HARN ENGINEERING SOLUTIONS PUBLIC COMPANY LIMITED

INFORMATION TECHNOLOGY DEVELOPMENT POLICY AND PLAN

Information Technology Security Policy

To ensure that the information technology systems, computer networks, and computer systems of Harn Engineering Solutions Public Company Limited are used appropriately, securely, and capable of continuously supporting the Company's operations, and that such systems are utilized in compliance with applicable computer crime laws and other relevant regulations, as well as to prevent threats that may cause damage to the Company, the Company hereby establishes this Information Technology Security Policy.

Definitions

The definitions in this section provide clarification of terms used in this Information Technology Security Policy and related practices to ensure clear and consistent understanding.

1. "Company" means Harn Engineering Solutions Public Company Limited utilizing information systems and computer network systems.
2. "Human Resources Department" means the Human Resources Department of Harn Engineering Solutions Public Company Limited.
3. "Information Technology Unit" means the Information Technology Unit of Harn Engineering Solutions Public Company Limited.
4. "Facilities Management Unit" means the Facilities and Premises Management Unit of Harn Engineering Solutions Public Company Limited.
5. "User" means directors, executives, employees, authorized internal users, and external users who are permitted to access the Company's network systems.
6. "Personnel" means permanent employees, probationary employees, and temporary employees of the Company.
7. "Related Users" means individuals or juristic persons who are contractual counterparties of the Company and conduct activities within the Company.
8. "External Users" means individuals or juristic persons other than those specified in Items (6) and (7).
9. "System Administrator" means the Manager of the Information Technology Unit or other personnel assigned by a supervisor at director level or above to be responsible for the development, modification, improvement, and maintenance of the Company's information systems and network systems, or any unit directly responsible for such systems.

10. “Information” means facts derived from data that have been processed and organized, which may be in the form of numbers, text, documents, diagrams, maps, photographs, film, video recordings, audio recordings, computer records, or graphics, arranged in a manner that is easily understood by users and can be utilized for management, planning, decision-making, and other purposes.
11. “Information System” means the Company’s work systems used to store, process, and disseminate information, operating through the integration of hardware, software, data, users, and processing procedures to produce information that supports planning, management, and the Company’s operational mechanisms.
12. “Network System” means systems used for communication or transmission of data and information among the Company’s information technology systems, such as LAN, Wireless, Intranet, Internet, and other communication systems.
13. “Assets” means any tangible or intangible property of value 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 of value to the Company.
14. “Information Technology Security” means the security of the Company’s information technology and network systems by preserving the confidentiality, integrity, and availability of information, as well as other attributes including authenticity, accountability, non-repudiation, and reliability.
15. “User Privileges” means the levels of access rights to information for personnel and related users, including general privileges, privileged access, and other rights associated with the Company’s information and network systems.
16. “Access to or Control of Information Usage” means the authorization, assignment of rights, or delegation of authority to users to access or utilize network or information systems, whether electronically or physically, including the establishment of rules governing unauthorized access.
17. “User Account” means a username and password assigned to personnel, related users, and external users.
18. “Information Security Event” means any identified occurrence, service state, or network condition indicating a possible breach of security policy, failure of safeguards, or any event potentially related to information security.
19. “Undesirable or Unforeseen Information Security Situation” means any situation that may result in the Company’s systems being breached or attacked, or in information security being threatened.

20. “Encryption” means the process of encoding data to prevent unauthorized access, whereby encrypted data can only be accessed using a decryption program to restore it to usable form.
21. “Authentication” means a security process for system access involving verification of a user’s identity, typically through a username and password.
22. “SSL (Secure Socket Layer)” means data encryption technology used to enhance the security of communications or data transmission over the Internet between a server and a web browser or application.
23. “VPN (Virtual Private Network)” means a virtual private computer network that transmits data over the Internet using encrypted communication, preventing unauthorized parties from reading or viewing the transmitted data until it reaches its destination.

