STP&I Public Company Limited

Information Technology System Security Policy

(has been approved by the Board of Directors When the Committee Meeting No. 3/2023

March 10 , 2023)

Information Technology System Security Policy

STP&I Public Company Limited recognizes the pivotal role of Information Technology (IT) systems in enhancing employee performance. In line with this recognition, the company aims to provide clear guidelines for the use of its IT systems to ensure both convenience and safety for employees. This initiative is crucial not only to prevent potential issues stemming from misuse but also to mitigate risks and threats that could jeopardize the integrity of the company's business operations.

In this regard, maintaining the confidentiality, accuracy, and accessibility of information within the company's IT systems is paramount. Hence, establishing a comprehensive IT security policy is deemed necessary to standardize practices and effectively manage the company's computer resources and IT infrastructure. This policy serves as a framework for the administration and maintenance of IT systems across the organization, ensuring efficiency and adherence to best practices. Below are the detailed provisions of this policy.

1. Objective

1.1 Establishing the direction, principles, and framework for managing information technology security requirements.

1.2 Fostering knowledge and comprehension among employees regarding compliance with policies, standards, and operational frameworks, including relevant laws pertaining to computer systems.

1.3 Enabling employees and authorized individuals to effectively and appropriately utilize the company's computer systems.

1.4 Safeguarding the company's computer systems and information from compromise, theft, or disruption, which could potentially harm business operations.

2. Scope

This policy is applicable to STP&I Public Company Limited and its subsidiaries. It encompasses authorized external parties granted access to the network system, computer systems, portable communication devices, or telecommunications equipment for accessing company information.

3. Security Principles

The practice of maintaining security is guided by the following principles to achieve specific objectives:

- Confidentiality: Safeguarding information from unauthorized access or disclosure, including personal or company-proprietary data.
- Integrity: Ensuring that company information remains unaltered, intact, and protected from unauthorized modification or destruction.
- Availability: Guaranteeing swift and reliable access to information for authorized users.
- Accountability: Defining the roles and responsibilities of individuals, emphasizing ownership and accountability for outcomes.
- Authentication: Enforcing thorough identity verification processes to control access to computer systems and information.
- Authorization: Granting access rights to computer systems and information based on the principle of Least Privilege and according to essential needs (Need to Know Basis).
- Non-repudiation: Preventing parties involved in transactions from denying their involvement in those transactions.

Effective security maintenance requires mutual agreement and dedicated attention to all aspects involved, which encompasses:

- Recognizing security as the responsibility of all employees and external parties.
- Ensuring that security management and operations are continuous processes.
- Cultivating awareness of duties and responsibilities, adhering to policies, standards, operational frameworks, and procedures. Clearly communicating these expectations to employees and external parties fosters understanding and ensures effective security maintenance.

4. Definition

4.1 "Company" refers to STP & I Public Company Limited and its subsidiaries.

4.2 "Information Technology Section" is responsible for managing information technology operations.

4.3 "Employee" includes probationary, regular, special contract employees, and executives under the employment of the company.

4.4 "User" denotes employees, as well as external individuals granted access privileges or passwords to the company's information processing equipment.

4.5 "Supervisor" signifies an employee overseeing an internal unit based on the company's organizational structure.

4.6 "Computer System" encompasses all hardware, software, data link network equipment, storage materials, and telecommunications equipment utilized within the company's premises, whether owned by the company, employees, partner companies, or other necessary parties.

4.7 "Information Technology" encompasses data, records, documents, computer programs, images, sounds, and symbols stored in various formats for human understanding, either directly or through tools or equipment.

4.8 "Important Information" or "Confidential Information" pertains to data crucial for the company's business operations or bound by legal, ethical, or contractual

obligations, which cannot be disclosed or utilized for other purposes. Leakage of such information may impair business operations or damage the company's reputation.

