Information Technology Security Policy

SiamEast Solutions Public Company Limited

Information Technology Security Policy

SiamEast Solutions Public Company Limited

The company has established a policy regarding the security of information systems for SiamEast Solutions Public Company Limited, in order to implement it effectively according to the policy. The policy is based on the authority of the Computer Crime Act B.E. 2550 (2007), including its amendments, and related laws. The details are as follows:

Objective

1. To provide the company with a policy framework for the operation and management of information technology and to ensure that all stakeholders involved with the company's information—including executives, personnel, external units, and individuals interacting with the company's information systems—have a clear plan and operational guidelines.
2. To ensure efficient coordination in service delivery, with maximum security and enhanced standards.
3. To establish appropriate preventive measures to control and minimize damages that may occur from situations where assets are unusable, lost, damaged, malfunctioning, or threatened in terms of security.
4. To inform users of prohibitions and practices to ensure the security of information systems and avoid violating related laws.

Definitions

"Company" refers to SiamEast Solutions Public Company Limited and its office that uses a shared computer network and information system.

"Computer" refers to an electronic data processing device that operates at high speed by executing commands via software to achieve desired results. This includes servers, personal computers (PCs), and portable computers (notebooks).

"Computer Equipment" refers to electronic devices used alongside a computer to support its operation, including computer hardware.

"Computer Network" refers to the company's computer network.

"Supervisor" refers to the person authorized to give orders according to the company's organizational structure.

"Personnel" refers to company employees, including probationary staff, temporary employees, or other individuals assigned to work under the company's contract.

"User" refers to an employee of the company or an external person who has been granted permission to use the

company's computer system.

"User Account" refers to the account used by a user to access and use the computer system, according to the agreement between the user and the system service provider.

"Data" refers to information that conveys meaning, facts, or anything else, whether the meaning is conveyed by the nature of the object itself or through any method, and whether in the form of documents, files, reports, letters, maps, charts, photographs, films, audio/video recordings, computer records, or any other method of recording that makes the information observable.

"Authentication" refers to the process of verifying the correctness of identity evidence that proves a person's claimed identity.

"System Administrator" refers to the person responsible for managing the company's computer network.

"High Privilege User" refers to a user account with the highest level of privileges.

"Personal Data" refers to personal data that is directly or indirectly related to the company, but excludes the data of deceased individuals.

"Data Controller" refers to the person assigned by the company to make decisions regarding the collection, use, or disclosure of personal data.

"Data Processor" refers to the person instructed by the data controller to carry out activities related to the collection, use, or disclosure of personal data.

"External Service Provider" refers to Obplus Company Limited or an external party or organization with specialized expertise in a specific area, capable of performing tasks better than the organization could on its own, under a contract in exchange for fees or benefits as compensation.

Roles, Duties, and Responsibilities

1. **Executive Committee (ExCo)**

   Approves the information technology policies, including any changes that may arise. Overall responsibility for the security of information assets to ensure that the developed information technology policies cover critical information, and that practices are aligned with the company's business objectives and the needs of users.

2. **Chief Executive Officer (CEO) / Deputy Chief Executive Officer (Deputy CEO) / Chief Financial Officer (CFO)**

   Approves procedures, including any changes that may arise, sets directions, and supports the development of information technology policies and related procedures. Decides on communication with law enforcement

agencies and investigative units when there is a suspicion of serious violations. Approves and supports information security activities and projects, and is a key figure in raising awareness of information security. Reviews, summarizes, and presents the information technology policy to the board for approval of implementation, including any changes that may arise.

3. **Department-Level Executives**

   Respond to information security incidents that have a significant negative impact on the organization or the company as a whole, such as incidents affecting the company's reputation, customer trust, and operations. They must report to the CEO, support investigations, and propose corrective actions for the information security incidents that occur.

4. **System Administrators**

   Develop and document supporting processes, guidelines, and operational procedures to ensure alignment with the information technology policy. Monitor and maintain the confidentiality, integrity, and availability of the information systems and assets under their control, ensuring proper protection and access control of these assets.

5. **Users**

   Understand the policies, procedures, and operational steps set by the company or relevant departments, and cooperate with regulations. Report information security incidents to supervisors and the IT department immediately, and assist in responding to such incidents.

6. **External Organizations**

   Assign confidentiality levels to information based on its importance to the company, according to policies and requirements. Ensure that relevant parties are informed, sign confidentiality agreements, and comply with the company's information technology policies when providing services. Take necessary actions to protect the confidentiality of information, information systems, and services provided by the company. Access to the information system should be restricted to authorized users only. Information obtained during work with the company must be treated as confidential, and no action should be taken that involves using, disclosing, transmitting, or modifying the information without explicit consent from the responsible company department. Report information security incidents immediately to the responsible company department and IT department, and assist in responding to the incidents.

7. **Data System Owners**

   Responsible for overseeing the use of information systems, such as data, applications, email, wireless LAN

systems, and the internet.

Section 1

Accountability, Identification, and Authentication

1.1 Users are responsible for protecting, maintaining, and safeguarding their account information (Username) and password (Password). Each user must have their own username and must not share it with others, nor should they disclose, distribute, or allow others to learn their password.

1.2 Users are responsible for any actions taken under their username, regardless of whether the actions are performed by the user themselves or someone else.

1.3 Users should set a password for logging into the computer system according to the following requirements:

1.3.1 The password must be at least 8 characters long.

1.3.2 The password must contain a combination of lowercase letters, uppercase letters, numbers, and symbols.

1.3.3 The password must not be based on the user's name, surname, family members' names, or the names of people with close personal relationships.

1.3.4 The password must not be based on words found in a dictionary.

1.3.5 The password will be suspended after five consecutive incorrect attempts.

1.3.6 The password must not be the same as any of the last three previously used passwords.

1.3.7 Users must change their password at least every 90 days.

1.3.8 High Privilege Users must change their password at least every 90 days.

1.4 Users must consent to identity verification checks by company staff or representatives without prior notice.

1.5 The system administrator will verify user account information to assess the user's continued status within the company and ensure that all rights are up-to-date. This will be reviewed at least once a year.

1.6 Access for High Privilege Users must be strictly controlled and granted only when necessary. The following factors must be considered:

1.6.1 A set usage period must be defined, and access must be suspended immediately once the time limit is exceeded or when usage ends.

