IT Security Policy

Srisawad Capital 1969 Public Company Limited

บริษัท ศรีสวัสดิ์ แคปปิตอล 1969 จำกัด (มหาชน)
99/392 อาคารศรีสวัสดิ์ ชั้น 1,5,6
ซอยแจ้งวัฒนะ 10 แยก 3 (เบญจมิตร)
ถนนแจ้งวัฒนะ แขวงทุ่งสองห้อง เขตหลักสี่
กรุงเทพมหานคร 10210
เลขประจำตัวผู้เสียภาษี 0107536000722

Content

0 2691 5600 | info@srisawadcapital.co.th | www.srisawadcapital.co.th

1. Objective

The objective of this framework is to establish policies and procedures for maintaining the security of our information and information technology systems in accordance with local and global standards. Furthermore, it aims to promote security awareness among employees and related parties, building strong confidence and credibility in the services provided to our customers, shareholders, investors, and stakeholders. Ultimately, this policy ensures our strict compliance with the regulatory requirements of the Bank of Thailand, relevant Acts, and all applicable laws.

2. Scope of Policy

This Information Security and Information Technology Systems Policy apply to executives and employees at all levels, including temporary and probationary staff, consultants, business partners, contractors, vendors, and any individuals utilizing the Company's information resources and IT systems. This scope encompasses all data assets, computer networks, operating systems, and software applications developed, maintained, leased, or owned by the Company, including all associated intellectual property and legally protected rights.

Furthermore, this policy shall be reviewed at least once a year, or promptly whenever changes occur that may impact system security, or when relevant regulatory rules, regulations, and laws are amended.

3. Definitions

Data means anything that conveys stories, facts, information, or any matter whatsoever, whether such communication is made by the nature of the thing itself or through any method, and whether it is prepared in the form of documents, files, reports, books, diagrams, maps, drawings, photographs, films, audio or video recordings, computer records, or any other method by which the recorded content can be displayed.

Information means facts derived from processing data and organizing data, which may be in the form of numbers, text, or graphics, into a system that users can easily understand, such as reports, tables, charts, and others, and which can be used for management, planning, decision-making, and other purposes.

Information Technology means knowledge embodied in products or operational processes that rely on technology, software, hardware, communications, information collection, the use of information, or information dissemination.

Information System means a system that utilizes computer system technology and communication system technology to create information and use it for planning, administration, development, and control. It consists of Computer Systems, Communication Systems, and Information operating within computer systems.

Computer System means equipment or a set of computer equipment connected together and configured with instructions, programs, or other commands and operational procedures to automatically process data. It consists of Hardware, Software, and Peopleware used to process data and generate information.

Information Technology Network means communication or data transmission between information systems, such as an Intranet system, Internet system, and others.

Communication System means a system consisting of senders, receivers, and communication media used to transmit data (such as text, numbers, images, and sound), including wired communication systems such as Cable, Coaxial Cable, and Fiber Optic systems, and wireless communication systems such as mobile phones, Microwave, and Satellite systems, including other equipment such as Hubs, Switching devices, and Routers.

Information System Workspaces means areas used for installing computer systems, network systems, or other information systems, preparing data, storing computer equipment, and offices used by computer personnel, including personal computers installed at workstations.

- **Information Security** means the protection of information confidentiality, integrity, and availability. The details of information security are as follows:
- **Confidentiality** means protecting information appropriately to ensure that only authorized persons are permitted to access systems and information.
- **Integrity** means protecting information to ensure its completeness and accuracy. Any modification or change to information must be properly authorized.
- **Availability** means maintaining systems and information so that they can be used efficiently and continuously in accordance with specified time requirements.

Threat means any danger that may arise to an information system from persons, objects, or events, whether intentional or unintentional, causing information within the information system to be disclosed, altered, distorted, destroyed, denied operation, or otherwise affected according to the nature of the threat.

