



Announcement No. 3/2026

Cyber Security Policy

Silamas Transport Co., Ltd., Silamas Services Co., Ltd., Renewable Energy Service Co., Ltd., and their affiliated companies (referred to as the "Company") recognize the importance of digital technologies and the use of data in conducting business. The Company is committed to ensuring information security and protecting against cyber threats. Therefore, this Policy has been established to safeguard information assets and support secure business operations.

Objective

- To establish the direction, principles, and governance framework for cybersecurity management.
- To promote awareness and understanding among employees to ensure compliance with the Company's policies, standards, operational frameworks, procedures, guidelines, and applicable laws and regulations relating to computer systems in a correct and appropriate manner.
- To ensure that employees and all individuals who use or connect to the Company's computer systems do so in a secure, proper, and appropriate manner.
- To protect the Company's computer systems and information assets from unauthorized access, theft, destruction, disruption, interference, and other forms of cyber threats that may adversely affect the Company's business operations.

Scope

This policy covers the protection of information and cybersecurity of the company, whether on-premise or cloud-based systems procured by the Company. It applies to:

- All employees and departments within the Company
- External parties authorized to access Company-related computer systems and information

Definitions Term

User: Employees of the Company, as well as authorized external parties who have been granted user accounts and/or passwords to access the Company's information processing systems, computer systems, or information technology resources.

Computer System: All computer equipment and devices, including hardware and software of any type or size; wired and wireless network infrastructure; data storage media and data transfer devices; Internet and Intranet systems; as well as electrical and telecommunications equipment capable of performing functions similar or equivalent to those of computer systems. This includes assets owned by the Company, its business partners, or other organizations that are in the process of installation and have not yet been handed over, as well as employees' personal devices that are installed or used within the Company's premises.



Information Technology: Information, records, data, documents, computer programs, computer data, images, audio, marks, symbols, and any other forms of information, whether stored in a format that can be directly understood by individuals or in a format that requires processing or interpretation through computer systems, electronic devices, or other equipment.

Sensitive Information: Information that is critical to the Company's business operations or that the Company is obligated to protect under applicable laws, business ethics, contractual obligations, or other legal requirements, and which must not be disclosed to unauthorized parties or used for any purpose other than the Company's legitimate business purposes. The unauthorized disclosure, leakage, or misuse of such critical or confidential information may disrupt the Company's business operations, reduce operational effectiveness, or cause reputational damage to the Company.

Remote Access: The ability to connect to and access the Company's computer systems or network, either through the Company's internal communication network or from external networks, using authorized communication channels.

Administrator: An individual assigned responsibility for the operation, administration, maintenance, and support of the Company's computer systems, including hardware, software, and related peripheral devices. A System Administrator is authorized to configure, modify, enhance, maintain, and update the Company's computer systems to ensure they operate correctly, efficiently, securely, and in accordance with the Company's business requirements.

Security: The processes, measures, and practices implemented to protect, monitor, and maintain the security of the Company's computer systems and information assets. These include preventive, monitoring, enforcement, and due care activities designed to safeguard critical systems and information from unauthorized access, theft, destruction, alteration, disruption, or other malicious activities by both internal personnel and external parties that could adversely affect the Company's business operations.

External Party: any external individual or organization that conducts business with or provides services to the Company and may be granted authorized access to the Company's information, information assets, or information processing facilities, such as;

- Business Partner
- Outsource
- Supplier
- Service Provider
- Consultant

Roles and Responsibilities

1. Responsibilities of Supervisors

- Communicate and ensure that employees understand the Company's cybersecurity policies, standards, governance framework, operating procedures, work instructions, guidelines, and other relevant processes relating to cybersecurity and information security.
 - Provide oversight, guidance, and corrective advice to employees, and take appropriate action when improper or non-compliant practices are observed.
-



- Ensure that disciplinary actions for policy violations are administered consistently, fairly, and in accordance with the Company's disciplinary procedures.

2. Responsibilities of Employees

2.1 All Employees shall:

- Read, understand, and strictly comply with the Company's cybersecurity policies, standards, governance.
- Framework, operating procedures, work instructions, guidelines, and other related processes concerning cybersecurity and information security.
- Fully cooperate with the Company in protecting its computer systems, information assets, and information processing facilities from cybersecurity risks and threats
- Immediately report to the Company any improper or non-compliant practices, as well as any actual or suspected unauthorized access, theft, destruction, interference, cyberattack, or other security incidents that may compromise the confidentiality, integrity, or availability of the Company's computer systems or information assets.

