TCM Corporation Public Company Limited

Information Technology Security Policy

In order to secure the continued suitability, security, and operational integrity of information technology (IT), network, and computer systems used by TCM Corporation Public Company Limited, its subsidiaries, and affiliated companies (the "Company"), and to assure lawful and compliant usage of these systems in strict accordance with the Computer Crime Act and other relevant legislation, while simultaneously safeguarding the Company from potential threats, this Information Technology Security Policy is hereby established.

Definitions

This section provides definitions for the terms used in this Information Technology Security Policy and Procedures to ensure clarity and consistency of understanding.

1. “Company” refers to TCM Corporation Public Company Limited, its subsidiaries, and affiliated companies that use the same information technology, network, and computer systems.
2. “User” refers to any individual authorized to access the Company's network systems, including but not limited to Company Directors, Executives, Employees, Related Users, and External users.
3. “Employee” refers to any individual engaged in employment with the Company, including but not limited to: Full-time Employees, Probationary Employees, and Temporary Employees.
4. “Related User” refers to a person or legal entity that is a contractor of the Company and enters the Company's premises to carry out activities.
5. “External User” refers to a person or legal entity other than those mentioned in Clauses (3) and (4).
6. "System Administrator" refers to the Information Technology Manager or other employee who has been assigned by a director or higher-level manager to be responsible for the development, modification, improvement, and maintenance of the information technology and network systems used by the Company or the department that is responsible for the information technology and network systems.
7. "Information" refers to facts derived from processed and organized data. This information may be presented in various formats, including numbers, text, documents, diagrams, maps, photographs, films, image recordings, sound recordings, computer recordings, or graphics. A well-designed system presents information in a way that facilitates user understanding, enabling effective management, planning, decision-making, and other purposes.
8. "Information System" refers to the Company's system that stores, processes, and disseminates information. This system comprises hardware, software, data, users, and data processing, collectively facilitating the generation of information that supports the Company's planning, management, and operations.
9. "Network" refers to a system that enables communication and transmission of data and information among the Company's various information technology systems, including LAN, Wireless, Intranet, Internet, and other communication systems.
10. "Asset" refers to any tangible or intangible property with value or worth to the Company, including data, information systems, and information and communication technology assets, such as personnel, hardware, software, computers, mainframe computers, information systems, networks, network equipment, IP addresses, or copyrighted software, or any other resource deemed value to the Company.
11. "Information Technology Security" refers to the security and safety of the Company's information technology and network systems, by maintaining the confidentiality, integrity, and availability of

information, as well as other qualities such as authenticity, accountability, non-repudiation, and reliability.

12. "User Account" refers to a username and password for employees, related users, and external users.
13. "Encryption" refers to the process of converting data into secret code to prevent unauthorized access. Only those with the correct decryption key or password can revert the encrypted data file to its original form (plaintext) for normal use.
14. "Authentication" refers to a security step in the system login process that is generally used to verify the identity of a user. It is verified using a username and password.
15. "SSL (Secure Socket Layer)" refers to a data encryption technology that enhances the security of communication or data transmission over the Internet between servers and web browsers or applications.
16. "VPN (Virtual Private Network)" refers to a private virtual computer network that creates a secure, encrypted connection across a less secure network. The data transmission is encrypted and routed through the Internet, making it unreadable and invisible to others until it reaches its destination.
17. "Cloud Computing" refers to the use of external information technology services from a third-party provider for information technology infrastructure or information technology systems. These services, based on cloud computing technology, are delivered over the internet and support various information technology functions for the Company, including storing data, processing data, or performing any other data or system-related operations.

Scope

This Information Technology Security Policy applies to all users and administrators with authorized access to the Company's information technology (IT), network, and computer systems. The policy shall remain in effect until superseded or amended by a formally issued revision.

Section 1

Good Governance of Enterprise IT

IT governance aims to align information technology resources with the Company's strategic goals, while proactively managing associated risks that may arise from the use of information technology. Effective IT management necessitates a strong integration among IT processes, resources, and data to uphold the policies, objectives, and risk management protocols of the Company. This includes reporting and monitoring to ensure that the Company's IT resources support business strategies, drive competitive advantage, and deliver value. The Company must at least consideration to the following:

1. Information Technology Security Policy

1) The Company shall establish a written Information Technology Security Policy (IT Security Policy) to serve as a framework for managing, preventing, and maintaining the security of the Company's information and information technology systems. This policy must be communicated to all users for their understanding and compliance, especially between the information technology department and other departments within the Company, to ensure coordination and the ability to conduct business in accordance with the established goals.
2) The Company shall arrange for a review of the Information Technology Security Policy at least once a year or when there are changes that affect the Company's information security.

2. Information Technology Risk Management Policy

The Information Technology Risk Management Policy shall be aligned with the Corporate Risk Management Policy and encompass the following:

1) Designation of Roles and Responsibilities for IT Risk Management

   The IT Manager shall be responsible for studying and identifying methods or guidelines related to information technology to mitigate or manage existing risks. They shall then present these to the management for consideration in managing information technology system risks.

