Information Security Policy for the Organization's Information Systems

IT CITY

IT City Public Company Limited

Table of Contents

Information Security Policy for the Organization's Information Systems of IT City Public Company Limited

To ensure that the information technology, network, and computer systems of IT City Public Company Limited are properly managed, secure, and capable of continuously supporting the Company's operations — in compliance with the Computer Crime Act and other relevant laws — as well as to prevent potential threats that may cause damage to the Company, the Company has established this Information Security Policy to maintain appropriate management, stability, and security of its information systems.

Section 1: Definitions

The definitions in this section are provided to clarify the terms used in this Information Security Policy and Practices, ensuring that all terms are clearly defined and consistently understood.

- "**Company**" means IT City Public Company Limited.
- "**Human Resources Department**" means the Human Resources Department of IT City Public Company Limited.
- "**Information Technology Department**" means the Information Technology Department of IT City Public Company Limited.
- "**Building and Facilities Management Department**" means the Building and Facilities Management Department of IT City Public Company Limited.
- "**User**" means the Company's directors, executives, employees, relevant users, and external users who are authorized to access the Company's network systems.
- "**Employee**" means the Company's regular employees, probationary employees, and temporary staff.
- "**Relevant User**" means any individual or legal entity that is a contractual partner of the Company and engages in activities within the Company.
- "**External User**" means any individual or legal entity other than "Users" and "Employees."
- "**System Administrator**" means the IT Department Manager or any other employee assigned by a supervisor at the managerial level or higher, who is responsible for developing, modifying, improving, maintaining, and overseeing the Company's information systems and network, or any department directly responsible for managing such systems and networks.
- "**Information**" means factual data that has been processed and organized into a meaningful format, which may appear in the form of numbers, text, documents, diagrams, maps, photographs, films, video recordings, audio recordings, computer data, or graphics, allowing users to easily understand and utilize such information for management, planning, decision-making, and other purposes.
- "**Information System**" means the Company's systems used for storing, processing, and distributing information, which operate through the integration of hardware, software, data, users, and processing procedures to generate useful information for planning, management, and supporting the Company's operational mechanisms.

- "**Network System**" means a system used for communication or data and information transmission among the Company's various information technology systems, such as LAN, Wireless, Intranet, Internet, and other communication systems.
- "**Asset**" means any tangible or intangible property or item of value or importance to the Company, including data, information systems, and information and communication technology assets, such as personnel, hardware, software, computers, servers, information systems, network systems, network equipment, IP addresses, licensed software, or any other items that hold value for the Company.
- "**Information Technology Security**" means the stability and protection of the Company's information technology and network systems by maintaining Confidentiality, Integrity, and Availability of information, as well as other key attributes such as Authenticity, Accountability, Non-Repudiation, and Reliability.
- "**User Privileges**" means the levels of access granted to employees and relevant users to the Company's information, including general privileges, special privileges, and any other rights related to the Company's information systems and network systems.
- "**Access or Control of Information Usage**" means the authorization, assignment of rights, or delegation of authority to users to access or use the Company's network systems or information systems, either electronically or physically, as well as the establishment of rules and restrictions to prevent unauthorized access.
- "**User Account**" means the Username and Password assigned to employees, relevant users, and external users for system access.
- "**Security Incident**" means any identified event, condition, or network/service occurrence that indicates a possible breach of security policies, failure of protective measures, or any unidentified event that may be related to information security.
- "**Unwanted or Unforeseen Security Incident**" means a situation that may cause the Company's systems to be compromised or attacked, resulting in a threat to the Company's information security.
- "**Encryption**" means the process of encoding data to prevent unauthorized access. Only authorized users with the decryption software or key can restore the encrypted data to its original, usable form.
- "**Authentication**" means the security process used to verify a user's identity when accessing a system, typically performed through a username and password verification.
- "**SSL (Secure Socket Layer)**" means a data encryption technology used to enhance security in communications or data transmissions over the Internet between a server and a web browser or application.
- "**VPN (Virtual Private Network)**" means a virtual private computer network that transmits data over a public network (such as the Internet) through encrypted communication, ensuring that third parties cannot read or view the transmitted data until it reaches its destination.

Section 2: Governance of Enterprise IT

IT Governance aims to ensure that the Company achieves its established objectives by utilizing information technology as a tool to support its operations and effectively manage risks that may arise from its use.

Good IT management requires a strong connection between IT governance processes, efficient utilization of resources and information, and alignment with the Company's policies, strategies, and objectives, as well as appropriate risk management practices. Furthermore, there must be continuous reporting and monitoring to ensure that the technologies implemented by the Company effectively support business strategies, achieve corporate goals, enhance competitiveness, and create long-term value for the organization.

Accordingly, the Company shall consider undertaking at least the following actions:

2.1 Information Technology Security Policy (IT Security Policy)

1) The Company shall establish a written Information Technology Security Policy and communicate this policy effectively to ensure understanding and compliance across all relevant departments — particularly between the Information Technology Department and other departments — to promote coordination and ensure that business operations align with the Company's objectives.
2) The Company shall review the Information Technology Security Policy at least once a year, or whenever there are changes that may affect the Company's IT security, to ensure that the policy remains appropriate and effective.

2.2 Information Technology Risk Management Policy (IT Risk Management)

The policy shall be consistent with the Corporate Risk Management Policy and shall cover the following key areas:

1) The Information Technology Manager is responsible for studying and identifying methods or approaches in information technology to reduce or manage existing risks, and shall propose such methods or approaches to the Deputy Managing Director of Warehouse Management Division for consideration in managing the Company's information technology system risks.

