(Translation)

Information Security Guidelines
Saha Pathana Inter-Holding Public Company Limited
(2nd Revised Edition)

1. Introduction

The Company's information and communication technology systems are essential for providing services to the Board of Directors, executives, employees, and authorized external parties. Therefore, to ensure that electronic transactions, operations, and management are conducted appropriately, efficiently, securely, reliably, and with continuity, the Company has established the Information Technology Security Policy and Information Security Guidelines as a framework for proper implementation.

2. Objective

2.1 To ensure that the Company's information and communication technology systems are stable, secure, continuously operational, and efficient, resulting in accurate and reliable transactions in compliance with electronic transaction security standards.

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

2.3 To prevent system users and related persons from committing offenses under the Computer-Related Crime Act and other laws related to information technology.

3. Definitions

The definitions used in this guideline include:

"The Company" refers to Saha Pathana Inter-Holding Public Company Limited.

"User" refers to authorized persons to access, manage, or maintain the Company's information and communication technology systems with rights and duties as determined by the Company.

"Executive" refers to the Company's executives.

"System Administrator" refers to information technology managers or responsible persons for managing and overseeing the information technology and communication systems of the Company.

"Officer" refers to persons who are employed by the Company.

"Assets" refer to the Company's computer data, computer systems, and information and communication technology assets, such as network equipment and legally acquired software purchased by the Company for proper use.

"Access to or Control the Information Usage" refers to the management and restriction of user rights to the Company's information and communication technology systems related to services and data, based on operational necessity, including safeguards against unauthorized access to the systems by both internal and external parties.

"Information Security" refers to maintaining confidentiality, accuracy, and readiness of data within the Company's information and communication technology systems.

"Security Incidents" refer to events affecting the Company's information and communication technology systems or suspected vulnerabilities that could potentially cause damage, resulting in violations of the Company's Information Technology Security Policies. Examples include granting unauthorized access to systems, failing to set system access passwords, disclosing confidential documents to external parties, malware infections, network intrusions, or unauthorized disclosure of sensitive information.

"Undesirable or Unforeseen Security Situations" refer to incidents that system administrators neither intend nor anticipate, which cause harm to the Company's information and communication technology systems. Examples include malware infections, software malfunctions or errors, network intrusions, unauthorized alteration or loss of critical data, website defacement, unauthorized disclosure of sensitive information, denial-of-service (DoS) attacks, disruptions to computer and network systems, or any other events that violate the Company's information technology security policies.

"Information Technology Department" refers to the department and/or persons responsible for managing the Company's information technology systems and computer systems, which serves as the central hub for the Company's information technology network, focusing on the study and analysis required to develop the Company's information systems and computer systems and collaborating with or supporting the operations of other related departments.

"Computer Data" refers to data, text, commands, sets of commands, or any other items stored in a computer system in a form that can be processed by the system, including electronic data as defined by the electronic transactions law.

"Information Center" refers to the server room, backup room, control room, network room, and the air conditioning system.

"Computer System" refers to a computer device or a set of interconnected devices that operate according to specified commands, sets of commands, or other instructions and procedures, enabling the device or set of devices to automatically process data.

"Communication Network" refers to a system facilitating communication, connection, or data exchange between the Company's various information technology systems. The connection may be established via wired or wireless means. Communication networks include Local Area Networks (LAN), Wide Area Networks (WAN), Intranet, and Internet systems.

"Local Area Network (LAN)" refers to a network that connects devices within a limited geographical area.

"Wide Area Network (WAN)" refers to a network that connects devices across geographically-distant locations.

"Intranet" refers to an internal communication network connecting various computer systems within the organization, designed for internal communication and information sharing purposes.

"Internet" refers to a communication network linking the Company's computer systems to the global internet infrastructure.

"Information" refers to processed, organized data presented in formats such as numbers, text, or graphics, designed to be easily understood and utilized for management, planning, decision-making, and other purposes.

"Information and Communication Technology System" refers to the Company's system comprising computer systems, databases, communication networks, system users, system developers, system administrators, and executives working collaboratively to set objectives, gather and store data, process information, and deliver results or information for operational, planning, decision-making, management, analysis, and performance monitoring purposes across different organizational levels.

"Password" refers to a combination of characters, symbols, or numbers used to verify user identity and control access to information and Information and Communication Technology System, thereby ensuring the security and protection of data.

"Information Security" refers to the measures taken to safeguard the Company's information and communication technology systems. It encompasses three fundamental principles:

(1) Confidentiality: Ensuring that information is kept secret and accessible only to those who have the appropriate authority.

