# Information Security Policy

**Millennium Group Corporation (Asia) Public Company Limited**

Amendment No.: 1
Effective date: February 25, 2025
Approved by: The Board of Director's Meeting 1/2025

**Table of contents**

# Information Technology Security Policy

## Principles and Rationale

Millennium Group Corporation (Asia) Public Company Limited ("the Company") possesses information assets that support operational efficiency in achieving business objectives. These information assets are critical resources that employees must use and maintain in a state that ensures their effective usability at all times.

Maintaining the security of information technology systems requires cooperation from all departments in continuously adhering to the policy. Regular monitoring and updates are necessary to align with rapidly advancing technology. The policy and practices established for information security will serve as an essential tool for users, system administrators, and those involved in the company's IT systems, guiding them in safeguarding the security of these systems.

## Objectives

The goal is to provide a clear policy framework for the organization's IT operations and management. This policy will guide those involved in information management, including executives, personnel, external organizations, and individuals accessing the company's information, with a clear action plan and framework. This will lead to better coordination, higher security in service delivery, and increased standards. It also defines appropriate preventive measures to control and reduce damage from situations where assets are inaccessible, lost, damaged, or compromised. The policy ensures that the company's IT systems maintain confidentiality, integrity, and availability.

## Applicable Laws and Regulations

1. Computer - Related Crime Act B.E. 2550 (2017) (as amended)
2. Copyright Act B.E. 2537 (1994) (as amended)
3. Royal Decree on Secure Methods of Electronic Transactions B.E. 2553 (2010)
4. Notification of the Ministry of Information and Communication Technology Center (ICT) RE: Traffic Data Retention for Service Providers B.E. 2550 (2007)
5. Notification of the Electronic Transactions Development Agency RE: Information Security Standards for Systems
6. Computer - Related Crime Act (No. 2) B.E. 2550 (2017) (as amended)
7. Personal Data Protection Act B.E. 2562 (2019) (as amended)

## Enforcement and Penalties

This information technology security policy is effective from the date of its announcement and applies to all users of the company's IT systems without exception. Violations will result in disciplinary action in accordance with the company's regulations.

## Disciplinary Offenses

- Altering or modifying another person's contact or communication information without authorization.
- Disclosing the Company's confidential or proprietary business information to any third party without the Company's authorization.
- Illegally copying, forging, or otherwise misappropriating another user's password or user credentials to access the Company's computer systems with intent to commit fraud against the Company's or clients' assets or to damage the Company's reputation.
- Using another person's password, user credentials, or one-time password (OTP) to access the

Company's computer systems and thereby reading, copying, approving, modifying, changing, or deleting data for personal gain or for the benefit of others.

- Negligently handling or carelessly disclosing one's own password, user credentials, or OTP, or intentionally allowing others to use one's credentials or privileges to access the Company's IT systems.
- Intentionally exporting, transmitting, selling, distributing, or otherwise disclosing Company data for personal gain or the benefit of others without authorization, or in a manner that causes damage to the Company.
- Attempting to access systems, resources, or data for which one does not have authorization.
- Intentionally or maliciously disrupting, damaging, or destroying information, computer systems, networks, or IT equipment to cause harm to the Company.
- Illicitly monitoring, eavesdropping, tracing, or decrypting electronic information by using tools or technologies to obtain confidential information of individuals or the Company, with intent to cause harm.
- Installing or using hacking tools or other software designed to probe, exploit, or access the Company's critical information assets, except by personnel or units specifically authorized to perform information security duties.
- Connecting any computer or electronic device to the Company's computer systems or networks without authorization from the responsible unit.
- Manually configuring or changing IP addresses without authorization from the responsible unit.
- Downloading, storing, or possessing unlawful or inappropriate content (e.g., pornographic or obscene material), or any content that defames, undermines, or insults the monarchy, the nation, religion, or that incites division among the public or employees, or otherwise harms the Company.
- Sending inappropriate messages or data using the Company's e-mail or communication tools (e.g., defamation, harassment, extortion, threats, abusive language, or chain letters).
- Using the Company's intranet, internet access, e-mail, computers, or other IT assets for personal entertainment or other non-business activities unrelated to the Company's operations.
- Using unlicensed or unauthorized software, or software not approved by the Company, which may expose the Company to legal or operational risk.
- Assisting or collaborating with external parties to gain access to the Company's IT systems or information, or aiding in copying or destroying the Company's information or computer systems.

**Disciplinary Sanctions**

- Verbal warning
- Written warning
- Temporary suspension without pays
- Dismissal
- Termination

- Criminal or civil legal action

The Company reserves the right to impose any disciplinary action as deemed appropriate without following the above sequence, depending on the severity and nature of the violation.

**Policy Dissemination**

The Information Technology Department is responsible for announcing and disseminating this policy to all users of the Company's information systems to ensure that all employees and relevant personnel fully understand their roles and responsibilities in using the Company's IT systems securely and in protecting the Company's information assets.

**Policy Review**

This Information Security Policy shall be reviewed and updated at least once a year or whenever there are significant changes in the business environment, regulations, laws, or technology. The Information Technology Department is responsible for reviewing and updating the policy, with oversight by the IT Department Head to ensure timely and proper implementation of revisions as required.

**Implementation Procedures**

The Company's Information Security Policy has been developed in alignment with the ISO/IEC 27001:2022 (Information Security Management Systems) standard to ensure a high level of information security and effective risk management across the organization.

**Policy Components**

1.1. Definitions

1.2. Physical and Environmental Security

1.3. Access Control Security

1.4. Networks and Servers Security

1.5. Wireless Network Security

1.6. Firewall Security

1.7. Email Security

1.8. Internet Security

1.9. Intrusion Detection Security

1.10. Data Backup and Recovery Security

1.11. Information Security Awareness

The Information Security Policy comprises the objectives, guidelines, and procedures necessary to ensure the effective protection of the Company's information systems. This Policy establishes a framework for maintaining an adequate level of information technology security across the organization, minimizing potential risks or damages to operations, assets, and personnel, and ensuring the Company's ability to conduct business securely and sustainably.

This Policy serves as the standard for the secure use of the Company's information technology systems. All employees and external parties granted access to the Company's information systems are required to strictly comply with the provisions set forth herein.

Effective information security requires shared responsibility and continuous commitment from all individuals within the organization. Achieving this requires collective awareness and consistent attention to every aspect related to information security, including:

- Information security is the responsibility of every employee and external party with access to the Company's information systems.
- Information security management is a continuous process that requires ongoing monitoring, maintenance, and improvement.
- Awareness, accountability, and compliance with the Company's established policies, standards, frameworks, procedures, and operational guidelines are essential. Clear communication of these responsibilities to all employees and relevant external parties ensures understanding of their duties and promotes the effective implementation of information security measures.