2) Identification of Information Technology Related Risks (Information Technology Related Risk)

   - Physical and Environmental Risks refer to the Data Center Room, which houses the server computers, network equipment, and other related devices. Access to and usage of this room must be strictly controlled and monitored. In addition, various systems must be regularly inspected — such as the temperature monitoring system and the fire alarm system — to ensure operational safety and prevent potential damage.
   - Risks related to the use of computer programs on company computers include preventing the use or installation of unsafe or malicious programs, such as downloading and installing external software that may contain malware, computer viruses, or network vulnerabilities, which could allow external connections to attack the computer in use or other devices within the same network.
   - Risks related to the use of the company's computer network system require regular inspection and monitoring of internal network and internet usage. Protective systems must be implemented to prevent unauthorized access and external attacks on both

servers and client computers used by employees, such as internet access control systems, antivirus programs, and email data filtering systems.

- Risks related to personnel require defining access rights to computer systems, network equipment, and data in accordance with authorized permissions, in order to prevent unauthorized modification or alteration of information.

3) Risk assessment shall cover both the likelihood of occurrence and the potential impact, in order to prioritize risk management actions. The risks are categorized into four types as follows:
   - Technical risks: Arising from possible attacks on computers and equipment.
   - Operational risks: Caused by improper management of user access rights, leading to unauthorized access beyond assigned duties and potential damage to information assets.
   - Emergency and disaster risks: Resulting from natural disasters or other emergency situations, such as power outages or public demonstrations.
   - Management risks: Occurring when existing policies and practices are not aligned with potential or emerging risks.
4) Establish methods or tools for managing and controlling risks to a level acceptable to the company. A Description of Risk table shall be prepared, including key elements such as the risk name, risk type, risk characteristics, risk factors, and potential impacts. The table should also define the likelihood level and severity level of each risk, along with the preparation of a Risk Map to visualize and prioritize risk management.
5) Define Information Technology Risk Indicators (IT Risk Indicators) and ensure that regular monitoring and reporting of these indicators are conducted to responsible parties, enabling timely and appropriate management and mitigation of risks.

Section 3: IT System Security (IT Security)

3.1 Additional Guidelines on Information Security Policy and Measures (Information Security Policy)

Objective

To prevent any violations of the Information Technology Security Policy.

Guidelines

1) It is prohibited to use the company's computer resources and network for any illegal activities or actions contrary to public morality, such as creating websites for illegal trade or publishing unlawful or immoral content.
2) Do not access any computer network or system using another person's user account, whether authorized or unauthorized by the account owner.
3) It is prohibited to access protected computer systems or data belonging to others for the purpose of modifying, deleting, adding, or copying information.
4) Do not disclose or distribute any information belonging to others or the organization without permission from the data owner.
5) It is prohibited to disrupt, obstruct, or damage the company's computer resources or network, such as by sending computer viruses or introducing programs that cause computers or network devices to deny service (Denial of Service).
6) Do not intercept or capture data being transmitted through the company's or others' computer networks without authorization.
7) Before using any portable storage media, opening email attachments, or downloading files from the internet, all files must be scanned for viruses using antivirus software.
8) Users must not allow others to use their personal user accounts and passwords to access shared computer systems.

3.2 Organization of Information Security

Objective

To establish a framework for managing information system security within the company.

Guidelines

1) Senior management shall be responsible for overseeing and ensuring that information system security is maintained in accordance with the company's policies and practices on information security management.
2) The IT Manager shall assign duties to IT personnel who are responsible for maintaining the company's information systems to ensure their security, and shall supervise operations to ensure compliance with the company's information security policies and procedures.
3) The IT Manager shall be responsible for managing, supervising, monitoring, and reviewing the overall implementation of the company's information security policy.
4) IT personnel assigned as system administrators shall be responsible for maintaining the security of the systems under their supervision. They must monitor and ensure proper

system operation and, in the event of any security incidents or unforeseen situations, take corrective action and report promptly to their supervisor.

5) All users, as well as internal and external departments, shall be responsible for complying with the company's information system security policies and practices, and must refrain from any actions that violate laws related to computer crimes.

3.3 Human Resource Security in Information System Management

Objective

To ensure that all users understand the policies, roles, and responsibilities related to the use of the company's information systems.

Guidelines

1) Duties and responsibilities related to information system security must be clearly defined in writing for any individuals or external parties hired to perform work for the company. These responsibilities must comply with the company's information security policy.
2) A Non-Disclosure Agreement (NDA) must be signed between the worker and the company, stating the obligation to maintain confidentiality of the company's information. This agreement shall form part of the employment contract and remain binding both during employment and for at least one year after the termination of employment.
3) To ensure accurate and up-to-date management of user accounts, the Human Resources Department or relevant unit must promptly notify the IT Manager when any of the following events occur:
    - Employment commencement
    - Change in employment status
    - Resignation, termination of employment, or cessation of directorship or work with the company
    - Transfer to another department
4) All users and external contractors must be informed of the policies related to information technology security.
5) New employees must receive training on the company's Information Technology Security Policy as part of their orientation program.
6) Upon termination or change of employment, or completion of a project, access to the company's information systems must be immediately revoked.

3.4 Information Asset Management

3.4.1 Computer and Peripheral Access Control

Objective

To ensure that all users understand their duties and responsibilities in using the company's computers and peripheral devices, and that they strictly comply with the established procedures. This is to protect the company's resources and data, ensuring their security, accuracy, and continual availability.