4.9 "Important System" denotes computer systems directly generating income or supporting income generation, along with other electronic systems vital for normal business operations, as determined by the company's information security and information system department. Malfunction or reduced functioning of such systems may disrupt business operations.

4.10 "Remote Access" refers to accessing the company's information system from a remote location.

4.11 "System Owner" is the internal organization responsible for a computer system and its management.

4.12 "Data Custodian" is an individual appointed by the system owner to manage and control access to information in accordance with specified requirements or permissions.

4.13 "Administrator" oversees the use and maintenance of computer systems, including hardware, software, and peripherals, with authority to modify, add, edit, and enhance the system to ensure efficiency and security.

4.14 "Maintaining security" or "Security" involves preventive measures, caution, and diligence in safeguarding computer systems and critical information from unauthorized access, theft, destruction, or interference that may disrupt business operations.

4.15 "External Party" includes personnel or agencies engaged in business or service provision, granted access to information and company's information processing equipment, such as

- Business Partner
- Contractor performing work for the company (Outsource)
- Contractor for system development or procurement of various materials and equipment (Supplier)

- Service Provider
- Consultant

5. Responsibilities

5.1 Managing Director (MD) Duties

5.1.1 Define the overall strategy and oversee operations within the company, including approving the security policy for the company's information technology systems.

5.2 Administrative Department Manager Duties

5.2.1 Align goals and the company's information technology system security policy with the company's strategic plan.

5.2.2 Evaluate the need for information resource utilization, ensure value for money, and procure and develop information systems in alignment with the company's strategy.

5.2.3 Manage the company's information resources to efficiently support internal operations.

5.3 Information Technology Section Manager Duties

5.3.1 Establish management and operational guidelines for the security of the company's information technology system, aligning them with the company's information technology system security goals and policies.

5.3.2 Develop information technology system security policies, standards, procedures, and guidelines to maintain information confidentiality, integrity, and system stability.

5.3.3 Supervise and monitor system attacks and potential threats, including planning for business continuity management to ensure system recovery during emergencies.

5.3.4 Conduct risk management and analyze potential risks that may impact system functionality and the company's business operations.

5.3.5 Present operational plans, policies, budgets, and workforce requirements to top executives according to the organizational structure.

5.3.6 Continuously prepare for and stay updated on new techniques in information security.

5.4 Managers Duties

5.4.1 Educate and encourage users to comply with the information technology system security policy and enforce warnings and disciplinary actions for improper or inappropriate practices.

5.5 Users Duties

5.5.1 Learn, understand, and adhere strictly to the company's information technology system security policies.

5.5.2 Collaborate fully with the company to safeguard computer systems and information, overseeing and protecting company data and information to ensure safety.

5.5.3 Immediately report to the company when devices are lost, important information is compromised, or incidents of intrusion, theft, destruction, or unauthorized access occur that may harm the company.

5.6 Data and Information Owners Duties

5.6.1 Documents preparation, measures, and procedures to control data access in accordance with the company's information technology system security policy.

5.6.2 Ensure employee compliance with the company's information technology system safety policy.

5.6.3 Control and approve access to data, information, and computer systems as per assigned duties and responsibilities.

5.6.4 Report incidents related to data and information security promptly.

5.6.5 Notify the responsible information technology department for user account management and rights adjustments in case of changes in employees, authorities, or duties/transfers.

6. The Company sets Security Policies for Information Technology Systems in important areas, including:

6.1 Security for Information Assets

6.1.1 Information assets encompass databases, data files, software, development tools, computer and network equipment, communication devices, external storage media, and various peripherals. Owners of information assets, along with relevant department personnel, are responsible for compiling an inventory of these assets.

6.1.2 The company is obligated to assess the level of confidentiality and assign appropriate classifications to safeguard information assets. Documents or reproductions derived from originals with assigned secrecy levels are treated with equivalent confidentiality.

6.2 Personnel Safety

6.2.1 Define and document duties and information security responsibilities for all users, including external contractors. Implement measures to prevent and ensure the security of company information.