**Definitions**

The Information Security Policy defines the terminology used throughout this Policy to ensure a consistent and accurate understanding of all terms and references, as follows:

| Term | Definition |
|---|---|
| **Organization / Company** | |
| organization | Millennium Group Corporation (Asia) Public Company Limited. |
| Subsidiaries | Companies over which Millennium Group Corporation (Asia) Public Company Limited has control. |
| Information Technology Department | The department responsible for managing and overseeing all information technology operations of the organization. |
| **Person** | |
| Department level executives | The highest-ranking executive responsible for each division or department. |
| Authorized Person | A person holding the position of Department Director or above, or any person formally delegated with decision-making authority. |
| System Administrator (Administrator) | An IT Department officer assigned to manage and maintain computer systems or networks, resolve system-related issues, and perform administrative tasks requiring access to system configurations or network management functions. |
| Employees | Employees of Millennium Group Corporation (Asia) Public Company Limited. |
| External Person | Any individual or employee of an external organization who interacts with or gains access to the Company's information assets. |
| Third Party / External Service Provider | Vendors, business partners, contractors, outsourcers, or any individuals or legal entities — domestic or international — that provide information technology services to the Company under a contractual or service agreement, including subcontractors authorized to access the Company's premises or information assets and systems within their assigned responsibilities. |
| User | Employees, external individuals, or third parties who are granted authorized access to the Company's information systems. |
| Project Owner | The internal department or unit of Millennium Group Corporation (Asia) Public Company Limited responsible for managing a project that engages an external service provider or contractor. |
| Data Owner / Asset Owner | A person, unit, or department that owns specific data or information assets and would suffer the greatest impact in the event of data loss, damage, or unauthorized disclosure. |
| **Other Term** | |
| Data | Any text, message, record, document, sound, or other form of information that conveys meaning — whether in numerical, linguistic, pictorial, or symbolic form — in electronic or physical |

| Term | Definition |
|---|---|
| | format. This includes “computer data” as defined under the Computer Crime Act and “electronic data” as defined under the Electronic Transactions Act. |
| Electronic Data | Information that is created, transmitted, received, stored or processed by electronic means, such as by methods of electronic exchange, electronic mail, telegram, teletype, or facsimile. |
| Computer Data | Data, text, commands, instructions, or any other information contained within a computer system that can be processed by that system. This term also includes electronic data under the Electronic Transactions Act. |
| Sensitive Information | Information that is critical to the Company’s business operations or that the Company is obligated to protect under applicable laws, professional codes of conduct, or contractual agreements. Such information must not be disclosed or used for purposes other than the Company’s legitimate business activities. Any unauthorized disclosure or leakage of this information could disrupt operations, reduce efficiency, or damage the Company’s reputation. |
| Computer System | All computer hardware and software, wired and wireless network equipment, data storage and transfer media, Internet and Intranet systems, and any electronic or telecommunication devices capable of performing computer functions. This includes assets owned by the Company, its partners, or third parties under installation or acceptance testing, as well as employee-owned devices used within Company premises. |
| Important System | A computer system utilized by the Company to deliver business services—both revenue-generating systems and revenue-enabling/support systems—including any other electronic systems that facilitate the Company’s normal business operations, as designated by the Company’s Information Security and IT functions. A disruption or degradation of such systems would cause the Company’s operations to be interrupted or impaired. |
| System Owner | The internal unit that owns a given computer system and is responsible for that system. |
| Custodian | A person delegated by the System Owner or Information Owner to support the administration and control of access to information in accordance with the permissions and access levels specified by the owner. |
| Administrator | A person assigned to operate and maintain computer systems, including hardware, software, and peripherals. Administrators are authorized to configure, modify, and improve Company systems to ensure correct, efficient, secure operation aligned with business needs. |

| Term | Definition |
|---|---|
| External Party | An external individual or organization that conducts business with or provides services to the Company and may be granted privileged access to the Company's information and processing facilities, e.g., Business Partners, Outsourced personnel, Suppliers/Vendors, Service Providers, and Consultants.<br>▪ Business Partner<br>▪ Outsource<br>▪ Supplier/Vendor<br>▪ Service Provider<br>▪ Consultant |
| Remote Access / Virtual Private Network (VPN) | Access to the Company's information systems from a remote location |
| User Account (Username or Account) | A set of data used to identify an individual user, define access rights, and specify any restrictions related to accessing the organization's information systems. |
| Password | A sequence of characters used for authentication and to control access to information systems or information assets. |
| Privilege | An elevated level of access rights that exceeds those of standard users or system administrators, such as *Root* or *Administrator* privileges. |
| Information System | Computer systems, data storage systems, electronic mail systems (E-mail), all forms of communication systems, communication devices, printers, scanners, and any related equipment owned by the organisation and/or authorised for use by the organisation in accordance with applicable laws |
| Information Security | The preservation of confidentiality, integrity, and availability of information, including additional attributes such as authenticity, accountability, non-repudiation, and reliability. |
| Information Security Event | An identified occurrence indicating a possible breach of information security policy, failure of protective controls, or an event that cannot yet be determined but may be related to a security threat. |
| Incident | An event that results in the disruption of an information system's ability to deliver services as expected or a degradation in service quality—for example, email system outages, server failures, or abnormal system performance. |
| Information Security Incident | An unwanted or unexpected security-related situation that may result in system intrusion, cyberattacks, or any compromise of the organization's information security. |
| Encryption | The process of transforming data into a secure, unreadable format by using cryptographic keys, ensuring that unauthorized |

| Term | Definition |
|---|---|
| | individuals cannot access or interpret the original information without the correct decryption key. The method and strength of encryption depend on the cryptographic technique used. There are two primary types of encryption:<br>• **Symmetric Key Encryption** – A method that uses a single shared key for both encryption and decryption, referred to as the *Secret Key*.<br>• **Asymmetric Key Encryption (Public Key Cryptography)** – A method that uses a pair of keys, known as a *Private Key* and a *Public Key*. In this Policy, this pair of keys is collectively referred to as the *Key Pair*. |
| Key | A cryptographic key used in the processes of encryption and decryption, depending on the encryption technique and its intended use. Keys are classified into two types:<br>• Secret Key – Used in *Symmetric Key Encryption*, where the same key is applied for both encryption and decryption. Examples of symmetric encryption algorithms include 3DES, RC5, RC6, and AES.<br>• Key Pair – Used in *Asymmetric Key Encryption (Public Key Cryptography)*, consisting of a *Private Key* and a *Public Key*. Examples of asymmetric encryption algorithms include RSA (Rivest–Shamir–Adleman), Diffie–Hellman Key Exchange Protocol, and Elliptic Curve Cryptography (ECC).<br>• |
| Vulnerability | A flaw, weakness, or deficiency in an information asset resulting from design, manufacturing, or operational shortcomings. Such weaknesses may be exploited, creating risks and potential threats. Examples include software vulnerabilities that allow unauthorized access without authentication. |
| Security Awareness | Providing knowledge and understanding related to information security to enhance awareness of threats, risks, and issues associated with information security among personnel. |
| Data Backup | The process of creating copies of data within a system to ensure that modified, corrupted, or lost information can be restored when needed. |
| Source of Data and Information | A repository or location where data or information is stored, in various forms, including both dedicated data sources and centralized data sources. |
| Information asset | Means: |

| Term | Definition |
|---|---|
| | • Information technology equipment and any related devices used in conjunction with IT systems;<br>• Software, system applications, and any programs used alongside the organization's information systems;<br>• Data, information, electronic records, computer data, and any form of intellectual property. |
| Secure Area | A designated location used for storing information system equipment. Secure areas are categorized into:<br>**1)** Patching Room<br>**2)** Computer Operation Room<br>**3)** Data Center |
| Computer Operation | A workspace used for data entry, report generation, and operational activities related to the organization's information systems |
| Patching Room | A designated area used for storing equipment related to computer network and telephone connections on each floor. |
| Data Center | A secure facility used to store computer equipment and critical computing infrastructure, including servers, core network devices, and other essential systems that support business operations |
| Logs | Records of system activities, system access, information processing, and security-related events used to verify security performance and identify abnormalities in information system operations |
| Monitoring | The process of observing and analysing information security events to detect anomalies or irregular activities through system logs—for example, unauthorised system access, misuse of information, or system-related issues |
| Risk | The probability of errors, damage, data leakage, loss, undesirable events, or actions occurring under uncertain circumstances that may impact the achievement of business objectives or service delivery |
| Malicious Code or Malware | Software or code that poses a threat to the performance and security of information systems, such as viruses, worms, and trojans |