2) Identification of Information Technology Related Risks
   - Physical and Environmental Risks: The Data Center Room, which houses and stores network servers and other critical equipment, shall have controlled access and usage. To mitigate environmental risks, systems such as air conditioning, fire alarms, and other critical infrastructure must be regularly inspected and maintained.
   - Software Usage Risks on Company Computers: To prevent the use of unsafe or malicious software, the downloading and installation of programs from external sources are prohibited. These programs may contain malware, computer viruses, or vulnerabilities that could allow unauthorized external network access, compromising the computer in use or other computers within the Company's network.
   - Computer Network Security Risks: Effective network security measures must be implemented to monitor and safeguard both internal network usage and internet access. This includes establishing robust access control and protection systems for both network servers (Servers) and employee workstations (Clients). These measures may include Internet gateway controls, Installation of antivirus software, Email filtering.
   - Personnel Security Risks: Access rights to computer systems, network devices, and data must be strictly assigned in accordance with the principle of least privilege. This policy aims to prevent unauthorized access, modification, or destruction of data.

3) Establishing Procedures and Work Practices for IT Risk Management
   - Clearly defined and documented IT-related operational procedures must be established to ensure IT personnel adhere to consistent and accurate practices.

- Establish a formal process for approving exceptions to documented procedures. This process should involve risk assessment, risk mitigation, obtaining approval from the designated authority before proceeding with the exception, and include documentation to maintain detailed records of all exception approvals.
- Conduct an annual review of the appropriateness of exception requests and risk control measures. This review ensures procedures remain aligned with the evolving risks associated with changes in the business environment and the use of IT within the business.

4) Conduct a comprehensive risk assessment that encompasses the likelihood of occurrence and potential impact of each identified risks. This assessment will facilitate the prioritization of risk management efforts.

5) Formalize methodologies and implement appropriate tools to manage and mitigate risks within a threshold deemed acceptable by the company. Establish a "Description of Risk" section to detail the attributes for each identified risk: Title, Name, Type, Description, Contributing Factors, and Potential Consequences. Assess the probability and severity of each risk, and subsequently construct a visual risk map to present this analysis.

6) Establish Information Technology Risk Indicators and implement a monitoring and reporting process to provide regular updates on these indicators to the responsible parties. This will ensure effective and timely risk management.

Section 2

Information Technology (IT) Security Maintenance

1. Supplementary Guidelines on IT Security Policy and Measures

- Objective:
  To prevent violations of the IT Security Policy.
- Guidelines:
  - Refrain from using IT resources and networks for illegal activities or actions that are contrary to good social morals. This includes, but is not limited to, creating websites for illegal or unethical purposes.
  - Do not access computer networks or computers using another person's user account, whether with or without the permission of the account owner.
  - Do not access computer systems and data that are restricted to others for the purpose of modifying, deleting, adding, or copying information.
  - Do not disclose the personal information of others or of the Company without the authorization of the data owner.
  - Do not disrupt, interfere with, or damage the company's IT resources or networks. This includes, but is not limited to, the transmission of computer viruses or the introduction of programs designed to cause denial of service in computers or network devices.
  - Do not intercept data in the company's or others' computer networks that is being transmitted over the network.
  - Prior to using any mobile media, opening email attachments, or downloading files from the internet, a comprehensive virus scan must be performed using a reputable antivirus program.

2. Organization of Information Security

- Objective:
  To delineate a framework for management of information security within the company.
- Guidelines:
  - Top Management: Responsible for the overall governance of information security in accordance with the company's information system security policy and guidelines.
  - Information Technology (IT) Manager: Responsible for assigning duties to IT personnel, ensuring the security of the company's information systems, and overseeing operations in strict compliance with the company's information system security policy and guidelines.
  - Information Technology (IT) Manager: Responsible for managing, overseeing, monitoring, and periodically reviewing the company's information system security policy to ensure its continued effectiveness.
  - IT Personnel assigned as system administrators at the Administrator level: Responsible for the security of the systems they administer, including monitoring system security during operation. In the event of an unforeseen or unexpected security incident, they shall take corrective action and report the incident to their supervisor.
  - Users and Departments (Internal and External): Responsible for strict adherence to the company's Information system Security Policy and guidelines, including refraining from actions that violate relevant computer crime laws.

3. Human Resource Security

- Objective:
  Ensure that all users understand the company's Information System Security Policy, as well as their individual roles and responsibilities when utilizing the company's information systems.
- Guidelines:
  - Clearly define and document information system security responsibilities for external individuals or entities contracted to perform work for the company. This documentation must formally outline their obligations and ensure alignment with the company's Information System Security Policy.
  - Require all contractors to sign a Non-Disclosure Agreement (NDA) prohibiting the disclosure of confidential company information. This NDA should be a condition of employment and remain in effect for a minimum of one year after the termination of employment.
  - To ensure accurate and up-to-date user account management, the HR department or relevant entity must promptly inform the IT Manager of any of the following events:
    - New hires
    - Changes in employment conditions
    - Employee resignations or terminations
    - Departmental transfers
  - Obtain acknowledgement of the company's IT Security Policy from all users and external contractors and ensure their comprehensive understanding of its contents.
  - Provide new company employees with training on the IT Security Policy as part of their orientation or onboarding process.
  - Immediately revoke access to IT systems for terminated employees, contractors, or upon project completion.

