AI Energy Public Company Limited

Information Technology Security Policy

- English Translate Version -

- English Translate Version -

Information Technology Security Policy

1. Principles

AI Energy Public Company Limited ("The Company") and its affiliated companies recognize the importance of information technology and communication technology as factors that promote business operations, enhance efficiency, ensure security, and allow for continuous operations. This includes preventing problems that may arise from improper use of information technology systems and guarding against various threats to align with good corporate governance principles, as well as relevant laws, to suit the context of business operations.

The Company, therefore, establishes policies and guidelines to provide a framework for overseeing and managing information technology security systems ("The Policy"). However, it is crucial for all users, system administrators, and individuals involved in the Company's information technology systems to cooperate in implementing the policy and guidelines provided by employees and external parties.

2. Objectives

To ensure that the Company's information technology systems are efficiently and stably managed and aligned with business operations and risk management, allowing the Company to achieve its objectives and main goals. This is done through appropriate resource utilization and risk management in accordance with good governance practices, providing a framework to guide and support security operations for the organization's information to comply with or align with business requirements, laws, and relevant regulations.

3. Scope of Enforcement

This policy applies to all employees, managements, and directors of the Company and its affiliated companies, as well as external individuals who work for the Company, to recognize the importance of maintaining security when using information technology systems within the Company and to respond to the Company's mission and policies. By referencing the ISO/IEC 27001:2013 standard, the Company ensures that managements and employees at all levels, and external individuals working for the Company are aware

of and strictly follow this policy. Violations or breaches of this policy may result in appropriate corrective actions or penalties. Regular monitoring and reviewing of operations are conducted to ensure compliance with relevant laws and regulations, emphasizing managing the information technology systems to be continuously operational and updating policies and practices in information technology security to align with technological changes.

4. Definitions

The Company:	AI Energy Public Company Limited
Managements:	Level of department manager or above
Company Personnel:	Directors, managements, and employees
Users:	Employees, contractors, suppliers, or customers
External Service Providers:	External entities hired by the Company IT services
IT Systems:	Information and communication technology (ICT) systems, computer systems, network systems, information security systems, software systems (off-the-shelf or custom software), and communication systems of the Company. This includes systems related to personal data.
Information:	Data that has been processed, organized into numeric, text, or graphical form for easy understanding and utilization in management, planning, decision-making, and other purposes. This also includes personal information.
Data:	Information, text, instructions, command sets, or anything else that resides within computer systems that can be processed by computer systems. This term includes electronic data under electronic transaction laws and personal data protected by personal data protection act.
Personal Data:	Meaning as defined in personal data protection act and as specified in the Company's Personal Data Protection Policy.

Assets:	Hardware, software, and data under the responsibility of the Company's information technology department, including the Company's IT assets.
IT Assets:	1) Asset type includes system assets such as computer network systems, computer systems, computer workloads, and information systems. 2) Equipment-type includes computer hardware, computer peripherals, data recording devices, and other equipment. 3) Information Asset Types includes data, information, electronic data, computer data, and encompasses personal data in electronic or computerized form. 4) Information Asset Copyright refers to assets derived from development or usage rights by product owners.
Information System:	Company's operational systems that store, process, and disseminate information, working in coordination between hardware, software, data, users, and processing procedures to generate information that can be utilized for planning, management, and supporting the Company's operational mechanisms.
Network System:	Systems used for communication, data transmission, and information exchange between various information technology systems of the Company, such as LAN systems, wireless systems, Intranet systems, Internet systems, and other communication systems.

5. Roles and Responsibilities

Information Technology Department

1. Establish guidelines, criteria, and regulations related to the policy.

2. Define specific guidelines, criteria, and regulations regarding the protection of personal data in electronic or computerized forms.
3. Ensure that users comply with the Company's policies, criteria, and regulations related to information security and report any incorrect practices to the management.
4. Communicate policies to users, business-related personnel, and external parties in an easily accessible manner to ensure understanding and proper adherence.

Users

1. Learn, understand, and adhere to the Company's information security policy diligently.
2. Fully cooperate with the Company in safeguarding the Company's computer systems and information data. Safeguard and secure the Company's data and information.
3. Immediately report to the Company any intrusion, theft, destruction, or tampering with the Company's computer systems, information, and information systems that may cause harm to the Company.

Head of Department / Unit Head

1. Explain and promote compliance with the information technology security policy among users and issue disciplinary warnings in case of inappropriate and non-compliant actions.