Information Technology Security Policy

Section 1

Governance of Enterprise IT

Information technology governance aims to ensure that the Company can achieve its established objectives by utilizing information technology as a supporting tool and by effectively managing risks arising from the use of information technology. Effective IT management requires integration of IT management processes, resources, and information to support organizational policies, strategies, objectives, and appropriate risk management, together with reporting and monitoring mechanisms to ensure that the technologies adopted by the Company support business strategies, achieve business objectives, enhance competitiveness, and add value to the Company. The Company shall, at a minimum, undertake the following:

1. Information Technology Security Policy

1.1. The Company shall assign responsibility for establishing a written Information Technology Security Policy and shall communicate such policy to ensure understanding and proper compliance, particularly between the Information Technology function and other internal units, to enable coordination and achievement of business objectives.

1.2. The Company shall review the Information Technology Security Policy at least annually or whenever changes occur that may affect the Company’s information technology security.

2. Information Technology Risk Management Policy (IT Risk Management)

This shall be aligned with the Corporate Risk Management policy and shall cover the following:

2.1. Definition of roles and responsibilities for IT risk management. The Manager of the Information Technology Unit shall be responsible for studying and identifying IT solutions or approaches to mitigate or manage existing risks and proposing them to management for consideration in managing IT system risks.

2.2. Identification of Information Technology–related risks, including:

2.2.1. Physical and Environmental Risks: The Data Center Room, where servers, network equipment, and other devices are installed, shall have controlled access and usage, and monitoring systems such as temperature alarms and fire detection systems.

2.2.2. Risks from Software Usage on Company Computers: Measures shall be in place to prevent installation or use of unsafe or unauthorized software, such as downloading and installing external programs that may contain malware, computer viruses, or vulnerabilities enabling external network attacks on the user's computer or other devices on the same network

2.2.3. Risks from Use of the Company's Network Systems: The Company shall monitor and supervise internal network and Internet usage, and implement protective systems against unauthorized access and external attacks on servers and client computers used by personnel, such as Internet access control systems, antivirus software installation, and email filtering.

2.2.4. Personnel Risks: User access rights to computer systems, network equipment, and data shall be assigned strictly according to authorized privileges to prevent unauthorized modification or alteration of information.

3. Risk Assessment

Risk assessment shall cover both the likelihood of occurrence and the potential impact in order to prioritize risk management. Risks are categorized into four types as follows:

3.1. Technical Risks: Risks arising from attacks on computers and equipment.

3.2. Personnel Risks: Risks arising from improper access rights management, resulting in access to information beyond assigned duties and potential damage to information assets.

3.3. Disaster and Emergency Risks: Risks arising from disasters or natural events, as well as other situations such as power outages or civil disturbances.

3.4. Management Risks: Risks arising from policies or practices that may not align with existing or emerging risks.

4. Risk Management Methods and Tools

   The Company shall establish methods or tools to manage risks within acceptable levels. A risk description table shall be prepared, including risk name, risk category, risk characteristics, risk factors, and impacts. Likelihood and impact levels shall be defined, and a Risk Map shall be developed.

5. Information Technology Risk Indicators

   Information Technology Risk Indicators shall be defined, with monitoring and reporting to responsible parties to ensure appropriate and timely IT risk management.

Section 2

Information Technology Security (IT Security)

1. Additional Practices Relating to the Information Security Policy

   - Objective

     To prevent violations of the Information Technology Security Policy.

   - Practices

     - Do not use the Company's IT resources and computer networks for illegal activities or activities contrary to public morality, such as creating websites to conduct unlawful trade or disseminate illegal or unethical content.
     - Do not access computer networks or computers using another person's user account, whether or not permission has been granted by the account owner.
     - Do not access protected computer systems or data of others to modify, delete, add, or copy information.
     - Do not disclose another person's or any department's information without authorization from the data owner.
     - Do not disrupt, obstruct, or damage the Company's IT resources or computer networks, such as by transmitting computer viruses or introducing programs that cause denial of service (DoS) to computers or network equipment.
     - Do not intercept or eavesdrop on data transmitted over the Company's or others' computer networks.
     - Before using any removable storage media or opening email attachments or files downloaded from the Internet, always scan for viruses using antivirus software.

