which access rights have been granted, the Organizational and Personnel Development Department shall immediately notify the Information Technology Department and the Office Administration Department through the personnel management system, so that the rights of the departing employee may be revoked or changed immediately upon notification.

(4) When it is necessary to grant special privileges to a user, sufficiently strict controls over such privileged users must be established, including: restricting usage to only necessary cases, defining a usage period and immediately suspending access upon expiry of that period, strictly changing the password every time after the need for use has ended, or in cases where prolonged use is necessary, changing the password every 3 months, and obtaining approval from the Information Technology Department Manager or assigned person.

(5) Users who have not been granted access rights are strictly prohibited from intruding into the information and communication technology system by any means whatsoever.

1.3 Password Management for Key System Users of the Company

(1) The system administrator shall set an initial password for users or use an automatic password generation system, and the system must not display the password on screen.

(2) The system must require users to change their password upon first login.

(3) The system administrator shall define a password change interval, and the system must maintain a password change history to prevent password reuse. For example, the SAP system within the Company requires a password change at least every 90 days.

(4) For reporting issues regarding username and password usage such as forgetting a username or password, users must contact the system administrator.

1.4 Password Usage for Users

(1) Users must use their own username and password when accessing the system to prevent repudiation of responsibility.

(2) Users who receive a password for the first time or receive a new password must change it immediately.

(3) Users must set and change their own password at least every 90 days, or in accordance with the criteria set by the system administrator and must consent to the system administrator taking any action necessary to ensure the security of the information and communication technology system.

(4) Users must keep their password confidential and take care to prevent their password from being disclosed to others, and must not give it to others for any reason whatsoever — except in the case where a user with any approval authority in the information and communication technology system is unable to perform their duties in a way that would prevent the system from continuing to operate, in which case a substitute operator shall be appointed for that period as evidence for auditing the use of access rights, and after the substitute operator has completed their tasks, the password owner must change their password immediately.

(5) Passwords must contain eight or more characters, combining regular letters, numbers, and symbols together.

(6) Passwords must not follow predictable patterns, such as "abcdef," "aaaaaa," or "123456."

(7) Passwords must not be based on information related to the user, such as name, surname, date of birth, or address.

(8) Passwords must not be dictionary words.

(9) Users must log off immediately when not using the system, to prevent other users from illicitly using their access rights to the information and communication technology system.

1.5 User Access Management

(1) Users must obtain authorization from the staff member responsible for the relevant data and system.

(2) The data owner and/or system owners shall grant users access to the system only in areas relevant to their duties and responsibilities.

(3) The system administrator is responsible for verifying approvals and setting system access rights for users. When requesting system access, the required information as specified by the Information Technology Department must be recorded, and the relevant documents must be signed and approved by the authorized data owner and/or system owner, to be retained as evidence.

(4) Registration, Staff are required to establish procedures for registering new employees, or upon transfer, change of position, resignation, or retirement within the Company. The department/user must prepare a memo and submit a request in the system as specified by the Information Technology Department, to grant or revoke various usage rights, in accordance with the Standard Operating Procedure on Requesting Services from the Information Technology Department (SOP-IT-01).

1) New users must record their information for registration in both the personnel management system and the Help Desk system.
2) In the Help Desk system, requests submitted by new users under "Request for Information Technology System Improvement and Permission to Access the SAP System" must receive approval from both the requester's supervisor and the Information Technology Department Manager.
3) The system administrator shall define access rights to the information and communication technology system in areas relevant to the user's duties and responsibilities, with approval from the authorized person, and shall review rights regularly at least once a year, or when the Human Resources Department notifies of a transfer, change of position, resignation, or retirement, or when the user's home department submits a request to the Information Technology Department to grant or revoke various usage rights.

(5) Storage and Maintenance of Usernames and Passwords for Highest Privilege User Accounts

1) The system administrator shall store usernames and passwords in sealed envelopes kept in a secure location.
2) The system administrator shall record the history of every envelope opening.

3) The envelope containing usernames and passwords shall only be opened in emergency case.