Guidelines

1) Users of the company's computers and peripheral devices are responsible for the assets they are assigned to use.
2) It is prohibited to use the company's computers and network systems for personal business, commercial purposes, or any inappropriate activities.
3) Users are not allowed to install, modify, or alter any software on company computers unless under the guidance or approval of a system administrator or an authorized person.
4) It is prohibited to alter or modify any components of computers or peripheral devices unless approved by the system administrator or the responsible department. Users must maintain all devices in their original condition.
5) Users must not store or use computer equipment in environments that are hot, humid, or dusty, and must handle the equipment carefully to prevent impact damage.
6) Do not use or place any computer equipment near liquids, magnetic fields, high-voltage sources, vibration-prone areas, or environments with temperatures above 35°C.
7) When moving computer equipment, handle with care; do not place heavy objects on or throw the equipment.
8) Do not move a computer while the hard disk is operating or while the machine is turned on.
9) Avoid pressing or touching the computer screen with hard objects, as this may cause scratches or breakage. When cleaning the screen, wipe it gently in one direction only—do not wipe in circular motions to prevent scratches.
10) Users who resign or complete a project must return all assigned computers and peripheral devices to the responsible department in good working condition.
11) When moving computer equipment outside the office for work purposes, users must comply with the company's regulations on taking company property off-premises.
12) Users are responsible for preventing loss or theft of company devices and must not leave equipment unattended in public or high-risk areas.

3.4.2 Mobile Devices and Teleworking

Objective

To ensure the security of information when performing remote operations or working outside the office, as well as during the use of portable computer devices.

Guidelines

1) Mobile Device Policy

A policy or supporting measures must be established and implemented for the use of portable computer devices (such as notebooks, tablets, smartphones, and other mobile communication equipment) used for work purposes. The policy should aim to manage risks associated with such devices and take into account the potential risks of working in unsecured environments.

2) Teleworking

2.1) Personal devices used to access the organization's information technology systems remotely must be verified to ensure they have proper antivirus protection and firewall configurations as required by the organization.

2.2) The organization must provide the necessary equipment, data storage tools, and communication devices to support remote work operations.

2.3) All remote users must undergo authentication before accessing the system to enhance security, such as using passwords or encryption methods.

2.4) The use of personal devices to access the organization's IT systems remotely is not permitted if such devices are not under the organization's information security control or policy.

2.5) 2.5) The organization must define the types of work, working hours, data confidentiality levels, and systems or services that are permitted or not permitted for remote work.

2.6) 2.6) Procedures must be established for requesting approval, revoking access, assigning or modifying access rights, and returning remote work equipment to ensure proper control and compliance with security standards.

3.4.3 Media Handling

Objective

To prevent potential damage to the company's data storage media caused by unauthorized disclosure, alteration, transfer, deletion, or destruction of information.

Guidelines

1) Management of Removable Media

The management of removable data storage media must be governed by established procedures that align with the organization's information classification and confidentiality guidelines. Any media containing data must be protected against unauthorized access, misuse, or damage during transfer or transportation. Appropriate operational procedures and access rights must be defined to ensure the secure use, handling, and movement of such removable media.

2) Disposal of Media

Type of Media	Disposal Method
Paper	Shred using a paper shredder.
Flash Drive	- Destroy data according to the U.S. Department of Defense Standard DOD 5220.22-M, which involves overwriting existing data multiple times. - Physically destroy by smashing or crushing.

Type of Media	Disposal Method
CD/DVD	Smash, crush, or burn for destruction.
Tape	Smash, crush, or burn for destruction.
Hard Disk	- Destroy data according to the U.S. Department of Defense Standard DOD 5220.22-M, which involves overwriting existing data multiple times. - Physically destroy by smashing or crushing.

3) Physical Media Transfer

Methods for transferring data storage media (information or software) must be established to ensure security during delivery.

3.4.4 Software License Control

Objective

To ensure that users are aware of their duties and responsibilities in using computer software, understand the proper use of licensed software, and strictly follow the company's guidelines. This includes using software securely and in compliance with the Computer Crime Act and other relevant laws.

Guidelines

1) Requirements for System Administrators

- Responsible for controlling and supervising the use of computer software, as well as allocating software usage within the company according to the defined user rights.
- Responsible for installing and upgrading computer software for users according to the scheduled date and time.
- Must immediately remove or revoke software usage rights when notified by the company and/or department of cancellation or transfer of such rights.

2) Requirements for Users

- Users must use computer software responsibly, as they would with their own property, and must not use it in any way that violates the law or infringes upon others' rights, which could cause damage to the company.
- All software installed on company computers is legally licensed. Therefore, users are strictly prohibited from copying, installing, modifying, or distributing such software for use on other computers.
- It is forbidden to copy, sell, or distribute pirated software or unauthorized programs, especially those intended to facilitate illegal activities.
- The installation or use of any illegal software on company computers is strictly prohibited. If a user installs or uses software other than that provided by the company — whether it is licensed software or freeware — the user shall be solely responsible for any resulting damage or legal infringement.

- For software installation, removal, transfer, or return of computers and software, users must submit a request for approval to authorized personnel, and the IT administrator shall carry out the necessary actions in accordance with the approved request.

3.4.5 Information Asset and Computer System Access Control

Guidelines

Information assets — including documents, data storage media, computers, and information — must be protected from unauthorized access when unattended. Users must log out of the information system when not in use, as follows:

1) Log out of the information system immediately after finishing work.
2) Protect the computer by using appropriate authentication before access.
3) Store and back up important departmental information in a secure location. User data may be stored as follows:
    - In the application's internal database located within the company's Data Center — exporting data from the application is not permitted.
    - In the shared drive (Shared File) within folders according to assigned access rights.
4) Shut down the computer after being idle for more than one hour or after completing daily work, except for servers that must operate 24 hours a day.
5) Set the computer's screen saver to automatically lock the screen after 10 minutes of inactivity.
6) Obtain approval from the department head or higher authority before taking any information assets — such as documents, data storage media, or computer equipment — outside the company, following the company's property removal procedures.
7) Handle and protect company assets under one's responsibility as if they were personal property. In the event of loss due to negligence, the user shall be responsible for or compensate for the damage.