6. IT Risk Management Policy

The Company specifies that IT risk management must align with the Company risk management policy and encompass the following aspects;

6.1 Defining Roles and Responsibilities for IT Risk Management: The IT managers are responsible for studying, acquiring methods or IT guidelines to mitigate and manage existing risks. They present these to the management for consideration in risk management regarding information technology systems.

6.2 Identification of Information Technology Related Risks:

- **Physical and Environmental Risks:** This includes the Data Center Room, which houses servers, network equipment, and other devices. Control measures should be in place for access, exit, and usage, along with system monitoring, such as temperature and fire alert systems.

- **Risks Related to Computer Program Usage:** To prevent the use of insecurely downloaded and installed programs, safeguards should be established, including preventing unauthorized downloads or installations, especially malicious software like viruses that can attack computers within the network.
- **Network System Usage Risks:** There should be checks and monitoring of internal network usage and internet systems. Security measures, such as firewalls and email data filtering, should be implemented to safeguard servers and client computers used by employees.
- **Personnel Risks:** Access rights and permissions for computer systems, network equipment, data, and personal information must be appropriately assigned to prevent unauthorized access, usage, modification, or misuse.

6.3 Comprehensive Risk Assessment: The Company should assess the likelihood and impact of risks to prioritize risk management. These risks can be categorized into four (4) types:

6.3.1 Technical Risks related to computer and equipment attacks.

6.3.2 Operational Risks arising from operational errors in users' management, causing unauthorized access to data and damages in IT processes data.

6.3.3 Risks from Disasters and Emergency Situations arise from disasters or natural events, including other situations like power outages, protests, and more.

6.3.4 Management and Operational Risks stem from existing policies or the application of policies that may not align with potential risks.

6.4 Defining Methods or Tools for Risk Management: The Company aims to maintain risks at an acceptable level. It creates a detailed risk description table that includes risk title, risk type, risk characteristics, risk factors, and impact. It also specifies the probability and severity of risk events, along with creating a risk map.

6.5 Information Technology Risk Indicators: The Company establishes indicators and monitoring systems to report results to responsible parties. This ensures effective and timely risk management.

7. IT Security Policy

7.1 Additional Guidelines on Information Technology Security Policy and Measures

Objectives:

To prevent actions that violate the IT security policy regarding information technology security.

Guidelines:

- Prohibit the use of computer resources and networks for unlawful activities or actions contrary to societal norms, such as conducting commercial activities or disseminating illegal or unethical content.
- Do not access computer systems and data using another user's account, password, or identity confirmation data without permission.
- Prohibit unauthorized interference with, deletion, addition, copying, or any other action on computer systems and data that are protected by the Company's access control mechanisms or any action exceeding one's authority.
- Refrain from disclosing another person's information, organization's data, or any personal information without permission.
- Do not disrupt, impede, or engage in any activities that cause damage to or render the Company's computer resources and networks unusable or inoperable, such as sending malicious commands, injecting programs causing computer or network devices to deny service, etc.
- Do not covertly intercept or receive data within the Company's computer network and data transmission processes.
- Before using portable storage, media or opening attached files in emails or files downloaded from the internet, there must be a check for malicious code, such as viruses, through antivirus programs every time.
- Users must not permit others to use their user accounts and passwords, which the Company has assigned for individual use only.
- **Users must comply with measures to control the use of the internet system within the Company.**

8. Information Technology Security Structure

8.1 Internal Structure

Objectives:

To control network access, computer systems, and data access based on the type, security level, and position and role of users. The administrators are responsible for managing access to data based on security levels to prevent information security breaches and damage to Company information systems. They also manage network system access and network service usage, and database usage according to the Company's policies. This is done to manage and maintain the security of the organization's information systems.

Guidelines:

Executives Committee

The Committee must oversee security in compliance with policies and guidelines.

Human Resources and Corporate Support Manager

The manager must assign responsibilities to IT supervisor and officer regarding information security. They must ensure compliance with policies and practices for maintaining information security within the Company.

IT Supervisor

The supervisor who serves as the system administrator, is responsible for enhancing and maintaining system security. In case of incidents affecting information security, they must take corrective actions and report to the Manager promptly to address issues in a timely manner.

IT Officer

IT officer is responsible for maintaining and monitoring system security and ensuring that users comply with policies and practices. In the event of security incidents, they must take corrective actions and report them to IT supervisor in timely manner.

Users

User must be aware and strictly adhere to the information security policy. Users may request access rights to access the information processes within the Company, and such requests must be approved by the authorities.

8.2 Notebooks/Laptops Devices and Remote Access

Objectives:

To maintain the security of remote access and the use of notebooks/laptops devices.

