INFORMATION AND CYBER SECURITY MANAGEMENT POLICY

Information Technology	Issue/Effective Date: 29 February 2024	Issue 01, Rev 04

Prepared by:	Reviewed by:	Approved by:
Ms.Naruemon Chuenchoojit **Senior Manager** **Information Technology**	**Mr. Santi Bangor** **Chairman** **of Corporate Government Committee**	**Mr. Prasert Bunsumpun** **Chairman** **of Board of Directors**

Preface

To ensure the continuous, effective, and secure operation of the information technology system of Thoresen Thai Agencies Public Company Limited, hereinafter referred to as the 'Company,' per its business policy, it is crucial to prevent potential issues stemming from improper usage of the information system network and to guard against various threats that could impact the business system, potentially resulting in damages. Given these considerations, the Company deems it necessary to establish an information system and cybersecurity framework, to which operational personnel and various departments involved in the Company's operations must strictly adhere. The primary goal is to maintain the confidentiality, integrity, and availability of the Company's information system.

Definitions

TERM	MEANING
Company/Organization	Thoresen Thai Agencies Public Company Limited and its subsidiaries and affiliated companies that utilize integrated information and network systems.
Date Recovery	The process of retrieving and repairing damaged computer data, computer systems, and information systems to ensure complete and accurate functionality, following specified conditions.
Data Backup	The duplication of data, including files, databases, and computer systems, to alternative storage locations as a precaution in case of damage, loss, or disaster affecting the primary data.
Computer Center	A facility designed for housing information processing equipment and storing information with a high level of security.
Controlled Area	The designated space housing the Company's critical information systems, including the computer center.
Verification and Identity Confirmation	The process of verifying and confirming the accuracy of an individual's identity (referring to the Electronic Transactions Act B.E. 2562).
Remote Work	Accessing the Company's information system externally.

TERM	MEANING
Personal Data	Information about an individual that allows for direct or indirect identification, excluding data about deceased persons (referring to the Personal Data Protection Act B.E. 2562).
Owner of Personal Data	The individual who possesses personal data.
Date Controller	An individual or legal entity with the authority to make decisions regarding the collection, use, or disclosure of personal data.
Data Processor	An individual or legal entity engaged in the collection, use, or disclosure of personal information on behalf of, or according to the instructions of, the data controller. However, the entity performing these operations is not the data controller.
Abnormality	Any event that impacts the security of information systems.
Staff	Regular employees, contract employees, or temporary employees.
User	Employees, staff, operational personnel, executives of the Group, or external individuals authorized to use the Company's information system.
User account	A set of characters or numbers assigned for accessing specified permissions in the information system.
Password	A set of characters, numbers, or symbols used for verifying and confirming an individual's identity to control access to information and information systems.

1. Information Security

1.1. Information Security Policy

Objectives and Scope

This policy articulates the objectives and scope of the information security policy, outlining management's directives for ensuring the security and proper utilization of information, with an aim to establish a secure information system that supports business operations, adheres to legal requirements, and complies with relevant regulations.

The Company prioritizes the safeguarding of information systems, emphasizing readiness to address cyber threats. The enforcement of this policy is designed to align closely with the provisions of the Cybersecurity Act, B.E. 2562 (2019). Furthermore, the Company underscores the significance of personal information protection in accordance with the Personal Data Protection Act, B.E. 2562 (2019).

Hence, this security policy encompasses the safeguarding of both the organization's information and personal data. Recognizing information as a crucial asset in the organization's business operations, the policy aims to ensure the confidentiality, integrity, and availability of sensitive data, as any compromise in these aspects could adversely affect the financial reliability and reputation of the organization.

Policy and Procedures

1.1.1. Policies for Information Security and Cybersecurity

This policy, formulated per its objectives and scope, has received approval from the management or the Board. It is declared and adopted as the organization's overarching practice, applicable to all levels of the Company, including executives, employees, and authorized external individuals with access to the Company's information systems and assets.