1.6.2 A log must be maintained to track the access of High Privilege Users each time they use the system.

1.7 The system administrator will prepare a user list every three months to monitor if any users have been canceled, transferred, or are still active.

Chapter 2

Asset Management

2.1 Users must not connect any tools or other equipment to the network for personal business purposes.

2.2 Users must not use or delete other people's files under any circumstances.

2.3 Users must not copy or duplicate files that are copyrighted without obtaining permission.

2.4 Users are responsible for the assets assigned to them by the company as if they were their own. The asset lists that users are responsible for will be documented in the "Asset Loan Agreement." This regulation requires that asset receipt and return be recorded and verified each time.

2.5 Users are liable for any damages to assets, whether they are damaged or lost, according to the asset's value, if the damage is caused by the user's negligence.

2.6 Users must not allow others to borrow computers or laptops under any circumstances, unless the loan is approved in writing by an authorized person.

2.7 The assets and information systems provided by the company are intended for company use only. Users are prohibited from using company assets and information systems for activities not defined by the company or that could cause harm to the company.

2.8 The company has a maintenance schedule, detailed maintenance procedures, and a Maintenance Checklist for each piece of information equipment.

Chapter 3

Corporate Management

3.1 Users must be aware and cautious when using data, whether it is company data or external data.

3.2 All data stored within the company's assets is considered company property. It is prohibited to disclose, modify, reproduce, or destroy this data without permission from the supervisor.

3.3 Users are responsible for safeguarding and maintaining company data or client data. If data is lost, misused, or disclosed without authorization, the user must share responsibility for the resulting damage.

3.4 Users must protect, maintain, and ensure the confidentiality, accuracy, and availability of data.

3.5 Users have the legal right to store, maintain, use, and protect personal data as they see fit. The company will support and respect personal privacy rights and will not allow any individual to violate personal data without permission from the data owner, unless the company needs to investigate the data or believes it is related to company operations. In such cases, the company may designate an authorized person to conduct an investigation at any time, without notifying the user.

3.6 Users have the right to request additional/change/cancel permissions within the information system by following these steps:

3.6.1 Employees must fill out a request form to access or cancel access, providing the reasons.

3.6.2 The employee's supervisor must approve the request for a change in permissions.

3.6.3 The system administrator will implement the changes to the permissions.

3.7 Data Access Control

3.7.1 A user account system is established for accessing information, categorized by user groups and their rights.

3.7.2 Access rights to information systems are granted as follows:

3.7.2.1 Define the rights of each user group, such as:

- Read-only
- Create data
- Input data
- Modify data
- Approve
- No rights

3.7.2.2 Guidelines for suspending, canceling, or delegating authority will follow the rights defined by the company.

3.7.2.3 Users seeking to access the organization's information systems must request and receive approval from the designated system administrator.

3.7.3 The company categorizes data into three levels of importance:

- Data of highest importance
- Data of medium importance
- Data of low importance

3.7.4 The company classifies data confidentiality levels as follows:

- Top-secret: Disclosure of all or part would cause severe damage.
- Highly confidential: Disclosure of all or part would cause serious damage.
- Confidential: Disclosure of all or part would cause damage.
- Public: Information that can be disclosed or published freely.

3.7.5 The company defines access levels as follows:

- Executive level
- General user level
- System administrator or assigned personnel level

3.7.6 The data owner of each system is responsible for controlling and authorizing changes to the data in the systems they manage.

3.8 Control of wireless network access from external parties: To prevent unauthorized access to wireless network services, individuals seeking access must fill out an Internet service request form and log in with their user name. Authentication via password is required before access.

3.9 The company aims to review access rights to various systems at least once a year.

3.10 Access logs are recorded for all types of user accounts.

3.11 Activity logs are recorded for critical operations, including:

3.11.1 Changes to database structures and data modifications (Update/Insert/Delete).

3.11.2 Changes to system security settings.

3.11.3 Changes to user accounts and access rights.

3.12 Collection of personal data: When collecting personal data, the data controller must inform the data owner unless the data owner is already aware of the details. Consent must be obtained from the data owner before using or accessing the data.

3.13 Use or disclosure of personal data: The data controller is prohibited from using or disclosing personal data without the

consent of the data owner, except for data collected under exemption from consent requirements.

3.14 The data owner has the right to access and request copies of personal data related to them stored by the data controller or request disclosure of the source of such personal data that they did not consent to.

Chapter 4

IT Infrastructure Management

4.1 Users are prohibited from presenting illegal information, violating copyrights, displaying inappropriate messages or images, or anything contrary to the moral traditions of Thailand, especially when creating web pages on the computer network.

4.2 Users must not open or run Peer-to-Peer programs or similar high-risk programs, such as BitTorrent, eMule, etc., unless authorized by a supervisor.

4.3 Users are prohibited from using the company's communication resources or other provided equipment to disseminate information, messages, images, or anything that conflicts with morality, national security, laws, or the company’s mission.

4.4 Users are prohibited from using the company’s communication resources or other equipment to disrupt, cause damage, or engage in data theft or any other illegal or immoral activities that affect the company’s mission.

4.5 Users must not use any company resources for commercial purposes.

4.6 Users are prohibited from engaging in data interception, including messages, images, sounds, or anything else on the company’s information network, by any means.

4.7 Users must not interfere with, damage, or cause the company's information systems to stop functioning.

4.8 Users are prohibited from using the company's information systems to control external computers or information systems without authorization from the appropriate authority.

4.9 Users must not engage in any actions that involve unauthorized use or knowledge of another individual's personal credentials, for the purpose of accessing information or using resources.

4.10 Users must not install any equipment or take actions to access the company’s information systems without authorization from the relevant authority.

Chapter 5

Supplier Relationship & Services and **Logging & Monitoring**

Supplier Relationship & Service Policy

1. An agreement must be made to control the services provided by external suppliers, such as accepting the company's information security policies and service scope, details, and service levels. The agreement must be reviewed by the legal department, including a confidentiality agreement regarding the company's information.
2. External suppliers who are authorized to access the company's information systems must accept and comply with the company's information security policies.
3. The company will assess the risks associated with external suppliers accessing the information systems or having an impact on the company. If it is necessary to disclose such information, the external supplier must sign a confidentiality agreement to protect the company's secrets.
4. The company will review services or agreements made with external agencies and individuals who provide services to the company. This review will be done regularly as necessary, including updating the terms of service with external suppliers, such as when information systems are upgraded, new information systems are developed, or new technologies are introduced.