4) The system administrator must regularly verify highest privilege user accounts to ensure they remain fully functional, at least once a year, or whenever changes occur.

1.6 Communication Network Access Control

This involves controlling persons who access the communication network system, including systematic intrusion prevention, and ensuring that access to information systems is limited only to authorized services. The system administrator must design the communication network system according to the groups of information and communication technology services in use, user groups, and information technology system groups such as Internal Zone, External Zone, and DMZ Zone and must therefore establish the following security measures:

(1) The system administrator must ensure that users can access the information technology system only for services they are authorized to access.

(2) The responsible staff member must register every device used to connect to the communication network system in the Company's information asset management system.

(3) The system administrator must register and define user access rights to the communication network system in areas relevant to the user's duties and responsibilities before allowing access to the communication network system.

(4) The system administrator provides Network Management System software capable of identifying devices on the network at the level of IP Address, Computer Name, and MAC Address, and capable of generating a Network Diagram.

(5) The system administrator shall maintain a network diagram and keep it regularly updated.

(6) The system administrator shall manage the communication network as follows:

1) Separate the communication network into internal, external, and wireless networks.

2) Divide the communication network into segments/groups for access prevention and control, including public segments, internal connection segments, segments related to critical or sensitive assets, information service groups, user groups, and information technology system groups.

3) Install Gateway devices between communication networks to serve as a control mechanism for data communicated between networks.

4) Configure devices within the communication network to be capable of controlling or filtering data communicated between networks.

(7) The system administrator shall retain computer traffic data in accordance with the Computer Crime Act and other laws related to information technology, with the ability to audit historical data within a period of 1 year.

(8) The system administrator shall back up the configuration data of communication network devices.

1.7 Operating System Access Control

This involves controlling persons who access operating systems within the Company's communication network system in order to maintain the security of data and resources. The following security measures must therefore be established:

(1) Installation of Utility Programs/Software for use with the operating system:

1) Pirated or copyright-infringing software must not be installed

2) Only programs relevant to job functions must be installed, and programs unrelated to work operations must not be installed.

3) Only programs specified by the Information Technology Department must be installed, in accordance with the Standard Operating Procedure on Software Installation and Basic Computer Procurement (SOP-IT-03). For any software outside the standards set by the Information Technology Department, a request must be submitted in the Help Desk system and must receive approval from the user's supervisor, the Information Technology Department Manager, or the authorized approver.

(2) The Information Technology Department shall establish connection time limitation measures for high-risk or high-importance information and communication technology systems or applications, to ensure security. Users may connect for a maximum of 30 minutes per session, and only during the organization's business hours.

1.8 Cryptography

To ensure appropriate and effective data encryption, and to protect the confidentiality, integrity, and authenticity of information against forgery or tampering:

(1) The Company must establish a policy controlling the use of data encryption systems, taking into account the type and encryption algorithm appropriate to the level of risk that may arise with confidential or sensitive data, and must designate a person responsible for implementing the policy and managing encryption key management.

(2) The Company must establish a policy for encryption key management throughout the entire Key Management Whole Life Cycle, by defining guidelines for selecting encryption methods, determining key lengths, activating and deactivating encryption keys, and managing encryption key processes, as well as regularly monitoring compliance with such policies and guidelines.

Section 2 Entry Control of the Information Center

Data Center Management, particularly in terms of Physical Entry Controls, is critically important to maintaining the security of the Company's data and information technology infrastructure. This can be implemented in the form of Best Practices as follows:

(1) There shall be procedures for requesting permission, defining access rights, and controlling entry to the Information Center and critical areas within the Information Center.

(2) There shall be an automatic system for recording the date and time of entry and exit within the Information Center, capturing information on individuals and the times they pass through, for use in subsequent audits when necessary.

(3) Entry and exit to the Information Center and critical areas within the Information Center shall be controlled with identity cards combined with fingerprint verification, or identity cards combined with passwords, to authenticate authorized persons.

(4) The activities of external parties shall be supervised and monitored while they are working within the Information Center until their tasks are completed, to prevent loss of assets or unauthorized physical access.

(5) Persons without business or legitimate purpose shall not be permitted to enter critical areas or zones within the Information Center.