1.1.2. Review of the Policies for Information and Cybersecurity

This policy requires updates at least annually or when significant changes occur to align with evolving trends and potential future risks. Changes may be influenced by factors like modifications to the organization's technological infrastructure, amendments to legal regulations, or shifts in the direction of information technology trends.

2. Organization of Information Security

2.1. Organizational Information Security Structure

To establish a comprehensive and clear framework for managing information security within the Company, including planning and defining roles and responsibilities for security management.

2.1.1. Information and Cybersecurity Role and Responsibilities

This entails appointing a group or working committee for information and cybersecurity, assigning responsibilities, and ensuring accountability for security measures.

2.1.1.1. Internal Departments

1) Information Technology Department

- Establish policies, guidelines, and operational plans for maintaining information and cybersecurity that align with business operations.
- Assume responsibility for information security and lead all activities related to information security within the Company.
- Oversee the infrastructure of information systems and ensure the smooth operation of business application systems.
- Manage and monitor information security threats by implementing prevention, detection, and alert systems for intruders or malicious software, as well as defining operational procedures in crisis or emergency situations to ensure business continuity.
- Act as consultants and provide assistance in developing or implementing various systems. Additionally, organize educational activities to raise awareness of information security and cybersecurity threats.

2) Department Heads/Supervisors

- Define roles, responsibilities, and asset management under their supervision, ensuring the confidentiality, integrity, and availability of the assets.
- Communicate and emphasize the importance of information security to employees under their supervision.
- Respond to information security incidents impacting the department or the entire organization, including cooperation in investigations and proposing solutions for resolution.

3) Personal Data Protection Officers

- Provide guidance and knowledge on compliance with the Personal Data Protection Act to individuals or other relevant departments.
-

- Collaborate with various departments to build awareness and understanding of the Personal Data Protection Act, conducting checks on the processing of personal data to ensure compliance.
- Coordinate and collaborate with the Office of the Personal Data Protection Commission in case of issues related to the collection, use, and disclosure of personal data, or if complaints arise within the Organization.

4) Data and Information Owners/Assets Owners

- Define the classification of data sensitivity, establish measures, and control procedures for accessing information. Notify relevant parties of changes when they occur.
- Inform the Information Technology Department of incidents related to data and information security or changes in access rights due to transfers, resignations, or changes in responsibilities.

5) Employers/Users

- Learn, understand, and strictly adhere to the Information System and Cybersecurity Policy.
- Maintain the confidentiality of organizational information.
- Safeguard the confidentiality of personal data and adhere to the consent received from data owners.
- Immediately report information and cybersecurity breaches to the authorities and the Information Technology Department to assist in responding promptly to such incidents.
- Efficiently and accurately use organizational data and assets following permissions or assigned access rights.

2.1.1.2. External Organizations

- Access information systems only as authorized.
- Treat information obtained through collaboration or access during work with the Organization as confidential. It is strictly prohibited to disclose, forward, or modify information without explicit consent from the overseeing department.
- Immediately report information and cybersecurity breaches to the supervising department and the Information Technology Department.

2.2. Information Classification

Objectives and Scope

To ensure information is adequately protected in alignment with its importance within the Organization:

Policy and Procedures

Information must be classified based on sensitivity, taking into account importance, legal requirements, and vulnerability levels. Prevention efforts should consider confidentiality, integrity, and availability. Control and prevention measures should cover the entire information lifecycle, including creation, utilization, storage, and disposal processes.

2.2.1. Public

Information that is accessible to everyone, both internally and externally to the organization, or information mandated by law to be disclosed. For example, Company information displayed on the Company's website.

2.2.2. Internal
Information that every employee or authorized personnel can access. Authorized personnel may include individuals external to the organization.

2.2.3. Restricted
Information that cannot be disclosed to all employees. This type of information is designated for relevant parties who need awareness of such information for job performance. Encryption may be applied, and disclosure to external individuals is possible if authorized to access the information.