Vulnerability means any weakness or defect in an information system that may be exploited by a suitable Threat to cause harm to that information system

4. Policy Content

4.1. Security Policy

Information Security Policy

4.1.1. Establish a written Information Security Policy, which must be approved by Senior Management prior to implementation, and communicate the policy to employees and relevant external parties.

4.1.2. Assign a responsible unit to establish Information Security Policies and review such policies at specified intervals or whenever significant changes occur.

4.2. Internal Organization Security

4.2.1. Internal Organization

- Establish clear security management measures and procedures that are consistent with the organizational structure, including the appointment of representatives within each unit to manage, coordinate, and provide advice regarding security matters.
- Define and segregate employees' duties and responsibilities clearly and conduct periodic reviews to ensure compliance with the Information Security Policy.
- Establish measures for approving the use of new information systems and/or information processing equipment and ensure compliance with such measures.
- Require employees to sign confidentiality agreements and regularly update relevant terms and conditions.
- Establish control over the exchange of information related to security systems. The measures implemented should be sufficiently stringent to prevent important information from being disclosed to unauthorized people.
- Maintain contact lists and information for security coordination with internal departments, government agencies, and organizations related to information security.
- Require independent auditors to review information security management, operations, and practices at specified intervals or whenever significant changes occur.

4.2.2. External Parties

- Establish measures governing access to information by external parties, including risk assessments associated with access to information or equipment used to access information.
- When customers, service users, or external parties need access to the Company's information or information assets, a security agreement or contract must clearly state the reason for and necessity of that access. Their activities must be strictly controlled.

4.3. Asset Management

4.3.1. Responsibility for Assets

- Establish and maintain an accurate inventory of information assets, identifying responsible persons, information owners, and assets related to information processing, and review the inventory at specified intervals.
- Establish rules or procedures governing the use of information assets to prevent damage resulting from improper use.

4.3.2. Information Classification

- Classify information according to its level of importance and the value of information assets and establish appropriate protection and control measures in accordance with legal requirements.

4.4. Human Resources Security

4.4.1. Prior to Employment

- Establish employment conditions, duties and responsibilities, personnel screening requirements, and employment agreements/contracts for personnel to be hired and personnel provided by external parties. Compliance with employment agreements, Information Security Policies, and security procedures shall be strictly enforced.

4.4.2. During Employment

- Conduct regular training and awareness programs on Information Security Policies to ensure that employees and external parties are informed and able to comply appropriately. Relevant departments shall prepare and maintain up-to-date manuals and operating procedures.
- Establish disciplinary measures for employees who violate or fail to comply with Information Security Policies and/or security procedures.

4.4.3. Termination or Change of Employment

- Establish procedures for personnel whose employment is terminated or whose employment status changes and require responsible departments to enforce such procedures strictly.
- Employees whose employment is terminated or whose employment status changes shall not be permitted to access, modify, or perform any actions on the Company's information systems. Responsible departments shall promptly revoke all access rights to information and information systems and ensure the return of all assets under the employee's responsibility during the period of employment.

4.5. Physical and Environmental Security

4.5.1. Secure Areas

- Establish controlled areas to prevent unauthorized access. Access to and exit from such areas shall be strictly controlled in order to prevent damage to information systems, equipment, and information processing facilities.
- Monitor and supervise all activities of external parties performing work within controlled areas. An assigned employee responsible for the area must oversee these activities throughout the entire duration of the work.
- Implement physical security controls and security procedures for offices, work areas, and other assets of the Company to protect them against risks arising from accidents and external events, such as accidents, fire, flooding, earthquakes, terrorism, and other similar incidents.