3.4.6 Use of Electronic Mail (Email Usage)

Objective

To ensure that the exchange of information via electronic mail supports work operations effectively, accurately, conveniently, promptly, and securely, in compliance with laws, regulations, company rules, and information security measures. It also aims to help users understand the importance of proper email usage and be aware of potential issues arising from using email services over the internet. Users must understand and comply with the rules established by system administrators, refrain from violating others' rights or causing disruptions, and strictly follow the administrators' instructions.

Guidelines

1) Users of the company's electronic mail service must not violate the Computer Crime Act, the Electronic Transactions Act, other related laws, or the company's IT policies and regulations.
2) Departments or employees using the company's electronic mail service must use it solely for the benefit of the company.
3) Employees are granted email usage rights through registration by the system administrator, based on the employee list provided by the Human Resources Department.

4) Users must not access or send emails using another person's email address without consent. The email owner shall be held responsible for all activities under their account.
5) Users must not falsify sender names or other user accounts when using the company's email system.
6) When sending emails related to company business, users must use the company's email system only. Other email systems may be used only if the company's system is unavailable and permission has been obtained from a supervisor.
7) Emails must be written in polite language, not contrary to good morals, not inciting, provocative, or illegal, and users must not express personal opinions as company statements or in ways that could harm the company.
8) The company's email system must not be used to distribute any content—text, images, or otherwise—that violates morality, national security, the law, the monarchy, or disrupts company operations, nor to harass other users or company clients.
9) Users must not use their company email address for personal matters, such as private business or social media registration. Any violations will be the responsibility of the email account owner.
10) Users must not engage in activities that misuse system resources, such as creating chain mail, sending spam mail, letter bombs, or distributing computer viruses.
11) Users must not send confidential company information to unauthorized persons or entities unrelated to company business.
12) Confidential company information sent by email should be encrypted, and the importance of such information should not be specified in the email subject line.
13) After using the company's email system, users must log out every time.
14) In case of complaints, requests, or discovery of unlawful acts, the company reserves the right to suspend or terminate email access for investigation.
15) If users witness any inappropriate or illegal actions within the company, they must report them through the company's whistleblowing channel.
16) Any dissemination of information through email or personal webpages is the sole responsibility of the user; the system administrator and the company bear no responsibility.

3.4.7 Access Control for Information and Information Systems

Objective

To establish measures for using the internet through the company's network to ensure efficiency and security, and to raise users' awareness when accessing various websites via the company's network.

Guidelines

1) The IT Department must define network connection routes for internet access through security systems such as a firewall or proxy.
2) Company computers must have antivirus software installed and system vulnerabilities patched before connecting to the network.
3) After using the internet, users must close the web browser to prevent unauthorized access.
4) Users must access data sources according to their assigned roles and access rights to maintain network efficiency and company security.
5) Users are prohibited from disclosing confidential company information, except in accordance with the company's official disclosure policy.

6) Users must exercise caution when downloading software or internet applications, including updates, ensuring that all downloads comply with copyright and intellectual property laws.
7) Users must verify the accuracy and reliability of information obtained from the internet before using it.
8) Users must not use the company's internet network for personal business or access inappropriate websites, including those that violate moral standards, threaten national security, religion, or the monarchy, harm society, or contain pornographic content.
9) Users must not use the internet in ways that violate others' rights or cause damage to the company, and must not engage in any actions that violate the Computer Crime Act or related laws. All internet usage for company operations must strictly comply with the company's established procedures.

3.4.8 Cryptographic Control

Objective

To prevent unauthorized individuals from accessing, disclosing, or modifying information or system operations beyond their authorized responsibilities.

Guidelines

1) Data Management
    - Information must be classified according to confidentiality levels, categorized based on business functions and priority, with specific management procedures defined for each type of information, including handling methods for confidential or critical data before disposal or reuse.
    - Transmission of important information over public networks must be encrypted using international standards such as SSL (Secure Socket Layer) or VPN (Virtual Private Network).
    - Measures must be in place to ensure data integrity during storage, input, processing, and output. In cases where identical data are stored in multiple locations (distributed databases) or when related datasets are maintained, controls must ensure that all data are accurate, complete, and consistent.
    - Data security measures should be implemented when computers are taken outside company premises (e.g., for repair), and all stored data on media must be securely erased beforehand.

2) User Privilege Control
    - Access to data and data processing equipment must be controlled with consideration for both operational requirements and information system security. Rules for authorization and access rights must be established so that all users understand and strictly follow the defined guidelines, while recognizing the importance of maintaining information system security.
    - Access rights to information and information systems — such as application systems or internet usage — must be assigned appropriately based on users' roles and responsibilities. Access shall be granted only to the extent necessary for duty performance and must be approved in writing by authorized personnel. Such privileges must also be reviewed regularly.

- In cases where the use of accounts with special privileges is necessary, their usage must be strictly controlled. The company will determine whether control over privileged users is sufficient based on the overall following factors.
    - Should be approved by authorized personnel.
    - The use of privileged accounts should be strictly controlled, allowing access only when absolutely necessary.
    - The duration of use should be defined, and access must be immediately revoked once the period expires.
    - Passwords must be changed strictly — for example, immediately after the need for use has ended, or at least every six months if long-term access is required.
- When the user is not present at the computer, measures must be implemented to prevent unauthorized individuals from accessing or using the system — for example, requiring users to log out during periods when they are not working at their computers.
- In cases where a user who owns important data needs to grant access or editing rights to another user — such as file sharing — such authorization must be limited to specific individuals or groups only. The granted rights must be revoked immediately when no longer necessary, with proper documentation of the authorization, a defined usage period, and automatic termination of access after the period expires.
- If it is necessary to grant access to another person for emergency or temporary use of the information system or network, a formal procedure must be in place. Approval must be obtained from authorized personnel, reasons and necessity must be recorded, and the access period must be clearly defined and revoked immediately upon expiration.