6.2.2 Conduct training sessions to educate users on information technology security awareness and procedures. Documentation of training sessions must be signed and maintained in personnel files, with updates provided to employees as needed.

6.2.3 Establish disciplinary measures for policy violations in accordance with company rules and regulations. Legal violations will be addressed according to the severity of the offense and company policies.

6.2.4 Notify the Human Resources Division of any transfers, appointments, or terminations. Employees must return all company property related to the information system upon leaving their position. The Information Technology Department is responsible for revoking access rights accordingly.

6.2.5 Provide new employees with basic security awareness training and obtain their consent to adhere to the company's information technology system usage policies.

6.3 Safety in Storage and Operations

6.3.1 Establish physical security measures for offices, workspaces, and assets to mitigate various threats, including fire, floods, disturbances, and natural disasters. Adequate security arrangements must be in place for areas requiring heightened protection.

6.3.2 Designate a separate area for third-party product deliveries to prevent unauthorized access to company information assets.

6.3.3 Employees should safeguard office equipment to minimize exposure to environmental risks and unauthorized access.

6.3.4 Store information assets in secure areas with designated usage classifications. Separate the computer center from general workspaces, maintaining controlled entry and exit for authorized personnel only.

6.3.5 Protect various cables from unauthorized access and ensure proper labeling to identify their origin and destination.

6.3.6 Regularly maintain computer systems, network infrastructure, and host computers as per manufacturer recommendations.

6.3.7 Implement measures to protect equipment used outside the office premises to prevent damage.

6.3.8 Prior to discarding devices containing data storage media, employees must ensure sensitive data is deleted or overwritten, following guidelines provided by the Information Technology Department.

6.3.9 Establish procedures for handling portable storage media.

6.3.10 Implement measures to safeguard system documents from unauthorized access.

6.3.11 Establish protocols for managing and storing information to prevent unauthorized access.

6.3.12 Develop written procedures for the disposal of media used for recording information, such as burning, cutting, shredding, or destruction, to prevent unauthorized access. Personnel must supervise the removal or destruction of data storage media, with approval from the data owner and appropriate documentation of the process.

6.4 Security in Information System Administration

6.4.1 Develop and maintain a manual outlining operating procedures, including system recovery, maintenance, and administration. Regular updates to the manual should occur following any changes in procedures or personnel. Implement change control processes for enhancing or rectifying computer systems, network infrastructure, and hardware and software.

6.4.2 Delegate administrator responsibilities to minimize the risk of unauthorized alterations or modifications.

6.5 Safety in External Agency Services

6.5.1 Establish agreements to regulate services provided by external agencies, including adherence to the company's information technology system security policy, service scope, details, and level. Review agreements with the company's legal department, ensuring provisions for non-disclosure of company information.

6.5.2 External agencies or third parties granted access to the company's information systems must accept and adhere to the company's information technology system security policy.

6.5.3 Conduct risk assessments for external agency access to information systems or activities impacting the company. If disclosure of information is necessary, external agencies or third parties must sign non-disclosure agreements.

6.5.4 Regularly review services or contracts with external agencies and service providers. Update terms as needed, especially during the implementation

of new information systems, technology developments, or changes in service conditions.

6.6 Computer Network Security

6.6.1 Implement measures to safeguard against various network threats and regulate network usage permissions to authorized personnel only.

6.6.2 Restrict external connections to the internal network system, including remote network access via the Internet. Prohibit the installation of any hardware or software related to network services without proper authorization.

6.7 Security in Data and Information Exchange

6.7.1 Establish policies, guidelines, and measures to mitigate issues related to information exchange within the company, among company groups, and with external agencies through various communication channels such as electronic messaging.

6.7.2 Implement a review process prior to disseminating information to the public. Assess risks and determine measures to mitigate risks before releasing information.