- Users shall not permit others to use their user accounts or passwords to access computers or systems.

2. Organization of Information Security

- Objective

  To establish a framework for managing information security within the Company.

- Practices
  - Senior management shall be responsible for overseeing information security to ensure compliance with the Company's Information Security Policy and related practices.
  - The Manager of the Information Technology Unit shall assign responsibilities to IT personnel for maintaining the security of the Company's information systems and for controlling operations to ensure adherence to the Company's information security policies and practices.
  - IT personnel designated as system administrators shall be responsible for the systems under their care, including monitoring and maintaining operational security. In the event of an undesirable or unforeseen information security situation, they shall take corrective action and report to their supervisors.
  - Users and both internal and external units shall be responsible for complying with the Company's Information Security Policy and practices and shall not engage in any actions that violate applicable computer-related laws.

3. Human Resource Security for Information Systems

- Objective

  To ensure that users understand the Company's policies, duties, and responsibilities in using the Company's information systems.

- Practices
  - Duties and responsibilities related to information system security shall be defined in writing for personnel or external parties engaged by the Company and shall be consistent with the Company's Information Security Policy.
  - A Non-Disclosure Agreement (NDA) shall be signed between personnel and the Company, forming part of the employment or engagement terms. Such agreement shall remain binding during employment and for at least one year after termination.

- To ensure that user account administration remains accurate and up to date, the Human Resources Department or relevant unit shall immediately notify the IT Manager when any of the following events occur:
  - Hiring or engagement
  - Change in employment status or terms of engagement
  - Resignation or termination of directorship and employment with the Company
  - Transfer to another department or unit
- All new personnel of the Company shall receive training on the Information Technology Security Policy as part of the orientation program.
- The Company shall enhance employees' knowledge and skills in the effective and secure use of digital technologies to ensure beneficial utilization and readiness for future technological advancements.
  - The Company shall disseminate knowledge on precautions for the use of the Internet and e-mail.
  - The Company shall conduct random testing and risk assessments regarding the receipt of and responses to phishing e-mails.
  - The Company shall provide training on the use of software applications, such as MS Office, e-mail, and calendar systems.
  - The Company shall support employees in undertaking proficiency testing in the use of software applications, such as MS Office.
- Upon any change or termination of employment, or upon completion of a project, access to information within the information systems shall be revoked immediately.

4. Asset Management

4.1 Computer and Peripheral Access Control

- Objective

  To ensure that users are informed of their duties and responsibilities in relation to the use of the Company's computers and peripheral devices, and that they understand and strictly comply with the relevant requirements, thereby safeguarding the Company's assets and information to remain secure, accurate, and continuously available.

- Practices
  - Users of the Company's computers and peripheral devices shall be responsible for the assets assigned to them.
  - The Company's computers and network systems shall not be used for personal business, commercial activities, or any inappropriate purposes.
  - Users are not permitted to install, modify, or alter any software on the Company's computers unless they have received consultation or guidance from the system administrator or authorization from the head of the relevant department.
  - Modification or alteration of any components of computers or peripheral devices is prohibited unless approved by the system administrator or responsible department. Users shall maintain such equipment in its original condition.
  - Users shall not store or use computer equipment in locations with excessive heat, humidity, dust, or where there is a risk of impact.
  - Computer equipment of any kind shall not be used or placed near liquids, strong electromagnetic fields, vibration sources, or in environments with temperatures exceeding 35 °C.
  - When transporting computer equipment, users shall handle it with due care and shall not place heavy objects on top of it or throw it.
  - Computers shall not be moved while the hard disk is in operation or while the device is powered on.
  - Users shall avoid contact of hard objects with computer screens, which may cause scratches or damage. Screens should be cleaned gently in a single direction and not in a circular motion to prevent scratching.
  - Users whose employment has ended or whose project has been completed shall return all computers and peripheral devices under their responsibility to the responsible department in good working condition.
  - When transporting computer equipment for work outside the office, users shall comply with the Company's regulations on the removal of Company property from the premises.
  - Users are responsible for preventing loss and shall not leave computers unattended in public places or in areas with a risk of loss or theft

4.2 Software License Control

- Objective

  To ensure that users are aware of their duties and responsibilities in the use of computer software, understand the proper use of legally licensed software, and strictly comply with the prescribed practices, as well as to ensure that software usage remains secure and in compliance with the Computer Crime Act and other applicable laws.