3) User Account and Password Control
    - A reliable identification and authentication system must be implemented to verify users' identities and access rights before entering the information system — for example, by requiring passwords that are difficult to guess. Each user must have their own unique User Account. The company will evaluate the strength and adequacy of password control based on the following overall factors.
        - Passwords should have a reasonable length; most international standards recommend a minimum of 8 characters (alphabetic and numeric).
        - Special characters should be included, such as : ; < > $ @ #, etc.
        - Regular users should change their passwords at least every 6 months, while privileged users such as System Administrators and Default Users should change theirs at least every 2 months.
        - Each new password must not be the same as any of the previous three passwords.
        - Passwords should not follow predictable patterns or be easily guessed, such as "abcdef," "aaaaaa," "123456," "password," or P@ssw0rd.
        - Passwords should not contain personal information such as the user's name, surname, date of birth, or address.
        - Passwords should not be dictionary words.

- The number of logon attempts allowed should be limited — typically to 5 attempts; after exceeding this limit, the system or program should deny or suspend access.
- Passwords must be delivered securely to users, for example, in a sealed envelope.
- Users must immediately change the initial (default) or newly issued password upon receipt.
- Users must keep passwords confidential and not write them down or post them near their computers. If a password is suspected to be known by someone else, it must be changed immediately.
- For systems using Shared User Licenses (such as SAP), administrators will send email notifications to the responsible user to change the system password whenever there is a change in personnel under their supervision.

- The system must encrypt files containing passwords to prevent unauthorized access or alteration.
- User accounts in critical systems must be regularly reviewed, and any accounts that no longer have authorized access — such as those belonging to resigned employees or default system accounts — must be promptly disabled, removed, or have their passwords changed immediately upon detection.

3.4.9 Physical and Environmental Security

Objective

The purpose of controlling access to the Data Center Room is to prevent unauthorized individuals from accessing, disclosing, modifying, or causing damage to data and computer systems. Damage prevention aims to protect data and computer systems from environmental factors or disasters. This section covers guidelines for controlling access to the Data Center Room and implementing protective systems that the company should maintain within the facility.

Guidelines

1) Data Center Room Security

- Critical IT equipment, including servers, network devices, and other essential infrastructure, shall be located in a secure Data Center Room or other restricted-access areas. Access to the Data Center Room shall be granted only to authorized personnel whose responsibilities require such access, such as system administrators.
- Where access by non-authorized personnel is necessary, appropriate supervision and access controls shall be implemented. Such personnel shall be accompanied and supervised by authorized system administrators and/or responsible personnel throughout their activities within the Data Center Room.
- The Data Center Room shall be protected by an access logging system that records the identity of individuals and the date and time of entry and exit. Access logs should be reviewed periodically to ensure compliance with security requirements.

- The Data Center Room should be appropriately segregated into designated operational zones, such as the **Network Zone**, **Server Zone**, **UPS Zone**, and **Battery UPS Zone**, to facilitate efficient operations and strengthen physical access controls for critical IT infrastructure.

2) Protection Against Physical Damage

- Fire Protection
  - Fire detection systems, such as smoke detectors and heat detectors, shall be installed to enable the timely detection and response to fire incidents.
  - The primary Data Center Room shall be equipped with an automatic fire suppression system. At a minimum, disaster recovery or backup data centers shall be provided with appropriate fire extinguishers for initial fire response.
- Power Protection
  - Appropriate measures shall be implemented to protect IT systems from damage caused by unstable or interrupted power supplies.
  - Critical IT systems and network infrastructure shall be supported by an uninterruptible power supply (UPS) or other backup power systems to ensure business continuity.
- Temperature and Humidity Control
  - The Data Center environment shall be maintained within appropriate temperature and humidity ranges in accordance with the specifications of the installed IT equipment to ensure reliable system performance and prevent equipment malfunction.
- Water Leak Detection
  - Where raised floors are used for air conditioning, power distribution, or network cabling, water leak detection systems should be installed in areas where water pipes are present to enable early detection and response.
  - Where the Data Center Room is located in areas exposed to water leakage risks, regular inspections shall be conducted to identify and address potential water intrusion.

3.4.10 Operations Security

Objective

To ensure that the Company's information systems are operated in a secure, reliable, and controlled manner, protecting information assets from unauthorized access, loss, alteration, disruption, and malicious software, while maintaining the confidentiality, integrity, and availability of information.

Guidelines

1) Establish documented operating procedures for the Company's critical information systems to ensure consistent and secure operations and minimize operational errors.

2) Implement formal change management procedures for information systems. All changes shall be reviewed and approved by authorized personnel prior to implementation.
3) Ensure that critical information is backed up before any system or information changes are performed.
4) Monitor the utilization of information system resources, such as CPU, memory, and storage capacity, and use the monitoring results for capacity planning and resource management.
5) For critical information systems, development, testing, and production environments shall be segregated to prevent unauthorized changes and reduce operational risks.
6) Identify and classify information assets, determine backup requirements, and establish appropriate backup frequencies based on the criticality of the information.
7) Critical information shall be backed up at an appropriate frequency, and off-site or secure external backups should be maintained to support disaster recovery.
8) The availability and recoverability of backup systems shall be tested at least once a year to ensure their effectiveness.
9) Implement appropriate controls to protect information systems against malware, including but not limited to:

    - Personal computers and laptops connecting to the Company's network shall have up-to-date anti-malware software installed and all critical operating system and web browser security vulnerabilities remediated.
    - Users shall regularly install security updates, patches, and hotfixes for operating systems and software applications obtained from authorized vendors.
    - All files transmitted via email shall be scanned for malware before being sent or opened.
    - Only software approved or provided by the Company may be installed. Any additional software must be reviewed and approved by the Information Technology Department prior to installation.