| Term | Definition |
|---|---|
| Business Continuity Plan | A plan that ensures continuity of critical business operations to prevent disruptions stemming from environmental incidents, security incidents, or other threats |
| DRP: Disaster Recovery Plan | A preparedness plan outlining procedures for responding to emergencies—such as relocating operations or activating backup information systems—to restore business functionality |
| Fallback Plan | A plan outlining steps to revert operations to the last known stable state when disaster recovery efforts fail or are not fully successful |
| Recovery Time Objective: RTO | The target timeframe within which products, services, or processes must be restored to normal operations after a major disruptive event |
| Recovery Point Objective: RPO | The maximum acceptable amount of data loss, expressed in time, used as a basis for determining appropriate data backup strategies |
| Maximum Tolerable Period of Disruption (MTPD) | The maximum period during which business operations may be disrupted. If the disruption exceeds this duration, the organisation will be unable to restore operations to normal conditions |
| Service Level Agreement (SLA) | A formal agreement between the service provider and the service recipient that specifies the service details, performance levels, measurement criteria, and service targets, including clearly defined responsibilities of both parties |
| Operational Level Agreement (OLA) | An internal agreement between departments that outlines how they will work together to support and achieve the service levels specified in the SLA |
| Underpinning Contracts (UC) | Contracts between the service provider and external service recipients/vendors that support and ensure the service levels committed to in the SLA |
| High Priority Application System | A system that supports core business transactions or provides essential information required for regulatory reporting |
| Development Area | An information system environment used for system development, simulating production resources and conditions to enable the creation of new applications or system enhancements |
| User Acceptance Area | A testing environment that simulates production conditions to evaluate the performance, functionality, and security of newly developed systems |
| Disaster Recovery Center (DRC) | A secondary site comprising backup systems, data, and network infrastructure separate from the primary information systems, established to ensure continuity of critical business operations and to minimise the impact in the event of an emergency |
| Production Area | An information system environment used for live operations and real-time services for users. This environment must be strictly |

| Term | Definition |
|---|---|
| | protected, with controlled access, and must be segregated from development and testing environments |
| Mobile Device | Portable electronic devices authorized by the organisation to connect to and access the organization's information systems, such as laptop computers, smartphones, and tablet computers. |
| Media | Electronic devices used for recording or storing data, including Hard Drives, Flash Drives, Handy Drives, Thumb Drives, External Hard Drives, and other similar storage devices |

## 1. Information Security Policy

**Objective**

To ensure that all users and relevant parties recognize the importance of safeguarding the organization's information systems, understand their responsibilities, and adhere to the established practices for mitigating information security risks. The organization shall establish and maintain information security policies and measures. The key management directions are as follows:

- **Management Directions for Information Security**

1. Policy for Information Security

   1.1 The organization shall establish a written Information Security Policy, duly approved by the Board of Directors or a delegated authorized person.

   1.2 The organization shall disseminate the policy to all users and relevant external parties, ensuring accessibility and compliance as required by the policy.

2. Review of the Policies for Information Security

   2.1 The organization shall perform regular reviews and assessments of the Information Security Policy in accordance with the review conditions specified within the policy.

## 2. Organization of Information Security

**Objective**

To establish control measures and monitoring mechanisms for information security responsibilities across the organization, and to define guidelines for the proper and secure use of mobile computing devices in alignment with the organization's Information Security Policy.

- **Internal Organization**

1. Information Security Roles and Responsibilities

   1.1 Department Heads shall clearly define and document the information security roles and responsibilities for personnel within their departments, ensuring alignment with the organization's Information Security Policy.

2. Segregation of Duties

   2.1 Department Heads shall ensure appropriate segregation of duties for activities related to information security, enabling adequate cross-checking and reducing security risks.

3. Contact with authorities

   3.1 The Information Technology Department shall maintain up-to-date contact information for essential agencies such as legal authorities, hospitals, police stations, fire departments, and emergency services to ensure effective communication in case of emergencies.

4. Contact with special interest groups

   4.1 The Information Technology Department shall maintain a list of relevant information security expert groups and establish communication channels for receiving updates from such groups. These channels shall enable timely coordination, access to information, and requests for assistance in the event of incidents that may impact the organization's information security. The list and communication channels shall be reviewed and updated regularly to ensure accuracy and effectiveness.

5. Information Security in Project Management

    5.1 Department Heads shall implement risk controls, monitor project activities, and evaluate overall project performance, including both internal projects and those involving procurement or engagement of external service providers.

    5.2 Supervisors shall provide guidance, reinforce compliance with the organization's Information Security Policy, and take disciplinary action when improper or non-compliant practices are identified.

6. User Responsibilities

    6.1 Users shall learn, understand, and strictly comply with the organization's Information Security Policy.

    6.2 Users shall fully cooperate with the organization in protecting its computer systems and information assets, including monitoring, safeguarding, and maintaining the confidentiality and integrity of such information.

    6.3 Users shall immediately report to the organization any loss of equipment or critical information, or any observed incidents of intrusion, theft, destruction, or unauthorized access to information systems that could cause harm to the organization.

7. Responsibilities of Data and Information Owners

    7.1 Develop and maintain documentation, controls, and procedures governing data access to ensure alignment with the Company's Information Security Policy.

    7.2 Ensure that employees comply with the Company's Information Security Policy and relevant procedures.

    7.3 Oversee and approve access rights to data, information, and computer systems within their assigned roles and responsibilities.

    7.4 Notify the Information Technology Department responsible for user account administration and access rights management to remove or modify access privileges when there are changes in personnel, roles, authority, or departmental transfers.

- **Mobile Computing and Teleworking Control**

1. Mobile Computing and Communication

    1.1 The Information Technology Department shall establish appropriate measures to ensure the security of mobile computing and communication devices, taking into account the risks associated with connecting such devices to the Company's network and when they are used outside Company premises.

    1.2 All users who utilize mobile devices to access the Company's information systems must strictly comply with the Information Security Policy and exercise heightened awareness regarding information security. Where personal mobile devices must be used to access or store the Company's information, prior approval must be obtained from the department head or the highest-level supervisor.

    1.3 The Company reserves the right to inspect, suspend, revoke access, or wipe all data on mobile devices whether Company-owned or personally owned—used to access or store the Company's information, if such usage is deemed to pose risks to the Company's infrastructure, systems, data, or information assets.

2. Teleworking

2.1 All users performing work outside Company premises must comply with the Information Security Policy to the same extent as when working onsite.

2.2 Users who work with the Company's information outside the office, or who require remote access to Company systems, must obtain authorization from both the relevant Data Owner and their supervising department, with valid justification.

2.3 Users requiring remote system access must obtain prior approval from the System Administrator before access is granted.

## 3. Human Resources Security

**Objective**

To establish control measures for supervising and monitoring the recruitment of personnel to work within the organization, the management of personnel during employment, and the management of personnel upon termination of employment or when there is a change in job responsibilities.

- **Prior to Employment**

1. Screening

1.1 The organization shall require background checks to be conducted on job applicants and external parties who are required to provide services within the organization.

2. Terms and Conditions of Employment

2.1 The Human Resources Department shall ensure that employees sign employment contracts or work agreements, and that contracts or agreements with external parties are executed, specifying their responsibilities related to information security. Users must acknowledge and accept the organization's rules by reading, understanding, and complying with the policies, rules, and regulations prescribed by the organization.