5.1 Domain Name: se.local consists of the following:

5.1.1 AD (Active Directory Users and Computers): The service provider (Orb Plus Co., Ltd.) will manage the addition and removal of user accounts for the service user (SiamEast Solutions Public Co., Ltd.) with a maximum of 5 changes per month. The service user must submit a request for the addition/modification of User AD to Orb Plus Co., Ltd. (according to the IT system usage manual).

5.1.2 DNS (Domain Name System): This involves converting the Domain Name into the IP address of each computer in SiamEast Solutions Public Co., Ltd.

5.1.3 GPO (Group Policy Management): This involves adding, removing, and setting the access rights of each user according to the policy defined by the service user (Orb Plus Co., Ltd.), based on the organizational structure (according to the IT system usage manual).

5.1.4 VPN (Virtual Private Network): This service creates a secure private network connection between devices via the internet, allowing data to be transmitted safely and anonymously. The VPN hides the user's IP address and encrypts the data to prevent unauthorized parties from accessing it through the Global Protect program (according to the IT

system usage manual).

5.2 DHCP Configuration Hostname (IP Address Allocator): "BKKVMDC01."

The service provider will use ClearPass Authentication Aruba control to verify the IP address and USER DOMAIN registered, allowing access to SiamEast Solutions Public Co., Ltd.'s data according to each user's privileges, and the login logs of the users can be monitored.

5.3 E-mail Exchange or Mail Server: The service provider will provide the following:

- Email Hosting: @siameastsolutions.com
- SMTP server (Simple Mail Transfer Protocol Server): Responsible for sending emails from the server to other destinations.
- POP server (Post Office Protocol Server): Receives emails from client machines to check for viruses or harmful emails (SPAM). If an email is deemed harmful, it will be quarantined in Bright Mail before notifying the user, with antivirus mail gateway installed.
- Record: For routing incoming emails to the Mail Server.
- Bright Mail: Email filtering program using Kaspersky Messaging Gateway to filter safe emails and block harmful ones. Emails identified as dangerous cannot be opened to ensure safety.
- Logs are maintained for all incoming and outgoing emails, and their statuses can be checked through the Kaspersky Secure Mail Gateway.

5.4 Web Server includes the following services:

- Web Hosting: Website: https://www.siameastsolutions.com
- Database: www.siameastsolutions.com
- SSL installation to confirm email security.

5.5 Backup: The service provider will back up data from the Mail Server and Web Server onto the Harddisk Server to protect data integrity:

5.5.1 Daily Incremental Backup stored on Storeonce Harddisk, with a retention period not exceeding 10 days.

5.5.2 Weekly Differential Backup stored on Storeonce Harddisk.

5.5.3 Monthly Full Backup stored on Tape Backup at the end of each month and sent to the service user with a report on data restore testing.

5.5.4 The service user can request data restoration (Restore) from the Storeonce Harddisk. Data is stored both at the service provider's site and at the service user's site for Tape Backup.

5.6 Internet UIH media: The service provider will switch the internet connection from TOT to UIH Orbplus automatically when the main internet signal is down.

5.7 The service provider provides Orb Plus support for Firewall and server maintenance on Server Name: BKKVMEXP01, located at the service user's office, as follows:

5.7.1 The service provider will check the server's performance, such as CPU, RAM, and disk usage, ensuring they do not exceed 80%, using Remote Desktop.

5.7.2 Check the Firewall license and operations. If problems occur, the service provider will assist in coordinating the resolution, and any changes to hardware will be the responsibility of the service user.

5.7.3 The Express for Account program will be backed up daily at 24:00, with the data stored on BKKVMFS02 at the service provider's server, which has high security measures.

5.8 The Salesystem program is an effective sales management tool, where user access rights to the program are determined based on the service user's policies (according to the procedure for adding/removing users).

5.9 Logging & Monitoring of Information Systems: Logs are records of events within the information system, and logs from the systems storing and processing data should be monitored and followed up on. Specifically:

5.9.1 Email: Logs are maintained for all incoming and outgoing emails, and their statuses can be checked via the Kaspersky Secure Mail Gateway.

5.9.2 Internet access within the company network can be monitored through ClearPass Authentication Aruba control, verifying the IP address and USER DOMAIN registered.

5.9.3 The Express for Account program can monitor users who modify or access information.

5.9.4 The Salesystem program tracks who created, modified, approved, and canceled documents.

The service provider (Orb Plus Co., Ltd.) has policies for tracking information systems as follows:

- Events related to the use of information systems and user activities must be regularly logged, and data related to information system usage must be protected from unauthorized changes or edits. Also, the actions of personnel involved in those systems must be logged.
- Errors related to the systems should be logged, analyzed, and corrected as necessary. The time on all company computers must be synchronized with an accurate time source for auditing purposes.
- If a company system is breached, access and use of the information systems by employees must be reviewed and audited periodically by the internal audit department, which has the authority to oversee any suspected violations

of these policies.

Chapter 6

Law and Compliance

All laws enacted in Thailand, including the regulations of the company, are essential for users to be aware of and strictly comply with, and not to violate. Therefore, if a user commits a violation according to the relevant laws, such violation will be considered the personal responsibility of the user, and the user will be held accountable for the offense that occurs.

Relevant laws and regulations:

1. The Personal Data Protection Act B.E. 2562 (2019)
2. The Computer Crimes Act B.E. 2550 (2007) and its amendments (No. 2) B.E. 2560 (2017)
3. The Copyright Act B.E. 2537 (1994) and its amendments (No. 2) B.E. 2558 (2015) and (No. 3) B.E. 2558 (2015)
4. The Royal Decree on Secure Methods for Electronic Transactions B.E. 2553 (2010)
5. The Ministry of Information and Communication Technology's Notification on the Retention of Computer Traffic Data of Service Providers B.E. 2550 (2007), and the Electronic Transactions Commission's Announcement on the Policy and Practices for Ensuring Information Security of Government Agencies B.E. 2553 (2010) and its amendments (No. 2) B.E. 2556 (2013)
6. The Electronic Transactions Commission's Announcement on the Standards for Ensuring Information Security of Systems Using Secure Methods

Enforcement

This Information Technology policy will be enforced from the date of its announcement to all users of the information systems of SiamEast Solutions Public Company Limited, without exception. All employees, at all levels, are required to strictly follow the policy and regulations. If a supervisor finds that a subordinate has violated the policy, the supervisor must report the violation in accordance with the chain of command to enforce discipline against the offender. Neglecting duties is considered an offense, just as much as committing the violation itself.