4. Information Asset Management

- Computer and Peripheral Access Control
  - Objective:
    To instruct all users regarding their duties and responsibilities when utilizing the company's computers and peripheral devices. Emphasize the necessity of strict adherence to all relevant guidelines in order to safeguard the company's resources, maintain the accuracy of data, and ensure its continuous availability.
  - Guideline:
    - Users of the company's computers and peripheral devices are accountable for the assets they utilize.
    - Company computers and network systems are strictly prohibited from being used for any personal or inappropriate business or services.
    - Users are not permitted to install or modify programs on company computers without prior consultation or guidance from the system administrator or authorization from the highest-ranking authority within their department.
    - Altering or modifying any components of computers and peripherals is strictly prohibited unless authorized by the system administrator or the responsible department. Users are responsible for maintaining the original condition of computers and peripherals.
    - Users must refrain from storing or using computer equipment in environments free from excessive heat, humidity, and dust. Precautions must be taken to prevent accidental drops or impacts.

- Do not use or place any type of computer equipment near liquids, strong magnetic fields, or high-voltage electricity.
- When moving computer equipment, exercise extreme caution. Avoid placing heavy objects on the equipment or taking any actions that could cause impact damage, such as dropping or throwing it.
- Do not move computer equipment while the hard drive is spinning, or the computer equipment is powered on.
- Avoid touching the computer screen with hard objects, as this could cause scratches or damage. Instead, clean the computer screen gently in one direction only and avoid circular motions, which can also cause scratches.
- Upon termination of employment or project completion, users must return all company-issued computers and peripherals to the responsible department in fully functional condition.
- When computer equipment is required for off-site work, users must comply with the company's policy on removing assets from the premises. This requirement excludes personally owned laptops.
- Users are responsible for safeguarding equipment against loss or theft. Do not leave equipment unattended in public areas or in areas where it is at risk of being lost.

- Software License Usage Control
  - Objective:

    To instill in users an awareness of their duties and responsibilities when utilizing computer software, including understanding the proper use of licensed software, strictly adhering to established guidelines, ensuring secure and safeguard software operation, and complying with the computer-Related Crime Act and relevant laws.
  - Guidelines:

    Guidelines for System Administrators:
    - Responsible for overseeing and managing software usage, allocating software licenses within the company in strict accordance with designated usage rights.
    - Responsible for Installing and upgrading software for users according to scheduled dates and times.
    - Configure screensavers on all company computers to automatically engage a screen lock after 15 minutes of inactivity.
    - Immediately revoke software licenses and uninstall programs upon notification of program termination or license transfer by the company and/or relevant departments.

    Guidelines for Users:
    - Utilize computer software with the utmost diligence and responsibility, refraining from illegal or unlawful use that may cause harm to the company or any individual.
    - Utilize only legally licensed software installed on company computers. The copying, modification, or distribution of software to others is strictly forbidden.
    - Copying, distributing, or disseminating unlicensed software or unauthorized command sets is strictly forbidden, especially when used for malicious or illegal purposes.
    - The installation of illegal or unlicensed software on company computers is strictly prohibited. Users shall bear sole responsibility for any damages or legal violations resulting from the use of unauthorized software, whether licensed or freeware.
    - Software installation, uninstallation, transfer, or return must receive prior authorization from the relevant authority and be executed by the IT administrator in accordance with the issued approval.

- Information Asset and Computer System Access Control
  - Guidelines:

    The control of Information assets, including documents, data storage media, computers, and information, must be protected from unauthorized access when not in use. Users must be logged out of information systems when not actively engaged. This includes:
    - Promptly log out of information systems upon completion of work.
    - Implement appropriate authentication measures to protect computers before access.
    - Store and back up critical organizational information in a secure location. User data storage options include:
      - Storage within the application system's database located in the company's Data Center.
      - Storage in a Shared File (Common Drive) within a dedicated folder based on assigned permissions.
    - Power off workstation computers after daily work completion, except for network servers, which necessitate continuous 24-hour operation.
    - Authorization is required from the highest-ranking authority within the department or above before removing any information assets from the company premises (excluding personal laptops). This includes documents, data storage media, and various computer equipment. Adhere to company policies regarding the removal of company property.
    - Exercise due care and diligence in managing company assets entrusted to you, treating them as if they were your own personal property. In cases of negligence leading to loss or damage, users will be held accountable for any resulting costs.