- **During Employment**

1. Management Responsibilities

1.1 Department management shall implement controls and supervision to ensure that employees and external parties engaged to perform work or provide services to the organization comply with the Information Security Policy for information systems and the information security procedures enforced by the organization.

2. Information Security Awareness, Education and Training

2.1 The Information Technology Department shall provide channels for personnel to study and understand the Information Security Policy for information systems, as well as their information security roles and responsibilities, before they are authorized to commence work with the organization.

2.2 The Information Technology Department shall coordinate with responsible units to provide general operational training so that contracted personnel can regularly learn and understand relevant topics, such as system usage, use of standard software, basic computer troubleshooting, and compliance with applicable laws, rules, and regulations.

2.3 The Information Technology Department shall organize information security awareness and training programs on a regular basis to ensure that contracted personnel understand these topics and can perform their duties effectively and securely.

3. Disciplinary Process

    3.1 The organization shall establish a disciplinary process to take action against users who violate or fail to comply with the Information Security Policy for information systems, information security procedures, or work procedures related to the organization's information security.

- **Termination or Change of Employment**

1. Termination or Change of Employment Responsibilities

    1.1 The Human Resources Department shall define rules and responsibilities relating to information security for employees and external parties after termination of employment or when there is a change in employment responsibilities, in written form.

    1.2 The Human Resources Department shall monitor and ensure that employees and external parties strictly comply with these rules.

## 4. Asset Management

**Objective**

To ensure that the organization's assets and information systems are protected at an appropriate level to reduce the risk of unauthorized disclosure of organizational information, prevent the misuse of information assets, and avoid damage to the organization's information assets.

- **Responsibility for Assets**

1. Inventory of Assets

    1.1 The Information Technology Department shall ensure that internal units maintain an inventory of information assets to enable proper management and control of such assets and that the inventory is kept up to date at all times.

2. Ownership of Assets

    2.1 The head of the Information Technology Department shall ensure that asset owners are identified, including persons responsible for overseeing and controlling the use of information assets and those responsible for such assets at an appropriate level.

3. Acceptable Use of Assets

    3.1 The Information Technology Department shall establish acceptable use requirements for assets in order to manage computer equipment appropriately, achieve maximum efficiency, and ensure protection from potential damage. These requirements shall be communicated to all personnel in the organization, who must comply with them.

4. Return of Assets

    4.1 The Human Resources Department, supervisors, or managers shall monitor and ensure that employees and external parties providing services return the organization's assets (Return of Assets), such as laptop computers, documents, keys, and employee ID cards, to the relevant units.

- **Information Classification**

1. Classification of Information

    1.1 The organization shall establish the classification of information assets and information confidentiality levels, taking into account applicable laws and requirements relevant to the organization in determining appropriate classification levels.

    1.2 Internal units shall categorize the information and information assets used in the

organization's operations and assign confidentiality levels to such information and information assets.

1.3 Internal units shall manage information classification in accordance with the operating guidelines set out in the organization's information security procedures.

2. Labeling of Information

2.1 The organization shall ensure that information in document form is appropriately controlled and protected throughout its lifecycle from initial printing, labeling, storage, copying, and distribution through to destruction. Such requirements shall be established as procedures to be followed by personnel and relevant parties to ensure that information is properly controlled and protected.

2.2 The Information Technology Department and relevant units shall label all computer equipment with asset tags corresponding to the asset register and usage procedures.

3. Handling of Assets

3.1 The Information Technology Department shall control and supervise the implementation of procedures for handling information assets to prevent the leakage of critical organizational information or the misuse of information assets.

- **Media Handling**

1. Management of Removable Media

1.1 The Information Technology Department shall document operating procedures for managing removable media used to store information, keep such procedures up to date, and communicate them to all users in the organization.

1.2 The management of removable media shall be aligned with the defined information classification levels.

2. Disposal of Media

2.1 The Information Technology Department shall establish procedures for the secure disposal of media to prevent the leakage of confidential or critical information.

2.2 The Information Technology Department shall define control measures for media destruction by referencing internationally recognized standards.

3. Physical Media Transfer

3.1 The Information Technology Department shall establish operating procedures or requirements for maintaining information security when media is transferred outside its installed location or normal operating area.

## 5. Access Control

**Objective**

To establish guidelines for maintaining security in controlling access to and use of the organization's information systems, and to prevent unauthorized intrusions through the network, including malicious programs that may cause damage to the organization's information.

- **Business Requirement for Access Control**

1. Access Control Policy

1.1 The organization shall establish a written Access Control Policy, ensure that the policy is regularly updated, and communicate it to all users within the organization for acknowledgment and compliance.

2. Access to Networks and Network Service

2.1 The Information Technology Department must determine that access to user data and information systems must be approved by a supervisor only.

2.2 The Information Technology Department must limit users' access to the network system to only those services that the users are authorized to access. The rights granted must be in accordance with their responsibilities and the necessity of use.

- **User Access Management**

1. User Registration and De-Registration

1.1 The Information Technology Department and data owners shall jointly establish written procedures for managing user registration and de-registration, ensure that such procedures are regularly updated, and communicate them to all users within the organization for acknowledgment and compliance.

2. User Access Provisioning

2.1 The Information Technology Department and data owners shall assign or define user access rights to information or information systems in accordance with each user's roles and responsibilities.

2.2 The Information Technology Department and data owners must prepare documents for assigning access rights to data or information systems and keep them as evidence for operations.

2.3 The Information Technology Department and data owners shall establish a process for managing access rights in cases where users require access to information or information systems beyond their assigned privileges.

3. Management of Privileged Access Right

3.1 The Information Technology Department shall securely store high-privilege user credentials, such as Administrator/root accounts on servers or Application Administrators and ensure that their use is permitted only when necessary.

3.2 The Information Technology Department shall establish written operational procedures for managing high-privilege user credentials and communicate them to all relevant personnel to ensure understanding and compliance.

4. Management of Secret Authentication Information for Users

4.1 The Information Technology Department shall establish a written method for managing user authentication confidentiality and keep it current and communicate it to users within the organization for their acknowledgement and compliance.

5. Review of User Access Rights

5.1 The Information Technology Department and data owners shall establish written procedures for reviewing access rights to information systems and applications, ensure that such procedures are regularly updated, and communicate them to all users within the organization for acknowledgment and compliance.

5.2 The Information Technology Department and data owners shall clearly define the schedule for reviewing access rights to information and information systems and notify all relevant parties accordingly.

5.3 The review of access rights shall take into consideration the following factors:

- The defined review schedule
- Termination of employment within the organization
- Changes or transfers in job responsibilities
- Requests for access beyond the assigned roles and responsibilities

5.4 When the rights review process is complete, the data owner or system administrator shall keep the evidence of the rights review, separating the evidence according to the rights review period.

6. Removal of Access Rights

6.1 Data owners and system administrators shall establish written criteria and procedures for the revocation of access rights and communicate them to all users within the organization for acknowledgment and compliance.

- **User Responsibilities**

1. Use of Secret Authentication Information

1.1 Users shall not use password structures or characteristics that are easily guessable, such as dictionary words, derivatives or combinations of usernames, sequential characters, personal information, or any easily predictable phrases.

1.2 Users shall not write down, record, or store passwords near the system or device associated with those passwords, nor display them in any visible location.

1.3 Users shall be responsible for all actions taken under their user accounts and shall not permit others to perform any actions using their accounts, nor use any accounts for which they do not have authorization.