(2) Integrity: Guaranteeing that data remains accurate and unaltered, whether any changes are intentional or not.

(3) Availability: Ensuring that information and INFORMATION AND COMMUNICATION TECHNOLOGY systems are accessible and available when required for usage.

"Malware" refers to malicious code that can cause damage, destruction, alteration, or disruption to the Company's information and communication technology systems, or lead to system malfunctions that deviate from intended operations.

"Electronic Mail (E-mail)" refers to a system that allows individuals to send and receive messages through computers and the connected communication networks. The transmitted data may include text, photos, graphics, animations, and audio. The senders can send messages to a single recipient or multiple recipients. Common protocols for this type of communication include SMTP, POP3, or IMAP.

4. Information Technology (IT) Security Infrastructure

To establish a comprehensive framework for managing the Company's information security from the outset-covering both operational controls and security measures, the Company has designated key persons and defined their roles and responsibilities in managing information security as follows:

4.1 Information Technology (IT) Department

(1) Developing plans, goals, and operational guidelines for the Company's IT security, including budget and personnel headcounts considerations, to align with the Company's strategic plan.

(2) Developing the security protocols, including policies, standards, guidelines, and manuals to ensure data confidentiality, integrity, and system availability.

(3) Conducting risk management and analysis to identify potential threats that may impact Company's operations.

(4) Supervising and monitoring IT systems to ensure effective implementation of security measures, while managing surveillance against potential system attacks and threats to the IT systems and preparing business continuity plans for emergency recovery.

(5) Maintaining readiness by staying informed on emerging information security techniques and threats and providing regular training to prepare personnel for potential emergencies.

(6) Assessing IT resource requirements, ensuring cost-effectiveness, and supporting the procurement and development of systems that are aligned with the Company strategies.

(7) Overseeing information resource management to enhance the efficiency of internal operations.

4.2 Internal Department refers to all employees in the organization that are related to the information one way or another.

(1) Conducting and operating under the IT security guidelines.

(2) Maintaining the confidentiality of Company information and not disclosing passwords for system access.

(3) Reporting incidents of information security breaches and issues to the IT department.

(4) Using data and information assets of the Company responsibly and using them only for the purpose of his/her own responsibilities or as authorized.

4.3 External Stakeholders refers to those who operate in or work for the Company, and use Company's data or information assets, such as service providers/vendors, contractors, or authorized parties.

(1) Conducting and operating under the IT security guidelines.

(2) Maintaining the confidentiality of Company information and not disclosing passwords for system access.

(3) Reporting incidents of information security breaches and issues to the IT department.

(4) Using data and information assets of the Company responsibly and using them only for the purpose of his/her own responsibilities or as authorized.

5. Information Security Guidelines

5.1 Ensuring Security for Access and Control of Information and Communication Technology Systems

5.1.1 User Access Control

(1) Defining system access rights for users by considering roles, responsibilities, and information usage levels for each user group.

(2) Requiring users to submit a written request to the IT department or a responsible party.

(3) Approval of information usage is authorized by the IT department manager or a responsible party.

5.1.2 User Access Rights Management

(1) The IT administrator shall assign access rights to the Information and Communication Technology systems in accordance with the user's service requirements and responsibilities, as stipulated by Company's regulations. These rights shall be reviewed regularly, at least once a year, or upon notification from the Human Resources department regarding transfers, changes in job positions, resignations, retirements, or upon request from the originating department to the IT department for granting or revoking access rights.

(2) The IT administrator must establish access rights to new user accounts and passwords for initial use and verifying the actual identity of users accessing the INFORMATION AND COMMUNICATION TECHNOLOGY systems.

(3) When an employee leaves the Company or changes their responsibilities within the system for which access rights were granted, the Human Resources department must immediately notify the IT department to revoke the departing employee's access rights or adjust the access rights accordingly upon notification.

(4) In cases where it is necessary to grant special privileges to users, there must be stringent control measures in place. This includes restricting usage to essential cases only, setting usage time limits, and immediately suspending access once the specified period has expired. Passwords must be changed rigorously after each period of necessity, or every three months for prolonged usage, with approval from the IT manager or an authorized party.

(5) Unauthorized users are strictly prohibited from accessing the Information and Communication systems by any means.

5.1.3 User Password Management

(1) The system administrator shall assign initial passwords to users or utilize an automatic password generation system. The system must ensure that passwords are not displayed on the screen.