2.2.4. Confidential
Information with a significant impact on the organization's business. This is accessible only to specific user groups, requiring authorization and approval from management. Encryption may be applied for additional security.

2.2.5. Personal Data
Information that can identify an individual directly or indirectly. The use of this data must align with the purposes for which the data owner has given consent.

2.3. Managing Mobile Device and Teleworking

Objectives and Scope

To ensure the security and safety of remote work practices and system access.

Policy and Procedures

2.3.1. Mobile Device

To control the use of portable communication devices related to the Organization's data securely, the following guidelines are established:

- Devices used must be registered for access by the Information Technology department, with access permissions defined to ensure cybersecurity and protection of personal data.
- Devices must have antivirus software installed and regularly updated to safeguard against computer viruses.
- Device readiness must be verified to ensure performance. Legitimate and necessary programs should be installed, adhering to licensing agreements.
- Users are responsible for the care and protection of the provided portable devices.
- In the event of damage to portable devices due to user negligence, the user will be held accountable for the incurred damages.

2.3.2. Teleworking

When remotely accessing systems or information within the Company, such as working from home, the information accessed, processed, or stored from the said location must be protected.

- Individuals seeking to work remotely must secure approval from both their department head and the head of the Information Technology department. Access will be granted based on the necessity to know and the necessity to use.
- Approval from the head of the Information Technology department is required for remote access to systems or data.
- Session timeout is implemented to log users out of the system when there is no activity or when a screen is left unattended, based on the specified time duration.
- Users working remotely must adhere to the Information System and Cybersecurity Policy, similar to onsite work.

- Details of activities during system or data access must be recorded, including identifiable personal information and timestamps.

2.4. Information Security and Cybersecurity Risk Management

Objectives and Scope

To conduct examinations and assess information and cyber risks to guide prevention, detection, response, and reduction of risk levels to an acceptable level.

Policy and Procedures

2.4.1. Risk Assessment and Management

- Establish risk acceptance criteria and assessment criteria for information and cyber systems.
- Identify relevant risks and assign responsibilities for management.
- Evaluate impacts and severity if identified risks occur.
- Assess the likelihood or probability of the identified risks occurring.
- Provide guidelines for managing, mitigating, diversifying, and preventing risks in line with risk assessment results.
- Conduct reviews and assessments of risks at least annually or when significant proposals or changes occur, considering both the likelihood of risk occurrence and its impact on operations and business, to devise management strategies.

2.4.2. Risk Monitoring and Review

- Define processes for monitoring risks related to information and cyber systems.
- Report the progress of risk management plans at scheduled intervals.

3. Asset management

3.1. Asset management responsibilities

To identify the Company's assets and define the responsibilities for safeguarding these assets appropriately. The ultimate responsibility for these assets remains with the owner, even if others are delegated to oversee or control them on behalf of the owner.

3.1.1. Inventory of Assets

Establish and update asset accounts at least annually or when changes occur. This process includes documenting changes in ownership or transfers of asset ownership, specifying the individuals holding the assets.

3.1.2. Ownership of Assets

In maintaining the asset register, each organizational unit must designate an asset owner responsible for maintaining the respective assets, including verifying the accuracy of asset details in the asset register and informing the asset custodian of any changes that occur with the assets.

3.1.3. Acceptable Use of Assets

There must be a documented agreement, obtained in written form, from users, employees, or external entities, outlining the terms for using information and information assets.

3.1.4. Return of Assets

All employees and contractors from external entities must return all organization-held assets upon the termination of employment, expiration of the contract, or conclusion of the employment agreement. If the property is found to be damaged, the asset holder will be responsible for any incurred damages.