- Electronic Mail Usage Guidelines
  - Objective

    To ensure that electronic mail (e-mail) is used in a manner that supports company work accurately, conveniently, promptly, timely, efficiently, and securely, while complying with all applicable laws, regulations, and company data security measures. Additionally, these guidelines educate users about the potential risks associated with e-mail usage on the internet. Users must understand and adhere to all policies established by system administrators, refrain from actions that could cause harm or violate policies, and strictly follow the instructions of system administrators.
  - Guidelines
    - Users of the company's e-mail service must not engage in any activities that violate the Computer - Related Crime Act, the Electronic Transactions Act, or any other applicable laws, policies, or information technology guidelines established by the company.
    - Company departments or employees using the company's e-mail service must utilize it solely for the benefit of the company.
    - Authorized employees will be granted access to the company's e-mail service upon registration by the system administrator. The system administrator will utilize the employee list provided by the Human Resources department for registration.
    - Refrain from using the email addresses of others for the purpose of reading or sending messages without obtaining the explicit consent of the email address owner. The owner of the email address shall be held responsible for all activities conducted using their email account.
    - Users must not impersonate other users or send emails with false sender information.
    - When communicating electronically with clients or partners for business purposes, users must exclusively utilize the company's email system. The use of any other email system

is strictly prohibited, except in instances where the company's email system is unavailable and prior authorization has been obtained from a supervisor.

- Users must employ respectful and professional language in all email communications. Emails should not be inflammatory, provocative, or violate any laws or ethical standards. Users must refrain from expressing personal opinions as if they represent the company's stance or could potentially harm the company's reputation.
- The company's email system must not be used to distribute content that is immoral, threatens national security, violates laws, disrespects the monarchy, or disrupts the company's operations. Users must also avoid sending emails that could disturb other users or the company's clients.
- Users must not utilize company email addresses for personal purposes, such as private businesses or social media registrations. If such actions are discovered, the email account holder or user will be held responsible.
- Users must refrain from actions that could disrupt system resources, such as creating or forwarding chain emails, sending spam mails, distributing letter bombs, or disseminating computer viruses.
- Users must not share confidential company information with individuals or entities not directly involved in company missions.
- When transmitting confidential company information, users should encrypt the data and avoid indicating the data's sensitivity in the email subject line.
- Upon completing email usage, users must always log out of the system.
- In cases of complaints, requests, or suspected illegal activities, the company reserves the right to temporarily suspend or terminate the services of the involved employee for investigation and verification purposes.
- If users observe any inappropriate or potentially illegal behavior within the company, they must report it through the company's designated reporting channels.
- Any actions related to the dissemination of content, whether through email or user homepages, are solely the responsibility of the user. Neither the system administrator nor the company shall be held liable for such actions.

- Data and Information System Access Control

  Company Network Usage
  - Objective:

    To establish guidelines for utilizing the company's network to access the internet, ensuring efficiency, security, and user awareness when accessing websites through the company's network.
  - Guidelines:
    - The network connection path for internet access must be defined, incorporating security measures such as firewalls.
    - The installation of antivirus software and the application of operating system security patches are mandatory prior to network connection.
    - Upon completion of internet-related tasks, terminate all web browsers to preclude unauthorized access.
    - Users must access data only within their authorized scope of responsibility to maintain network efficiency and safeguard company security.
    - The disclosure of sensitive company information is strictly prohibited unless authorized in accordance with formally established disclosure protocols.

- Users must exercise the utmost caution when downloading internet-related software, including updates, All software downloads must be obtained from legitimate sources to avoid copyright infringement and respect intellectual property rights.
- Users are responsible for verifying the accuracy and reliability of internet-based data before utilizing it.
- Users must not use the company's internet network for personal business gain. Accessing websites of an inappropriate nature is strictly prohibited. This includes, but is not limited to, websites that contravene ethical standards, jeopardize national security, Threaten the monarchy, societal well-being, or public decency, contain sexually explicit materials and promote online gambling.
- Users must use the internet in a manner that demonstrates respect for others and avoids causing harm to the company. Actions that violate the Computer Crimes Act or related laws are strictly prohibited. All internet usage for company business must be conducted in accordance with established company procedures.

- Cryptographic Control
  - Objective:

    To restrict unauthorized individuals from accessing, comprehending, or altering sensitive information and system operations within their unauthorized purview.
  - Guidelines:

    Data Management Guidelines:
    - Implement a data classification hierarchy based on mission-criticality and sensitivity. Establish clear guidelines for managing each data type, including procedures for securely handling sensitive or critical data before disposal or reuse.
    - Encrypt sensitive data transmitted over public networks using industry-standard protocols, such as SSL (Secure Socket Layer) or VPN (Virtual Private Network).
    - Implement data integrity controls for storage, input, processing, and output. In cases of distributed databases or related datasets, ensure data consistency and accuracy across all locations.
    - Implement security measures when taking company computers off-site, such as for repairs. Securely destroy data stored on media before disposal.