4.5.2. Securing Data Center

- Establish procedures and security controls governing access to and exit from the Data Center and provide adequate preventive and warning systems to protect against potential threats. Such procedures and systems shall be regularly reviewed and tested.
- Access to the Data Center shall be controlled, monitored, and restricted to authorized employees or external parties who have been granted approval by the Data Center administrator.
- Data Center operations shall be supported by documented operating procedures, and personnel shall comply with such procedures.
- Operational manuals and documentation shall be maintained, regularly updated, and readily available for use.
- Install appropriate monitoring and protection systems, such as CCTV systems, power failure protection systems, fire protection systems, humidity monitoring systems, and smoke detection systems.
- Implement measures to protect computer systems against damage resulting from unstable power supplies.
- Uninterruptible Power Supply (UPS) systems shall be installed to ensure continued service availability in the event of power shortages or power failures.
- Backup power systems shall be provided as necessary to ensure adequate service continuity in the event of power outages or power shortages.
- Protective systems within the Data Center shall be regularly inspected and tested in accordance with the maintenance schedules specified for each device or system.

4.5.3. Equipment Security

- Office equipment shall be positioned with consideration given to the risks of unauthorized access, environmental threats, and other potential hazards. Appropriate measures shall be established to ensure the secure placement of such equipment.
- Critical supporting systems and equipment, including backup power systems, backup communication systems, temperature control systems, air-conditioning systems, and ventilation systems, shall be adequately protected to ensure continuous operation without adversely affecting information systems.
- Power cables, communication lines, and other cables shall be appropriately protected and maintained to prevent unauthorized access, interference, obstruction, or damage.

- Establish clear maintenance procedures and assign responsible personnel to ensure that all critical equipment is regularly maintained, kept in good working condition, and continuously ready for operational use.
- Removal of any information assets from Company premises shall require prior authorization and shall be subject to strict controls. Relevant procedures shall be established based on the assessment of risks or circumstances that may result in damage to such assets.

4.6. Communication and Operation Management

4.6.1. Operational Procedures and Responsibilities

- Establish changing management controls for system modifications, enhancements, and updates to information processing facilities and ensure that relevant departments are informed of and comply with such controls.
- Segregate duties and responsibilities, operating procedures, and procedures for handling abnormal events or information security incidents relating to information systems and networks in order to reduce the risk of unauthorized changes, modifications, or misuse of information assets.
- Separate development, testing, and production environments. Computers used for information system development shall be segregated from production systems to reduce the risk of unauthorized access to or modification of production systems.

4.6.2. Third Party Service Delivery Management

- Where services are provided by external parties, service providers shall comply with information security requirements and/or agreements relating to security controls, service characteristics, service levels, usage controls, and system access rights. Service conditions shall be reviewed and updated whenever significant organizational changes occur within the service provider that may affect systems or service-related processes.

4.6.3. System Planning and Acceptance

- Relevant departments shall conduct planning and determine additional information resource requirements to ensure that systems remain efficient and capable of supporting increased business and operational demands in the future.
- Establish acceptance criteria and testing requirements for new information systems, system enhancements, version upgrades, and other modifications prior to implementation in the production environment.

4.6.4. Protection against Malicious

- Establish measures and procedures for the detection, prevention, recovery, and regular updating of protection mechanisms against malicious software. Awareness programs shall be conducted regularly to encourage users to exercise caution and avoid the use of computers and devices that may increase the risk of computer infection or propagation of malicious software.

4.6.5. Back-up

- Information shall be backed up regularly and backup data shall be tested periodically, including off-site backups, in accordance with the Company's Backup Policy and Backup Standards.

4.6.6. Network Security Management

- Establish security measures and define responsibilities for the management of operating systems, network-based applications, and information transmitted through information networks in order to reduce risks and protect against network-related threats.
- Define information security requirements, service levels, network service management requirements, internal network services, and services provided by external parties for all network service agreements.

4.6.7. Media Handling

- Establish procedures and authorization requirements for the management of removable storage media.
- Establish procedures for the secure destruction of information stored on devices or storage media to ensure that sensitive information and licensed software contained therein are completely destroyed before such devices or media are retired or disposed of. This is to prevent unauthorized disclosure of information should the devices or media be reused.
- Establish procedures for the management, storage, and protection of information and system documentation in order to prevent unauthorized access, misuse, information leakage, or unauthorized disclosure of sensitive information.