3.2. Media Handling

- To prevent potential damage to media used for data recording, such as unauthorized access, alteration, movement, deletion, or destruction of data, adequate control and management should be in place.
- Registration procedures must be implemented to control usage.
- Operational procedures must align with the Company's information classification methods or procedures.
- Risk assessment should be conducted following the Company's asset risk management guidelines, particularly when there are new assets or significant changes to existing assets.
- Media used for data recording must be securely disposed of or destroyed, adhering to internationally accepted standards for destruction processes.
- When transferring media, measures must be in place to prevent unauthorized access, misuse, or damage during transportation or transit of the data recording media.

4. Physical and Environmental Security

4.1. Security area policy

Objectives and Scope

To establish standards for maintaining physical security in locations, including the premises and workspaces of the information technology system, as well as computers, data, and information assets owned by the Company. This involves defining appropriate protective measures based on the importance and risk level of each area.

Policy and Procedures

4.1.1. Physical Security Perimeter

The computer center is within a controlled area, and access must be authorized. The surrounding area is equipped with security measures according to the standards of the computer center.

4.1.2. Physical Access Control

- Users with access rights must register for entry and exit to perform tasks according to their assigned permissions.
- Entry and exit are allowed only for individuals with job responsibilities within the area or those authorized as necessary, with sufficient reasons required for permission.
- Identity verification is implemented to control area access, such as recording entry and exit times, and using cards for entry and exit.
- In the case of external individuals, an information technology staff member must be present with the person at all times.

4.1.3. Securing Office, Workspaces, and Facilities

Security measures for the computer center access include:

- Controlled entry-exit system with keycard access and constantly locked doors.
- Surveillance cameras installed, recording images continuously, with historical data review for 21 days.

4.1.4. Protecting Against External and Environmental Threats

- Fire prevention system, smoke detectors, and electronic fire suppression equipment in place.
- Water leakage detection system for immediate caretaker alerts.

- Temperature and humidity control system with three alternating air conditioners set for computer equipment operation.
- Backup power system and protection against electrical instability.

- Closed-circuit cameras for internal monitoring.
- Regular equipment maintenance scheduled.

4.2. Equipment Management Policy

Objectives and Scope

To prevent unauthorized use of computer equipment due to loss, damage, theft, or actions that pose a threat to property. Staff or users must take care and protect the Company's equipment to minimize risks from threats, including unauthorized access.

Policy and Procedures

4.2.1. Server Monitor

- Daily reports on the operational status of servers, including peripheral devices.
- Summary reports on the status of servers every 6 months for management awareness.

4.2.2. Supporting Utilities

- Critical computer equipment and network devices must have emergency power backup systems to ensure continuous operation or proper shutdown during power failures.
- Surveillance systems and personnel are in place to promptly report any detected errors.
- Notification systems for abnormalities are installed within the Data Center.
- Regular checks or testing of systems and support equipment must take place at least twice a year to ensure normal operation.

4.2.3. Equipment Maintenance

- Schedule maintenance of equipment according to manufacturer recommendations or maintenance standards.
- Record problems and solutions encountered with equipment for assessment and improvement purposes.
- Maintain a log of equipment maintenance activities for each service to facilitate post-service checks or evaluations.

5. Cryptography

Objectives and Scope

To maintain the security of sensitive data and personal information by appropriately using data encryption systems. This ensures the prevention of unauthorized access and modification of confidential or critical data, focusing on both data confidentiality and accuracy.

Policy and Procedures

5.1. Use of Cryptographic Controls

Establish a policy to control the use of data encryption systems, considering the type and corresponding encryption method suitable for the level of risk associated with confidential or important information. Clearly define responsibilities for implementing policies and managing encryption keys. Provide guidelines for users on accessing confidential or important information when encryption is employed, including:

- Specifying Wireless Security formats such as WPA/WPA2 (WIFI Protected Access) for encrypting data between Wireless LAN Clients and Access Points.

- Using internationally standardized encryption, such as VPN, for transmitting critical data over public computer networks.
- Ensuring that passwords stored in databases are encrypted and only accessible to the owner of the password.