Section 3 Computer Usage

Maintaining computer security is an important part of information security within the Company. The following guidelines should be implemented:

3.1 User Practices

(1) Password setting, changing, and keeping shall be in accordance with Clause 4.1 on Password Usage for Users.

(2) Users must log off immediately when not using the information technology system, to prevent others from continuing to use the system. If there is any suspicion that a password has been compromised, the user must change it immediately.

(3) Persons who have not been granted access rights are strictly prohibited from intruding into the information technology system by any means whatsoever.

(4) Installing any software or programs on computer, installing additional network connection devices, connecting computers to networks other than the Company's network, or using personal computers with the information technology system is prohibited, unless authorized by the system administrator.

(5) File sharing on a computer is not permitted, except in cases of systems designated by the Company. If necessary, file sharing shall be limited to the duration of use and must be disabled immediately upon completion, to prevent potential damage to computer systems and data.

(6) Downloading data or programs unrelated to work operations, or from unreliable or potentially unsafe websites, is prohibited.

Section 4 Internet and Electronic Mail Usage

Maintaining security in the use of the Internet and electronic mail (Internet & Email Security) is critically important, as these are the primary channels used by malicious actors to attack and deceive users. The guidelines can be divided as follows:

4.1 Internet Usage

(1) Users must not use the internet system for purposes unrelated to work, such as streaming multimedia content, downloading files unrelated to work, or any actions that result in unnecessary consumption or occupation of network bandwidth.

(2) System administrators must configure computer network routing so that internet access is connected through security systems such as Proxy, Firewall, IPS, IDS, and Anti-Virus, etc.

(3) Personal computers, laptops, and portable computing devices must have antivirus software installed and operating system vulnerabilities patched before connecting to the internet via a web browser.

(4) Users must not use the company's internet for personal business gain, or access inappropriate websites, such as websites that are contrary to public morals, websites with content that undermines the nation, religion, or the monarchy, or websites that are harmful to society.

(5) Users will be granted access rights to information resources according to their responsibilities, in the interest of network efficiency and the company's information security, subject to approval by the system administrator.

(6) Users are prohibited from disclosing important confidential information related to the company's business that has not yet been officially announced, through the internet.

(7) Users must exercise caution when downloading software from the internet and must do so without infringing on intellectual property rights.

(8) Users must strictly comply with the Computer Crime Act.

4.2 Email Usage

(1) Users must register for an authorized username and password as a means of identity verification to access the company's email system. Each user is responsible for safeguarding their own credentials to prevent unauthorized use. Should any action constitute an offense under the Computer Crime Act, the account owner shall be held fully responsible for any resulting damage and may not deny liability.

(2) Users must use the company's email system for sending and receiving emails related to work duties. related to work duties.

(3) Users must exercise caution when using email so as not to cause damage to the company, annoyance to others, or act contrary to public morals, and must not seek personal gain with the company's email system.

(4) Users must log out of the email system immediately after each session to prevent unauthorized access by others.

(5) Users must verify the credibility of the sender every time before opening any email attachments.

(6) Users must not open or forward emails or messages received from unknown senders.

(7) Users should check their email inbox daily to avoid missing important work-related information. For the sake of organization, users should retain only necessary files and emails and should regularly archive inactive emails or files to reduce unnecessary data, enable faster email retrieval, and support efficient storage management of the email system.

(8) Users must regularly back up important data contained in emails.

Section 5 Asset and Network Management

5.1 Computer System Management

(1) Maintain an asset register in the information asset management system.

(2) Computer System Security, by:

1) Assign computer system names and IP addresses as specified by the Information Technology Department.

2) Clearly designate responsible personnel for defining, modifying, or changing various system software parameters.

3) Establish procedures or practices for auditing and verifying computer system security.

4) In case of abnormal usage or parameter changes are detected, corrective action must be taken immediately, and the responsible administrator must be notified without delay.

5) Enable only necessary services; if a required service poses a security risk, additional safeguards must be implemented.

6) Regularly install necessary patches for critical systems to close vulnerabilities in system software — such as operating systems, DBMS, and web servers.