Guidelines:

- Registered all notebooks/laptops devices and must be specifying the brand, model, and operating system, in accordance with the Company's information technology security policy.
- Requires the use of Company-provided notebooks/laptops devices for accessing or storing Company information. If it is necessary to use personal notebooks/laptops devices for work purposes, approval must be obtained from the human resources and corporate support manager.
- Remote Access (VPN) is limited to department managers, and access must be password-protected. In cases where users need to use VPN, approval must be obtained from the human resources and corporate support manager. VPN access should be terminated immediately when no longer needed.

9. IT Security for Company Personnel

Objectives:

To ensure that users understand the policies, responsibilities, and proper use of the Company's information technology systems. This is done to reduce the risk of errors and inappropriate use of information systems and other information resources by employees.

Guidelines:

Prior to Employment:

- Human Resources supervisor conducts background checks on all job applicants before they are hired to ensure there are no records of intrusion, tampering, destruction, or unauthorized access to information technology systems of any organizations.
- Employees are required to sign a Non-Disclosure Agreement (NDA) stating that they will not disclose Company secrets, including personal data under control. This agreement is a part of the employment contract and is binding both during employment and for a period of not less than one year after the termination of employment.

During Employment:

- Those in charge must supervise and provide guidelines to ensure that users are aware and responsible for their roles regarding information technology security.
- Disciplinary measures shall be defined formally and communicated to employees to address any violations of the Company's IT security policies.
- New employees must receive training on the information technology security policies and the Personal Data Protection Policy as part of their orientation.

Terminations and Change of Employment:

- To maintain accurate and up-to-date users' management, the human resources supervisors inform the IT supervisor immediately of employee resignations, terminations, or job rotation.
- Employees who terminate their employment with the Company must return company assets, such as notebooks/laptops. After this, the system administrator will revoke their access rights within the specified timeframe.
- In cases of job rotation within the Company, the administrator will review and adjust access rights as appropriate to the new responsibilities and roles.

10. IT Asset Management

10.1 Responsibility for IT assets

Objectives:

To ensure that users are aware of their responsibilities and obligations regarding the use of computers and computer equipment and to understand the importance of keeping Company assets and data secure, accurate, and available at all times.

Guidelines:

- Users of computer and equipment are responsible for the assets they use.
- Prohibited use of Company's computer and network systems for personal business or purpose and inappropriate.

- Users are not allowed to install or modify software on Company computers unless authorized by the established guidelines. IT department is responsible for software installation and modification.
- Users are prohibited from altering or modifying the components of computers and equipment. Users must also maintain the condition of computers and equipment to keep them in their original state.
- Users must avoid storing or using computer in locations with high temperatures, humidity, dust, or the risk of physical impact.
- Do not use or place computer near liquids, magnetic fields, high-voltage electricity, in vibrating environments, or in environments with temperatures exceeding 35 degrees Celsius.
- Exercise caution when moving computer or equipment, avoiding stacking heavy objects on top or tossing them.
- Avoid hard objects encountering computer screens, as this can lead to scratches or damage. Ensure screens are cleaned lightly with clean hands and in a consistent direction, without circular movements that could create streaks.
- Users who are no longer with the Company must return all computer or equipment and to the IT department in working condition.
- When moving or using computer or equipment for offsite work, users must adhere to Company's procedures for taking assets out of the Company, or other regulations or guidelines related to the personal data protection policy.
- Users are responsible for preventing loss of computers or equipment, do not place unattended in public area or the area that foreseen potential of loss.
- All networked computers and notebooks/laptops of the Company must be protected through user authentication. Users must use their designated usernames and passwords, provided by system administrators, to access information systems each time they need to log in. Users should also implement a screen saver and log off when not using the computer.
- The Company prohibits users from bringing their personal devices (BYOD) into the organization without prior approval from the human resources and corporate support manager.

- The Company mandates the proper disposal of assets that are no longer required, such as paper documents (using document shredders), CD/DVD discs (using disc cutters or shredders), and formatting data storage media (Low Level Format) like Hard Disk Drives (HDDs), Solid State Drives (SSDs), or USB Flash Drives.
- Passwords must be set for data storage media to prevent unauthorized access, misuse, or damage during transportation or movement. Access should be granted only to authorized personnel who are responsible for data media transfer, ensuring the security of information security.

10.1.1 Software License Control

Objectives:

The objective is to make users aware of their responsibilities and obligations when using computer software. Users should understand the importance of using software in compliance with copyright laws and adhere to best practices. This includes using computer software securely and in accordance with relevant computer-related laws.