4.6.8. Exchange of Information

- Establish policies, procedures, and controls to govern and protect office automation systems and the exchange of information through all forms of communication channels, ensuring protection against unauthorized access, misuse, and damage to information during transmission outside the Company.
- The exchange of information and software between the Company and external parties shall be governed by written agreements.

- Establish procedures governing the use of electronic mail to protect information transmitted electronically.
- Establish policies, procedures, and controls governing the connection of the Company's information systems with external persons or organizations.

4.6.9. Monitoring

- Maintain audit logs of information system activities, user activities, denial-of-service events, error logs relating to information processing, and other information security-related events. Such records shall be maintained and reviewed regularly in accordance with established retention periods and analyzed to identify appropriate corrective actions.
- Establish procedures for Monitoring System Use and regularly review recorded user activities in accordance with established schedules. Appropriate controls shall be implemented to protect logs, activity records, and security-related event records from unauthorized access, modification, or destruction.
- Activities performed by system administrators and other relevant personnel shall be logged and reviewed on a regular basis.
- All Company computer systems shall maintain synchronized time settings based on an authoritative and accurate time source to support monitoring, auditing, and forensic investigations.

4.7. Access Control

4.7.1. Business Requirements for Access Control)

- Establish policies and procedures for controlling access to information based on business requirements and the risks associated with access to information assets.

4.7.2. User Access Management

- Establish procedures and assign responsible departments for granting access rights to new employees, including procedures for revoking access rights when employees resign or change positions within the Company.
- Grant, control, and restrict access rights to each information system according to job responsibilities and business requirements. A formal user access review process shall be conducted periodically in accordance with established schedules.
- Implement a password management process to ensure the secure allocation and administration of passwords for users.

4.7.3. User Responsibilities

- Establish procedures for password creation and usage, protection against unauthorized access to unattended information processing facilities, and controls to ensure that critical information assets are maintained in secure locations.

4.7.4. Network Access Control

- Establish procedures and controls governing access to the Company's network services, specifying which services are authorized and unauthorized for users. External users shall be required to undergo authentication prior to being granted access to the Company's network and information systems.
- Require network-connected devices to be identified and authenticated to verify that connections originate from authorized devices or locations. Authentication controls shall also be implemented for computers prior to connecting to the network.
- Establish controls to protect ports used for system monitoring and configuration activities, including both physical security controls and logical access controls through information networks.
- Define categories of network usage, including segmentation based on information services, user groups, and information system groups.
- Establish restrictions governing network connections between the Company and external organizations, taking into consideration access control requirements and business application requirements.
- Define network routing controls to regulate connectivity and the flow of information across networks in accordance with the Access Control Policy. Such controls shall cover shared networks and client-to-server communications in order to prevent the use of unauthorized communication paths.

4.7.5. Operating System Access Control

- Establish secure procedures and controls for access to and use of operating systems.
- Require user authentication prior to system access. Each user shall be assigned a unique user identifier for access to information systems.
- Password management shall be governed by procedures and controls designed to ensure the effectiveness and security of passwords.
- The use of utility programs shall be appropriately restricted and controlled to prevent the circumvention or violation of the Company's information security controls.

- Implement automatic session termination when users remain inactive for a specified period of time and establish limits on system usage duration and connection periods for critical or high-risk information systems. Such controls shall also apply to unattended client workstations.

4.7.6. Application and Information Access Control

- Restrict access to information and application functions based on user roles and categories.
- Information systems classified as critical or high-risk shall be segregated within specifically designated and controlled environments.

4.8. Information Systems Acquisition, Development and Maintenance

4.8.1. Security Requirements of Information Systems

- Analyze and identify information security requirements for new information systems or enhancements to existing information systems.
- Information systems shall be designed to support Straight-Through Processing (STP) in order to minimize duplicate data entry (Re-keying) and reduce manual intervention in processing activities.