1.4 Users shall comply with all other password management requirements established by the organization.

1.5 Users or employees assigned to use computers shall comply with the following requirements:

- Log out of all systems when they are not in use for an extended period and shut down computers and peripheral devices at the end of the workday.
- Lock their screens with a password-protected screen lock when leaving their desks, even for a short period, to prevent unauthorized use.
- Scan all data introduced into their computers using up-to-date anti-virus software.
- Exercise caution when posting messages or expressing opinions on social media that could infringe on others' rights or create misunderstandings about the company.
- Be vigilant against fraudulent or fake information, commonly referred to as "phishing", which attempts to trick users into clicking links or entering information via email, websites, chat applications (e.g. Line), or other channels with the intent of obtaining sensitive data

- Use the corporate email address provided by the company for internal communications within the company and its affiliates, as well as with customers and external partners. Users shall not use personal email accounts to communicate any business-related information of the company with external parties or partners.
- Keep passwords and any other codes issued by the company for accessing its computer systems, information systems, or company data strictly confidential and must not allow others to know or share their use.
- Exercise caution when using personal email accounts to send or disclose the company's sensitive or confidential information.
- Employees who interact with external parties shall ensure that such external parties are informed of and comply with the company's Information Technology System Usage Policy.

- **Application and Information Access Control**

1. Information Access Restriction

1.1 Data owners and system administrators must define methods of access to information system data and system functions, which must be restricted in accordance with access control policies.

1.2 Data owners and system administrators must determine the method of using important information systems, whether they be data, computer systems, application programs (Application), electronic mail (E-mail), wireless networks (Wireless LAN), or Internet systems (Internet). They must grant specific rights to perform their duties and must receive written approval from the supervisor of that department.

2. Secure Log-on Procedures

2.1 The Information Technology Department must establish a written method for logging into a secure information system, referring to international standard methods and keeping them current, including communicating them to users within the organization for their acknowledgement and compliance.

3. Password Management System

3.1 The Information Technology Department shall implement a system for managing user accounts and passwords for accessing the organization's information systems to ensure standardized and consistent management practices.

4. Use of Privileged Utility Programs

4.1 The Information Technology Department shall establish controls on the use of utility programs and limit the use of utility programs for important information systems or computer programs to prevent violations or circumvention of established security measures, as the use of certain utility programs may enable users to circumvent the system's security measures.

5. Access control to program source code

5.1 The Information Technology Department shall establish control measures for accessing program source code and for its use in system development, to prevent errors in the development of the organization's information systems and applications.

## 6. Cryptographic

**Objective**

To establish guidelines for data encryption to ensure that the organization's information systems maintain the confidentiality of information, authenticate system users, and/or prevent unauthorized data modification in an appropriate and effective manner. The following practices shall apply:

- **Cryptographic Controls**

1. Policy on the Use of Cryptographic Controls

    1.1 The Information Technology Department shall establish data encryption measures and guidelines for selecting encryption standards that are appropriate to the potential risks associated with the data, in accordance with the defined levels of information confidentiality.

2. Key Management

    2.1 The Information Technology Department shall establish methods for managing encryption keys, covering the entire Key Management Life Cycle, and shall regularly monitor compliance with the established policies and procedures.

## 7. Physical and Environment Security

**Objective**

To establish measures for the prevention, control, and maintenance of the physical use and upkeep of information assets and information technology equipment, which serve as the infrastructure supporting the organization's information systems. These measures aim to ensure that such assets remain in good working condition and to prevent unauthorized access to or disclosure of information assets

- **Secure Area**

1. Physical Security Perimeter

    1.1 The organization should identify and establish secure areas, which should include physical boundaries such as walls or fences, designated entry and exit points, and appropriate security systems to ensure adequate protection.

2. Physical Entry Controls

    2.1 The organization should control access to work areas and locations containing critical information, allowing entry only to authorized personnel.

    2.2 The list of personnel authorized to access work areas and locations containing critical information shall be regularly reviewed, updated, and properly maintained.

    2.3 The Information Technology Department shall establish controls for access to secure areas, including computer rooms and system administrator workspaces. Access shall be limited to authorized personnel only, and records of entry and exit to the computer room shall be maintained, including details such as the individual's identity, time of access, and purpose of entry. These access records shall be reviewed regularly.

3. Securing Offices, Rooms, and Facilities

    3.1 The Information Technology Department shall design and implement physical security systems to protect work areas, locations containing critical information, computer rooms, and system administrator workspaces, as well as information equipment used in operations, from damage and unauthorized access.

4. Protecting Against External and Environmental Threats

    4.1 The Information Technology Department shall ensure that physical security measures are designed and installed to protect against external threats, whether human-made or natural, such as fire, flooding, earthquakes, explosions, riots and similar events.

5. Working in Secure Areas

    5.1 The Information Technology Department shall establish physical protection guidelines for working in secure areas, including computer rooms and administrator work areas, and shall ensure strict adherence to such guidelines.

6. Delivery and Loading Areas

    6.1 The Information Technology Department shall implement controls in areas where unauthorized persons might gain access, including establishing designated delivery, loading and staging areas for information equipment prior to its transfer into computer rooms. These areas shall be clearly segregated to prevent unauthorized access to information systems and information.

- **Equipment**

1. Equipment Setting and Protection

    1.1 The Information Technology Department shall place information equipment in secure rooms or areas. Cabinets and doors housing servers and network communication devices must always remain locked, and only authorized personnel shall be permitted to open them for maintenance or configuration adjustments (reconfiguration), to minimize the risk of unauthorized access to the equipment.

2. Supporting Utilities

    2.1 The Information Technology Department shall ensure the installation of system failure-prevention and supporting equipment within the computer room including fire suppression equipment, smoke detectors, uninterruptible power supplies, temperature and humidity control systems, water-leak detection/alarms, and alert systems for abnormal operation of information equipment and shall maintain such equipment to ensure continuous readiness.

3. Cabling Security

    3.1 The Information Technology Department shall ensure that the installation and maintenance of electrical and communication cabling within work areas and computer rooms comply with industrial safety standards to prevent unauthorized access, data interception, or physical damage.

4. Equipment Maintenance

    4.1 The Information Technology Department shall ensure that all core information system equipment used for operational processing, including supporting devices, is maintained and serviced periodically in accordance with the manufacturer's recommendations to ensure continuous operation and optimal working conditions.

    4.2 The Information Technology Department shall ensure that maintenance activities, as well as any equipment issues or defects identified, are properly recorded to support evaluation and improvement efforts, ensuring that all equipment remains in optimal working condition.

5. Removal of Assets

    5.1 Personnel responsible for overseeing secure areas and facilities shall not permit the removal of information technology equipment from the organization unless authorization has been granted by the designated personnel responsible for approving asset removal.

    5.2 Personnel responsible for overseeing secure areas and facilities shall not permit the removal of information technology equipment from the organization unless authorization has been granted by the designated personnel responsible for approving asset removal.

    5.3 The Information Technology Department shall establish written procedures for the removal of assets from the office, ensure that such procedures are regularly updated, and communicate them to all users within the organization for acknowledgment and compliance.

6. Security of Equipment and Asset Off-Premises

    6.1 Department-level executives or higher should be authorized to approve the use of the organization’s information technology equipment outside the office. Appropriate protective measures should be implemented for such equipment to prevent damage, taking into consideration the potential risks associated with its external use.

    6.2 The Information Technology Department shall establish security measures to control assets used outside the office, to mitigate risks associated with the external use of the organization’s equipment or property.

7. Secure Disposal or Re-Use of Equipment

    7.1 The User shall inspect the Device containing the storage media to ensure that any sensitive information or copyrighted software contained within the storage media has been properly erased, moved or destroyed in accordance with the data confidentiality level prior to destroying or disposing of the Device or reusing the Device.