Guidelines:

For System Administrators:

- System administrators have the responsibility to control and oversee the use of computer software and allocate software usage rights as defined.
- They are responsible for the installation and upgrading of computer software for users at scheduled times.
- Immediate revocation and cancellation of software usage rights are required when authorized for cancellation and/or transfer of software usage rights.

For Users

- Users should use computer software as if it were their own property, ensuring that it is not used illegally or in violation of laws affecting third parties, resulting in damage to the Company.
- Software installed on computer systems must be legally licensed, and users are prohibited from copying, modifying, or distributing software to others.

- Copying, selling, or distributing copyrighted software or customized software without proper authorization is strictly prohibited, especially using such software for illegal activities.
- Prohibited illegal and/or unauthorized software install into Company's computers. If the use of such unauthorized software, licensed software, or freeware results in losses, changes, or compromises users' personal data, users may face legal consequences in accordance to the personal data protection act.

10.1.2 IT Asset Management and Network System Usage Control

Guidelines:

Preventing IT assets; documents, data record, computers, information technology and personal data, from unauthorized access by individuals without proper authorization or users exceeding their job responsibilities. Ensure that no unauthorized access occurs when equipment is unattended, and ensure users log out from network systems or computers when not in use.

- Immediately log out from information system when abstain from use
- Authenticate users before access computers
- Secure the storage and back-up of the important files, which store in Shared Drive that requires access permission for each Shared Folder.
- Shut-down the computers when not in use more than 2 hours, except those computers that run the networking system 24 hours.
- Set screen saver and lock the screen automatically when the computer not in use for more than 15 minutes.
- Users shall take good care of Company' IT assets as their own assets, if the loss or damage occurred by negligence such user must be responsible or compensate for the damage.

10.1.3 Email Usage

Objectives:

The objective is to facilitate the proper and efficient exchange of information through email, supporting work processes while adhering to legal requirements, regulations, and security measures for the Company's information. Users should understand the importance and be aware of the potential issues that may arise from using email services on the Internet, and they should follow the guidelines set by the system administrators.

Guidelines:

- Assets such as documents, data records, computers, and information must be controlled to prevent unauthorized access by individuals without proper authorization or individuals exceeding their duties. Access should be restricted when there are no users of the equipment, and users must be logged out of the information system when not in use.
- Users of email services must not commit offenses related to computer crimes, electronic transaction laws, personal data protection act, relevant regulations, and policies related to information technology or other specified policies.
- Users of the Company's email service must use it for the benefit of the Company within the defined scope of usage rights.
- Users will be granted email service privileges, and the system administrators will register users based on a list provided by the relevant department.
- It is prohibited to use someone else's email address to read, send, or receive data without the owner's consent. The owner of the email address is responsible for its use.
- When using email, users must not impersonate the sender's account or any other user account.
- When sending emails to customers related to the Company's business or contacting other organizations or individuals involved in the user's duties, users must use the Company's email system exclusively, and other email systems are prohibited.
- Email usage must be polite, respect ethical norms, comply with laws, and must not incite harassment, insults, illegal activities, or harm to groups of the Company.

- Using the Company's email system for distributing information, messages, images, or other content that is considered inappropriate, harmful to the country's security, violates computer-related laws, or disrupts the operation of business groups is prohibited.
- Users are prohibited from using email addresses for personal business or online social networking purposes, such as applying for online social networks. If such actions are detected, the owner of the email address or user account will be held responsible.
- Actions that create problems for the use of system resources, such as creating chain mail, sending spam emails, sending letter bomb, or distributing malicious computer viruses, are prohibited.
- Sending confidential Company information to unrelated individuals or organizations is prohibited.
- In case the Company receives complaints or requests or identifies any actions related to the use of the email system that pose security risks to the network and computers, breach personal data, or involve any illegal activities, the Company reserves the right to temporarily cancel or suspend services for the users or others involved for investigation.
- If users encounter inappropriate actions, criminal activities, or privacy breaches, they should report them through the Company's reporting channels.
- Any actions related to publishing, forwarding, or importing data into the system, both in the form of email and user homepages, are the sole responsibility of the user. System administrators and the Company not be involved in such actions.

10.2 Information Classification

Objectives:

To protect information appropriately in line with its importance to the Company, information classification must consider legal requirements, the value of importance, and sensitivity levels to

prevent unauthorized disclosure or alteration. Users are required to handle information according to the appropriate information classification levels.

Guidelines:

The human resources and corporate support manager determine the type of information, importance levels, classification levels, access levels, and access methods in writing and communicate these to relevant personnel.