3.4.11 Backup Policy

Objective

To establish a standardized approach for backing up the Company's servers, critical network infrastructure, and other essential information assets, ensuring business continuity and enabling the timely recovery of information and systems in the event of emergencies, system failures, or incidents that may result in the loss, damage, or unavailability of information.

Guidelines

1) Backup copies of critical information and software shall be maintained based on the priority and criticality of the Company's information systems.
2) Documented procedures shall be established for backup and restoration activities, covering both software and data. Backup and recovery procedures shall be maintained separately for each information system.
3) Backup media shall be clearly labeled with relevant information, including the system name, backup date and time, and the person responsible for the backup. Backup copies should be stored securely at an off-site location, and backup media shall be tested periodically to ensure their integrity and recoverability.

4) A Business Continuity Plan (BCP) and appropriate disaster recovery procedures shall be established to ensure that critical information systems and data can be restored within an acceptable timeframe following an emergency or disruptive incident.

3.4.12 Communications Security

Objective

To protect information transmitted through the Company's computer networks from unauthorized access, malware, and other malicious code, and to safeguard the confidentiality, integrity, and availability of information and information systems.

Guidelines

1) Network Security Management
    - Appropriate network security controls shall be implemented to protect the Company's network infrastructure from unauthorized access and cybersecurity threats.
    - The Company's network shall be segmented to separate internal users from external users and other external connections, thereby reducing security risks and protecting critical information systems.
2) Information Transfer
    - Information transfer activities shall be governed by documented Information Transfer Agreements, taking into account appropriate information security requirements. System administrators shall ensure that all information transfer activities maintain the confidentiality, integrity, and availability of information.
    - A Non-Disclosure Agreement (NDA) or equivalent confidentiality agreement shall be executed between the Company and external parties prior to the exchange of confidential or proprietary information to protect the Company's confidential information from unauthorized disclosure.

3.4.13 System Acquisition, Development and Maintenance

Objective

To establish controls over the acquisition, development, and modification of information systems to ensure that systems are developed, enhanced, and maintained in a secure, accurate, and reliable manner, while meeting business and user requirements. The controls are designed to reduce information integrity risks by governing the entire system development lifecycle, from change requests and system design through development, testing, approval, and deployment into the production environment.

Guidelines

1) Documented procedures shall be established for the development and modification of information systems. At a minimum, these procedures shall include requirements for change requests, system development or modification, testing, approval, and deployment to the production environment.

2) Procedures shall be established for emergency changes (Emergency Changes) to information systems. The business justification for each emergency change shall be documented, and all emergency changes shall be reviewed and approved by authorized personnel.
3) The documented procedures shall be communicated to users and all relevant personnel, and compliance with these procedures shall be monitored and enforced.

System Development and Change Control

1) Change Request

- All requests for the development, enhancement, or modification of information systems shall be submitted in a documented form. Electronic requests, such as email or other approved electronic workflows, are acceptable, provided they are reviewed and approved by authorized personnel, such as the requesting department manager or the information system owner.
- Significant system changes should be supported by a documented change impact assessment, covering operational impacts, information security implications, and system functionality to ensure that potential risks are properly identified and managed.
- Applicable legal, regulatory, and compliance requirements shall be reviewed prior to implementing significant system changes to ensure that the proposed changes do not adversely affect the Company's compliance obligations.

2) System Development Activities

- Development, testing, and production environments shall be segregated, and access to each environment shall be restricted to authorized personnel based on their roles and responsibilities. Environment segregation may be achieved through separate physical infrastructure or logically separated environments within the same infrastructure.
- Requesting departments and relevant users should participate throughout the system development or change process to ensure that business requirements are accurately captured and effectively implemented.
- Information security and system availability requirements shall be considered from the earliest stages of system development and throughout the system change lifecycle to ensure that security and resilience are incorporated by design.

3) Testing

- The requesting department, the Information Technology Department, and other relevant users shall participate in system testing to verify that the developed or modified information system operates effectively, processes information accurately and completely, and meets defined business and user requirements before being deployed to the production environment.

4) Deployment to the Production Environment

- The deployment of information systems to the production environment shall be verified to ensure that the migration has been completed accurately and in its entirety.

5) System Documentation and Version Management

- Documentation of all production systems shall be maintained, including records of system development, enhancements, modifications, and version history.
- Following any system development or modification, all relevant system documentation shall be updated to reflect the current system configuration. Such documentation may include data models, system manuals, user access registers, operating procedures, program documentation, and technical specifications. Documentation shall be securely maintained and made readily available to authorized personnel.
- Previous versions of application software shall be securely retained to support system rollback and recovery in the event that the current version fails or cannot be operated as intended.

6) Post-Implementation Testing

- Following the deployment of a newly developed or modified information system, post-implementation testing should be conducted after an appropriate period of operation to verify that the system performs effectively, processes information accurately and completely, and continues to meet defined business and user requirements.

7) Change Communication

- All relevant users shall be informed of significant system changes in a timely manner to ensure they understand the changes and are able to use the information system correctly and effectively following implementation.