Policy Dissemination

The Information Technology Department is responsible for announcing and disseminating the policy to users of the company's information systems, in order to help them understand their role in using the information technology and protecting the company's assets.

Policy Review

The company will review the information systems policy to ensure it remains up-to-date and consistent with the company's needs. The review will take place annually or, in case of urgent circumstances, the policy will be reviewed and updated before the scheduled review date.

Offenses and Penalties

Offense: A user intentionally violating the company's information security policy, even if the violation is not fully successful, will still be considered a complete violation.

Penalty: Violations of the company's policies and regulations will result in disciplinary action according to the company's regulations and applicable laws.

Chapter 7

Human Resource Security

7.1 Responsibilities for information security are clearly defined for users or external contractors performing work on behalf of the company, including the establishment of measures to protect and maintain the security of the company's information.

7.2 The qualifications of all job applicants must be thoroughly checked, such as verifying reference letters, work history, educational qualifications, or companies that can be referred to, as well as completion of training programs. New employees must also be made aware of basic security awareness and sign a consent form for using the company's information technology systems securely.

7.3 Training must be provided to all users regarding awareness and practices to maintain information security. The signed acknowledgment must be stored in the employee's file. If there are any changes in security protocols, employees must be informed.

7.4 Disciplinary actions must be defined for those who violate the company's policies, rules, and practices. If a violation involves breaking the law, the penalties will be based on the specific offense and in accordance with the company's regulations.

7.5 In the case of appointments, transfers, dismissals, or changes in position, the human resources department must inform the employee, and the employee must adhere to the terms of the employment contract until the end of employment. Employees who leave the company for any reason must return any company property related to information systems, such as keys, employee ID cards, access cards for the data center, peripheral equipment, manuals, and documents, to their supervisor before their last working day. The IT department must also revoke access rights for these systems.

Chapter 8

Software Licensing and intellectual property

8.1 The company places great importance on intellectual property. Therefore, software that the company authorizes for use or holds the copyright for, may be used by users as necessary for their duties. The company prohibits users from installing or using any software that is not licensed. If a violation of copyright is detected, the company considers it a personal offense, and the user will be solely responsible for it.

8.2 The software provided by the company for users is essential for work purposes. Users are prohibited from installing, uninstalling, modifying, altering, or copying the software for use elsewhere.

Chapter 9

Preventing Malware

9.1 Users' computers must have antivirus software installed as specified by the company, unless the computer is for educational purposes related to system development, and prior approval from the supervisor is required.

9.2 Any data, files, software, or other items received from other users must be scanned for viruses and malicious programs before being used or stored.

9.3 Users must regularly update and patch their operating systems to prevent potential damage.

9.4 Users must always be cautious of viruses and malicious programs. If any abnormalities are detected, users must report the issue to the system administrator.

9.5 If a user discovers that their computer is infected with a virus, they must disconnect the computer from the network and notify the system administrator.

9.6 Copying, modifying, or deleting data, messages, documents, or anything that is company or third-party property without authorization is strictly prohibited.

9.7 Users are prohibited from distributing computer viruses, malware, or any harmful programs that could cause damage to the company’s property.

Chapter 10

Electronic mail

10.1 The practices or prohibitions in this section are in accordance with the "Computer Crime Act B.E. 2550" (2007), Section 11, which states that anyone who sends computer data or electronic mail to another person by concealing or falsifying the source of the data, disrupting the normal use of another person's computer system, shall be liable to a fine not exceeding 100,000 Baht.

10.2 The company has established guidelines regarding the use of the electronic mail system (Email) as follows:

10.2.1 All email accounts and emails created and stored on the company's computer systems or networks are considered company assets.

10.2.2 The email storage space on the company's central mail server (Mailbox Size) must be no less than 1 TB. The company has set the following mailbox size limits for users: • General employees: 4 GB • Managers and above: 10 GB When the email volume approaches the set limit, users will receive a notification. If the email volume exceeds the storage limit, users must back up the data (Backup) and delete unnecessary emails from their mailbox to maintain the storage space as per the company's specifications.

10.2.3 The company prohibits the use of company email accounts for any illegal activities, violations of laws or regulations, or actions that contravene any company policies.

10.2.4 Users must draft email content carefully, always considering that the email is being sent on behalf of the company. Users must not send or forward emails with content or images that damage the reputation of others, involve racism, threats, obscene material, sexual harassment, or emails with content that could cause cultural or religious controversy, or that affect national security or the monarchy, or any file unrelated to work that could harm the company.

10.2.5 Users must exercise extra caution when opening email attachments from unknown senders, as these attachments may contain viruses, email bombs, or malware (trojans).

10.2.6 If a user receives a notification from antivirus software that their computer has a virus, they must immediately cease sending emails until the computer is fixed and restored to normal.

10.2.7 The company does not permit the use of personal email accounts for communication or contacting others on behalf of the company. Only the company email account should be used.

10.2.8 Employees are prohibited from accessing other people's email information without authorization.

10.2.9 Company email addresses should not be used to register on websites unrelated to the company’s work.

10.2.10 Sending spam emails is prohibited.

10.2.11 Sending chain emails is prohibited.

10.2.12 Sending emails that violate intellectual property laws or infringe on the rights of others is prohibited.

10.2.13 Sending emails with malicious software to others intentionally is prohibited.

10.2.14 Forging another person's email is prohibited.

10.2.15 Sending or receiving emails on behalf of another person without authorization is prohibited.

10.2.16 Users must use polite language when sending emails.

10.2.17 For sending critical emails, always mark the subject with "This is Confidential Information."

10.2.18 Emails larger than 25 MB are prohibited.

10.2.19 Emails containing confidential information of the company must be sent using secure methods as specified by the company and the software development contractor.