Information Classification Levels:

Top Secret Information:	Opening all or part of it may result in severe damage.
Highly Confidential Information:	Opening all or part of it may result in serious damage.
Confidential Information:	Opening all or part of it may result in damage.
Internal Use Information:	Information for internal office use only.
Public Information:	Information that can be disclosed or made public.

Access Levels for Classified Information:

- Access to and usage of top-secret Information: The Company sets access and usage rights for this information through approval for storage. The agreement for non-disclosure must be in writing and signed by managements unless disclosure is authorized by law or under legitimate circumstances.
- Access to and usage of highly confidential and confidential information: The Company sets access and usage rights for this information separately for data owners, based on job roles/departments/units or individuals, through consideration and approval by the human resources and corporate support manager.
- Access to and usage of internal use information: All users in the office have access to and can use this information.
- Access to and usage of public information: There are no special regulations; it can be disclosed to the public.

10.3 Media Handling

Objectives:

To prevent unauthorized disclosure, alteration, handover, deletion, or destruction of information stored on media.

Guidelines:

10.3.1 Management of removable media

- For data classified as "Top Secret," the Company mandates destruction when it's no longer in use.
- Before removing media from the office, ensure that data on the media cannot be retrieved.
- All media must be securely stored and protected from hazards.
- Do not use removable media for activities unrelated to the Company's operation.

10.3.2 Disposal of media

In cases where removable media is no longer needed, the Company requires it to be destroyed, ensuring data cannot be recovered, e.g., by tearing, shredding, smashing tapes, hard drives, or flash drives.

10.3.3 Physical media transfer

- Packaging must protect against damage during transportation as appropriate.
- Transfer should be done by Company personnel for data security.
- If there is a need to transport media outside, access should be locked to prevent unauthorized access.

11. Access Control

11.1 Business requirements of access control

Objectives:

To establish measures for using the Company's internet system via the Company's network and access to information based on classification levels and users' positions. System administrators are responsible for managing access control based on the classification of data. Authentication is required

to access the Company's network and data systems, and users must be aware of accessing various websites through the Company's network.

Guidelines:

Access rights for each department/section/unit should be appropriately defined. Periodic reviews of departmental and information security requirements should be conducted. Access permission requests, grants, revocations, and modifications should be recorded, both for authorized and unauthorized users, serving as evidence for audits. Authorized access updates should be documented in the Access Control and Permission Control List.

11.2 User access management

Objectives:

To control access rights effectively and prevent unauthorized access to information systems.

Guidelines:

- Access to information systems should be requested and terminated immediately when an individual is no longer authorized, terminated employment, or job rotation. This is to control access rights and termination of users.
- System administrators must perform identity verification and authentication before accessing the Company's information systems. This includes setting up complex passwords to confirm user identities, with each user having their user account provided by system administrators.
- **Set Logon Attempt – Retires,** if the user enters the wrong password exceeding the limit, access should be suspended, and the system administrator should investigate and prepare a report. Access suspension should be lifted only after verification. For ERP access; SAP the accounting and finance manager is the system administrator who manages username and password (Authentication) and access rights/authorizations of SAP.
- System administrators should periodically audit the usage of the Company's information systems. This includes auditing user accounts for identity verification into Company network twice a year and auditing VPN (Virtual Private Network) access rights annually.

11.2.1 User Privilege Control

- The Company provides High Privilege User IDs (HPID) to executive director (1) and to HR and corporate support manager. For ERP system, one executive director has an HPID for controlling modifications.
- In cases where system administrators need to use accounts with high privileges (HPID), strict control is required. The use of such accounts must be approved by authorized personnel and accompanied by justifications.
- Access to data, critical information, personal information, and data processing equipment must be controlled, taking into consideration usability and information security within the information system. Guidelines should be established regarding who is authorized to access, permissions for employees or individuals responsible for important data and personal information. Users at all levels should be made aware, understand, and adhere strictly to the established guidelines. They should also be aware of the importance of maintaining information system security.
- Permissions for data, critical information, personal information, and information systems must be defined. For example, permissions for using information system applications, internet access, database access, etc., should be granted to users according to their roles and responsibilities. These permissions should be limited to what is necessary for performing their duties and should receive approval from authorized personnel. Regular reviews of these permissions should be conducted.
- In cases where it is necessary to use users with special privileges, strict control is required. To determine whether the control of users with special privileges is sufficient, the Company will consider several factors including;
  - obtaining approval from authorized personnel,
  - tightly controlling the usage of users with special privileges (e.g., limiting usage to essential cases), and
  - setting time limits for usage, suspending usage immediately when the time limit expires.