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

(3) The system administrator shall set a password change interval and ensure the system records the password change history to prevent reuse. For instance, the Company's SAP system requires password changes at least every 90 days.

(4) For issues related to usernames and passwords, such as forgotten credentials, users should contact the system administrator.

5.1.4 User Password Usage

(1) Users must utilize their own usernames and passwords to access the system to prevent denial of responsibility.

(2) Users who receive an initial or new password must change it immediately upon receipt.

(3) Users are required to set and change their passwords at least every 90 days, or as per the guidelines set by the system administrator. They must also consent to any actions taken by the system administrator to ensure the security of the Information and Communication Technology systems.

(4) Users must keep their passwords confidential and take precautions to prevent their passwords from being leaked to others. They must not share their passwords under any circumstances, except in cases where an authorized user is unable to perform their duties, which would otherwise disrupt the operation of the Information and Communication Technology systems. In such cases, a temporary replacement should be appointed, and the original user must change their password immediately after the replacement's task is completed.

(5) Passwords must be at least 8 characters long and include a mix of uppercase letters, numbers, and symbols.

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

(7) Passwords should not be related to the user, such as names, birthdates, or addresses.

(8) Passwords should not be dictionary words.

(9) Users must log off immediately when not using the system to prevent unauthorized access by others.

5.1.5 User Access Management

(1) Users must obtain authorization from the responsible officer with authority to manage data and system.

(2) Data and/or system owners will grant users access only to the areas relevant to their duties and responsibilities.

(3) The system administrator is responsible for verifying approvals and assigning access rights to users. Requests for system access must be documented and submitted using forms specified by the IT department, with the necessary approvals from the data and/or system owners, to be kept as records.

(4) Staff registration procedures must be established for new hires, transfers, job changes, resignations, or retirements within the Company. Departments/users must document, and complete forms as specified by the IT department to grant or revoke access rights.

1) New users must record their information and submit a **"System Access Request"** form.
2) The **"System Access Request"** form submitted by new users must be approved by their supervisor and the IT manager.
3) The IT administrator shall assign access rights to the Information and Communication Technology systems in accordance with the user's service requirements and responsibilities, as stipulated by Company's regulations. These rights shall be reviewed regularly, at least once a year, or upon

notification from the Human Resources department regarding transfers, changes in job positions, resignations, retirements, or upon request from the originating department to the IT department for granting or revoking access rights.

(5) Management of usernames and passwords for highest privilege users:

1) The system administrator shall store usernames and passwords in sealed envelopes in a secure location.

2) The system administrator shall record the history of each envelope opening.

3) Envelopes containing usernames and passwords may only be opened in emergency situations.

4) The system administrator must regularly review the accounts of highest privilege users to ensure they can access the system as usual, at least once a year or upon any changes.

5.1.6 Network Access Control

This involves controlling individuals accessing the communication network, systematically preventing intrusions, and ensuring access to information systems is limited to authorized services only. The system administrator must design the communication network based on the groups of information and communication technology services in use, user groups, and information system groups, such as Internal Zone, External Zone, and DMZ Zone. The following security measures must be established as follows:

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

(2) Responsible officers must register all devices used to connect to the communication network in the Company's information asset management system.

(3) The system administrator must assign user access rights to the communication network relevant to their duties and responsibilities before they begin using the network.

(4) The system administrator must provide software for managing and controlling the network (Network Management System), which can identify devices on the network down to the IP address, computer name, and MAC address, and create a network diagram.

(5) The system administrator must create and regularly update the network diagram.

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

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

2) Segmenting the network/group to prevent and control access, including public areas, internal connections, critical or hazardous assets, information service groups, user groups, and information system groups.

3) Installing gateway devices between networks to control data communication between them.

4) Configure network devices to control or filter data communication between networks.

(7) The system administrator must store computer traffic data in accordance with the Computer-Related Crime Act and other relevant information technology laws.

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

5.1.7 Operating System Access Control

This involves controlling individuals accessing the operating system within the Company's communication network to ensure the safety of data and resources. The following security measures must be established:

(1) Installation of utility programs/software for use with the operating system:

1) Unauthorized/copyright infringement software must not be installed.

2) Software installations must be Company's mission-related and not include programs that are unrelated to work duties.

(2) The IT department shall establish measures to limit connection time for the Information and Communication Technology systems or applications that are high-risk or critically important. To ensure security, these are the measures:

Setting connection time limits for high-risk or critically important Information and Communication Technology system or applications, allowing users to access them for a maximum of 30 minutes per connection, only during working hours.