4.8.2. Correct Processing in Applications to prevent errors, loss, unauthorized modification of information, or misuse of information during processing, appropriate data validation and processing controls shall be implemented as follows:

- Input Data Validation
- Control of Internal Processing
- Message Integrity Validation
- Output Data Validation
- Information shall not be extracted for processing outside the system and subsequently re-entered into the system through manual intervention. Where such processing is unavoidable due to system limitations, formal procedures shall be established to ensure appropriate controls over data accuracy, completeness, timeliness, retention, confidentiality, and availability in accordance with business requirements.

4.8.3. Cryptographic Controls

- Establish policies and procedures governing the use of cryptographic processes and encryption technologies. Critical information systems and sensitive information about the Company shall be encrypted, and encryption controls shall be implemented in strict accordance with established procedures.
- Establish encryption standards that support the effective management of cryptographic keys used for encryption and decryption processes. Key length and cryptographic strength standards

shall be reviewed and updated periodically to ensure alignment with operational requirements and technological advancements.

4.8.4. Security of System Files

- Establish procedures to control the installation of software on production systems. All software shall be tested and approved prior to deployment in order to reduce the risk of system malfunction or service disruption.
- Production data shall not be used for system testing purposes. Where the use of production data is unavoidable, formal approval procedures, security controls, and strict usage restrictions shall be implemented.
- Access to software libraries and source code repositories for production systems shall be restricted and controlled in order to prevent unauthorized or unintended modifications.

4.8.5. Security in Development and Support Processes

- Establish procedures for controlling changes to information systems and perform technical reviews following system modifications. Such controls shall minimize the risk of system failures, service disruptions, or operational impacts. Each change shall also incorporate appropriate measures to prevent information leakage and reduce the risk of unauthorized disclosure of information.
- Modifications to vendor-supplied software shall be limited strictly to what is necessary and shall be subject to rigorous control procedures.
- Establish controls to govern and monitor software development performed by external parties. In particular, system development agreements shall address key requirements, including intellectual property rights, system usage rights, system audit rights, and quality assurance requirements.

4.8.6. Technical Vulnerability Management

- Establish measures for managing technical vulnerabilities and ensure that identified vulnerabilities are remediated appropriately and in a timely manner in order to reduce risks arising from vulnerabilities in information systems, hardware, and software.

4.9. Information Security Incident Management

4.9.1. Reporting Information Security Events and Weaknesses

- Establish procedures and guidelines for reporting information security incidents and weaknesses. Employees, contractors, and personnel of external parties shall strictly comply with such procedures to ensure that incidents can be addressed and resolved in a timely manner.

4.9.2. Management of Information Security Incidents and Improvements

- Define responsibilities and procedures to ensure that information security incidents are managed in a systematic and effective manner.
- Establish requirements for incident recording, including incident type, frequency of occurrence, financial impact, and other relevant details, in order to provide evidence and support future corrective actions and improvements.
- Collect and preserve evidence relating to information security incidents to support legal proceedings, whether civil and/or criminal in nature.

4.10. Business Continuity Management

4.10.1. Information Security Aspects of Business Continuity Management

- Establish information security requirements necessary to support business continuity. Business continuity planning and operational disruption risk assessments shall be conducted in a manner consistent with and supportive of the Information Security Policy. Business continuity plans shall be tested, reviewed, and updated at appropriate intervals to ensure their continued effectiveness and relevance.

4.11. Compliance

4.11.1. Compliance with Legal Requirements

- Identify and document applicable legal requirements, as well as contractual obligations between the Company and external persons or organizations. Such requirements shall be maintained, updated, and strictly complied with.
- Establish measures to protect personal information, information subject to legal or regulatory requirements, contractual obligations, and business requirements from loss, damage, destruction, falsification, misuse of information processing facilities, unauthorized use, or use for purposes other than those intended.
- Cryptographic controls implemented by the Company shall be consistent with the Company's Information Security Policy and shall comply with all applicable legal and regulatory requirements.