11.3 User Responsibilities

Objectives:

To prevent unauthorized access, disclosure, leakage, or covert duplication of personal information and to prevent theft of data processing computer/equipment.

Guidelines:

- Users must keep their usernames and passwords for the Company's information system confidential. They should not share them with others, such as allowing others to access their accounts or leaving passwords on their desks or computer screens.
- In cases where no one is working at the computer or device, precautions must be taken to prevent unauthorized usage by others who do not have the authority or responsibility. For example, users should log out of the system when they are not actively using the computer.
- In cases where users or employees are authorized to grant access or modify data in their responsibilities, they should only grant access or permissions to individuals or groups as necessary (share files). Access should be revoked immediately when no longer needed, as permitted by authorized personnel. Additionally, evidence of such permissions should be documented for auditing purposes.
- Users are prohibited from disclosing confidential and proprietary information of the Company, except as required by the Company's official disclosure policies.
- Users are prohibited from disclosing, transferring, or forwarding personal data under the control of the Company, except as necessary to fulfill their rights and responsibilities under the terms of this policy and the personal data protection policies of the Company group.
- Users must use the internet system in a manner that does not violate the rights of others and must not cause harm to the business group. Users must not engage in any actions that could be considered violations of computer-related laws or relevant legal provisions. In all cases of internet system usage for Company operations, users must adhere strictly to established procedures or regulations.

- Users must not use the Company's internet network for personal purposes and must not access inappropriate websites, such as those that go against moral standards, endanger national security, religion, the monarchy, or society, or promote illegal activities, among others.

11.4 System and application access control

Objectives:

To prevent unauthorized access to information systems and applications.

Guidelines:

The Company establishes controls for information technology system usage, including specifying access rights to data, such as read, write, delete permissions. In cases where external individuals need to work within the Company, they must follow the information technology security policies, and system administrators must supervise and ensure compliance.

12. Cryptography

12.1 Cryptographic Control

Objectives:

To ensure that the use of data encryption is appropriate, efficient, and capable of protecting confidential or important data from unauthorized access or modification.

Guidelines:

The Company establishes controls for data encryption, considering the types and methods of data encryption algorithms that are consistent and appropriate. Key management is also specified, with system administrators responsible for managing encryption keys.

13. Physical and Environmental Security

13.1 Secure Areas

Objectives:

To establish standards for physical security regarding the location and workspace of information technology systems, as well as computer equipment, data, and information assets of the Company.

Guidelines:

13.1.1 Access to the server room

- The Company defines access rights to the server room to be granted only to authorized personnel and individuals as determined by the Company. This is done to prevent unauthorized access, pre-knowledge, modification, or damage to data and computer systems within the Company.
- Access to the server room is limited to specific individuals: the company's executive director, the HR and corporate support manager, and system administrators (IT officer/IT supervisor of IT department).
- Access rights to the server room are periodically reviewed according to the organizational structure and IT department work plan.
- Employees within the Company or external individuals who wish to perform various tasks within the server room must request permission through the system administrators. Approval from the HR and corporate support manager is required, and reasons, as well as timeframes for performing tasks, must be specified. System administrators will control and supervise the tasks to prevent any damage to data and information systems within the Company.

13.1.2 Damage Prevention

- Fire Safety Systems within the Server Room: Automatic fire extinguishers and smoke detectors are installed within the server room to provide initial fire protection. A safety department is responsible for inspecting the system's use.
- Uninterruptible Power Supply (UPS): The server room is equipped with an uninterruptible power supply that protects against damage caused by electrical anomalies, such as power outages, to ensure continuous operation of the server and CCTV systems.

- Temperature and humidity sensor: The server room is installed with air conditionings and set the temperature to be appropriate for the room conditions. There is also a temperature and humidity sensor installed in the server room. The temperature and humidity status in the server room will be shown to the system administrator.
- Security of signal wiring and communication cables (Cabling Security) by creating labels for signal cables and communication cables.

13.2 Equipment

- Equipment Maintenance
  - System administrators are responsible for maintaining information technology equipment properly to ensure its readiness for continuous and correct operation.
  - System administrators are responsible for establishing preventive maintenance procedures and maintenance agreements, which include contracting external service providers for parts replacement or repair of various components of the computer server, uninterruptible power supply (UPS), CCTV systems, and various application software to always keep them operational.
- Removal of Assets

The Company has determined that only managers level and above can authorized to take information assets to outside the Company. The data is encrypted before access such assets for security purposes.