- Practices

  Requirements for System Administrators

  - System administrators shall be responsible for controlling and overseeing the use of computer software, including allocating software usage within the Company in accordance with the prescribed licensing rights.
  - System administrators shall be responsible for installing and upgrading computer software for users at scheduled times.
  - System administrators shall promptly uninstall software and revoke software usage rights upon notification from the Company and/or the relevant department of termination and/or reassignment of such rights.

  Requirements for Users

  - Users shall use computer software with the same care as a reasonable person would exercise in using their own property and shall not use it for any unlawful purposes or in violation of the rights of others that may cause damage to the Company.
  - Software installed on the Company's computers is legally licensed; therefore, users are prohibited from copying, installing on other computers, modifying, or allowing others to use such software.
  - Users shall not copy, distribute, or disseminate copyright-infringing software or unauthorized command sets, particularly for use as tools in unlawful activities.
  - The installation of illegal software on the Company's computers is strictly prohibited. If users wish to install any software other than that provided by the Company—whether licensed software or freeware—prior approval from the Information Technology system administrator must be obtained. Users shall be solely responsible for any damage or infringement arising therefrom.

- For the installation, removal, transfer, or return of computers and computer software, users shall submit a request for approval to the authorized approver in each case, and the Information Technology system administrator shall be responsible for carrying out the actions in accordance with the granted approval.

4.3 Information Asset and Computer System Access Control

- Practices

Information assets—including documents, storage media, computers, and information data—shall be controlled to prevent exposure to the risk of access by unauthorized persons when not in use, and users shall be required to log off from information systems when leaving them unattended, as follows:

- Users shall log out of information systems immediately upon completion of their tasks.
- Computers shall be protected by appropriate authentication mechanisms prior to access.
- Important information of each department shall be stored and backed up in secure locations. User data may be stored in the following forms:
  - Within the database of the relevant application system hosted in the Company's Data Center; export of data from such application systems is not permitted.
  - Within shared files (central drives) in folders according to the access rights granted.
- Users shall shut down their computers when not in use for more than one hour or upon completion of daily work, except where such computers function as servers required to operate continuously on a 24-hour basis.
- Screen saver settings on users' computers shall be configured to automatically lock the screen after 15 minutes of inactivity.
- Prior approval from the head of department or higher authority shall be obtained in all cases where information assets—such as storage media or computer equipment—are to be taken off the Company's premises, in accordance with the Company's regulations on the removal of Company property.
- Users shall exercise due care in safeguarding the Company's assets under their use as if they were their own property; any loss resulting from negligence shall be the user's responsibility, and the user shall be liable for the resulting damage.

4.4 Electronic Mail (Email) Usage

- Objective

  To ensure that communication and information exchange via electronic mail effectively supports operations and is conducted accurately, conveniently, promptly, and efficiently, with appropriate security, in compliance with applicable laws, regulations, rules, and the Company's information security measures. This is also to ensure that users understand the importance of and are aware of issues arising from the use of electronic mail services over the Internet. Users shall understand and comply with the rules established by the system administrator, shall not infringe the rights of others or engage in any actions that may cause problems or violate such rules, and shall strictly follow the system administrator's instructions.

- Practices

  Users of electronic mail services shall not engage in any acts in violation of the Computer Crime Act, the Electronic Transactions Act, other applicable laws, or the Company's information technology policies and requirements.