4.11.2. Compliance with Security Policies, Standards, and Technical Requirements

- Establish supervisory measures to ensure that managers and supervisors effectively monitor and control the activities of their subordinates in compliance with the Information Security Policy.
- Conduct regular reviews and assessments of information systems and related technical configurations supporting operational and production environments to ensure compliance with the Company's Information Security Policies and Standards.

4.11.3. Information Systems Audit Considerations

- Information systems audits shall be planned and conducted in a comprehensive manner. Audit activities shall be designed to minimize disruption to information systems and business operations.
- The use of audit tools for information systems assessments shall be governed by controlled access procedures and appropriate safeguards to prevent misuse or unauthorized disclosure of information.

4.11.4. Compliance with the Computer Crime Act B.E. 2550 (2007)

- Identify the requirements of the Computer Crime Act B.E. 2550 (2007) and establish relevant operational procedures to ensure that business operations remain compliant with the provisions of the Act.
- Support the protection of the Company's computer systems to prevent their misuse by employees as a means of causing damage or committing unlawful acts. Employees shall be informed of their responsibilities under the Act, and any violation shall be considered the direct responsibility of the employee concerned.
- Cooperate with competent authorities in the examination of computer systems and information relating to individuals who have committed offences under the Computer Crime Act.

4.12. Security Measures for Personal Data Controllers

Principles and Rationale

Personal Data Security means maintaining Confidentiality, Integrity, and Availability of personal data in order to prevent the loss, unauthorized access, use, alteration, modification, or disclosure of personal data. The Personal Data Protection Act B.E. 2562 (2019), the Notification of the Ministry of Digital Economy and Society Re: Standards for Personal Data Security B.E. 2563 (2020), and the Notification of the Personal Data Protection Committee Re: Security Measures of Personal Data Controllers B.E. 2565 (2022) require Personal Data Controllers to implement appropriate security measures for the protection of personal data.

The objective of personal data security is to protect the privacy rights of Data Subjects and their rights to control their personal data as recognized and protected by law. Accordingly, safeguarding personal data is one of the legal obligations of a Personal Data Controller to prevent the loss, unauthorized access, use, alteration, modification, or disclosure of personal data, which may result in a personal data breach.

Personal Data Security Measures

The Company shall implement personal data security measures covering the collection, use, and disclosure of personal data in accordance with applicable laws. Such measures shall include Administrative Safeguards, Technical Safeguards, and Physical Safeguards, as follows:

1. Administrative Safeguards

1.1. The Company shall communicate its Personal Data Security Measures to directors, executives, employees, personnel at all levels, all categories of workers, business partners, strategic partners, and/or stakeholders. The Company shall also promote awareness of the importance of personal data protection among such persons to ensure strict compliance with the prescribed measures.

1.2. The Company shall identify risks associated with information assets, implement measures to prevent such risks, monitor and detect threats and personal data breach incidents, and ensure compliance with the Information Security Policy. Responsibilities for responding to personal data breaches, as well as procedures for mitigating and recovering from damage resulting from threats and personal data breach incidents, shall be established as follows:

1.2.1. Designate responsible personnel and establish clear procedures for reporting personal data breach incidents to the Company's representatives, including reporting channels such as email notifications and mobile phone communications in cases involving severe or urgent incidents.

1.2.2. Establish procedures requiring the Company's designated representatives to notify the Personal Data Protection Committee of a personal data breach within seventy-two (72) hours from becoming aware of the incident.