10.2.20 Users must carefully check the recipient's email address to prevent sending emails to the wrong

person.

10.2.21 The sender's name must be included in every email sent.

10.2.22 The recipient list for an email should be limited to those who need to know the information in the email.

10.2.23 Regularly back up email data as necessary.

10.2.24 When sending emails to clients containing operational data, such as daily or monthly reports, or emails containing Confidential Information, the following guidelines must be followed:

10.2.24.1 Only authorized individuals or groups are allowed to send emails to clients.

10.2.24.2 Emails must be prepared by the relevant staff member and sent to authorized individuals who are permitted to send emails to clients.

10.2.24.3 The authorized individual must verify the email content before sending it to the client.

10.2.24.4 Emails should be sent to clients using the "forward" function if no errors are found. If errors are detected, the email must be sent back to the preparer for correction before being re-sent for review.

10.2.24.5 When sending an email, it must be encrypted if there are attachments, in accordance with the company’s data encryption and transfer policy.

Chapter 11

System Development and Change Management

The company recognizes the necessity of developing computer systems and information systems. The existing system is outdated, involves multiple steps, and is cumbersome in gathering data, making it difficult to provide the required information for summarizing reports for management to track the overall performance of the company. Therefore, it is essential to develop and improve an information system that can help make internal operations and management processes more efficient.

11.1 The development or modification of the information system shall adhere to the following criteria:

11.1.1 Guidelines should be set to align with the objectives, goals, and business operations of the company.

11.1.2 Personnel should be provided with knowledge and understanding to ensure cooperation from the

involved employees.

11.1.3 Methods and techniques should be selected that are suitable for the nature of the information system.

11.1.4 Technology: The company must carefully consider the selection of information technology to ensure it is appropriate for the nature, scope, and budget.

11.1.5 Budget: A sufficient and appropriate budget should be prepared in advance to support the development.

11.2 Project Management:

11.2.1 Establishing a development team: The company should appoint individuals with knowledge and expertise to be responsible for the system development process, including the following roles:

11.2.1.1 Steering Committee

11.2.1.2 Project Manager

11.2.1.3 MIS Manager

11.2.1.4 System Analyst

11.2.1.5 Technical Specialist

11.2.1.6 Users and General Managers

11.3 Defining the system development process to ensure maximum efficiency in development should include the following steps:

11.3.1 Defining and selecting the project: The decision from the committee, such as approval, disapproval, or project postponement.

11.3.2 Starting and planning the project: Set up the team, assign responsibilities, study the feasibility of the project, and consider the return on investment, costs, and the cost-effectiveness of system development.

11.3.3 System analysis: This step involves data collection.

11.3.4 System design: The design should include both logical and physical aspects.

11.3.5 System implementation: This includes procuring equipment, writing programs, testing, preparing documentation, transferring systems, and training users.

11.3.6 System maintenance: There should be procedures for maintaining the system to ensure its

efficiency.

11.4 The company may consider the appropriateness of using the following methods for the development of information systems:

11.4.1 Outsourcing services

11.4.2 Using pre-packaged software applications (Application Software Package): This is an alternative for developing computer and information systems, such as payroll systems, accounting systems, or inventory control systems. If the pre-packaged software meets the company's needs and objectives, the company may not need to develop its own systems. Pre-packaged software is already designed and tested, helping to reduce costs and time in system development, and makes testing, installation, and maintenance easier.

Chapter 12

Server Room

To ensure the security of the equipment and data inside the Server Room, the following guidelines for accessing and using the Server Room are established:

12.1 Access to and Usage of the Server Room

12.1.1 Authorized personnel allowed to access include computer operators and system administrators.

12.1.2 Other department staff may need to enter the data center occasionally but must obtain permission by filling out an access request form.

12.1.3 A staff member should be assigned to monitor the operation of the data center at all times. There should be a system in place to record all entries and exits, including details about the individual and the time of access.

12.1.4 Unauthorized individuals are strictly prohibited from accessing the Server Room.

12.2 Access to and Usage of the Server

12.2.1 Every time the server is accessed or maintained, the activity must be recorded. The logs must be reviewed for the past month, and the contractor's staff will retrieve the data for review by the responsible personnel of SiamEast Solution Public Company Limited. The log will be stored for a period of 6 months.

12.3 Installation of Other Electronic Devices in the Server Room

12.3.1 Installing any electronic devices in the Server Room is prohibited without authorization, as this could potentially damage the equipment and information system, such as fire protection water sprayers or devices that emit radio waves.

Chapter 13

Data Backup and Recovery

To establish measures for backing up and recovering data from the server (Server), the main equipment responsible for linking the network system, and to prepare for emergency situations or events that cause damage to information, ensuring data can be recovered within a reasonable time frame.

There are correct procedures for creating backups and recovering data across software systems and IT systems, with specific steps for each IT system. The backed-up data should be stored on storage media in a backup location installed at a different site. The backup storage media should be tested regularly.

13.1 **Data Backup**

13.1.1 Backup data using semi-permanent backup devices.

13.1.2 Perform data backups on every business day.

13.1.3 Backed-up data must be stored in a safe location, separate from the Server room or stored with designated personnel.

13.1.4 The system administrator must record the results of each backup for tracking and review.

13.2 **Backup Storage Capacity**

13.2.1 Backup storage devices must have a minimum capacity of 3 TB.

13.3 **Restore Process (System Recovery)**

13.3.1 Before making any changes or updates to data on the server or modifying configurations on any devices, always back up the data first.

13.3.2 Test the system recovery process at least once a month.

13.3.3 Notify users before performing a system recovery.

13.3.4 Perform the restore process and verify the accuracy of the data and document the results. (As per the IT system user manual).

Chapter 14

Business Continuity Management

Objective

To establish guidelines for managing the continuity of information system services in the event of emergencies or any information security incidents that may disrupt the company's business operations.

14.1 There must be a backup data center and backup information systems to ensure continuous business operations and reduce the impact when an incident occurs that disrupts business operations. The highest-level executive of the company will have the authority to make decisions and issue orders in such cases.

14.2 The service user departments and the Information Technology (IT) department must control and oversee the development of a business continuity management plan under established standards and ensure its dissemination to relevant parties. The business continuity management plan should be tested at least once a year.