5.1.8 Cryptography

To ensure appropriate and effective data encryption, and to protect confidentiality, integrity, and authenticity of information:

(1) The Company must establish a policy for the use of encryption systems, considering the type and algorithm of encryption that aligns with the risk level associated with confidential or critical information. This policy should also define a responsible party for implementing the policy and managing encryption keys (key management).

(2) The Company must have a cryptographic key management policy throughout the entire lifecycle of the encryption keys. The policy should outline procedures for selecting encryption methods, determining key lengths, using and retiring encryption keys, managing the key lifecycle, along with ensuring compliance with the policy and guidelines on a regular basis.

5.2 Information Center Management with Physical Entry Controls as follows:

(1) Establishing procedures for authorization requests, defining access rights, and controlling entry to the information center and critical areas within it.

(2) Implementing an automated system to record the date and time of entry and exit, capturing individual identities and times for later verification if necessary.

(3) Controlling access to the information center and critical areas within it using ID cards and fingerprints, or ID cards and passwords, to verify the identity of authorized persons.

(4) Supervising and monitoring the activities of external personnel while they are working in the information center until their tasks are completed, to prevent asset loss or unauthorized physical access.

(5) Prohibiting unauthorized individuals from entering critical areas or zones within the information center.

5.3 Maintaining Security in Computer Usage

5.3.1 User Operations

(1) Passwords must be set, changed, and stored in accordance with Section 4.1.4 regarding Password Usage for Users.

(2) Users must log off immediately when not using the IT system to prevent others from using the system. If there is any suspicion of password leakage, the user must change the password immediately.

(3) Unauthorized individuals are prohibited from accessing the IT system by any means.

(4) It is prohibited to install any software or programs on work computers, install additional network connection devices, connect work computers to networks other than the Company's network, or use personal computers with the IT system without permission from the system administrator.

(5) File sharing on work computers is not allowed, except for the work systems designated by the Company. If necessary, a specific time period must be set, and file sharing must be canceled immediately after use to prevent potential damage to the computer system and data.

(6) Do not download data or programs unrelated to work or from websites that are unreliable or uncertain of their safety.

5.4 Maintaining Security in Internet and Email Usage

5.4.1 Internet Usage

(1) Users must not use the internet system for multimedia data usage or downloading data unrelated to work and occupying communication bandwidth.

(2) The system administrator must configure the connection routes of the computer system for internet access through security systems such as Proxy, Firewall, IPS, IDS, etc.

(3) Personal computers, portable computers, and portable computing devices, before connecting to the internet through a web browser, must have antivirus software installed and must patch vulnerabilities of the operating system where the web browser is installed.

(4) Users must not use the Company's internet for personal business purposes or access inappropriate websites, such as immoral websites, websites with content opposing the nation, religion, or the King, or websites harmful to society.

(5) Users will be assigned access rights to resources based on their responsibilities to ensure network efficiency and the Company data security, with approval from the system administrator.

(6) Users are prohibited from disclosing important confidential work-related information of the Company that has not been officially announced through the internet.

(7) Users must exercise caution when downloading application programs from the internet, ensuring that it does not infringe on intellectual property rights.

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

5.4.2 Email Usage

(1) Users must register to obtain usage rights and a password as a tool for verifying their identity when accessing the Company's email system. Each user must manage and protect their usage rights, and password to prevent others from using them. If any actions are taken that violate the Computer-Related Crime Act, the rights owner is responsible for the resulting damage and cannot deny responsibility.

(2) Users must use the Company's email system to send and receive emails related to work.

(3) Users must exercise caution in using email to avoid causing harm to the Company, creating annoyance to others, violating morality, or seeking personal benefits from using the Company's email system.

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

(5) Before opening attachments from emails, users must always use antivirus programs to scan the attachments.

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

(7) Users must check their email inbox daily and should keep their files and emails to a minimum.

(8) Users must regularly back up important information in their emails.

5.5 Maintaining Security in Asset and Network Management

5.5.1 Computer System Management

(1) Establishing an asset registry in the information asset management system.

(2) Maintain computer system security by

1) Assigning names and IP addresses in the computer system.
2) Clearly designating individuals responsible for setting, modifying, or changing various program system parameters.
3) Establishing procedures or methods for verifying computer system security.
4) In cases where abnormal usage or changes in parameter settings are detected, corrective actions must be taken, and the responsible administrator must be notified immediately.
5) In cases where abnormal usage or changes in parameter settings are detected, corrective actions must be taken, and the responsible administrator must be notified immediately.
6) Installing essential patches for critical work systems regularly to address vulnerabilities in system software such as operating systems, DBMS, and web servers.
7) Testing system software for security and overall performance before installation and after modifications or maintenance.