3.4.14 IT Outsourcing

Objective

To ensure that the Company's information assets accessed or managed by IT outsourcing service providers are adequately protected, and that appropriate information security controls and agreed service levels are maintained in accordance with the applicable outsourcing agreement or Service Level Agreement (SLA).

Guidelines

1) Information security requirements shall be established whenever an IT outsourcing service provider is granted access to the Company's information assets or systems. Such requirements shall be consistent with the Company's information confidentiality and security policies.
2) The Company's information security requirements shall be communicated to, acknowledged by, and contractually enforced with the IT outsourcing service provider before any access to the Company's information assets or systems is granted.
3) Outsourcing agreements or Service Level Agreements (SLAs) shall require the regular monitoring, review, and audit of the outsourced services to ensure continued compliance with the agreed service and information security requirements.
4) Any material changes to outsourcing agreements involving critical information systems shall be subject to an information security risk assessment before implementation.

3.5 Information Security Incident Management

Objective

To establish a consistent and effective approach for managing information security incidents, including the timely reporting, assessment, response, and resolution of information security incidents and vulnerabilities, in order to minimize their impact on the Company's information assets and business operations.

Guidelines

1) Roles, responsibilities, and procedures shall be established for the effective management and response to information security incidents.
2) Clear communication channels shall be established to enable the timely reporting of information security incidents and security vulnerabilities.
3) Users who identify or suspect an information security incident shall promptly report the incident to the Information Technology Department through the designated reporting channels.
4) Information security incidents shall be classified and reported according to their severity. Where an incident has a significant impact on a large number of users or critical business operations, timely notifications shall be issued to relevant stakeholders.
5) All information security incidents shall be recorded and documented. Incident records should include, at a minimum, the nature of the incident, its frequency or scale, the impact, and the associated losses or recovery costs, to support continuous improvement and preventive measures.
6) Evidence relating to information security incidents shall be collected, preserved, and handled in accordance with applicable legal and regulatory requirements to support investigations and, where necessary, legal proceedings.

3.6 Information Security Aspects of Business Continuity Management

Objective

To ensure the continuity of the Company's critical business operations by minimizing disruptions arising from crises, disasters, or other disruptive events, and to maintain the availability and resilience of information systems and supporting information technology infrastructure essential to business operations.

Guidelines

1) The Information Technology Department shall establish and maintain information technology disaster recovery procedures that align with the Company's Crisis Management Plan (CMP) and support the continuity of critical information systems during disruptive events.
2) Information security and information technology risks that may affect business continuity shall be assessed at least annually.
3) The Company's Business Continuity Plan (BCP) and emergency preparedness procedures shall be reviewed and updated at least once a year to ensure their continued effectiveness.
4) The operational readiness and recoverability of backup information systems and disaster recovery facilities shall be tested at least once a year.

3.7 Operational Security

3.7.1 Operating Procedures and Responsibilities

Objective

To ensure that the operation and management of the Company's information processing facilities are conducted in a secure, consistent, and controlled manner, thereby maintaining the confidentiality, integrity, and availability of information and information systems.

Guidelines

1) **Documented Operating Procedures**
   - Documented operating procedures and/or user manuals shall be established for information system operations. These shall include, as appropriate, procedures for incident reporting, system recovery, system maintenance, and other operational activities, together with clearly defined responsibilities for the relevant personnel or departments.
   - Operating procedures and user manuals shall be updated whenever there are changes to operational processes or assigned responsibilities. All documented procedures shall be reviewed at least once a year to ensure they remain accurate, effective, and up to date.
   - Roles, responsibilities, and procedures for handling operational abnormalities and information security incidents shall be clearly defined. Appropriate investigations shall be conducted in response to security violations or non-compliance to identify the root cause and determine appropriate corrective actions.

2) **Change Management**
   - All changes to network infrastructure, information systems, hardware, software, and related information technology assets shall be managed through a formal Change Management process.
   - Any changes to the physical environment supporting information systems, such as air conditioning, water supply, power supply, fire protection, alarm systems, or environmental monitoring equipment, shall be promptly communicated to and coordinated with the Information Technology Department.
   - All changes affecting the information technology environment shall be initiated through a formally documented Change Request prior to implementation.
   - The Information Technology Department shall conduct regular reviews of all Change Requests to assess the impact, risks, and readiness of the proposed changes before granting approval.
   - All change schedules and implementation plans shall be reviewed and approved by the Information Technology Department prior to execution.
   - A change record shall be maintained for every implemented change and communicated to relevant stakeholders. At a minimum, each change record shall include:
     - Date the Change Request was submitted and the implementation date;
     - Information owner and system administrator responsible for the change;
     - Description of the change implemented; and
     - Change implementation outcome (successful or unsuccessful).

3) **Capacity Management**
   - The utilization and performance of information and communication technology (ICT) resources shall be monitored and analyzed on a regular basis to ensure that system capacity remains adequate to support current business and operational requirements.
   - A Capacity Management Plan shall be developed and reviewed at least annually, taking into account projected business demand, future ICT resource requirements (e.g., increased CPU performance, storage capacity, and network resources), current resource utilization, and technological advancements.
   - The Capacity Management Plan shall include appropriate measures to optimize and enhance system capacity, such as performance tuning, resource optimization, and infrastructure expansion or procurement, where necessary.

4) **Separation of Development, Testing, and Production Environments**
   - Development, testing, and production environments shall be segregated to prevent unauthorized access, unintended changes, and operational disruptions. Information processing facilities, including computer systems and network infrastructure, used for development and testing shall be separated from the production environment. Where appropriate, development and testing networks should also be segregated from the production network to minimize security risks and maintain the integrity and availability of production systems.