14.3 The IT department must perform backups of data, documents, software, systems, as well as essential equipment and personnel, to support the fastest recovery of information systems after a disruption in service or a disaster.

14.4 The company has a Business Continuity Plan (BCP), which follows the steps and practices outlined in the company's BCP.

Chapter 15

Information System Risk Management Plan

Definition of Information System Risk

An information system risk refers to any event or action that may occur in uncertain circumstances and could impact, cause damage, failure, or reduce the chances of achieving success in managing an information system that uses computers for administration.

Definition of Information System

An information system is the system of data management, data storage, data processing, the flow of information both inside and outside the organization, and the presentation of information.

Components of a Computer System

1. **Hardware**: Refers to various devices that interact with data and documents, both computer and non-computer equipment.
2. **Software**: Refers to the set of instructions that command the computer to perform tasks.
3. **Personnel**: Refers to the individuals who work with the information system, managing data and extracting results from the computer system.
4. **Data and Files**: Refers to the data and information that the system stores over a period of time.
5. **Operational Functions**: Refers to the commands or rules used in the operation of the system.

Components of an Information System

- **Organization**: The structure of the organization; the information system will support the overall functioning of the organization, regardless of the department.
- **Personnel**: The individuals who use the information system from the computer system, including those who input data into the system for processing.
- **Technology**: The equipment used to manage information and deliver it to personnel utilizing the information system.

Note: The components of an information system that utilizes computers for management consist of both the computer system components and the organizational system components combined.

Risk Management

Risk management is the practice of controlling risks, which involves risk planning, assessing risks in various areas, developing alternatives for risk management, and monitoring risks to determine how they change over time.

Description of Risk

Risk Name	Risk Type	Risk Description	Risk Factor/Threat	Impact/Impacted Parties
1. Risk of unauthorized access to others' data	Operational Risk	Users lack caution when accessing the information system, such as sharing passwords or allowing others to use their account.	- Impersonation or identity spoofing - Unauthorized access to/alteration of data	- Users - Information System - Database System
2. Risk of unauthorized devices being connected	Operational Risk	Users fail to secure the network, such as connecting wireless routers or switches/hubs to the network without permission, leading to connectivity issues or security vulnerabilities.	- Unauthorized connection of devices - Technical failure	- Users - System Administrators - Information System - Database System - Servers
3. Risk from electrical disruptions (power failure, unstable voltage)	Emergency Risk	Power disruptions or voltage instability could damage computers and equipment, potentially causing data loss or preventing certain services from restarting.	- Power source failure or unstable voltage	- Users - System Administrators - Servers - Network Equipment - Computers - Database System - Information System

4. Risk of intrusion by malicious outsiders	Technical Risk / Operational Risk	Attack or intrusion by malicious entities (e.g., hackers), including data interception, malicious commands, viruses, or worms, leading to security vulnerabilities.	- Hackers - Crackers - Denial-of-Service (DoS) attacks - Data interception - Malicious commands - Software defects - Viruses/Worms	- Users - System Administrators - Servers - Database System - Information System
5. Risk from personnel shortage	Management Risk	A shortage of IT staff may cause operational delays if key personnel cannot work, or if the number of staff is insufficient to meet the growing demands of the information system.	- Government policies	- Users - System Administrators - Servers - Network Equipment - Database System - Information System
6. Risk from changes in management policies	Management Risk	Changes in leadership may lead to altered management policies, disrupting projects and ongoing initiatives.	- Users - System Administrators - Servers - Network Equipment - Database System - Information System	
7. Risk from insufficient budget support	Management Risk	Insufficient budget allocation may prevent the information system from operating efficiently and continuously.	- Users - System Administrators - Database System - Information System	

9. Risk from political instability or civil unrest	Emergency Risk	Violent or unstable situations may prevent personnel from performing their duties.	- Protests - Riots - Terrorism	- Users - System Administrators
10. Risk from computer or equipment failure	Technical Risk	Equipment failure due to technical issues or damage from rodents/insects.	- Technical failure - Rodent or insect damage	- Users - System Administrators - Servers - Network Equipment
11. Risk from theft of computers or equipment	Management Risk / Operational Risk	Theft of computers, computer equipment, or components (e.g., CPU, RAM), resulting in work disruptions or data loss.	- Theft	- Users - System Administrators - Servers - Network Equipment

Risk Estimation

Risk estimation involves assessing the likelihood of an incident or event occurring, as well as the potential consequences and the severity of damage. The criteria used for risk estimation include the level of likelihood of a risk occurring, the severity of its impact, and the level of risk itself. The department uses the following criteria:

Likelihood Levels of Events

Level	Likelihood of Occurrence	Description
5	Very High	5 times/year
4	High	4 times/year
3	Medium	3 times/year
2	Low	2 times/year
1	Very Low	No more than once/year

Impact Severity Levels

Level	Impact	Description
5	Very High	Total loss to critical IT systems and severe data security damage
4	High	Issues with critical IT systems and security that impact some data accuracy
3	Medium	System issues with limited loss
2	Low	Minor issues that can be fixed
1	Very Low	Insignificant issues

Risk Level Calculation = Likelihood Level × Impact Severity Level

- 1-5 = Low risk (Low impact, low likelihood)
- 6-10 = Acceptable risk (if 8-9, monitor closely)
- 11-15 = High risk (Present a risk mitigation plan within 15 days and monitor quarterly)
- 16 and above = Very high risk (Present a risk mitigation plan immediately within 7 days and monitor monthly)

Risk Map

Risk level measurement:

- **High Risk**: High impact, high likelihood
- **Medium Risk**: High impact, low likelihood
- **Low Risk**: Low impact, low likelihood

Risk Reporting

Once the risk assessment is completed, a report must be created that others can read. This document is key for communicating risk details throughout the organization. The report should include at least the following details about the risks:

1. **Management** should receive this information to:
    - Understand the significance of the risks the organization faces.
    - Recognize the effects on stakeholders in case an event occurs and damages operations or performance.
    - Promote awareness of risk issues throughout the organization.
    - Understand potential impacts on stakeholders' confidence.
    - Ensure risk management processes are effective.
    - Formulate policies regarding risk management, including the responsibilities of departments and individuals.
2. **Department Heads** should receive this information to:
    - Recognize risks related to their responsibilities and the potential effects on other departments or activities.