(3) Maintaining equipment in the computer system to ensure efficient operation by monitoring and adhering to scheduled maintenance intervals.

5.5.2 Program Management

(1) Establish a registry of programs

(2) Install programs that are properly licensed or free for use (Freeware, Open Source) and install only what is necessary for operations.

5.5.3 Communication Network Management

(1) Divide networks/groups (VLAN / Zone).

(2) Maintain a registry of network communication usage.

(3) Create diagrams and define the boundaries of the network communication system.

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

(5) Control routing on the communication network and set access methods for the Company's communication network.

(6) Establish a defense system to prevent intrusions and abnormal usage through the communication network.

(7) Test for communication network attacks and establish attack reports.

(8) Assign individuals responsible for setting, modifying, or changing communication network system parameters and connected devices.

(9) Review parameter settings at least once a year.

(10) Maintain the communication network system to ensure efficient operation by monitoring and adhering to scheduled maintenance intervals.

5.5.4 Asset Management

(1) Establishing an asset registry

1) Assign individuals responsible for the assets

2) Categorize the assets

(2) Requesting usage of Computer and Network Assets

1) Users who wish to request usage of assets must fill out the information in the "**Request for Usage of Computer and Network Assets**" form, specifying the list of assets to be used, including the storage or installation location, and submit it to the responsible officer for consideration and approval.

2) The responsible officer reviews the request according to procedures and the appropriateness of the asset usage request, seeking approval from the department head who owns the assets or the designated representative.

3) Once the asset usage is approved, the responsible officer must record the new storage or installation location of the asset in the "Computer and Network Asset Registry" form to maintain the asset history.

(3) Maintenance Reporting for Computer and Network Assets

1) When users detect abnormal operation of assets or are unable to use the assets for operations, they must report the issue for maintenance by filling in the **"Maintenance Request"** form with the relevant asset information.

2) The responsible officer analyzes the damage to the assets based on the information provided in the **"Maintenance Request"** form and their own testing. The officer also considers supporting information, especially the warranty period of the asset. If the asset is under warranty, the officer can send it to the manufacturer's service center for repair at no cost for items covered under the warranty. If the asset is no longer under warranty, the officer evaluates the damage and proceeds with repairs if feasible. If the damage is severe, the asset may need to be disposed of.

3) While the responsible officer sends the asset for maintenance, if there is another asset available that can replace the one being repaired, the officer must notify the user. The user is required to submit a usage request form by filling out the "Request for Usage of Computer and Network Assets" form, specifying the assets they wish to use, including the storage or installation location, and submit it to the responsible officer for approval. The office in charge of the asset registry must then record the information of the new asset in the **"Computer and Network Asset Registry"** form to update the Company's asset history.

4) After the damaged asset has been repaired, the responsible officer tests the previously damaged parts again before returning the asset to the user. The officer records the maintenance and testing details in the "Maintenance Request" form and then hands over the asset to the user.

5) The user inspects the asset upon return. If the asset functions normally, they sign to acknowledge receipt to reclaim the asset for operations. If the damage is detected on the original part or any new parts, the user must promptly notify the responsible officer for further maintenance.

(4) Taking company assets off-site must have permission recorded before taking equipment or assets off-site to serve as evidence for preventing loss, as well as record additional information when the equipment is returned.

(5) Disposal of Computer and Network asset

1) In cases where assets are damaged beyond repair, are out of warranty, and when considering the asset's value against repair costs, it is necessary to proceed with the disposal of the asset. The responsible officer must record the asset details in the **"Return of Computer and Network Assets"** form and notify the

task owner/project owner, who is the user or procurer of the asset, for acknowledgment and approval.

2) The task owner/project owner reviews the return of the asset. If they approve, they must sign the "Return of Computer and Network Assets" form. If they do not approve, they must state the reasons and return the matter to the responsible officer.

3) Submit the matter to the authorized department for approval to proceed with the disposal of the asset.

5.6 Controlling Operation Security

5.6.1 A job schedule should be created, prioritizing the order of tasks for processing into the computer and managing any errors that occur. The job schedule should also be tested to ensure that the tasks follow the defined order.