  - Departments or personnel using the Company's electronic mail services shall use such services solely for the benefit of the Company.
  - Personnel shall be granted access to electronic mail services, and the system administrator shall register e-mail user accounts based on the personnel list provided by the Human Resources Department.
  - Users shall not use another person's e-mail address to read or send messages without the owner's consent. The e-mail account owner shall be deemed responsible for all activities conducted through their account.
  - Users shall not falsify sender identities or other user accounts when using electronic mail.
  - In sending e-mail communications to service recipients in connection with the Company's operations, users shall use only the Company's e-mail system. Other e-mail systems shall not be used unless the Company's system is unavailable and prior approval from a supervisor has been obtained.
  - E-mail usage shall be conducted in polite language and shall not be contrary to good morals, incite or provoke, contain defamatory or unlawful content, or present personal opinions as those of the Company or otherwise cause damage to the Company.

- The Company's e-mail system shall not be used to disseminate information, messages, images, or other content that is contrary to public morals, national security, applicable law, the monarchy, or that may affect the Company's operations or disturb other users or service recipients.
- Users shall not use their Company e-mail address for personal matters, such as private business or registration for social networking services. Any such use shall be deemed the responsibility of the e-mail account owner.
- Users shall not engage in any activities that create problems in the use of system resources, such as chain mail, spam mail, mail bombing, or dissemination of computer viruses.
- Confidential Company information shall not be sent to any person or entity not related to the Company's operations.
- When transmitting confidential Company information, such information should be encrypted, and its sensitivity should not be indicated in the e-mail subject line.
- Users shall log out of the e-mail system after each session.
- In the event of complaints, requests, or suspected unlawful acts, the Company reserves the right to suspend or temporarily revoke the relevant user's e-mail services for investigation and verification.
- If users encounter inappropriate conduct or suspected misconduct within the Company, they shall report it through the Company's whistleblowing channels.
- Any acts relating to dissemination through electronic mail or a user's homepage shall be deemed solely the responsibility of the user. The system administrator and the Company shall bear no liability in this regard.

4.5 Access Control

Use of the Company's Network System

- Objective

  To establish measures for the use of the Internet through the Company's network system to ensure efficiency and security, and to promote users' awareness in accessing various websites through the Company's network.

- Practices
    - The Information Technology Department shall define network connection routes for Internet access through the Company's network, which must pass through security systems such as firewalls or proxies.
    - Company computers shall have antivirus software installed and operating system vulnerabilities patched prior to connection to the network.
    - After completing Internet use, users shall close the web browser to prevent unauthorized access by others.
    - Users shall access information sources only in accordance with the access rights granted based on their duties and responsibilities, to ensure network efficiency and Company security.
    - Users shall not disclose confidential Company information unless in accordance with the Company's formal disclosure requirements.
    - Users shall exercise caution when downloading software via the Internet, including updates, ensuring that such downloads do not infringe copyright or intellectual property rights.
    - Users are responsible for verifying the accuracy and reliability of computer information obtained from the Internet before use.
    - Users shall not use the Company's Internet network for personal business purposes or access inappropriate websites, including those contrary to public morals, national security, religion, or the monarchy, socially harmful sites, or pornographic content.
    - Users shall use the Internet in a manner that does not infringe the rights of others or cause damage to the Company and shall not engage in any acts constituting an offense under the Computer Crime Act or other applicable laws. In all cases of Internet use for Company operations, users shall strictly comply with the Company's prescribed procedures.

4.6 Cryptographic Control

- Objective

  To prevent unauthorized persons from accessing, becoming aware of, or altering information or the operations of information systems beyond their authorized duties and responsibilities.

- Practices

  1. Information Management

     - Information shall be classified according to confidentiality levels and categorized based on operational requirements and data criticality. Management methods shall be defined for each category, including procedures for handling confidential or critical information prior to disposal or reuse.
     - Transmission of sensitive information over public networks shall be protected by internationally recognized encryption standards, such as SSL (Secure Socket Layer) or VPN (Virtual Private Network).
     - Controls shall be implemented to ensure the integrity of data during storage, input, processing, and output. Where identical data is stored in multiple locations (distributed databases) or where related datasets are maintained, controls shall ensure that such data remains accurate, complete, and consistent.
     - Security measures should be implemented to protect data when computers are taken outside the Company's premises, such as for repair, or the data stored on the media shall be securely destroyed beforehand.