- Have performance indicators for activities to determine the impact of risks on operations.
- Report impacts from risks if they occur or are about to occur and suggest solutions.
- Report any new risks or failures in control measures for information protection.

3. **Employees** should receive this information to:
   - Understand their roles and responsibilities in managing each risk.
   - Understand the importance of continuous risk management development.
   - Recognize risk management as an important organizational culture.

Risk Treatment Process

Once the management receives the risk assessment report, it is necessary to make decisions based on the organization's risk acceptance criteria, whether to accept the risk without taking action or to proceed with risk treatment. The following are the processes involved:

1. **Risk Acceptance**

   This involves accepting the risk without taking any action and acknowledging the potential consequences. For example, if the authentication is done using only ID/password, there is a risk of it being stolen. Implementing biometric systems such as fingerprint or iris recognition could be costly and may not be worth the investment. In such cases, a hospital may accept the current system's risks and continue working without making any changes.

2. **Risk Avoidance**

   Risk avoidance means eliminating the risk by changing the way things are done. For instance, if a hospital currently backs up data in only one copy, which poses a risk of data loss, they may avoid this risk by making two backups and storing them in separate locations. Additionally, managing network connections via modems may become too difficult to control or manage, so the organization may choose to suspend this service and recommend employees use the ISP service during virus outbreaks. For example, the organization may also suspend the use of computers without antivirus software.

3. **Risk Transfer**

   Risk transfer involves shifting the responsibility for managing a risk to a third party. For example, when

purchasing networking equipment that comes with only one year of warranty, the organization may decide to purchase insurance or a maintenance service contract to cover the risk of the equipment failing.

4. **Risk Reduction**

   Risk reduction refers to implementing additional or stricter controls to mitigate the risk. For instance, using biometric authentication, in addition to the existing ID/password system, can reduce the risk of unauthorized access.

Residual Risk Reporting

Once risk treatment measures have been implemented, it is necessary to continuously report and review to assess whether the risk evaluation and control measures are effective. Standard practices typically involve internal or external departments conducting IT auditing processes. Since the environment and regulations are dynamic and change frequently, regular risk management and auditing are essential.

Monitoring

Monitoring ensures that the organization has appropriate and necessary risk management measures in place, that these measures are being followed, and that they are producing effective results. The monitoring process should consider whether:

1. The measures are being properly implemented and yielding results.
2. The established processes are feasible and can be carried out.
3. Learning has occurred within the department as a result of risk management efforts.

Conclusion

Risk management plays a critical role in protecting the organization's data and IT network systems, which are valuable assets. It also protects the "mission" of the organization from risks related to information technology. The risk management process should be the primary responsibility of the IT department, led by experts in information technology and supported by the organization's management. The organization must have a suitable and standardized process for managing IT and communication risks to safeguard against potential damage from risks and ensure the achievement of organizational objectives. This process should not only protect IT assets but also the organization as a whole.

Chapter 16

Incident Management Control

1. **Principles and Background**

Currently, the company has increasingly implemented information technology in its internal management and operational support. Along with the development of information technology to facilitate usage and information creation, organizational development planning, management, and personnel operations, the volume of information data is growing. Therefore, it is necessary to manage databases, monitor, store, and maintain information to ensure security and readiness for efficient use at all times.

The company has incorporated information technology to enhance operational efficiency and provide better services to the public, as well as to ensure greater convenience for personnel. At the same time, the information technology system may be at risk of damage due to attacks from computer viruses, personnel, electrical issues, fire hazards, or other internal and external factors, which may lead to operational disruptions. Therefore, to prevent and address these issues, it is necessary to have an emergency response plan for potential information technology system disruptions.

2. **Objectives**

2.1 To provide guidelines for maintaining the security and stability of databases and information technology systems, ensuring their readiness for use.

2.2 To reduce potential damage to the information technology system.

2.3 To ensure that the information technology system can operate continuously and effectively, capable of responding to emergencies promptly.

2.4 To prepare for possible emergency situations affecting the information technology system.

2.5 To foster mutual understanding between management and staff in maintaining the security of databases and information systems.

3. Risk Analysis

As the company increasingly relies on information technology for its operations, it is essential to manage information technology risks. This includes identifying preventive measures, reducing the likelihood of potential damages, and establishing methods for assessing and evaluating information security risks that may

impact the company's information technology systems. Ensuring the security, efficiency, and stability of these systems is crucial to maximizing the benefits of information technology in supporting operations.

The company's risk analysis and assessment have identified several categories of risks that may pose threats to its information technology systems:

1. **Technical Risks** – Risks arising from computer system failures, hardware and equipment malfunctions, cyberattacks from viruses or malicious programs, disruptions by hackers, system breaches by crackers (whether intentional or accidental), power outages, and other technical issues.
2. **Operational Risks** – Risks stemming from improper handling of system access, where users may access or utilize information beyond their authorized permissions. This can lead to unauthorized modifications, misuse, or even damage to critical data and information.
3. **Emergency or Disaster Risks** – Risks caused by natural disasters or severe events that could result in significant data loss or system failures, such as fires, building collapses, protests, or civil unrest.

Based on the company's risk assessment, these risks pose potential threats to its information technology systems. Therefore, to ensure the efficiency, security, and stability of these systems and to maximize their support for business operations, it is necessary to establish an **Emergency Response Plan**. This plan will serve as a framework for safeguarding the company's information technology systems, maintaining data integrity, and addressing potential threats that may impact database security and overall IT infrastructure.

4. Emergency Response Plan

4.1 Emergencies Arising from Technical Issues

4.1.1 Failure of Antivirus Protection

- In case of a virus or an intrusion, limit network connectivity to prevent further spread within the system.
- Analyze the cause and impact of the virus outbreak.
- Implement network security measures to contain the virus.
- Monitor and fix infected devices.
- If a computer becomes inoperable, notify the IT administrator. If the IT system is unable to provide network services, the IT administrator must inform all departments.

4.1.2 Failure to Prevent Intrusions

- In case of an intrusion, the system administrator must analyze the cause and impact by checking logs and firewall settings.
- The system administrator must immediately notify management.
- Take actions to stop the intrusion and close vulnerabilities.