6. Access control

6.1. Access Control According to Business Requirements

Objectives and Scope

To restrict access to information and information processing devices and minimize the risk of inappropriate usage, controlling access to information systems is essential. This involves evaluating the appropriateness of system access based on necessity and business requirements in conjunction with security specifications.

Policy and Procedures

6.1.1. Access control

Access rights to information, information processing systems, and other information technology assets must be defined according to the principle of necessity to know and necessity to use. Additionally, a log of access activities must be maintained, and this log should be reviewed based on business requirements and information security needs. The recorded information should include identifiable details about individuals, the duration of access, and the activities conducted.

6.2. User Access Management

Objectives and Scope

To control access to the system, allowing only authorized users and preventing unauthorized access.

Policy and Procedures

6.2.1. Account Registration and De-registration

1) Every employee with access rights to the information system must have a personal user account for system access.
2) User accounts are personal and should not be shared or used jointly with others.
3) In the event of an employee resigning, their user account must not be reactivated or reused.
4) If there is a need for shared user accounts, permissions must be set to the minimum necessary, such as read-only access.

6.2.2. User Access Rights Management

1) Access requests to any system must undergo review and approval by management within the Organization.
2) User accounts with special access rights to information systems, such as Root or Administrator, should be assigned based on necessary justifications.
3) System administrators must promptly update access rights upon receiving notifications from respective departments, particularly in cases of user resignation, job position changes, transfers, contract terminations, etc.

6.2.3. User Access Rights Review

An annual review of user access rights must be conducted at least once a year. The Information Technology department will compile user data and access rights information for system owners to verify and confirm accuracy. If any abnormalities are identified, the IT department should be notified to rectify and update the information accordingly.

6.3. User Responsibilities

Objectives and Scope

To prevent unauthorized access to the system and emphasize user responsibility in safeguarding data used for identity verification.

Policy and Procedures

6.3.1. Use of Confidential Authentication Information

- Users must keep their login passwords for information systems confidential, and they are prohibited from disclosing or sharing them with others.
- When users receive default passwords, they should promptly change them upon the first use of the system.
- Passwords must have a minimum length of 8 characters, including letters, symbols, and numbers. Personal information, such as birthdates or phone numbers, should not be used.
- Users must verify that the assigned system access rights are appropriate for their responsibilities. If inappropriate access rights are identified, users must notify supervisors for consideration and adjustment.
- Users are responsible for maintaining their own account and password, including personal information that may be used to request changes to account information for system usage.
- Avoid storing logs of confidential verification information unless securely protected.
- Passwords should not be written down on paper or stored in unprotected document files.
- Users are accountable for any actions performed through their user accounts and passwords. In case of suspected unauthorized access or a security breach, users must report the incident to the Information Technology department and promptly change all passwords.

7. Communications Management and Operations

Objectives and Scope

1) To safeguard the information within the Company's network system and the supporting infrastructure of the information system to ensure safety and effective communication.
2) To ensure the correct and secure operation of information processing equipment, encompassing the protection of information against various threats.
3) To establish a method for maintaining information security, encompassing both the internal transfer of data and the external transfer of data.

Policy and Procedures

7.1. Network Security Management

7.1.1. Security of Network Service

- Prevent internal network systems from unauthorized access and modification.
- Restrict access to network systems and information systems connected to the network, allowing only network users to access authorized information systems.
- Control and prevent unauthorized services from being activated on the network.
- Access to network devices for physical inspection and remote access must be controlled and limited to authorized personnel only.
- In cases where temporary access rights need to be granted to external individuals, a designated supervisor must be responsible for granting, monitoring, and promptly revoking access rights upon the completion of tasks.
- Maintain a security log to monitor events and issues that occur.
- Backup configuration data of network devices every time there is a change in settings.

7.1.2. Network Segmentation

- Segregate internal and external network systems to regulate access to systems or information within the Company.
- Develop a network diagram detailing the scope of the internal network system and its connections to external entities, regularly updating it to maintain relevancy.
- Evaluate the performance of the network system at least annually and strategize improvements to ensure its capacity for accommodating future expansion.