7) Test system software for security and general performance before installation, and after any modification or maintenance.

(3) Equipment Maintenance, maintain computer system equipment to ensure efficient operation by ensuring that maintenance is carried out on schedule as specified.

5.2 Software Management

(1) Maintain a software register.

(2) Install only properly licensed software or free-use software (Freeware, Open Source), and install only what is necessary for operations — in accordance with the Standard Operating Procedure on Software Installation and Basic Computer Procurement (SOP-IT-03).

5.3 Communication Network System Management

(1) Implement network segmentation by VLAN / Zone.

(2) Maintain a register for communication network system usage.

(3) Develop network diagrams and define the scope of the communication network system.

(4) Monitor communication network usage to ensure efficient operation.

(5) Control routing on the communication network and define access methods to the company's network.

(6) Implement an intrusion detection and prevention system to guard against abnormal network activity.

(7) Conduct penetration testing on the communication network and produce attack/incident reports.

(8) Designate responsible personnel for defining, modifying, or changing parameters of the communication network system and connected devices.

(9) Review parameter configurations at least once per year.

(10) Perform maintenance on the communication network system to ensure efficient operation, by ensuring that network maintenance is carried out on schedule as specified.

5.4 Asset Management

(1) Maintain an Asset Register

1) Designate a responsible owner for each asset.

2) Classify assets into categories.

3) Define computer standards for the company.

(2) Requisition of Computer and Network Assets

1) Any user wishing to requisition an asset must submit a request in the Help Desk system under "Request for IT System Usage", specifying the computer asset requested, the intended storage or installation location, along with all relevant details. The request must be reviewed and approved by the user's supervisor within the system and then verified by the IT Department Manager in accordance with the Standard Operating Procedure on Requesting Services from the IT Department (SOP-IT-01).

2) The responsible officer evaluates the requisition request according to established procedures and appropriateness and seeks approval from the management of the asset-owning department, or from a designated representative.

3) Once the request is approved, the responsible officer must record the new storage or installation location of the asset in the IT Asset Management System and register it in the Computer and Communication Network Asset Register to be retained as part of the company's asset history.

(3) Reporting Computer and Network Asset Repairs and Maintenance

1) When a user encounters abnormal asset behavior or is unable to use an asset for operational purposes, the user must submit a maintenance request by entering the asset details into the Help Desk system under "Submit a Request — Repair / Service", in accordance with the Standard Operating Procedure on Requesting Services from the IT Department (SOP-IT-01). The responsible officer analyzes the fault based on information from the Help Desk system and through hands-on testing also reviews supporting information — particularly the asset's warranty status. If the asset is still under warranty, it may be sent for repair at the manufacturer's authorized service center at no cost for items covered under the warranty. If the asset is no longer under warranty, the responsible officer must assess the extent of the damage, if repairable, corrective action should be taken; if severely damaged, disposal of the asset may be necessary.

2) While the asset is being sent for repair, if a replacement asset is available, the responsible officer must notify the user accordingly.

3) After the damaged asset has been repaired, the responsible officer must re-test the previously affected area before returning the asset to the user. The officer must also record the maintenance and testing details in the Help Desk system prior to returning the asset.

4) The user must inspect the returned asset, and if the original or any new issues are found, the user must promptly notify the responsible officer so that corrective action can be taken through the appropriate process.

(4) Audit & Inventory, Information assets should be audited and inventoried in coordination with the Accounting Department or relevant departments at least once per year.

5.5 Media Handling Policy

To prevent potential damage to the company's data storage media through unauthorized disclosure, modification, transfer, deletion, or destruction of data.

(1) Management procedures for removable storage media must be established and must align with the company's defined information classification methods or procedures. Storage media containing data must be protected against unauthorized access, misuse, or damage during transfer or transport. Usage procedures and access rights for storage media must be clearly defined. It is noted that the company does not have a policy permitting system users to use removable storage media.

(2) If the use of removable storage media is necessary, relevant parties must be notified, and approval must be obtained from the user's supervisor and the IT Department Manager — in order to maintain a usage history record.