    7.2 The Information Technology Department shall establish procedures for the destruction of data or information assets, as well as measures or techniques for data erasure to enable the reuse of information equipment. These procedures must align with the defined levels of information confidentiality.

    7.3 The Information Technology Department must designate a person responsible for destroying information that is not necessary for the organization's operations and is stored in storage media.

8. Unattended User Equipment

    8.1 The Information Technology Department shall establish control measures to protect unattended computers and information technology equipment to prevent unauthorized access to information.

    8.2 The administrator must require users to prevent others from accessing their computer or information technology system by entering the correct password before using the computer.

    8.3 Users shall log out of the information systems, computer systems, or computers they are using immediately when they are no longer needed or upon completion of their work.

8.4 Users must lock the computer screen or important devices when not in use or when away from the computer.

9. Clear Desk and Clear Screen Policy

9.1 System administrators should ensure that computer screens are automatically locked when not in use (Clear Screen), such as through Session Timeout or automatic Lock Screen mechanisms.

9.2 Users shall not leave important information, such as paper documents or data storage media, in unsecured, public, or easily visible areas. Users must store information in appropriate locations with adequate protection to prevent unauthorized access.

9.3 Users should not store important information on the computer desktop. Users must properly allocate storage locations within the computer and implement appropriate access controls to prevent unauthorized access to critical information.

## 8. Operations Security

**Objective**

To establish controls to ensure that the organization's information security operations and communications are conducted in accordance with clear, documented procedures and in a secure manner.

- **Operations Procedures and Responsibilities**

1. Documented Operating Procedures

1.1 The Information Technology Department shall establish written operational procedures for critical information systems, clearly segregating personnel duties and responsibilities according to the organizational structure, to ensure proper execution of tasks in compliance with the organization's information security policies.

1.2 The Information Technology Department must prepare manuals, system documentation, and knowledge bases to enable relevant personnel to understand the system, work characteristics, and work processes.

1.3 Units within the Information Technology Department shall regularly review manuals, system documentation, and knowledge databases to ensure they remain up to date. These operational procedures should be maintained in a readily accessible and usable condition and must be communicated to all relevant personnel for acknowledgment and compliance.

2. Change Management

2.1 The Information Technology Department shall oversee and control the management of organizational structure changes and information system operational procedures to ensure proper authorization and control before any modification or action that may affect system operations. All activities must comply with the organization's Change Management Policy for information systems.

3. Capacity Management

3.1 System administrators shall monitor the performance of critical systems and information technology equipment to ensure continuous and efficient operation.

3.2 System administrators must assess the capacity and adequacy of information resources, such as the use of servers and network devices such as processors (CPUs), memory, disks, or network bandwidth, and must plan to determine the need for information

resources so that the information system has appropriate efficiency and is sufficient for future use.

4. Separation of Development, Testing and Operational Environments

4.1 The Information Technology Department shall monitor and ensure that computer systems used for system development (Development Environment), system testing (Test Environment), and actual service operations (Production Environment) are properly segregated from one another.

4.2 The Information Technology Department shall control and define access rights for each environment and assign responsible personnel for system shutdown operations. The results of these activities shall be reported to supervisors, and in the event of any issues, the problems and corrective actions taken must be documented and reported to supervisors accordingly.

- **Protection from Malware**

1. Controls Against Malware

1.1 The Information Technology Department shall establish measures for detecting, preventing, and recovering systems from malicious software to protect organizational assets, as well as promoting appropriate user awareness regarding such threats.

- **Back up**

1. Information Backup

1.1 The Information Technology Department shall establish measures and define regular backup schedules for critical information systems to prevent data loss.

1.2 The information owner shall perform or ensure regular data backups and backup testing to confirm that the data can be successfully restored and reused when required.

1.3 Users shall be responsible for regularly backing up data from their computers onto other storage media, such as external hard drives, ensuring that the backups are kept up to date and stored in appropriate locations that minimize the risk of data leakage.

- **Logging and Monitoring**

1. Event Logging

1.1 System administrators shall retain event logs related to information security in sufficient detail to support audit and review activities.

1.2 System administrators shall monitor the use of information systems, and the monitoring results shall be reviewed regularly to detect any irregularities.

1.3 System administrators must control and oversee the recording of various fault logging events related to information usage, analyze them, implement corrective actions, and develop strategies to prevent future problems.

2. Protection of Log Information

2.1 System administrators shall ensure the protection of information, as well as logging and evidence storage systems related to information system usage, against alteration, damage, or unauthorized access.

3. Administrator and Operator Logs

3.1 System administrators shall ensure that operational activities performed by administrators and personnel involved with the system such as system startup and

shutdown times, configuration changes, system errors, and corrective actions are properly logged and regularly reviewed.

4. Clock Synchronization

    4.1 System administrators shall ensure that the organization's information equipment and information systems are synchronized with an accurate time source consistent with universal time references.

    4.2 System administrators shall regularly verify and update the time settings of the organization's information equipment and systems to prevent incorrect time recordings.

- **Control of Operational Software**

1. Installation of Software on Operational Systems

    1.1 The Information Technology Department shall establish operational procedures and control measures for software installation on production systems to restrict user installations and prevent the installation of unauthorized software.

    1.2 The Information Technology Department shall define a written list of Software Standards authorized for installation on the organization's computers, ensure that the list is regularly updated, and communicate it to all users within the organization for acknowledgment and compliance.

- **Technical Vulnerability Management**

1. Management of Technical Vulnerabilities

    1.1 The Information Technology Department shall ensure that the organization's information systems undergo technical vulnerability assessments at least once a year.

    1.2 System administrators shall regularly maintain and monitor systems to sustain the required level of information security, including vulnerability scanning, risk assessment of identified vulnerabilities, and remediation of system weaknesses.

2. Restrictions on Software Installation

    2.1 Users shall comply with software installation control regulations and shall not install any pirated or unlicensed software on the organization's computers.

- **Information Systems Audit Considerations**

1. Information System Audit Controls

    1.1 The Information Technology Department shall develop an information system audit plan consistent with the assessed risks, such as a Vulnerability Assessment plan for evaluating system vulnerabilities.

    1.2 The Information Technology Department shall notify all relevant units prior to conducting any information system audit.

    1.3 The Information Technology Department shall define the scope of the Technical Audit Test to cover critical risk areas and ensure that the audit activities do not disrupt normal operations. In cases where the audit may impact system availability, testing shall be conducted outside of regular business hours.

## 9. Communications Security

**Objective**

To establish measures for controlling the management of networks and the transmission of data through computer networks both inside and outside the organization to ensure security.

- **Network Security Management**

  1. Network Controls

     1.1 System administrators shall control and oversee the management of computer network controls to prevent potential threats and to maintain the security of information systems and applications operating on the computer network, as well as the information exchanged through the network.

  2. Security of Network Services

     2.1 System administrators shall ensure that security specifications, service levels, and management requirements for all network services are defined and included in network service agreements or contracts, whether the services are provided internally or externally.

  3. Segregation in Network

     3.1 The Information Technology Department shall ensure appropriate segmentation of computer networks, taking into consideration user access requirements, information security impacts, and the level of importance of the data residing on those networks.

- **Information Transfer**

  1. Information Transfer Policies and Procedures

     1.1 The Information Technology Department shall control and supervise the establishment of operational procedures for information exchange that are appropriate to the type of communication used and the classification level of the information.

  2. Agreements on Information Transfer

     2.1 The Information Technology Department shall control and supervise the establishment of information exchange agreements for both internal exchanges between departments within the organization and external exchanges with parties outside the organization.