7.2. Information Transfer

- Transfer information using secure methods that align with the information classification specified by the Company.
- Employ data encryption, per the encryption policy and procedures, for the exchange of confidential information or electronic files between internal or external entities.
- Establish written confidentiality or non-disclosure agreements with external service providers.

8. System Acquisition, Development and Maintenance

8.1. Information Security Requirements Specification

Objectives and Scope

To oversee the development or modification of information system data, ensuring that these operations consider both security and personal data protection. Risk assessments, along with controls adhering to international standards, will be conducted. This policy encompasses the entire process, from the request stage to the actual deployment of systems or data for operational use.

8.2. System Development Process

Objectives and Scope

To secure the information system, encompassing the entire process of information system development.

Policy and Procedures

8.2.1. Process for Controlling System Changes

- Requests for the development or modification of computer system functionalities must be documented in writing, including electronic transactions such as emails. Approval from authorized personnel, such as the head of requesting department, is required.
- A written assessment of the impact of any significant changes should be conducted, addressing aspects related to both operational security and the functioning of associated work systems.
- Ensure thorough communication of the change, informing all relevant users to enable correct usage of the system.

8.2.2. System Acceptance Testing

- A testing plan must be developed, covering both the existing system and the system that has been modified or updated.
- Requesting parties, IT departments, and relevant users must participate in the testing process to ensure that the developed or modified system operates efficiently, processes data accurately, and meets the specified requirements before being transferred for actual use.

8.3. Test data

Objectives and Scope

To prevent unauthorized access to or modification of data used in testing.

Policy and Procedures

1) The development, testing, and actual operation environments are separated to reduce the risk of unauthorized access or changes.
2) Personal data are not used for testing the system without consent from the data owner. If it is necessary to use sensitive data for testing, there should be no information that can identify individuals.
3) In the case in which copies of data from the actual operating system are used for testing, access to these data must be controlled similarly to the actual operating system, adhering to confidentiality levels and personal data protection.

9. IT Outsourcing

Objectives and Scope

To prevent unauthorized access to the Company's assets by external service providers.

Policy and Procedures

1) Security requirements for Company information must be established, and duties and responsibilities must be clearly defined in written form whenever external recipients need to access information or Company assets.
2) Formal authorization must be requested and obtained from the head of the department or system administrator assigned to grant access.
3) If there are changes to the service agreement, a security risk assessment must be conducted.
4) External service providers should undergo an annual evaluation using a standardized assessment form, and criteria for selecting vendors or service providers should be established.

10. Information System and Cybersecurity Situational Management

Objectives and Scope

To establish guidelines for managing and responding to abnormalities related to information technology and personal data, including cybersecurity threats, ensuring appropriate and timely actions are taken.

Policy and Procedures

10.1. Roles and Responsibilities and Operational Procedures

Roles and responsibilities must be defined along with operational procedures to address events related to the security of the Company.

10.2. Security Status Report and Evidence Collection

1) Clearly define communication channels for reporting the security status of information systems and cyber threats.
2) Users of the Company's information systems are responsible for reporting any breaches or vulnerabilities immediately to supervisors and/or the IT department. This ensures that issues are addressed promptly and mitigates potential damage. Examples of incidents that must be reported include, but are not limited to:

- Detection of viruses or malicious programs.
- Significant data alterations or loss.
- Unauthorized disclosure of critical information.
- Identification of vulnerabilities in software, systems, or hardware in use.
- Covert installation of software for data theft or network monitoring.
- Other incidents that violate the Organization's security policy.

3) All information and evidence related to the security incidents must be recorded and securely stored according to rules or criteria for preserving evidence referenced in legal proceedings when it is found that the incident is related to civil or criminal legal actions.