5.6.2 Roles and responsibilities of individuals responsible for operations and/or those involved in various stages of operations, including those, should be defined with approval of the authorized individual.

5.7 Maintaining Security of Data Backup and Recovery

5.7.1 There is a system for storing and backing up data according to the type of data, including operating system programs, application programs or applications software, scripts, and data, at least one set stored separately in a different location to ensure security and continuous usability.

5.7.2 Assign responsible individuals for data backups, verify the accuracy and completeness of the data at least once a year, and record the details of the verification. In cases where data is found to be missing or incomplete, corrections must be made immediately to ensure the data is accurate and complete.

5.7.3 Set intervals of data backups for systems and perform backups according to the specified intervals (systems that change frequently should have increased backup frequency). At least one set of backed-up data must be stored off-site.

(1) Establish procedures for performing data backups and data recovery correctly, including software.

(2) Verify whether the backups performed are complete and successful.

(3) Test the recovery of backed-up data at least once a year, including testing whether the entire system can function properly.

5.7.4 Develop an emergency plan to enable system recovery within the specified time frame, with guidelines for recovery of data lost from disaster as follows.

(1) Identify all critical work systems of the Company and establish a list of those work systems, updating the list regularly to reflect newly identified critical work systems.

(2) Assess the risks for those critical systems and define measures to reduce the identified risks, updating the risk assessment report at least once a year.

(3) Specify the types of data, such as software related to the work systems or database information.

(4) Set the frequency and methods of data backup, such as Full Backup or Incremental Backup, for those critical systems.

(5) Establish a recovery plan to address potential disasters, with the recovery plan including the following details:

1) Assigning roles and responsibilities for all involved parties.
2) Assessing risks for those critical systems and defining measures to reduce those risks, such as prolonged power outages, fires, earthquakes, or protests that prevent access to the systems.
3) Setting the procedures for recovering critical systems.
4) Setting the procedures for data backup and testing recovery of backed-up data.
5) Testing the emergency plan once a year
6) Setting communication channels with external service providers, such as network, hardware, and software providers
7) Raising awareness or providing knowledge to staff involved regarding operational procedures or actions required during emergencies.

(6) Revise the recovery plan at least once a year

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

(8) Test the recovery of backed-up data to ensure it can be fully restored at least once a year. If any issues arise during the recovery test, take corrective action and record the problem along with the resolution in written form.

5.7.5 Establish the emergency plan for situations where electronic methods cannot be utilized to ensure continuity of operations.

(1) Prepare forms/templates that can replace those generated from the IT technology system.

(2) Operate using the original processes before the current information and communication technology system was implemented, such as using a manual system

(3) Once the information and communication technology system returns to normal functionality, input the data generated during the emergency into the system.

5.8 Risk Assessment of IT and Communication Systems

5.8.1 A risk management team for the IT department is established to carry out the following:

(1) Prioritizing risks.

(2) Developing a risk management plan.

(3) Implementing the risk management plan.

5.8.2 Risk assessments and evaluations regarding IT and computer system security must be conducted at least once a year.

5.8.3 Audit and risk assessment reports must be submitted to responsible individuals and departments, and improvements will be made immediately according to the recommendations of those responsible departments.

5.8.4 Responsibilities are assigned to users or the management, requiring users and the management to take responsibility in cases of damage or harm caused by users or the management being negligent or failing to comply with IT security policies and practices for maintaining information security, as applicable.

5.9 Raising Awareness of IT Security

5.9.1 Public relations campaigns and training sessions are organized to ensure that company personnel are informed, understand, and do not commit offenses under the Computer-Related Crime Act and other laws related to information technology. They are also responsible for appropriately using the Company's IT resources.

5.9.2 The IT security policies and practices are reviewed and updated to remain current and meet accepted standards at least once a year.

6. Disciplinary Actions

The company shall impose disciplinary actions on individuals who violate or neglect the policies on IT security and/or practices for maintaining information security. Such individuals shall be subject to penalties as prescribed by law (if applicable).

This Information Security Guidelines was approved by the resolution of the Good Governance and Risk Management Committee Meeting No. 1 (Board #10) on July 4, 2024, and shall take effect from August 15, 2024, onwards. It supersedes the previous practice for maintaining information security, which was effective on February 28, 2022, and approved by the resolution of the Good Governance and Risk Management Committee Meeting No. 2 (Board #7) on February 28, 2022.

Atchaka Sibunruang

(Ms. Atchaka Sibunruang)

Chairperson of the Good Governance and Risk Management Committee