     2.2 Information exchange between the organization and external parties shall be approved by the data owner prior to each exchange and shall be controlled through written agreements specifying the conditions of the exchange. Appropriate measures shall be implemented to protect the information in accordance with its confidentiality classification.

  3. Electronic Messaging

     3.1 The Information Technology Department shall establish control measures for electronic messaging, such as electronic mail (e-mail), Electronic Data Interchange (EDI), or instant messaging. Important electronic messages shall be appropriately protected against unauthorized access, modification, disruption, or denial of service.

  4. Confidentiality or Non-Disclosure Agreements

     4.1 Department executives shall ensure that personnel and external parties performing work for the organization enter into a written confidentiality or non-disclosure agreement (NDA) to protect the organization’s information.

## 10. System Acquisition, Development and Maintenance

**Objective**

To minimize errors in requirement definition, design, development, and testing of newly developed or enhanced information systems, and to ensure that the developed or acquired systems comply with the defined agreements.

- **Security Requirements of Information Systems**

1. Information Security Requirements Analysis and Specification

1.1 The department assigned to develop or procure information systems for organizational use shall clearly define the information security requirements in the systems to be developed or acquired for use.

1.2 The department assigned to develop or procure information systems shall monitor the system development process to ensure that it meets the defined information security requirements as well as the specified functional requirements.

2. Securing Application Service on Public Networks

2.1 Measures should be implemented to ensure the security of information processed through application services, both in general cases and when transmitted over public networks, to prevent fraudulent activities, incomplete transmission or miss-routing, as well as unauthorized disclosure, copying, or modification of data.

3. Protecting Application Services Transactions

3.1 Information related to information service transactions shall be protected against incomplete transmission, miss-routing, unauthorized modification, unauthorized disclosure, and unauthorized copying.

- **Security in Development and Support Processes**

1. Secure Development Policy

1.1 The Information Technology Department shall establish regulations for the development of information systems to ensure security and coverage throughout the entire system development life cycle.

2. System Change Control Procedures

2.1 The Information Technology Department shall establish written procedures for changing control, covering all phases of the information system development life cycle.

3. Technical Review of Applications after Operating Platform Changes

3.1 System administrators shall perform technical assessments to analyze potential impacts prior to implementing any system changes or upgrades, such as version updates or security patch corrections. Testing shall be conducted in a test environment until it is confirmed that all systems operating on that environment function normally and securely before applying the changes or upgrades to the production environment.

3.2 System administrators shall perform technical verification after changes to the operating system in the production environment to ensure that the modifications do not affect system functionality or compromise information system security.

4. Restrictions on Changes to Software Packages

    4.1 Packaged software used within the organization should be utilized without modification. In cases where modification is necessary, the department assigned to perform such actions shall implement strict controls over the modification process.

    4.2 Any modification of packaged software shall be carried out in accordance with the change control procedures established by the Information Technology Department.

5. Secure System Engineering Principles

    5.1 The department assigned to develop information systems shall adhere to the following minimum principles of security system development.

    - Least Privilege: Granting the least privilege to information system users to prevent unauthorized modification or alteration of data or systems.
    - Need to Know: Granting access rights only as necessary for the performance of duties to prevent the leakage of sensitive information.
    - Defense In-Depth: Designing a system with multiple layers of protection to reduce the risk of unauthorized access to information.
    - Open Design: Open Design feature to allow for the development of systems or Algorithms are of the same standard and workable.

6. Secure Development Environment

    6.1 The department assigned to develop information systems shall control the development and integration of environments to ensure security by protecting system data generated during development, data transmission, data backup, and access control to information systems.

7. Outsourced Development

    7.1 The Information Technology Department shall establish written agreements for system development with external parties responsible for developing software for use within the organization.

    7.2 The department assigned to engage external parties for the development of information systems shall supervise, monitor, and regularly follow up on the development activities carried out by such external parties to prevent any damage that may affect information security.

8. System Security Testing

    8.1 The assigned department and system users shall jointly test the functional operations of the information system, and the information security functions in every newly developed or modified system.

    8.2 System development testing shall be conducted during the development phase and prior to the system's production deployment. Evidence for testing newly developed or modified systems shall be formally documented and retained.

9. System Acceptance Testing

    9.1 The Information Technology Department must establish criteria for accepting new or improved information systems, whether developed by the Information Technology System Development Department or procured by external agencies, and must test the systems before they are put into actual use.

- **Test Data**

1. Protection of Test Data

1.1 The assigned department and system users shall avoid using actual data from production systems for testing purposes. In cases where copies of production data are used for testing, such test data shall be controlled with the same level of protection as the data in the production system.

1.2 Actual use

## 11. Supplier Relationships

**Objective**

To establish various regulations and operational frameworks for external agencies in providing or using information technology services to ensure efficiency, security, and maximum benefit to the organization.

- **Information Security in Supplier Relationships**

1. Information Security Policy for Supplier Relationships

1.1 The Information Technology Department shall establish information security policies related to external parties. Relevant personnel should assess potential risks and determine preventive measures to mitigate such risks before granting external parties or individuals' access to the organization's information systems or information.

1.2 System administrators and departments assigned to coordinate with external parties shall supervise and ensure that individuals or external agencies providing services under contract comply with the terms and conditions specified in the agreement, which shall include provisions on information security, the nature of services, and the defined service levels.

2. Addressing Security within Supplier Agreements

2.1 The Information Technology Department shall ensure that there is a written agreement on information security related to the granting of access to information systems to external agencies or the use of information for reading, processing, managing or developing information systems.

2.2 System administrators and departments assigned to coordinate with external parties shall ensure that external parties are granted access only to the information to the extent necessary and only with the written consent of the information owner.

2.3 System administrators and departments assigned to coordinate with external parties shall ensure that external parties comply with the requirements or agreements established between the organization and the external parties.

3. Information and Communication Technology Supply Chain

3.1 The Information Technology Department shall ensure that agreements and responsibilities related to information security risks are defined in contracts with external parties providing information and communication technology services, including any subcontractors engaged by such external parties.

- **Supplier Service Delivery Management**

    1. Monitoring and Review of Supplier Services

        1.1 System administrators and departments assigned to coordinate with external parties shall regularly monitor and review the operations of external parties responsible for managing the organization's information processing systems, including their financial status, operational processes, and service performance.

    2. Managing Changes to Supplier Services

        2.1 In cases where external service providers make changes to their processes, procedures, operational methods, or security practices, system administrators and departments assigned to coordinate with external parties should conduct a risk assessment of such changes, report the findings to management and relevant parties, and establish appropriate risk management processes accordingly.

## 12. Information Security Incident Management

**Objective**

To establish guidelines for managing information security incidents, learning from issues that have occurred, and implementing corrective actions to prevent the recurrence of information security incidents.

- **Management of Information Security Incidents and Improvements**

    1. Responsibilities and Procedures

        1.1 The Information Technology Department shall define responsibilities for managing undesirable or unforeseen information security incidents and clearly assign operational authority to personnel within the department.

        1.2 The Information Technology Department shall establish a classification system for undesirable or unforeseen information security situations from general operational disruptions to determine appropriate solutions.

        1.3 The Information Technology Department shall establish channels and criteria for reporting incidents, vulnerabilities, or disruptions related to information security and communicate them to both internal personnel and external parties.

    2. Reporting Information Security Events

        2.1 Users and external parties shall report any incidents related to the organization's information security to their supervisors and the Information Technology Department through the designated reporting channels and must do so as promptly as possible.

    3. Reporting Information Security Weaknesses

        3.1 Users and external parties shall report any vulnerabilities related to the organization's information security to their supervisors and the Information Technology Department through the designated reporting channels and must do so as promptly as possible.