5.6 Use of Storage Media and File Sharing via Share File Systems

To establish guidelines for the use of file storage and sharing systems (Share File) — such as Microsoft SharePoint, Microsoft OneDrive, and internal Share Drive systems — in order to ensure security, privacy, and effective collaboration.

(1) Access and Usage

1) Users must log into the system using only accounts authorized by the IT Department.

2) Access rights must be restricted based on the Least Privilege principle, granting access only to those who require the data.

3) Sharing links or files configured for "Anyone with the link" access is strictly prohibited.

(2) File Storage

1) Files should be stored in folders designated by department or project.

2) Uploading files containing personally identifiable information (PII) or sensitive data such as national ID numbers or bank account numbers — without encryption or protective measures is strictly prohibited.

3) Storing pirated software or any files that violate applicable laws is strictly prohibited.

4) Storage space allocation shall be determined and managed by the IT Department.

(3) File Sharing

1) Files should be shared using "View Only" permissions unless editing access is required.

2) If sharing data with external parties is necessary, approval from the department head must be obtained beforehand.

3) Password protection or expiration dates should always be applied when sharing files, both internally and externally, where the system supports it.

(4) Data Backup and Recovery

1) The SharePoint system performs automatic backups. The IT Department is responsible for data recovery when necessary. Users may submit a request through the Help Desk system in accordance with the Standard Operating Procedure on Requesting Services from the IT Department (SOP-IT-01).

2) Users should avoid permanently deleting files unless necessary.

Section 6 Operational Security Controls

6.1 A job schedule should be established, outlining the sequence and order of tasks for submitting jobs to be processed by computer systems, as well as procedures for handling errors that occur (Job Schedule). The job schedule should be tested to verify that tasks are executed in the defined sequence as specified.

6.2 Roles and responsibilities should be defined for personnel responsible for carrying out operations and/or individuals involved in various operational steps, as well as those with approval authority.

Section 7 Data Backup and Recovery

To ensure that information and information processing equipment operate correctly and securely, and to prevent data loss:

7.1 A data storage and backup system must be maintained for each type of data — including operating system software, application software, command sets, and data — with at least one backup copy stored at a separate location, to ensure security and operational continuity. This must be carried out in accordance with the Standard Operating Procedure on Data Backup and Recovery (SOP-IT-02) of the IT Department.

7.2 Responsible personnel must be designated for data backup, and the accuracy and completeness of the backed-up data must be verified at least once per year, with detailed inspection records maintained. In case of data loss or incomplete data is discovered, corrective action must be taken immediately to restore the data to a complete and accurate state.

7.3 Define the backup frequency for each system and perform backups accordingly (systems with frequent changes should be backed up more often). At least one backup copy must be stored off-site.

(1) Establish correct procedures for data backup and recovery, including software backup.

(2) Verify that each backup has completed successfully and in full.

(3) Test the restoration of backed-up data at least once per year, including testing whether all systems are fully operational following recovery.

7.4 Develop an emergency preparedness plan to enable system recovery within a defined timeframe, with guidelines for disaster recovery, as follows:

(1) Compile a complete inventory of all critical systems within the company, and keep it regularly updated to reflect any changes or newly identified critical systems.

(2) Conduct risk assessments for those critical systems, define measures to mitigate identified risks, and update the risk assessment report at least once per year.

(3) Define the types of data involved such as system-related software and database records. Define the backup frequency and backup method such as Full Backup or Incremental Backup for each critical system.

(4) Develop a disaster recovery plan to address potential disasters.

(5) The plan must include the following details:

1) Definition of roles and responsibilities for all relevant personnel.

2) Risk assessment for critical systems and the definition of mitigation measures covering scenarios such as extended power outages, fire, earthquakes, or civil unrest that may prevent access to systems.

3) Defined procedures for system recovery.

4) Defined procedures for data backup and restoration testing.

5) Testing of the preparedness plan and its effectiveness at least once per year.

6) Defined communication channels with external service providers such as network, hardware, and software vendors.

7) Awareness-raising and training for all relevant personnel on the procedures and actions required during an emergency.