4.1.3 Network Failure

- Quickly analyze the root cause of the issue.
- If the issue is caused by an external internet service provider, contact them to determine the problem and expected resolution time, then inform all employees. The company has two internet providers for backup.
- If the issue is due to a broken cable, contact the ISP for repairs immediately.
- If only specific computers are affected, check the connection to the core switch in the server room.

4.1.4 Hardware or Computer Failure

- Notify relevant personnel.
- Replace the faulty device and restore backup data promptly.
- Verify data integrity and inform relevant personnel.

4.1.5 Power Outage

- The company has UPS backup power, which can last approximately 1.5 hours.
- If power is not restored within this period, notify management to approve the use of backup generators.
- If UPS backup fails, inform management to resolve the issue or acquire alternative power sources.

4.2 Emergencies Arising from Disasters

4.2.1 Fire

- If a fire breaks out during work, evacuate the building immediately. Employees trained to use fire extinguishers should attempt to put out the fire.
- If the fire cannot be controlled, system administrators should remove backup storage from the building (if possible) and call Map Ta Phut Fire Station at 038-675-562.

- The system administrator assesses damage and determines if operations can continue at the headquarters. If not, operations will be relocated to the Bangkok office.

4.2.2 Earthquake/Building Collapse

- Employees must evacuate the building immediately.
- The system administrator should take backup data if possible.
- After the incident, assess damage and determine if operations can continue at headquarters. If not, move to the Bangkok office.

4.2.3 Flood

- The system administrator must inform management and request approval to move operations to an alternate office.
- Shut down the system, relocate equipment, and back up data for installation at the alternate site.
- Once installed, test the system and report to management.

4.3 Emergencies Arising from Civil Unrest

- In case of civil unrest, such as terrorism or protests, employees may be unable to work on-site.
- If the office is inaccessible, move operations to the Bangkok office.
- After the situation stabilizes, the system administrator and asset auditors must assess damages. If damage is found, contact the responsible maintenance service.

4.4 Emergencies Involving Individuals

4.4.1 Theft

- Employees must immediately notify management.
- Conduct an inventory check to determine stolen assets.
- The system administrator must quickly replace missing equipment and restore backup data to ensure business continuity.

5. Emergencies Arising from External Service Providers

1. Emergencies Due to Technical Issues

1.1 Failure of Antivirus Protection

1.1.1 In case of a virus or intrusion, limit network connectivity to prevent further spread within the system.

1.1.2 Analyze the cause and impact of the virus outbreak.

1.1.3 Implement network security measures to contain the virus.

1.1.4 Monitor and fix infected devices.

1.1.5 If a computer becomes inoperable, notify the service provider. If network services become unavailable, the service provider must inform all relevant units.

1.2 Failure to Prevent Intrusions

1.2.1 If an intrusion occurs, the system administrator must analyze the cause and impact by checking logs and firewall settings.

1.2.2 The system administrator must promptly notify the service provider to take immediate action to stop the intrusion and close vulnerabilities.

1.3 Network Failure

1.3.1 The service provider must promptly analyze the root cause of the issue.

1.3.2 If a cable is damaged, the responsible maintenance company (UIH) must be contacted immediately for repairs as per the service agreement.

1.3.3 If only specific buildings experience network failure, inspect the connections to the building and core switch installed at that location.

1.4 Data Storage Device Failure

1.4.1 Notify relevant personnel.

1.4.2 Replace the damaged storage device and restore backup data promptly.

1.4.3 Verify data integrity and inform relevant personnel.

1.5 Power Outage

1.5.1 The service provider has UPS backup power, which can last up to 3 hours.

1.5.2 If the outage approaches the 3-hour limit and power is not restored, notify users so that administrators can shut down the system to prevent damage.

1.5.3 If the UPS fails, inform the supervisor to resolve the issue or acquire alternative backup power.

2. Emergencies Caused by Disasters

2.1 Fire

2.1.1 If a fire occurs while working, personnel must evacuate the building immediately. Those trained in fire extinguisher use should attempt to extinguish the fire using the available fire extinguishers.

2.1.2 If the fire cannot be controlled, the system administrator must evacuate backup storage devices from the building. The designated coordinator must contact the building maintenance team and the fire department via emergency hotline 199.

2.1.3 If a fire occurs when no personnel are present and equipment is damaged, repairs or replacements must be arranged promptly to ensure operations can continue. Fire detection and automatic suppression systems should be installed.

2.1.4 Conduct fire extinguisher usage and fire evacuation training for employees at least twice a year.

2.2 Flood

2.2.1 The system administrator must shut down systems and relocate operational equipment to the data center on the 2nd floor of Building A, PPMSPACE.

2.2.2 Restore backup data to recover lost or damaged information.

2.2.3 Inspect assets, assess damages, and arrange repairs or replacements to ensure continued operations.

2.3 Earthquake

2.3.1 Personnel must evacuate the building immediately.

2.3.2 The system administrator should attempt to take backup data along if possible.

2.3.3 Once the situation stabilizes, inspect damages and take necessary actions to restore operations.

3. Emergencies Due to Civil Unrest

3.1 Cases of Civil Disturbances (e.g., Terrorism, Protests)

3.1.1 If personnel cannot access the workplace, the system administrator must remotely monitor system operations. If issues arise, notify the IT support service provider, **TERABYTE**.

3.1.2 After the unrest, system administrators and asset inspectors must check for any damages. If damages are found, contact the responsible maintenance company for repairs.

4. Emergencies Caused by Individuals

4.1 Theft

4.1.1 Personnel must immediately report the incident to their supervisor.

4.1.2 Conduct an inventory check to identify stolen items.

4.1.3 The system administrator must procure replacement equipment and restore backed-up data to ensure operations can resume promptly.

4.2 Employee Absence

4.2.1 Notify the supervisor.

4.2.2 Follow operational guidelines if available, or coordinate with other personnel to cover responsibilities.

Emergency Preparedness Testing Plan for IT Incidents

1. Conduct **Work from Home** simulations.
2. Restore backup data on a pre-configured **Cloud environment**.
3. System administrators configure **VM and database settings**.
4. For clients using **on-premises servers**, the following steps must be taken in case of an emergency:

   4.1 Install **Express and API Sales System** software.

   4.2 Restore backup data as per the service agreement.

   4.3 Configure a new **VPN network** for clients to access the backup server environment.