  2. User Privilege Control

     - Access to information and data processing facilities shall be controlled with due regard to operational needs and information system security. Access authorization rules shall be defined, and user privileges established so that users at all levels are informed, understand, and strictly comply with the prescribed practices, and recognize the importance of maintaining information system security.
     - User access rights to information and information systems—such as application system access and Internet usage rights—shall be assigned in accordance with users' roles and responsibilities. Access shall be granted only to the extent necessary for the performance of duties, subject to written approval from the authorized authority, and such rights shall be reviewed regularly.

- Where the use of privileged user accounts is necessary, their use shall be strictly controlled. In determining the adequacy of such controls, the Company shall consider the following factors:
  - Prior approval from the authorized authority should be obtained.
  - Use of privileged accounts should be tightly restricted, limited to strictly necessary cases only.
  - A defined usage period should be specified, and access shall be revoked immediately upon expiry.
  - Passwords shall be changed strictly, such as immediately after completion of the required use or, where extended use is necessary, at least every three months.
- When users are not present at their computers, measures shall be in place to prevent use by unauthorized persons, such as requiring users to log out of systems when leaving their workstations unattended.
- Where necessary for a data owner to grant other users access to or permission to modify their data (e.g., file sharing), such access shall be granted only to specific individuals or groups, revoked when no longer necessary, and supported by documented authorization. A usage period shall be specified, and access shall be revoked immediately upon expiry.
- Where it is necessary to grant other persons emergency or temporary access to information systems or network systems, procedures shall be established and prior approval from the authorized authority shall be obtained in all cases. The reasons and necessity shall be recorded, a usage period specified, and access revoked immediately upon expiry.

3. User Account and Password Control

- Robust identification and authentication mechanisms shall be implemented to verify users' identities and access rights prior to access to information systems, such as requiring passwords that are difficult to guess. Each user shall be assigned an individual user account. In determining whether password complexity requirements and password controls are sufficiently stringent, the Company shall consider the following factors in aggregate:
  - Passwords should be of adequate length; most international standards recommend a minimum of eight characters (alphabetic and numeric).
  - Special characters should be included, such as : ; < > $ @ #.
  - For general users, passwords should be changed at least every three months.

- When changing passwords, the new password should not repeat 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 be related to the user, such as name, surname, date of birth, or address.
- Passwords should not be dictionary words.
- A limit should be set on the number of permitted failed logon attempts (logon retries), typically five attempts; exceeding this limit shall result in denial or suspension of access.
- Passwords shall be delivered to users through secure and controlled methods, such as sealed envelopes or restricted e-mail.
- Users receiving an initial (default) or newly issued password shall change it immediately.
- Users shall keep passwords confidential and shall not record them in visible locations (e.g., posted near the workstation). If a password is suspected to be compromised, it shall be changed immediately.
- In cases of shared user licenses (e.g., SAP systems), the administrator shall notify the responsible user by e-mail to change the system password whenever there is a change in the assigned users.

- Password files shall be encrypted to prevent unauthorized disclosure or alteration.
- User account lists for critical systems shall be reviewed regularly, and accounts that are no longer authorized—such as those of resigned personnel or default system accounts—shall be promptly verified and disabled, removed, or have their passwords changed immediately upon detection.

4.7 Physical and Environmental Security

- Objective

Control of access to the Data Center Room is intended to prevent unauthorized persons from accessing, becoming aware of, altering, or causing damage to data and computer systems. Environmental and disaster protection measures are intended to prevent damage to data and computer systems arising from environmental factors or disasters. This section covers access control measures for the Data Center Room and the protective systems that the Company should provide within the Data Center Room.