    User Privilege Control
    - Implement strict access controls for data and processing devices, considering both functionality and information system security. Establish and disseminate clear authorization regulations to ensure users at all levels understand and strictly comply with established guidelines. Underscore the criticality of maintaining information system security.
    - Access rights to data and information systems, such as application system usage rights and internet access rights, shall be granted to users in accordance with their roles and responsibilities. Only the minimum necessary access rights for the performance of duties shall be granted, with prior written approval from authorized personnel. Such access rights shall be reviewed periodically.
    - For users requiring special privileges, necessitate stringent usage controls. To ensure the adequacy of such controls, the following factors shall be considered:
      - Obtain approval from authorized personnel.
      - Strictly monitor the usage of privileged users, restricting access to essential cases only.
      - Define usage periods and promptly revoke access upon expiration.

- Enforce strict password policies, requiring changes after each use or every 6 months for extended usage.

- In instances of unattended workstations, safeguards must be in place to prevent unauthorized individuals who do not have rights and uninvolving. Require users to log out of the system during periods of inactivity.
- In instances where data owners grant access or modification rights to other users (e.g., file sharing), permissions will be granted with specificity, either individually or on a restricted group basis and revoke access when no longer required. Data owners must document granted permissions, specify usage periods, and promptly revoke access upon expiry.
- In instances necessitating the provision of emergency or temporary system and network access, establish procedures for such actions. Secure prior authorization from designated personnel, providing documentation outlining the rationale and necessity. Clearly define usage periods and revoke access immediately upon their expiration.

User Account and Password Usage Control

- Implement robust identification and authentication mechanisms before granting access to information systems. These mechanisms should include enforcing strong, unpredictable passwords and assigning individual user accounts whenever possible. To determine the effectiveness of password complexity and usage control measures, the company shall consider the following factors:
  - Implement a minimum password length of 8 characters, in accordance with prevailing universal standards.
  - Require the use of special characters to enhance password strength such as: ; < > $ @ #
  - General users are required to change their passwords with a minimum frequency of every 6 months. System Administrators and default users are required to change their passwords every 2 months.
  - Not allowed to reuse any of the last three passwords.
  - Refrain from the use of predictable or easily guessable passwords such as “abcdef” “aaaaaa” “123456” “password” “P@ssw0rd”
  - Avoid passwords that contain personal information such as names, surnames, dates of birth, or addresses.
  - Avoid using dictionary words as passwords.
  - Establish a limit for the number of incorrect password attempts (Logon Attempts - Retires). In common practice, this limit should be set to 5 attempts. If the number of incorrect attempts exceeds the defined limit, the system or program will deny or suspend access.
  - A secure and thorough method for delivering passwords to users should be implemented. For example, passwords can be communicated directly to supervisors.
  - Require users to change their default or newly received passwords immediately.
  - Users should keep their passwords confidential and avoid writing them down on paper or sticking them near their computers. In the event that a password is compromised, users should change their password immediately.
  - In cases where multiple users share a system license, such as in ERP systems, the administrator will send an email notification to the responsible user requesting a password change when there is a change in the assigned users.

- Implement a robust encryption mechanism to protect password files from unauthorized access or modification.
- Establish a regular schedule for auditing user accounts associated with critical systems. Proactively identify and disable inactive user accounts, including those belonging to former employees or default users. Upon detection of unauthorized accounts, promptly implement appropriate measures, such as disabling, removing, or resetting passwords.

- The establishment of physical and environmental security measures
  - Objective:

    The establishment of physical and environmental security measures aims to safeguard the Data Center Room (DC Room) from unauthorized access, disclosure, modification or damage to data and computer systems. Safeguard data and computer systems from damage caused by environmental factors or natural disasters. This document outlines guidelines for controlling access to the DC Room and implementing various preventive measures within the DC Room.
  - Guidelines:

    Data Center Room Access Control
    - Critical computer equipment, such as network devices and servers, must be stored within the Data Center Room or a designated restricted area. Access to the DC Room should be granted only to authorized personnel, such as system administrators.
    - In exceptional circumstances when non-authorized personnel require access to the DC Room, strict control measures must be implemented. This may include the presence of system administrators or designated personnel to supervise activities at all times.
    - A system must be place to log entry and exit to the Data Center Room. These logs must include the identity of the individual and timestamps for entry and exit. Logs should be reviewed regularly.
    - The Data Center Room should be partitioned into designated zones, such as a Network Zone, Server Zone, UPS Zone, and Battery UPS Zone, to facilitate operations and enhance access control for critical IT equipment.

    Prevention of Damage
    - Fire Protection System
      - Install fire warning devices, such as smoke detectors, to prevent or suppress fire hazards promptly.
      - A fire extinguisher must be present in the main Data Center Room for initial fire suppression.
    - Electrical Failure Prevention System
      - A system must be in place to protect computers from damage caused by electrical instability.
      - A backup power system must be provided for critical computer systems and computer networks to ensure continuous operation.
    - Temperature Control System
      - The environment must be maintained at an appropriate temperature and humidity level. The air conditioning temperature should be set according to the specifications of the computer system, as the computer system may malfunction under inappropriate temperature conditions.

- Operations Security for Information Systems
  - Objective:

To ensure that the company's information systems are operated in a secure and compliant manner, preventing data loss and protecting systems against the potential harm of malicious programs.