10.3. Personal Data Breach Notification

If the data controller or data processor assesses that a personal data breach has occurred and there is a high risk of adversely affecting the data subject's rights and freedoms, the breach shall be reported to the affected owner of personal data. The notification must include the following details:

1) General information regarding the nature of the personal data breach.
2) Contact channels of data protection officers or assigned personnel.
3) Potential impacts of the breach.
4) Remediation measures, preventive actions, suspensions, or corrections to address the breach.

Additionally, the Company will report such incidents to the Personal Data Protection Committee to comply with its obligations under the Personal Data Protection Act B.E. 2562 (2019).

11. Information Systems and Cybersecurity Business Continuity Management

11.1. Information Security Continuity

Objectives and Scope

To prevent interruptions in the Company's business operations resulting from system failures or halts, ensuring the ability to recover systems within a reasonable timeframe, minimizing the severity of impacts to acceptable levels, and enabling the continuous operation of the Company's business.

Policy and Procedures

11.1.1. Information and Cybersecurity Continuity Planning

An emergency preparedness plan must be developed to address potential situations, encompassing both electronic and physical methods. The plan should analyze and assess risks affecting the organization's business operations, with detailed specifications, including:

1) Defining the roles and responsibilities of involved individuals.
2) Outlining procedures for information system recovery.
3) Defining procedures for data backup and testing the recovery of backed-up data.
4) Requiring the periodic review or adjustment of the emergency preparedness plan at least once a year.
5) Mandating the testing of the emergency preparedness plan at least once a year.
6) Establishing communication channels to inform all employees about the operational plan in emergencies.

11.2. Preparation of Backup Processing Equipment

Objectives and Scope

To ensure the availability of information processing equipment for use.

Policy and Procedures

1) Evaluate and establish information systems for critical functions, including preparing equipment that can serve as suitable replacements.
2) Specify locations and prepare areas for the operational availability of backup systems.
3) Mandate regular testing of backup systems to ensure their capability to function as replacements for the primary systems when necessary.

12. Compliance

12.1. Legal and Contractual Compliance

Objectives and Scope

To avoid violations of legal obligations, regulations, or contractual agreements related to information security, including the protection of personal data.

Policy and Procedures

1) All employees must be aware, understand, and strictly adhere to the provisions outlined in policies, regulations, laws, or contracts related to the use of information technology and communication technologies. This includes, at a minimum:
   - The Company's Information System and Cybersecurity Policy
   - Electronic Transactions Act
   - Computer-Related Crim Act
   - Copyright Act
   - Cybersecurity Act
   - Personal Data Protection Act
2) Information generated, stored, or transmitted through the Company's information technology systems is regarded as the Company's assets (excluding information belonging to customers or external individuals, including software protected by patents or copyrights). The Company possesses the authority to disclose or utilize this information as evidence in investigating various violations without prior notification to users.
3) To manage and uphold the security of the Company's information technology systems, the Company retains the right to audit the usage of computers, computer systems, and network systems of users. This is done to ensure compliance with the various policies established by the Company.
4) The Company reserves the right to access, review, and inspect the emails of users without prior notice. However, the Company will conduct such inspections only when necessary.
5) Users are prohibited from engaging in any activities involving the assets and information technology systems of the Company that violate the laws of the Kingdom of Thailand and international laws, under any circumstances.
6) Users must adhere to the copyright terms when using intellectual property provided by the Company for operational purposes.
7) Users are strictly prohibited from using, duplicating, or disseminating any information or documents that violate copyrights. Moreover, the installation of unauthorized software that infringes on such rights on the Company's electronic devices is strictly prohibited.

12.2. Checking Compliance with Security Policy and Technical Details

The Information Technology department must conduct periodic audits of the entire organizational system per the Information Security Policy and within the specified timeframe.

Regular audits of the technical details of the systems in use or service must be performed as outlined to ensure the adequate maintenance of information security. This involves verifying the system's resistance to breaches, confirming secure configuration of system parameters, and conducting system checks through the use of vulnerability scanning software and vulnerability testing.