14. Operations Security

14.1 Operational Procedures and Responsibilities

System administrators create written work instructions (WI) that align with operational procedures and responsibilities for the Company's information systems. These WIs must be approved by the HR and corporate support manager and managing director.

14.2 Protection from Malware

The Company has implemented measures to protect against malware on both server and client computers to prevent malicious software from inside and outside the Company. Additionally, regular checks, updates, and improvements to malware protection measures are conducted monthly, with results documented and communicated to management.

14.3 Data Backup

The Company defines the frequency of data backups, including the server, network infrastructure devices, and the Company's data systems stored in Network Attached Storage (NAS). Regular testing of data backup completeness is conducted at least once a year, and external backups outside the Company's premise are maintained.

14.4 Logging and Monitoring

The Company mandates the logging of information, such as network firewall logging and NAS logging, to record details of system access. Logging files are separated from the internal network system to prevent unauthorized tampering. System administrators are responsible for monitoring system operations and ensuring that deviations from normal working conditions, caused by system errors or security incidents, are checked, prevented, and corrected according to standard procedures.

The Company has assigned system administrators to manage and monitor information system operations that do not follow normal procedures, caused by an error in the operation of the system and security incidents which must be checked, protected, and changed regularly by following the operating procedures in normal conditions.

14.5 Control Operational Software

The Company restricts the installation of additional software to system administrators, allowing them to install software for users. Requests for specialized or non-standard software must comply with Company regulations.

14.6 Technical Vulnerability Management

The Company actively monitors technical vulnerability-related information that could pose a risk to the security of its information systems. Reports on technical vulnerabilities are communicated to provide guidelines for mitigating threats arising from technical vulnerabilities, and this information is shared with personnel through Company's email notifications.

14.7 Information Systems Audit Considerations

The IT department must plan and execute information system audits, considering the potential impact on systems and operational processes with minimal disruption. The audit planning should align with the assessed risks and vulnerabilities.

15. Communications Security

Objectives:

The purpose is to provide guidelines for safeguarding the Company's information network systems from external threats and ensuring the security of data and information systems within the Company. This includes protection against viruses, malicious code, and preventing unauthorized access or damage to information systems.

Guidelines:

15.1 Network Security Management

The Company has established network security measures, including the installation of firewalls to secure connections to public networks. Network security administrators are responsible for implementing security measures for various information network systems to ensure their security. The following measures are in place:

- Network administrators manage and control the connections between public networks and the Company's internal network.
- Network administrators manage and control connections to wireless networks rigorously. They segregate internal and external computer network systems, including changing access codes for wireless networks to ensure the security of the systems and internal information.
- The Company maintains logging files for verification and modification, improving related systems, and ensuring compliance with legal processes and boundaries.

15.2 Information Transfer

- The Company establishes terms and agreements, or contracts, between employees and external service providers to define conditions for the use of the Company's services.

- It sets up management practices and protocols for transferring information data through various channels for both internal and external users of the Company's services.

16. System Acquisition, Development, and Maintenance

Objectives:

The objective is to assign responsibilities for the development, enhancement, or modification of information systems to align with the constantly changing information technology landscape while maintaining compliance with the Company's information technology security policy.

Guidelines:

16.1 Security Requirements of Information Systems

The Company mandates that system administrators develop, enhance, or modify the security of information systems within the Company to align with evolving technology and security changes. These changes must be approved by superiors or managers of HR and corporate support. Procedures and practices for modifying computer systems in emergency situations must also be established, with reasons documented and authorized by relevant authorities.

16.2 Security in Development and Support Processes

The Company sets controls to ensure software modifications are secure for information and information system lifecycles. System administrators or system owners, as well as relevant departments, are responsible for:

- Establishing system change control procedures to control changes and modifications to information systems.
- Supervising and monitoring outsourced development activities and ensuring that the outsourced agency is responsible for software development according to the service agreement.

16.3 Test Data

The Company stipulates that for ERP software, such as SAP, financial and accounting manager are responsible for system testing. In this context, test data must be separated from real-use data to ensure proper testing of the system.

17. Supplier Relationships

Objectives:

To protect the Company's assets accessed by external service providers involved in information technology outsourcing while maintaining the agreed-upon levels of security and service quality.

Guidelines:

17.1 Addressing Security within Supplier Agreements

The Company establishes agreements with external service providers related to access, storage, and communication to align with the Company's requirements and information system security.

17.2 Supplier Service Delivery Management

- The Company mandates tracking, reviewing, and evaluating external service providers using criteria set by the Company to ensure compliance with the Company's policies and mitigate risks associated with service providers.
- The Company defines practices and procedures for selecting service providers using company-defined criteria and assesses risks that may arise when changing external service providers to align with the Company's requirements.