- Guidelines:
  - Develop comprehensive manuals or operational guidelines for the company's critical information systems to prevent errors in information management practices.
  - Enforce strict change control procedures for information systems. For instance, require prior authorization from designated personnel before implementing any changes.
  - Implement data backup procedures before making any Information system modifications.
  - Implement a system to monitor and track information system resources, such as CPU, memory, and hard disk usage, to ensure adequate capacity. Analyze resource utilization data to plan for future resource allocation or expansion.
  - For critical systems, isolate development environments from production environments to prevent unauthorized data modification.
  - Conduct a thorough data inventory, classify data based on its criticality, and determine the appropriate backup frequency for each data category.
  - Implement a more frequent backup schedule for highly sensitive data. Consider storing copies of sensitive data offsite for additional protection.
  - Test the readiness of information system backups at least annually.
  - Implement malware protection measures, such as;
    - Install antivirus software and apply the latest operating system and web browser security patches to personal computers and laptops before connecting to the company's network.
    - Require users to regularly update operating systems and applications with the latest patches and/or hotfixes, which are typically available for download from the product vendor's website to address security vulnerabilities.
    - All computer data transmitted via email must be scanned for viruses using antivirus software before being sent or received.
    - Users must install only authorized software provided by the company. If users need to install additional software beyond what the company provides, they must notify the IT department for security review and approval before installation.

- Communications Security for Information Systems on computer networks
  - Objective:

    To protect information systems on the network from unauthorized access, viruses, and malicious code that could compromise data or disrupt information system operations.
  - Guidelines:

    Network Security Management
    - Implement stringent network access controls to ensure security.
    - Establish a clear segmentation of the network between internal users and external entities accessing the company's systems.

    Information Transfer
    - Formalize agreements for information transfer (Agreements on Information Transfer) with a primary emphasis on data security. System administrators must oversee these operations to guarantee the confidentiality, integrity, and availability of data at all times.

- Mandate the signing of non-disclosure agreements (NDAs) between the company and external entities to prevent the unauthorized disclosure of confidential information.

- Information Systems Acquisition, Development, and Maintenance
  - Objective:
    To control the development or modification of information systems to ensure that the resulting computer systems function accurately, comprehensively, and in accordance with user requirements. This approach mitigates Integrity Risk by encompassing the entire development or modification process, from initial requests to the deployment of the developed or modified system.
  - Guidelines:
    - Establish documented procedures for developing or modifying systems, including at least requirements for the request process, development or modification process, testing process, and system deployment process.
    - Implement procedures for handling emergency changes to computer systems, ensuring that the reasons for such changes are documented and that appropriate authorization is obtained.
    - Effectively communicate the details of these procedures to all relevant users and stakeholders, ensuring adherence to the established guidelines.

    Development control or modification of computer systems
    - Request Process
      - All requests for the development or modification of computer systems must be submitted in writing, which may include electronic transactions such as email. Approval must be obtained from an authorized individual, such as the head of the requesting department or the information systems manager.
      - A written impact assessment should be conducted for any significant changes, considering the operational, security, and functionality of related systems.
      - Relevant government regulations should be reviewed, as modifications may, in many cases, impact compliance with such regulations.
    - Information Systems Development Practices
      - Clearly separate development environments from production environments and restrict access to authorized personnel only. This separation can be implemented using dedicated computers or by partitioning a single computer.
      - Require the active participation of the requesters and relevant users throughout the development or modification process to ensure the system aligns with their requirements.
      - Prioritize system security and operational stability (Availability) from the inception of development or modification.
    - Testing
      - Requesters, IT department, and relevant users, must actively participate in system testing to ensure that the developed or modified computer system functions efficiently, processes data accurately and comprehensively, and fully meets defined requirements before deployment.
    - System Deployment
      - Thoroughly verify the accuracy and completeness of system deployment procedures.
    - Documentation and Details Related to System Development

- Maintain detailed records of currently used programs, including information on past development or modifications.
- Update all system-related documentation after development or modification to ensure up-to-date information. This includes, but is not limited to, data structure documentation, user manuals, user access lists, program workflow descriptions, and program specifications. Store these documents securely and in a user-friendly manner.
- Archive pre-development program versions for potential use in case the current version encounters errors or becomes unusable.

- Change of Communication
  - Effectively communicate all changes to relevant users to ensure proper system utilization.

- Information Systems services from outsourcing service providers
  - Objectives:
    Safeguard company assets from unauthorized access by IT outsourcing providers and maintain agreed-upon security and service levels as outlined in service agreements.
  - Guidelines:
    - Establish clear security requirements for company data or assets whenever access by IT outsourcing providers is required, ensuring alignment with company data confidentiality policies.
    - Effectively communicate and enforce security requirements for company data to IT outsourcing providers before authorizing access.
    - The Service Level Agreement must mandate regular monitoring, review, and evaluation of outsourced services.
    - Conduct a comprehensive security risk assessment upon any modifications to service level agreements pertaining to critical systems.

