

Policy and Regulations regarding the Use of Computer System

S&J International Enterprises Public Company Limited

S&J International Enterprises Public Company Limited has implemented a computer system to facilitate and speed up employees' work, ensuring continuity and efficient functioning of business operations. Hence, maintaining the confidentiality, correctness, and completeness of information, along with the availability of business data and information systems, are essential for the business to run efficiently, instill confidence among customers and partners, and comply with the legal requirements of computer crime and relevant laws. As such, policies and regulations regarding the use of computer systems are established as follows.

Definition

1. **“Company”** refers to S&J International Enterprises Public Company Limited.
2. **“Supervisor”** refers to a person with authority to give orders according to the company structure.
3. **“Employee”** refers to employees of S&J International Enterprises Public Company Limited and individuals who are authorized to work within the company.
4. **“Computer System”** refers to computers and computer data, including computer traffic data that are connected through a computer network.
5. **“Computer”** refers to computers, including various peripherals and network equipment that connect the work together, all of which are the property of the company.
6. **“Computer Network”** refers to the computer network of S&J International Enterprises Public Company Limited, including the computer networks of the company that are connected to each other.
7. **“Computer Data”** refers to data, messages, commands, sets of instructions, or anything else in the computer system that is in a condition that the computer system can process, and includes electronic data under the law on electronic transactions.
8. **“Computer Traffic Data”** refers to information about the computer systems' communication, which displays the source, origin, destination, route, time, date, quantity, duration, service type, or anything else that is related to the communication of such computer system.
9. **“Computer System Administrator”** refers to employees assigned by the Company with duties and responsibilities to maintain the computer system.

Policy for the Use of Computer Systems

1. Computer Security Policy

The Company has a written policy for maintaining the security of computer systems. The policy has been approved by the Executive Director and is reviewed or updated every three years or as needed in accordance with changes in related laws. The Company publishes the policy in a manner that is easily accessible to employees so that employees are aware of the policy and adhere to it accordingly.

2. Computer Security Structure

The Company's internal structure ensures distinct segregation of duties of supervisors in performing various tasks related to the security of computer systems in order to have a review of each other and prevent operational risks that may arise as follows:

1. Department Manager/Information Technology Section Manager
2. Computer System Administrator/Operator
3. Technical Support
4. Program Developer
5. Computer Operator

3. Security and Safety for Personnel

3.1 During employment

Employees with the right access to the Company's computer systems and networks must abide by these policies and regulations.

3.2 Termination or Change of Job Duties

3.2.1 Termination

When notified by the Human Resources Department upon an employee's resignation with approval from the supervisor of their original working unit, the computer system administrator shall disable such user ID to prevent access to the computer systems and store this user ID information according to the document storage criteria specified for this document.

3.2.2 Change of Job Duties

When notified of the transfer or change in job duties of employees from the Human Resources Department, the computer system administrator shall adjust their right to access the Company's computer systems as informed by the Human Resources Department.

4. Data Access Control

- 4.1 The Company has implemented security measures to control access to information. These measures include providing written basic security regulations and granting rights to only authorized personnel to access information and data processing programs. The Company also regularly reviews these regulations, which cover the following matters.
 - 4.1.1 Determining appropriate access rights to information and computer systems based on employees' job duties and responsibilities (SPI – CPR 106).
 - 4.1.2 Defining the roles and responsibilities of employees involved, such as requesters, authorized approvers, and access rights managers. (Announcement regarding signing responsibility and approval of general documents)
- 4.2 Employees' access to the computer systems is controlled by the access rights assigned to the user code (Username). Employees are required to provide their user ID (Username) and passcode (Password) every time they use the system and must always log off from the system after finishing their work.
- 4.3 For the security of data access with user ID and password on the computer system, employees must adhere to the following.
 - 4.3.1 Set the user ID's password of not less than 8 characters and not easily guessed. It must also be changed every 90 days or as appropriate for that system.
 - 4.3.2 Do not record a password in a place where others can access and use it.
 - 4.3.3 Do not use automatic password memorization programs.
 - 4.3.4 Do not share the user ID (Username) and password of every computer system with others.
 - 4.3.5 Do not access the computer system using a user ID that is not your own. If necessary, a document to assign the rights must be provided with approval from the supervisor in writing, except for the computer system administrator assigned by the Company.

5. Physical Security and Environment

- 5.1 Areas that require maintenance of security
 - 5.1.1 The Company determines the right to enter and exit restricted areas for only employees with relevant duties, including the provision of a rigorous control of the entry-exit system, and reviews such rights regularly.
 - 5.1.2 The Company provides security equipment to the computer center, such as smoke detectors, fire extinguishers, automatic fire extinguisher systems, backup power systems, and temperature and humidity meters, and ensures regular inspection and maintenance.

5.2 Computer and peripheral equipment

5.2.1 The Company stores important computer equipment such as servers and network devices in restricted areas and properly maintains the equipment to keep it in a ready-to-use condition.

5.2.2 Before cancelling the usage or selling computer equipment, the Company ensures that all data on the devices has been completely deleted and destroyed.