6.8 Security in Access Control to Information Systems

6.8.1 Implement procedures to regularly log events related to information usage and user activities, ensuring the protection of recorded information from unauthorized alterations. All operational activities within the system must be documented.

6.8.2 Log relevant error events, analyze them, and take corrective actions accordingly. Ensure computer time synchronization with accurate sources to facilitate timing determination in case of system compromise.

6.8.3 Conduct periodic reviews of employee access and usage of information systems by the Internal Audit Department. The department is authorized to monitor actions suspected of violating policy.

6.9 Security Measures for Information System Access Control

6.9.1 Establish procedures for user registration, access control, and rights management, including processes for revoking access rights upon resignation or position changes. Implement password management protocols for secure allocation and maintenance.

6.9.2 Users are responsible for maintaining the security of their user accounts and passwords.

6.9.3 Employees must have methods to prevent unauthorized individuals from accessing unattended office equipment, such as notifying the department head or security personnel whenever such instances are observed. Additionally, there should be a policy in place to prevent the placement of important information assets, such as documents or data recording media, in insecure or easily accessible locations.

6.9.4 A network usage policy must be established, outlining which services users are permitted to use and which services are restricted.

6.9.5 Access to the company's information systems and data can only be granted upon approval by department heads and the IT department head. Access is restricted to job-related tasks, and authorization must be obtained from the data owner.

6.9.6 Each access to the information system must be authenticated and confirmed using the provided Username and Password from the system administrator before usage rights are granted. For critical systems or remote access, two-step authentication must be implemented. Furthermore, usage rights must be reviewed at least once annually.

6.9.7 Any changes to information systems, network systems, or applications must be verified and approved by data owners and the Information Technology Section Manager.

6.9.8 Implement measures to prevent unauthorized access to ports used for system monitoring and configuration, including physical and network-based protections.

6.9.9 Provide password quality checking systems and enforce password change policies within specified time frames.

6.9.10 Control the use of utility programs to prevent security breaches, limiting their use to authorized personnel only. Establish protocols for managing computer usage time and restricting access to highly sensitive information systems.

7. Distribution of Information Technology System Security Policy Documents

7.1 Policy Dissemination Plan

7.1.1 The policy document will be accessible to all users for reading and understanding, and it will be posted on the Company's website.

7.2 Training plan

7.2.1 Develop a training plan for the information technology system security policy as needed.

8. Compliance with the Policy

The Information Technology Department, in collaboration with the Management Department, has formulated an information technology system security policy aligned with the ISO/IEC 27001:2013 Information Security Management Systems standards to uphold the security of the company's information.

9. Consideration of Disciplinary Measures

9.1 Users intending to breach the policies, terms, and agreements outlined in this document will be deemed to have committed a serious offense, regardless of the success of the breach.

9.2 Employees found to have intentionally or negligently violated the information technology security policy, resulting in or potentially causing harm to the company or any individual, will face disciplinary action, including civil and criminal repercussions as per relevant laws, regulations, or announcements.

9.3 Commanders who fail or neglect their duties, leading to violations of the information technology security policy by employees under their supervision, will be subject to disciplinary measures outlined in Section 9.2.

9.4 Violation any requirement stipulated in this information technology security policy, even if it doesn't directly harm the company or any individual, may be noted in the employee's work history. Such records may influence decisions regarding contract renewal, salary adjustments, or promotions.

9.5 Individuals found guilty of crimes related to the rules, regulations, terms, or security policies of the company's information technology systems will face disciplinary action according to company regulations. The Human Resources Department will conduct investigations and enforce disciplinary measures in accordance with established procedures.

10. Policy Review

The Information Technology Manager or the designated individual shall conduct regular reviews of this policy, at least once a year or whenever significant changes occur. Any proposed changes must be submitted to the Executive Chairman for approval.

This will be effective from March 10, 2023.

Official announced on March 10, 2023

(Mr. Masthawin Chanvirakul)

Managing Director