- Information Security Incident Management
  - Objectives:
    To establish a consistent and effective approach to managing information security incidents, including reporting information security situations and vulnerabilities.
  - Guidelines:
    - Define clear roles and responsibilities for handling company security incidents.
    - Establish clear communication channels for reporting information security situations.
    - In the event that a user detects an incident that may compromise the security of the information system, they must report the incident to the Information Technology Department.
    - Implement a reporting procedure for information security incidents, escalating notifications based on severity and promptly informing affected users in the event of major disruptions.
    - All security incidents must be thoroughly documented, including the incident type, frequency, associated costs, and any relevant details. This documentation facilitates analysis and the development of preventive measures.
    - Collect and preserve evidence in accordance with relevant laws and regulations for potential legal proceedings.

- Business Continuity Management for Information System Security
  - Objectives:
    To prevent disruptions to the company's operations caused by crises or disasters and to ensure the readiness of the company's information system equipment.
  - Guidelines:
    - The IT department must develop a contingency plan for addressing potential information system uncertainties and disasters, in accordance with the company's Disaster Recovery Plan (DRP) and the cloud vendor's Business Continuity Plan (BCP).
    - Conduct an annual risk assessment and evaluation of information system vulnerabilities at least annually.
    - Review the emergency preparedness plan at least annually.
    - Verify the readiness of backup information systems at least annually, in accordance with the cloud vendor's Business Continuity Plan.
    - Perform Vulnerability Assessments (VA Scans) at least annually to identify vulnerabilities in systems including operational flaws in systems, servers, and networks as well as security device weaknesses. This will enable targeted remediation and reduce the risk of potential cyber threats.

Section 3

Cloud Computing Services

In today's business landscape, information technology plays a pivotal role in supporting and driving core operations within the capital market industry. One widely adopted technology is cloud computing, which offers on-demand computing services over a network to significantly enhance processing capabilities and optimize cost management. Cloud computing involves the sharing of information systems on a computer network to manage computing resources in accordance with user demands. This may include dedicated resource allocation for specific users or shared usage among multiple users and legal entities, promoting efficient resource and cost management. However, the shared usage of resources on a network introduces technological complexities and potential risks to information stored on networks managed by external parties or cloud providers.

- Objective

  To provides guidelines for the company's effective governance and management of security within its cloud computing operations. The objectives are as follows:
  - Alignment of information systems activities with organizational goals (Value Delivery)
  - Optimal risk management
  - Resource Optimization for Maximizing Benefits
  - Comprehensive Cloud Computing Security Management

- Cloud Computing Governance and Management Guidelines

  Establish a comprehensive framework for the governance and management of shared information systems on cloud computing, tailored to user requirements and adhering to internationally recognized governance frameworks, encompassing the entire lifecycle of cloud computing management, from the establishment of governance frameworks to the definition of strategic usage guidelines, the management of cloud service providers, and the termination or end-of-life processes for cloud services.

Types of Cloud Computing Service Models

1) Software as a Service (SaaS): SaaS refers to the delivery of software applications hosted on cloud infrastructure. Users access these applications through a network using applications on their devices, such as web browsers or mobile apps. The cloud provider manages the underlying cloud infrastructure, including physical security, operating systems, networks, storage systems, and the core application functionality.
2) Platform as a Service (PaaS): PaaS provides a cloud-based platform for developing applications. Users access this platform to develop and deploy applications. The cloud provider manages the cloud infrastructure, including physical security, operating systems, networks, and services such as web services and database management systems. However, users control application management, such as code modifications.
3) Infrastructure as a Service (IaaS): IaaS offers shared cloud infrastructure resources, such as operating systems, networks, and storage. The cloud provider manages the physical infrastructure and IT resources that support the cloud infrastructure's operation.

Cloud Deployment Models

1) A public cloud means model utilizes a shared infrastructure over a public network.
2) A private cloud means model establishes a dedicated cloud infrastructure within an organization's private network, exclusively for its own use.
3) A hybrid cloud means model combines elements of both public and private cloud environments.

1. Governance and Management Guidelines for Cloud Computing Services

- Objective
  To establish a guideline for the organization's governance and management of Cloud Computing services.
- Guidelines
  - Develop a clear Cloud Computing strategy that addresses various factors including the business rationale and necessity, benefits and costs, compliance of internal and external legal and regulatory requirements, risks and risk management, information security and cybersecurity measures and a plan for human resource management and knowledge acquisition.
  - Formulate a Written Cloud Computing Usage Policy that should be approved by the company's board of directors. This policy should encompass the following key aspects:
    - Define the types of workloads for deployment on the cloud.
    - Specify the permissible types of cloud computing usage, including Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS), and/or Infrastructure-as-a-Service (IaaS) and the deployment models, such as Private, Public, and/or Hybrid clouds.
    - Data classification and categorization, including security measures and practices for each data type based on its confidentiality level.
    - Risk Assessment and Management for addressing information security and cybersecurity risks associated with cloud computing usage.
    - Cloud Provider Evaluation and Selection
    - Execution of Contract and Service Level Agreement
    - Performance Monitoring, Oversight and Service Level Agreement Implementation
    - Consistently Monitor and Report Cloud Service Incidents
    - Role and Responsibility of relevant personnel
  - Disseminate the Cloud Computing Usage Policy to relevant employees and officials, including business unit staff, system administrators, developers, integrators, end users, and any others impacted, to raise awareness of cloud computing security and safety.
  - Review the Cloud Computing Usage Policy at least once a year.
  - Review and update the Information Technology Risk Management Guidelines to comprehensively address risks associated with cloud computing services. This process should include identifying risks, assessing risks, implementing controls to mitigate risks to acceptable levels and assigning risk ownership.
  - Report the results of Cloud Computing risk assessments and risk management strategies to the Risk Management Committee or the designated committee.