1.2.3. Notification of a personal data breach pursuant to Clause 1.2.2 may be exempted where the breach is unlikely to result in a risk to the rights and freedoms of individuals. A risk assessment shall be conducted to evaluate the potential impact on the rights and freedoms of individuals, for example:

a) Example of a Low-Risk Incident: Personal data has been encrypted (and cannot be accessed without the decryption key) and subsequently rendered inaccessible due to a ransomware attack, while no personal data has been exfiltrated. Backup systems continue to support business operations without interruption. In such circumstances, the incident may be considered low risk to the rights and freedoms of individuals. The

Company shall record the incident internally and shall not be required to notify either the Office of the Personal Data Protection Committee or the relevant Data Subjects.

b) Example of a High-Risk Incident: An online recruitment website is compromised through the installation of malware, enabling an attacker to gain access to online job application data. Although the information involved consists of general recruitment information, the incident may pose a high risk to the rights and freedoms of individuals. In such circumstances, the Company shall record the incident internally, notify the Office of the Personal Data Protection Committee within seventy-two (72) hours, and inform the affected Data Subjects without undue delay.

In all cases involving a personal data breach, the Company shall review and reassess its personal data security measures.

1.3. The Company shall establish authorization and access rights management controls for personal data users (User Responsibilities), including rights such as viewing, updating, modifying, disclosing, publishing, data quality verification, and deletion or destruction of personal data.

1.4. The Company shall implement User Access Management controls to ensure that access to personal data is restricted solely to authorized persons.

1.5. The Company shall establish audit trail mechanisms to enable retrospective verification of access to, modification of, or transfer of personal data, in a manner appropriate to the methods and media used for the collection, use, or disclosure of personal data.

1.6. In the event of non-compliance with these Personal Data Security Measures resulting from the Company's failure and causing a personal data breach or unauthorized disclosure, the Company shall notify the affected Data Subjects of the details of the incident and any remediation measures (if applicable). However, the Company shall not be liable for any damages arising from the use, disclosure, negligence, or misconduct of the Data Subject or any other person acting with the Data Subject's consent.

1.7. Upon expiration of the retention period or when personal data is no longer necessary for the purposes for which it was collected, the Company shall delete or destroy such personal data from its storage systems, except where retention is required by applicable laws.

1.8. The Company shall conduct periodic reviews and assessments of the effectiveness of its personal data protection and security controls through the Internal Audit function.

2. Technical Safeguards

2.1. The Company shall implement mechanisms enabling the retrospective verification of access to, modification, deletion, or transfer of personal data, as appropriate to the methods and media used for the collection, use, or disclosure of personal data, as follows:

2.1.1. The Company shall regularly monitor personal data under its control (in its capacity as a Personal Data Controller) to identify records or datasets that have exceeded their retention periods as specified in the Privacy Notice provided to Data Subjects or as otherwise agreed through consent. Such personal data shall be deleted, destroyed, or anonymized, as appropriate.

2.1.2. Where a Data Subject exercises the right to request deletion of personal data or withdraws consent, and the Company relies on consent as the legal basis for processing such personal data, the Company shall delete, destroy, or anonymize the personal data, as applicable.

2.1.3. The deletion, destruction, or anonymization of personal data may not be required where the Company has a legitimate interest or legal basis that overrides the rights of the Data Subject, including the following circumstances:

(a) For historical, archival, research, statistical, or public interest purposes.

(b) For the performance of tasks carried out in the public interest by the Personal Data Controller.

(c) For assessing employee performance, medical diagnosis, provision of healthcare or social services, medical treatment, health management, or social welfare services.

(d) For the protection of public health against communicable diseases, epidemics, or public health threats, or for ensuring the quality, safety, and standards of medicines, medical products, or medical devices.

2.2. Access to personal data shall be restricted to authorized persons based on assigned access privileges, including rights relating to data entry, modification, amendment, disclosure, and deletion, including but not limited to the following:

2.2.1. Access to personal data and critical information system components shall be subject to appropriate identification, authentication, authorization, and access controls. Such controls shall be implemented in accordance with the Need-to-Know Principle and the Principle of Least Privilege.

2.2.2. Appropriate User Access Management controls shall be implemented, including user registration and de-registration, user access provisioning, privilege management, management of authentication credentials, periodic access reviews, and revocation or modification of access rights.

2.3. The Company shall maintain data backup and recovery capabilities to ensure the continued availability of systems and services in accordance with the Company's Information Technology and Information Security Standards and Procedures.