(6) The recovery plan must be reviewed at least once per year.

(7) Perform data backups according to the defined types, frequencies, and methods, and regularly verify that all backed-up data is complete and intact.

(8) Conduct restoration testing of backed-up data at least once per year. If any issues are encountered during recovery, corrective action must be taken and the details of the problem along with the resolution must be documented in writing.

Section 8 Information and Communication Technology Systems Risk Assessment

The Information and Communication Technology Risk Assessment aim to identify, analyze, and evaluate the level of risk that may affect information resources, to establish appropriate risk management and mitigation strategies. The risk assessment guidelines can be summarized as follows:

8.1 An Information Technology Risk Management Working Group shall be established to carry out the following:

(1) Prioritize risks

(2) Develop a risk management plan

(3) Implement the risk management plan

8.2 An inspection and risk assessment of information technology security and computer systems shall be conducted at least once per year.

8.3 The results of the inspection and risk assessment shall be reported to the responsible personnel and relevant departments, and improvements shall be made promptly in accordance with the recommendations of those responsible departments.

8.4 Responsibilities shall be assigned to users and management, holding them accountable in the event of damage or harm arising from their negligence or failure to comply with the Information Technology Security Policy and Information Technology Security Practices, as the case may be.

Section 9 Information Technology Security Awareness Promotion

To foster an organizational culture that prioritizes data security and reduces risks arising from negligence or lack of knowledge among users, with the primary goal of ensuring that personnel at all levels within the organization are able to follow these guidelines:

9.1 Awareness campaigns and training shall be conducted to ensure that company staff are informed, understand, and do not commit offenses under the Computer Crime Act and other laws related to information technology. Staff shall also be responsible for the appropriate use of the company's information technology resources. Training shall be organized at least once per year.

9.2 The Information Technology Security Policy and Information Technology Security Practices shall be reviewed and updated to remain current and in line with accepted standards at least once per year.

Section 10 Systems Acquisition, Development and Maintenance

10.1 Information Security Requirements Analysis and Specification, to ensure that information security is integrated into IT systems throughout the entire system development lifecycle, including security requirements for services delivered over public networks.

(1) Security requirements must be clearly defined for any system being developed, procured, or enhanced. The IT department responsible for system oversight must analyze the IT systems to identify risks that could lead to data damage or loss, with a focus on the following areas:

1) Pre-incident measures such as data backups and redundant network systems.

2) Post-incident measures such as data recovery plans and defined recovery periods.

(2) Securing Application Services on Public Networks and Information related to application services transmitted over public networks must be protected against unauthorized access, disclosure, or modification.

(3) Protecting Application Services Transactions and Information related to application service transactions must be protected against incomplete data transmission, misrouted data, unauthorized message alteration, unauthorized data disclosure, and unauthorized data replay.

10.2 Security in Development and Support Processes

To ensure that IT systems are secure throughout the entire information system development lifecycle, under a Secure Development Policy.

(1) Establish criteria for software development and ensure compliance with the company's defined procedures and requirements. For example, software development should incorporate security considerations at every stage of the development process, and developers should be capable of identifying and avoiding vulnerabilities in the software they develop, as well as remediating any discovered vulnerabilities.

(2) System Change Control Procedures, IT system developers must have a process in place to control software modifications for IT systems that are already in production or in active service. For example:

1) Change requests must originate only from authorized personnel.
2) Approval from authorized management must be obtained before proceeding.
3) Potential side effects following any modification must be monitored and controlled.
4) Upon completion, all changes must pass acceptance review by an authorized approver or end user.

(3) Technical Review of Applications After Operating Platform Changes — When an operating system is modified or upgraded, IT system developers must review and test all relevant software to confirm there is no impact on functionality or security.

(4) Restrictions on Changes to Software Packages, when using off-the-shelf software, changes must be controlled to the minimum necessary. All changes must be tested and documented so they can be referenced during future software updates.

(5) Secure System Engineering Principles, to ensure engineering-level security, principles must be formally documented, continuously updated, and applied to system development work. The Security Committee is responsible for overseeing security in relation to the office infrastructure.