2. Cloud Service Provider Management

- Objective
  Cloud Computing is a service delivery model managed by external providers. Therefore, the company should establish comprehensive and consistent guidelines for managing Cloud Computing services at each stage of the process.
- Guidelines
  Process and criteria for selecting Cloud Service Providers

- Conduct thorough due diligence to assess the readiness and suitability of potential providers. Ensure the provider's ability to deliver continuous services, considering key factors such as expertise, experience, and financial stability.
- Evaluate the provider's information security standards focusing on the provider's ability to maintain data confidentiality, data and system integrity, and service availability. Consider adherence to internationally recognized security standards such as ISO27001, ISO27017, PCI/DSS, and TIA.
- Evaluate the alignment between the Cloud Service Provider's (CSP) business continuity practices and the company's Business Impact Analysis for systems to be hosted on the cloud computing platform. This evaluation should consider the CSP's ability to meet the company's maximum tolerable downtime (MTD), recovery time objective (RTO) for data and system restoration, and the latest data sets to be recovered (Recovery Point Objective: RPO), as outlined in the Business Impact Analysis.

Engagement and Service Level Agreements

Execute written service agreements with Cloud Service Providers. Formulate a comprehensive Service Level Agreement clearly outlining the following aspects:

- Scope of services, service types, and terms of service delivery
- Data ownership conditions for service users, including user rights and associated licenses. Users should retain ownership of their data.
- Liability conditions in case of service failure to deliver services as agreed upon in the agreement should be clearly outlined. The company should consider damage assessment provisions, including any limitations of liability stipulated between the service provider and the service user.
- Data access provisions for the service provider, including access rights and data disclosure conditions. The service provider should obtain explicit user consent or comply with domestic legal requirements of the country where its data center is located. Users must be duly informed of such disclosures.
- Data Backup, Disaster Recovery, and Business Continuity Plan Requirements for Service Providers, includes clear and concise requirements as follows:
    - Data Recovery Location
    - Service Restoration Time
    - Recovery Time Objective (RTO)
    - Recovery Point Objective (RPO)
    - Data Leakage Prevention Requirements and Measures from service providers
    - Service Provider Contact Information for Operational Issues and Information Security Incidents

Cloud Computing Operations

The operation of cloud computing services should incorporate robust information technology (IT) security management practices aligned with the fundamental principles of information security which are confidentiality, integrity, and availability.

3. Exit Strategy or Terminating Cloud Computing Services:

- Objection:

  To establish a comprehensive exit strategy for terminating or ending the use of shared cloud computing services. This strategy aims to mitigate potential risks associated with service termination, including Service Disruption Risks, Information Security and Data Privacy Risks and Data Integrity and System Reliability Risks.

- Guidelines:
  The Company should carefully consider developing a comprehensive exit strategy and plan for terminating cloud computing services. This planning process involves 4 key steps:
  1) A pre-assessment of service cancellation or termination should evaluate the feasibility, risks, and procedures involved, taking into account the terms and conditions specified in the service level agreement. This includes service cancellation terms, roles and responsibilities of the service user and provider during the process of termination, data ownership, data conditions, data format and delivery, and any relevant rights and copyrights.
  2) A comprehensive exit strategy/plan should be developed for service cancellation or termination. This plan should outline detailed steps, timelines, responsible personnel, and their respective roles and responsibilities. It should also identify and address task dependencies and the potential impacts of related activities. To mitigate potential risks, develop a contingency plan to address any unforeseen challenges or failures during the cancellation or termination process. These measures will ensure the company maintains its ability to provide uninterrupted service.
  3) Service cancellation execution should be approved by authorized personnel and communicated to all affected users and stakeholders. Additionally, a process should be implemented to evaluate and securely delete data and programs stored on shared systems, ensuring the confidentiality and security of company information and programs.
  4) Establish a comprehensive post-service cancellation follow-up process to ensure the fulfillment of ongoing obligations, even after the service agreement expires. This process should include managing confidential data within the specified retention period in accordance with data privacy regulations, implementing procedures for prompt notification in case of data breaches, and addressing any residual liabilities arising from the terminated service.

In accordance with the decision adopted at the Board of Directors' meeting on 3rd. April 2024

TCM Corporation Public Company Limited

(Miss Piyaporn Phanachet)
Chief Executive Officer