- Practices

1. Data Center Room Control
    - Critical computer equipment, such as servers and network devices, shall be housed in the Data Center Room or other restricted areas, and access to the Data Center Room shall be granted only to authorized personnel with relevant responsibilities, such as system administrators.
    - Where persons without routine responsibilities require occasional access to the Data Center Room, such access shall be strictly controlled, for example by requiring supervision at all times by a system administrator and/or relevant personnel.
    - A logging system for entry to and exit from the Data Center Room shall be maintained, recording details of the individual and the time of access. Such logs should be reviewed regularly.
    - The Data Center Room should be organized into designated zones—such as Network Zone, Server Zone, UPS Zone, and UPS Battery Zone—to facilitate operations and enhance the effectiveness of access control over critical computer equipment.
2. Damage Prevention
    - Fire protection systems shall be implemented.
        - Fire detection devices, such as smoke detectors and heat detectors, shall be installed to enable timely prevention or suppression of fire incidents.
        - The primary Data Center Room shall be equipped with an automatic fire suppression system, and at a minimum, the backup computer center shall be provided with fire extinguishers for initial fire response.
    - Power Failure Protection System
        - Systems shall be in place to protect computers from damage caused by fluctuations or instability in electrical power supply.
        - Backup power systems shall be provided for critical computer systems and network infrastructure to ensure continuity of operations.
3. Temperature and Humidity Control System
    - Environmental conditions shall be controlled to maintain appropriate temperature and humidity levels. Air-conditioning temperature and humidity settings should be configured in accordance with the specifications of the computer systems, as improper temperature or humidity conditions may cause system malfunction.

4. Water Leakage Detection System

- Where the Data Center Room has a raised floor for installation of air-conditioning systems and routing of power and/or network cables beneath, water leakage detection systems should be installed near water pipes to enable timely prevention or mitigation of leakage incidents. If the Data Center Room is located in an area at risk of water leakage, regular inspections for signs of leakage should be conducted.

4.8 Operations Security

- Objective

  To ensure that operations involving the Company's information systems are conducted accurately and securely, preventing data loss and protecting systems from malicious software.

- Practices
  - Manuals or standard operating procedures for the Company's critical information systems shall be established to prevent operational errors in information system activities.
  - Information system changes shall be controlled, including requiring prior approval from the relevant supervisor before implementation.
  - Information shall be backed up prior to any system changes.
  - Monitoring systems should be implemented to track information system resources (e.g., CPU, memory, hard disk capacity) to assess adequacy and support future resource planning.
  - Highly critical systems should have development environments separated from production environments to prevent unauthorized data changes.
  - Information assets shall be inventoried and classified by criticality, with defined data sets to be backed up and specified backup frequency.
  - Highly critical data shall be backed up more frequently and should include offsite backups (e.g., cloud backup or disaster recovery site).
  - The operational readiness of backup systems for information systems shall be tested at least monthly.
  - Measures shall be implemented to protect against malicious software, such as:
    - Personal computers or personal portable computers shall have antivirus software installed and operating system and web browser vulnerabilities patched prior to connection to the Company's network.

- Users shall regularly update operating systems and application software with issued patches and/or hotfixes, which may be downloaded from the product owner's official website to remediate vulnerabilities.
- Computer data transmitted via e-mail shall be scanned for viruses using antivirus software prior to each transmission or receipt.
- Users shall install only software provided by the Company. Installation of any additional software not supplied by the Company shall require prior notification to and security verification by the Information Technology Department before installation.

4.9 Communications Security

- Objective

  To protect information within the network from unauthorized persons, viruses, and other malicious code that may access or cause damage to information or the operation of information systems.

- Practices

  1. Network Security Management
     - Access to the network shall be controlled to ensure security.
     - Networks shall be segregated between internal users and external users interacting with the Company.
  2. Information Transfer
     - Agreements on Information Transfer shall be established with due regard to information security, and the system administrator shall ensure that such activities are controlled to maintain the three core principles of security: confidentiality, integrity, and availability.
     - Non-Disclosure Agreements (NDAs) shall be executed between the Company and external parties to ensure that the Company's confidential information is not disclosed.

4.10 System Acquisition, Development and Maintenance

- Objective

  Control over the development or modification of information systems is intended to ensure that computer systems developed or modified process data accurately, completely, and in accordance with user requirements, thereby reducing integrity risk. This section covers the end-to-end process for development or modification, from request initiation through implementation into production use.