3.7.2 Protection from Malware

Objective

To protect the Company's information assets and information processing facilities from malware and other malicious software, ensuring the confidentiality, integrity, and availability of information and information systems.

Guidelines

1) **Malware Protection Measures**
   - Users shall install and use only software that has been approved, licensed, or provided by the Company. The installation or use of unauthorized or unlicensed software is strictly prohibited. Any copyright infringement resulting from unauthorized software shall be the sole responsibility of the individual user.
   - Software provided by the Company for business purposes shall not be removed, modified, copied, or used for any unauthorized purpose without prior approval from the user's supervisor.
   - All Company-managed computers shall be equipped with Company-approved anti-malware or anti-virus software, which shall be maintained and updated in accordance with the Company's information security requirements.
   - All files, software, and other digital content received from external sources or other users shall be scanned for malware before being accessed, executed, or stored.
   - Users shall ensure that operating systems, applications, and anti-malware software are kept up to date by installing the latest security patches and updates in a timely manner.

- Users shall remain vigilant for signs of malware infection or other suspicious activities and shall immediately report any suspected security incidents to the Information Technology Department or the designated system administrator.
- If a computer is suspected or confirmed to be infected with malware, it shall be immediately disconnected from the Company's network and reported to the Information Technology Department for investigation and remediation.
- Users shall not copy, modify, delete, or otherwise misuse the Company's information assets, documents, or other proprietary information without proper authorization.
- Users are strictly prohibited from creating, distributing, introducing, or facilitating the spread of malware, malicious code, computer viruses, or any software designed to compromise the confidentiality, integrity, or availability of the Company's information systems or information assets.
    - Do not develop any software or hardware designed to compromise information security controls, including password harvesting, unauthorized password cracking, or unauthorized copying of another person's information.
    - Do not develop any software or hardware that enables users to obtain unauthorized privileges or priority over other users in accessing system resources.
    - Do not develop any software capable of self-replication or propagation by attaching itself to other programs in a manner similar to computer worms or viruses.
    - Do not develop any software or hardware intended to circumvent or disable software licensing mechanisms.
    - Where users create web pages on the Company's computer network, they shall not publish any content that is unlawful, infringes intellectual property rights, contains inappropriate text or images, or is contrary to public morals or the good customs of Thailand.
    - Outsourced software development.
        - Software development projects performed by external service providers shall be subject to appropriate controls. The ownership of intellectual property rights, including the source code developed by external service providers, shall be clearly defined.
        - The Company shall consider reserving the right to review and verify the quality and integrity of software developed by external service providers, and such rights shall be specified in the relevant service agreement or contract.
        - All software shall be scanned for malware prior to installation.
        - Upon completion and delivery of software developed by external service providers, all relevant system passwords shall be changed.
        - External system developers (outsourced personnel) shall sign the Acceptable Use Policy (AUP) and a Non-Disclosure Agreement (NDA) before commencing any work.

- External system developers (outsourced personnel) shall comply with the Company's Information Security Policy and Information Security Procedures.

3.7.3 Logging and Monitoring

Objective

To ensure that logs and audit trails are maintained as evidence to support monitoring, investigation, and verification of information system activities.

Guidelines

1) **Event Logging**
   User activities, system service denials, and other information security-related events shall be logged on a regular basis and retained for the period specified by the Company.
2) **Protection of Log Information**
   Log information relating to the use of information systems shall be protected against unauthorized access, modification, deletion, or tampering.
3) **Administrator and Operator Logs**
   Activities performed by system administrators and other personnel responsible for operating information systems, including computer systems and network devices, shall be logged and monitored.
4) **Clock Synchronization**
   The clocks of all computers and information processing devices shall be synchronized with an authorized time source in accordance with the applicable Computer Crime Act to ensure the accuracy of timestamps for monitoring, investigation, and forensic purposes in the event of an information security incident.

3.7.4 Control of Operational Software

Objective

To ensure that software installed on production systems is properly authorized, managed, and controlled so that information systems operate correctly, securely, and reliably.

Guidelines

1) **Installation of Software on Operational Systems**
   Software developers shall control the installation of new software, software libraries, and security patches on production systems and servers. Prior to deployment to the production environment, all software shall be thoroughly tested to ensure that it functions properly and does not adversely affect existing production systems.

3.7.5 Technical Vulnerability Management

Objective

To protect the Company's information systems, software, and information assets by identifying, assessing, and addressing technical vulnerabilities in a timely manner, thereby reducing the risk of exploitation arising from publicly disclosed or known technical vulnerabilities.

Guidelines

1) **Management of Technical Vulnerabilities**
   Technical vulnerability information relating to the Company's information systems shall be monitored on an ongoing basis. Identified vulnerabilities shall be assessed to determine their associated risks, and appropriate remediation measures shall be implemented to reduce those risks.
2) **Restrictions on Software Installation**
   2.1 The Company shall comply with applicable copyright requirements governing the use of intellectual property and licensed software. Users shall ensure that they do not infringe any intellectual property rights.
   2.2 Software provided by the Company is intended solely for authorized business purposes. Users shall not uninstall, modify, alter, copy, or use such software for any other purpose unless prior authorization has been obtained from their supervisor or the authorized copyright owner.

3.7.6 Information System Audit Considerations

Objective

To ensure that information system audit activities are planned and conducted in a manner that minimizes disruption to the Company's business operations and information systems.

Guidelines

1) **Information System Audit Controls**
   The Information Technology Department shall plan and coordinate information system audit activities to ensure that audits are conducted with minimal disruption to the Company's information systems, business operations, and operational processes.

This Policy shall take effect on 1 June 2023.

Issued on 1 June 2023.

Mr. Sophon Intanate
President
IT CITY Public Company Limited