6. Security for Operations

6.1 Operating procedures and duties and responsibilities of the computer system administrator are as follows:

6.1.1 Maintain, improve and develop the computer system to ensure its efficient usage.

6.1.2 Notify employees in advance of the scheduled date and time to turn off and on the computer system for maintenance, improvements or changes.

6.1.3 Inspect the computer system usage to comply with company rules and regulations and follow orders from the supervisor assigned by the Company to suspend usage in the case that it may cause potential damage to the company.

6.2 The company has data backup for computer systems to ensure the continuity of operations as follows:

6.2.1 Data Backup

(1) A person responsible for backing up data shall set a program for the system to perform automatic backup at specified intervals and check the log when the backup is complete.

(2) The secondary storage media has a sticker indicating the backup of data and is kept off-site for safety in case of damage to the operating location.

(3) Arrange for testing of backup data and the data recovery process at least once a year or upon request to ensure that the computer system has been backed up.

6.3 Recording log data (Log File) and ensuring caution in retaining computer traffic data related to accessing internet services for 90 days from the date of service.

6.4 The Company provides the management of technical vulnerabilities as follows:

6.4.1 Automatically update Microsoft Windows via the internet.

6.4.2 Install firewall

6.4.3 Install an antivirus program on every computer.

6.5 The Company has planned an inspection of the computer system in accordance with the assessed risks in its risk management process, whereby the cyber security risk issues are surveillance and monitored for any incidents using the Treat Preventive Report and Antivirus Report.

7. Legal Compliance

7.1 Compliance with legal and contractual requirements

7.1.1. The Company examines various requirements by laws and the Company's needs in various contracts related to computer systems.

7.1.2. The Company uses legitimate software.

7.2 Review of computer system security

The Company has audited the operating procedures for computer system security to ensure adherence to the computer system security policy. The audit is conducted by an independent inspector who is not involved with the security management of the computer system. This inspector may be either the internal audit department of the business operator or external auditors to conduct the audit at least once a year.

Regulations for Using Computer Systems

1. Regulations that employees must comply with

- 1.1 Employees are prohibited from accessing computer systems with access prevention security measures specifically made by the Company or other individuals or disclosing such measures in any part or all parts that may potentially cause damage to the company or others.
- 1.2 Employees are prohibited from intercepting, receiving, sending, damaging, destroying, altering, changing, or adding to, whether in whole or in part, the Company's or others' computer data without permission.
- 1.3 Employees are prohibited from taking any actions that cause the Company's or others' computer systems to suspend, delay, obstruct, or disrupt resulting in an inability to work normally.
- 1.4 Employees are prohibited from sending computer data or electronic mail to others that conceals, disguises, or causes annoyance to the recipient without giving the recipient an opportunity to cancel or notify their intention to refuse to accept easily.
- 1.5 Employees are prohibited from using the Company's computer system to sell or disseminate instructions specifically created to be used as a tool for committing illegal acts.
- 1.6 Employees are prohibited from importing information into the computer system in a dishonest, deceptive, distorted, or forged manner, whether in whole or in part, or false information to cause damage to the Company or others.
- 1.7 Employees are prohibited from importing false data into the computer system that may cause damage to the security of the country, public safety, economic stability, or infrastructure that is of public benefit to the country, or cause panic among the people, or offences related to the security of the Kingdom, or offences related to terrorism as per the Criminal Code.
- 1.8 Employees are prohibited from importing into the computer system any data that is obscene in nature, and that such data may be accessible to the general public.

- 1.9 Employees are prohibited from importing into the computer system that may be accessible to the general public any computer data that appears as an image of another person and that such image is created, edited, added, or modified by electronic means or any other means in a manner that can damage the reputation of others, causing them to be despised, hated, or suffer from shame.
- 1.10 Employees are prohibited from importing into the computer system that the general public may access computer data that appears as an image of the deceased. This action is likely to cause the father, mother, spouse, or children of the deceased to lose their reputation, be disrespected, or be hated. or suffer shame.
- 1.11 When organizing meetings via electronic media, if sound and image are recorded, the meeting organizer must request permission from the participants before proceeding with the recording. The meeting organizer must also take care of and be responsible for the recorded information.
- 1.12 Employees must acknowledge and strictly adhere to the policies, requirements, rules and regulations, and recommendations for using the Company's computer system. This includes compliance with regulatory requirements and laws or acts related to computer use that may be announced later. Violation of these policies and regulations will result in disciplinary action in accordance with the Company's rules and regulations and the law.

2. Regulations that the Company must comply with

The Company will not cooperate, consent, or allow employees to take any action that is an offence according to the Computer Crime Act and other relevant laws. If the Company finds that any employees have violated this announcement, it will take legal action against the said employee.

The policy and regulations regarding the use of computer systems were approved by the resolution of the Board of Directors Meeting No.3/2022, dated 11 August 2022, and became effective from 11 August 2022 onwards.

Mr.Boomkiet Chokwatana

(Mr. Boonkiet Chokwatana)

Chairman

S&J International Enterprises Public Company Limited