        3.2 Users and external parties who discover any information security breaches or system vulnerabilities within the organization shall not disclose the incident to anyone other than their supervisors and the Information Technology Department and shall not attempt to verify or test the suspected information security vulnerabilities on their own.

4. Assessment of and Decision on Information Security Events

    4.1 System administrators shall assess information security incidents, categorize incidents or vulnerabilities based on predefined criteria, prioritize them accordingly, and notify relevant parties for corrective action when such incidents or vulnerabilities are determined to have potential impact on information security.

5. Response to Information Security Incidents

    5.1 Personnel assigned to resolve information security incidents and external agencies to whom they are contracted must follow the established procedures for resolving information security incidents.

    5.2 Personnel assigned to resolve security incidents, as well as external parties under contractual agreements, shall respond to and resolve security incidents within the specified timeframe. If the issue cannot be resolved within the designated period, they must promptly inform their supervisors.

6. Learning from Information Security Incidents

    6.1 Personnel assigned to resolve information security incidents, as well as external parties under contractual agreements, shall prepare reports on the analysis and resolution of incidents, vulnerabilities, or weaknesses related to information security. Such reports should be documented and retained as organizational knowledge to support operational learning and reduce the likelihood of recurrence in the future.

7. Collection of Evidence

    7.1 Personnel assigned to resolve security incidents and external agencies under contract must collect evidence related to the information security incidents that have occurred to gather sufficient evidence to present to the relevant agency executives and to use in further legal proceedings.

## 13. Information Security Aspects of Business Continuity Management

**Objective**

To prevent disruption or interruption of the organization's business operations and to protect critical business processes from failures of information systems, as well as to ensure that information systems can be restored within an appropriate timeframe.

- **Information Security Continuity**

1. Planning Information Security Continuity

    1.1 Data owners and the Information Technology Department shall jointly identify events that may impact business processes, assess risks and critical systems, and gather accurate and complete information to support the development of the information security continuity plan.

2. Implementing Information Security Continuity

    2.1 The Information Technology Department shall establish an emergency response plan that includes information security measures as an integral part, ensuring consistency with the organization's business continuity plan.

3. Verify, Review and Evaluate Information Security Continuity

    3.1 The Information Technology Department shall test the emergency response plan at least once a year and record the test results to ensure that the plan is accurate and can effectively support operational continuity.

    3.2 Personnel involved in information system recovery operations shall possess the necessary technical knowledge for system restoration and participate in recovery plan drills.

    3.3 Data owners and system users involved in the business continuity plan shall participate in plan testing and perform their duties in accordance with the established procedures.

- **Redundancies**

1. Availability of Information Processing Facilities

    1.1 The organization shall ensure that the availability requirements of critical information systems are properly assessed and maintained.

    1.2 The organization shall ensure the installation of backup information systems, backup equipment, or supporting systems sufficient to maintain appropriate business continuity.

## 14. Compliance

**Objective**

To ensure that the organization's operations comply with applicable laws, agreements, contracts, and security requirements that the organization and its personnel are obligated to follow, as well as to enable the verification of compliance with the established information security policies.

- **Compliance with Legal and Contractual Requirements**

1. Identification of Applicable Legislation and Contractual Requirements

    1.1 The Information Technology Department, in collaboration with the Legal Department and the Human Resources Department, shall collect all laws, regulations, rules, and requirements related to information security and document them as written operational guidelines, which shall be regularly reviewed and updated to ensure their relevance and accuracy.

    1.2 All personnel shall be responsible for strictly complying with the specified requirements.

    1.3 Employees of the organization are strictly prohibited from using the organization's assets or information technology systems to perform any actions that violate the laws of the Kingdom of Thailand or any applicable international laws under any circumstances.

2. Intellectual Property Rights

    2.1 The Information Technology Department shall establish processes for managing the use of licensed software and intellectual property to ensure that the use of information that may constitute intellectual property, as well as software developed by vendors, complies with applicable laws and contractual requirements.

    2.2 Users shall not copy or distribute software licensed and procured by the organization for its use, except for making backup copies solely for emergency purposes or as replacement copies for the original software.

2.3 Users are strictly prohibited from reproducing or distributing images, articles, books, or any documents that infringe copyright, as well as from installing pirated software on the organization's information systems.

2.4 Software developed for the organization, whether by external parties or internal personnel, shall be deemed the property of the organization. External parties or internal personnel are not permitted to copy or distribute the organization's proprietary software without prior authorization.

2.5 Users operating software within the organization's information systems shall strictly comply with applicable laws, information security policies, and the software manufacturer's terms and conditions.

2.6 Employees are prohibited from playing unlicensed music and music that is not provided by the Company into the Company's broadcasting system. This includes playing music from copyrighted records or from public networks such as radio, YouTube, etc., as such actions may be considered a copyright infringement under the Copyright Act of 1994 (and amendments) regarding the distribution of works to the public without permission from the copyright owner.

3. Protection of Records

3.1 Data owners shall comply with legal requirements related to specific types of information, such as accounting or customer data, and shall establish data management and retention requirements in accordance with such regulations.

3.2 Data owners shall control and protect log records from damage, loss, alteration, unauthorized access, or disclosure. Such controls shall be implemented in compliance with applicable laws, regulations, and business requirements.

4. Privacy and Protection of Personal Identifiable Information

4.1 The organization shall ensure the protection of personal data in compliance with applicable laws, government-issued regulations and guidelines, as well as any other requirements enforced upon the organization.

4.2 Customer information is considered highly confidential. The department responsible for managing such data shall ensure that only authorized personnel or employees, as assigned by their duties or approved by their supervisors, are permitted to modify or alter such information.

4.3 Personal information of personnel, employees, and customers should be treated as confidential and may be disclosed only to individuals authorized by the organization.

5. Regulation of Cryptographic Controls

5.1 The Information Technology Department shall control data encryption processes to ensure compliance with applicable laws, government-issued regulations and guidelines, as well as any other requirements enforced upon the organization.

- **Information Security Reviews**

1. Independent Review of Information Security

1.1 The organization shall conduct information security assessments through the internal audit function or independent external auditors to verify compliance with information security policies, standards, and procedures, as well as to review the adequacy of information system controls and the effectiveness of implementation.

2. Compliance with Security Policies and Standards

    2.1 Department heads should be responsible for regularly reviewing their subordinates' compliance with the organization's information security policies, standards, and operational procedures.

    2.2 In cases where department heads identify non-compliance with the organization's information security policies, standards, or procedures that do not yet impact the organization's information security, they shall explain and clarify the matter to ensure that subordinates understand and correct their practices. However, if the identified non-compliance affects the organization's security information, the department heads shall take disciplinary action in accordance with the organization's regulations.

    2.3 The Information Technology Department shall provide support and guidance on the use of information systems or compliance with information security policies, standards, procedures, and related requirements to other departments upon request.

3. Technical Compliance Review

    3.1 Regular technical reviews of information systems, such as penetration testing, shall be conducted to ensure compliance with the organization's information system security policies and international information security standards.

    3.2 The internal audit function should review the technical controls of information systems to verify their adequacy, appropriateness, and compliance with the established controls.

    3.3 System administrators shall regularly conduct information system security standard assessments, such as vulnerability assessments or penetration tests, to ensure alignment with the organization's information system security policies and international information security standards.

Information Security Policy was approved by the Board of Directors Meeting No. 1/2025 on 25 February 2025 and has been in effect since 25 February 2025.

*- Signed -*

_____

(Mr. Pachara Yutidhammadamrong)
Chairman of the Board of Directors