(6) Outsourced Development, Contracts for outsourced system development must be clear and comprehensive, covering software copyright, system usage rights, detailed system review prior to go-live, quality assurance, and the defined scope of the development engagement.

(7) System Security Testing, any program or system that has been developed should have its security features tested. Testing must be conducted throughout the development process. For System/User Acceptance Testing, a test plan and relevant acceptance criteria must be prepared and documented covering both new systems and upgraded systems.

10.3 Test Data Policy

To ensure the protection of data used in testing.

(1) Separation of Development, Testing, and Operational Environments.

1) Development, testing, and operational environments must be clearly separated to reduce the risk of unauthorized access to or modification of the live production system.

2) During system development, the Development System must be clearly separated from the Production System.

3) Clear procedures must be defined for migrating completed programs to the production system.

4) Compilers or other development tools must not be installed on any Production System.

(2) Protection of Test Data, any real data intended for use in system testing must first be authorized by the data custodian responsible for that data. Once testing is complete, all real data must be immediately deleted from the test environment. A record must be maintained as evidence of what real data was used in testing, including the date, time, and department involved, and the data custodian must be notified accordingly.

Section 11 Artificial Intelligence Usage

To establish secure practices for the use of Artificial Intelligence (AI) technology within the company, to prevent risks related to information security, legal violations, and ethical concerns with particular emphasis on preventing data leakage, damage to the company, and reputational harm.

11.1 Procedures, to ensure that the use of AI technology within the company is appropriate, secure, and compliant with applicable laws as well as business ethics, the company establishes the following operational procedures:

(1) Process Approval for new AI tools

1) Any employee wishing to use a new AI tool must submit a request through their supervisor, clearly stating the purpose and nature of the intended use, via the Help Desk system in accordance with the Standard Operating Procedure on Requesting Services from the IT Department (SOP-IT-01).

2) The supervisor will forward the request to the IT Department or the Risk Management Department for evaluation of its appropriateness and risk assessment.

3) Once approved, the employee may proceed to use the AI tool in accordance with the stated purpose.

(2) Permitted Use Guidelines, the company permits the use of AI in the following circumstances:

1) To enhance work efficiency such as drafting documents, preparing preliminary report summaries, translating languages, or performing general data analysis.

2) For use only with non-confidential or general information (Public / Non-Sensitive Data) that does not involve the company's internal data or any sensitive information.

3) Through AI systems or tools that have been reviewed and approved by the IT Department or an appropriately authorized department.

(3) Prohibited Use Guidelines, to prevent legal and ethical risks, the use of AI is strictly prohibited in the following circumstances:

1) Entering, transmitting, or disclosing the company's internal data such as financial data, customer data, employee data, or unpublished project information through any AI system not under the company's control.

2) Using AI to communicate on behalf of the company, or to carry out any form of communication with external parties without formal authorization.

3) Copying, generating, or distributing copyright-infringing content using AI tools without proper attribution or permission from the copyright owner.

4) Using AI to analyze or make decisions in place of a human on sensitive matters or those affecting individuals such as recruitment, performance evaluation, or disciplinary action unless strictly reviewed by authorized personnel and carried out in full compliance with the company's established procedures.

11.2 AI Training and Awareness Programs

(1) Organize training and promote awareness of ethical AI usage among employees.

(2) Coordinate with the IT Department and management to integrate AI usage with personnel policies.

6. Penalties

The company shall impose disciplinary action against any person who violates or disregards violations of the Information Technology Security Policy and/or Information Technology Security Practices and shall be subject to penalties as prescribed by law (if applicable).

These Information Technology Security Practices have been approved by a resolution of the Corporate Governance and Risk Management Committee Meeting No. 1 (Board #11) on 27 August 2025, and shall come into effect from 19 September 2025 onwards, superseding the Information Security Practices that came into effect on 28 August 2024, which were approved by the Corporate Governance and Risk Management Committee Meeting No. 1 (Board #10) on 4 July 2024.

Atchaka Sibunruang

(Mrs. Atchaka Sibunruang)

Chairman of Corporate Governance and Risk Management