- Practices
    1. Documented procedures for system development or modification should be established. At a minimum, these should define requirements for request initiation, development or modification, testing, and system migration or deployment.
    2. Procedures should be established for emergency changes to computer systems (Emergency Change), including documentation of the reasons and necessity and obtaining approval from the authorized authority in all cases.
    3. Details of such procedures should be communicated to users and relevant personnel comprehensively, and compliance with the procedures should be enforced.
- Control of System Development or Modification
    1. Request Initiation
        - Requests for system development or modification shall be documented in writing, which may be in electronic form (e.g., Change Request (CR), e-mail), and approved by the authorized authority, such as the requesting department head or the information system owner.
        - Significant changes should be assessed in writing for impact on operations, security, and system functionality of related systems.
        - Applicable regulatory requirements should be reviewed, as changes may affect regulatory compliance.
    2. System Development Activities
        - Development environments shall be segregated from production environments, with access restricted to relevant personnel in each environment. Such segregation may be achieved through separate machines or logically separated environments within the same system.
        - Requesters and relevant users should participate in the development or modification process to ensure alignment with requirements.
        - Security and system availability considerations should be incorporated from the outset of development or modification.

3. Testing
    - The requester, the Information Technology Department, and other relevant users shall participate in testing to ensure that developed or modified systems operate effectively, process data accurately and completely, and meet requirements prior to deployment into production.
4. Deployment to Production
    - System migration or deployment shall always be verified for accuracy and completeness.
5. Documentation and Version Management
    - Detailed information on currently used programs, including historical development or modifications, shall be maintained.
    - All system documentation shall be updated following development or modification to remain current (e.g., data structure documentation, user manuals, access registers, program workflows, and program specifications), and stored securely and in an accessible manner.
    - Previous program versions shall be retained for fallback use in the event the current version malfunctions or becomes unusable.
6. Post-Implementation Testing
    - Systems that have been developed or modified should be tested after a period of operation to ensure effective performance, accurate and complete processing, and conformity with user requirements.
7. Change Communication
    - Changes shall be communicated comprehensively to all relevant users to enable correct usage.

4.11 IT Outsourcing

- Objective

  To protect the Company's assets accessed by IT outsourcing providers and to maintain the agreed levels of information security and service performance as specified in service agreements.

- Practices

  1. Information security requirements for the Company's data shall be established whenever IT outsourcing providers are required to access the Company's data or assets, in alignment with the Company's data confidentiality requirements.

2. Such information security requirements shall be communicated and enforced prior to granting IT outsourcing providers access to the Company's data or assets.
3. Service agreements shall require regular monitoring, review, and audit of outsourced services.
4. Any changes to service agreements for critical systems shall be subject to information security risk assessment.

4.12 Information Security Incident Management

- Objective

  To establish consistent and effective methods for managing information security incidents, including the reporting of information security events and vulnerabilities.

- Practices

  1. Roles, responsibilities, and procedures shall be defined for responding to information security incidents affecting the Company.
  2. Clear communication channels shall be established for reporting information security incidents.
  3. If users detect any incident that may affect information system security, they shall report it to the Information Technology Department.
  4. Information security incidents shall be reported according to severity levels. Where incidents significantly impact a large number of users, prompt notification shall be issued.
  5. Information security incidents shall be recorded, including at minimum the type of incident, frequency of occurrence, and costs arising from damages, in order to support learning and preventive planning.
  6. Evidence shall be collected and preserved in accordance with applicable rules or legal requirements for use in judicial proceedings.

4.13 Information Security Aspects of Business Continuity Management

- Objective

  To prevent disruption to the Company's operations arising from crises or disasters and to ensure the readiness and availability of the Company's information system equipment.

- Practices

1. The Information Technology Department shall establish emergency response plans to address uncertainties and disasters that may affect information systems, in alignment with the Company's Crisis Management Plan.
2. Information system risks shall be assessed and evaluated at least annually.
3. Emergency preparedness and response plans shall be reviewed at least annually.
4. The operational readiness of backup information systems shall be tested at least annually.