3. Physical Safeguards

3.1. Access to personal data and equipment used for the storage and processing of personal data shall be controlled with consideration given to operational requirements and security needs. Such controls may include security personnel, CCTV surveillance systems, locked filing cabinets, and other appropriate measures. The level of protection implemented shall be commensurate with the risks and potential impact arising from unauthorized disclosure, modification, copying, or destruction of personal data.

3.2. The Company shall designate authorized personnel who are permitted to access equipment used for the storage or processing of personal data according to their roles and responsibilities. Appropriate measures shall be implemented to prevent unauthorized access, disclosure, awareness, copying, theft of storage or processing devices, unauthorized removal of equipment, and any act that may result in personal data leakage or compromise. Such measures may include, but are not limited to:

3.2.1. Refraining from displaying personal data files in public areas.

- Securing or concealing personal data when leaving a workstation unattended.
- Removing personal data files from shared printers and logging out of printer systems after use.
- Maintaining records of requests for access to personal data; and
- Personally, destroying personal data documents without delegating such destruction to unauthorized persons.

4. Agreement Between the Company and the Personal Data Processor

Where an agreement exists between the Company and a Personal Data Processor, the Company shall require the Personal Data Processor to implement security measures consistent with this Policy to prevent the loss, unauthorized access, use, modification, alteration, or disclosure of personal data, whether unlawfully or without legal authority. The Personal Data Processor shall also be required to

notify the Company of any personal data breach. The level of security measures implemented shall be commensurate with the risks and potential impact arising from unauthorized disclosure, modification, copying, or destruction of personal data.

4.1. Prior to Data Disclosure

4.1.1. Verify the authority, legal basis, and entitlement of any individual and/or legal entity requesting access to personal data.

4.1.2. Determine the purpose for which the personal data will be used in order to assess the appropriate level of detail to be disclosed. For example, assess whether the recipient requires full date of birth, residential address, personally identifiable information, such as full name or national identification number, or whether less detailed information, such as year of birth or postal code, would be sufficient. Consider whether anonymized information could adequately satisfy the intended purpose.

4.2. Upon Data Disclosure

4.2.1. Prepare a new dataset derived from the original data containing only the level of detail necessary for the intended purpose.

4.2.2. Disclose the data and maintain records of the recipient's name, contact information, date of disclosure, legal basis for access, and intended purpose of use.

4.2.3. Inform the individual or legal entity receiving the data that, upon receipt of the personal data, they shall assume the obligations of a Personal Data Controller in respect of the personal data received, within the scope and purposes communicated.

4.3. After Data Disclosure

4.3.1. Conduct periodic follow-up reviews to monitor the status of the disclosed data. Where the data is no longer required for the originally stated purpose, the recipient should be instructed to delete or destroy the data.

4.3.2. Establish procedures to ensure that disclosed information remains accurate, current, and suitable for the recipient's ongoing use.

5. Cross-Border Transfer of Personal Data

Any transfer or transmission of personal data to a foreign country, including the storage of personal data in systems or databases operated by service providers located outside Thailand, shall only be conducted where the destination country provides personal data protection standards that are equivalent to or higher than those prescribed under this Policy.

6. Violation of the Company's Security Measures

In the event of a violation of the Company's security measures resulting in a personal data breach or unauthorized public disclosure of personal data, the Company shall notify the affected Data Subjects without undue delay and, where applicable, communicate remediation measures intended to mitigate the consequences of such breach or disclosure arising from the Company's failure.

Review of the Measures

The Company shall review these Security Measures for Personal Data Controllers whenever necessary and/or when technological developments or changes warrant such review.

Reservation of Rights

The Company shall not be liable for any damages arising from the use or disclosure of personal data by third parties, including circumstances resulting from the negligence or failure of the Data Subject, or any person acting with the Data Subject's consent, to properly log out of the Company's databases, systems, or online communication platforms.