18. Information Security Incident Management

18.1 Management of Information Security Incidents and Improvements

Objectives:

To manage incidents or occurrences that may impact the security of information systems. This includes designating responsible personnel, addressing incidents and vulnerabilities related to information system security, reporting incidents, and taking appropriate actions promptly and in accordance with legal requirements.

Guidelines:

- Assign responsible personnel and establish procedures to deal with and mitigate incidents related to the information security of the Company's information systems.
- Define clear communication channels for reporting information security incidents.

- Users who detect incidents that may affect information security must report them to the information technology department.
- System administrators should monitor and observe for abnormalities and report to the information technology management in case of any issues.
- In the event of an incident or something that is suspected to be related to information security, it should be documented for reporting to managing director for further investigation and corrective action. This documentation will help in analyzing, improving, checking, and preventing harm to the Company's information system.
- Record security breaches, considering the type of incident, the extent of the occurrence, and the costs incurred from the damage. This is done to learn from the incident and prepare for prevention, as well as to report previously occurring information security incidents to relevant parties to help reduce the severity or likelihood of recurring incidents in the future.
- Perform risk assessments, audits, and report incidents or threats that may affect personal data related to the Company's information systems in accordance with legal requirements.
- Ensure that system administrators monitor and maintain intrusion detection and prevention devices and collect statistics related to attempts to breach the network system, such as firewalls and antivirus systems, to protect the internal computer network from threats.

19. Information Security Aspects of Business Continuity Management

19.1 Information Security Continuity

Objectives:

To provide guidelines for practicing the recovery of information systems in the event of emergencies to minimize disruptions to the Company's information systems. This is based on the Company's business continuity planning and aims to enhance information security for data and information systems within the Company while maintaining continuity in information systems.

Guidelines:

- IT department must prepare plans to address issues, uncertainties, and disasters that may occur with information systems, following the crisis management plan. This includes data backup plans

for information systems within the Company and logging data from firewall systems to ensure readiness for use and data recovery.

- Regularly check the readiness of backup information system conditions, at least once a year, and document and report the results to management.
- The Company defines the need for assessing the risk situation and the impact on information technology systems (Business Impact Analysis) to determine the level of technology-related emergencies. Preparedness equipment and contingency plans are maintained at least once a year.
  - Business Continuity Planning is in place and executed as per the Business Continuity Plan.
  - Regular testing and improvement of emergency plans are conducted at least once a year, and results are documented and reported to management.
  - Severity levels and resolution procedures are defined for each situation, and readiness is ensured in case of any incidents.
  - Data loss quantifications (Recovery Point Object) and recovery time frames (Recovery Time Object) are established to gather results from system recovery for further adjustments and informing management.

19.2 Redundancy of Information Processing Facilities

Objectives:

To ensure the readiness of redundant information processing equipment to maintain the operation of information systems.

Guidelines:

Prepare redundant systems sufficiently to support the operation of information systems to prevent disruptions to the Company's information systems and ensure compliance with the specified readiness conditions.

20. Compliance

20.1 Compliance with Legal and Contractual Requirements

Objectives:

To prevent legal violations, regulatory criteria, and contractual obligations related to maintaining information technology security.

- Identification of applicable legislation and contractual requirements clearly and make necessary updates.
- Protection of records: Departments/sections/units that contract with external service providers must enter into agreements that prohibit the unauthorized disclosure, destruction, or alteration of internal data in compliance with the law and business requirements.
- Privacy and protection of personal identifiable information: The Company collects personal data for processing in accordance with personal data protection policies and legal procedures, ensuring data confidentiality and compliance with laws and regulations.
- Ensure that IT department manager review the compliance of information systems and operational processes with policies, standards, and relevant security requirements.

20.2 Information Security Reviews

Objectives:

To ensure that information security management aligns with the policies, practices of the business entity, and international standards in information security.

Guidelines:

Ensure that there are regular reviews and improvements of procedures and practices related to information security management to align them with the information technology security policy and international standards.

21. Policy Review

Ensure that there is a regular review of this policy, at least once a year, to align it with the Company's strategy, changing risks, and regulations. The policy should be presented to the Company's board of directors for approval.

The Company recognizes the importance of developing an information technology security policy, which will enhance the efficiency of business operations, build trust with partners, customers, and shareholders in terms of being a well-governed company. The Company believes that the information

technology security policy will be a part of its efforts to develop the Company's prosperity and securely growth.

- translate version –

Miss Pimwan Thareratanavibool

Managing Director

- English Translate Version -