2.2 Employees Assigned to use Computer Systems shall:

- Log out (Log-out/Log-off) from all systems when they will be unattended for an extended period and shut down their computers and peripheral devices immediately after completing their work or at the end of the working day.
- Lock their computer screen using password-protected screen locking (Lock Screen) whenever leaving their workstation unattended, even for a short period, to prevent unauthorized access or use.
- Scan all files, data, and removable media before introducing them into their computers by using the Company's approved anti-malware or anti-virus software with up-to-date virus definitions.
- Keep passwords and any other authentication credentials issued by the Company for accessing computer systems, information assets, or Company data strictly confidential. Employees must not disclose, share, or permit the use of their credentials by any other person. Passwords and other authentication credentials shall be changed upon expiration in accordance with the Company's password policy or whenever compromise is suspected or a change is otherwise deemed necessary. Passwords shall be created with due care and must not:
 - reuse previously used passwords;
 - be easily guessed by others; or
 - be reused across multiple systems or accounts to which the employee has access.

- ### 2.3 Employees responsible for managing or coordinating with third parties shall ensure that such third parties comply with the Company's Cybersecurity Policy and applicable information security requirements.



3. IT Governance

The Company shall establish and maintain an effective information technology (IT) governance framework to manage the risks associated with the use of technology. Effective IT governance requires alignment among governance processes, technology resources, and information management practices to support the Company's policies, strategic objectives, and risk management activities.

The Company shall also establish appropriate reporting and monitoring mechanisms to ensure that information technology is managed effectively, delivers value to the business, supports the achievement of business objectives, and enhances the Company's competitive advantage.

Guidelines

1. Information Security Principles

The Company's information security practices are based on the following principles to ensure the effective achievement of the objectives of this Policy:

- **Confidentiality:** Protecting information from unauthorized access, disclosure, or exposure, including personal data, proprietary information, and other confidential information belonging to the Company.
- **Integrity:** Ensuring that the Company's information is accurate, complete, and protected from unauthorized modification, alteration, or destruction.
- **Availability:** Ensuring that authorized users have timely, reliable, and secure access to information, systems, and services whenever required.
- **Accountability:** Clearly defining the roles and responsibilities of individuals and ensuring that they are accountable for their actions and decisions in accordance with their assigned duties and responsibilities.
- **Authentication:** Ensuring that access to the Company's computer systems and information assets is granted only after a user's identity has been successfully verified through an approved authentication process.
- **Authorization:** Ensuring that access rights to the Company's computer systems and information assets are granted based on the principles of Least Privilege and Need-to-Know, and only to the extent necessary for the performance of authorized job responsibilities.
- **Non-repudiation:** Ensuring that parties involved in electronic transactions or other information processing activities cannot deny their participation, the authenticity of their actions, or the validity of the transactions they have performed.



2. Information Management and Confidentiality

The Company shall implement appropriate and adequate measures to ensure that information security is maintained in accordance with its business operations and the classification and criticality of each type of information. In doing so, the Company shall take into consideration both internal and external factors that may affect the security of its information assets. The Company places particular emphasis on maintaining the Confidentiality, Availability, Integrity, and Accuracy of information, in compliance with applicable laws, regulations, contractual obligations, and other relevant third-party requirements.

Directors, executives, and all employees are required to comply strictly with the Company's Cybersecurity Policy. This includes respecting the privacy of others, refraining from using confidential information without proper authorization, and avoiding unauthorized access to another user's information, files, systems, or other information assets.

Maintain the confidentiality of information belonging to the Company's customers, business partners, and other relevant parties.

Refrain from disclosing confidential information, documents, or trade secrets for a period of one (1) year following the termination of employment or separation from the Company's position.

During the period of employment, employees may have access to information of the Company that is considered "Trade Secrets." Such information has commercial value and is subject to appropriate measures to maintain its confidentiality. The designation of such information may be specified in employment agreements, contracts, or other agreements of the Company.

Employees agree to maintain the confidentiality of the Company's "Trade Secrets" that they become aware of or obtain as a result of performing duties for the Company. Employees shall not disclose, transfer, distribute, or reproduce such information for any unauthorized person or purpose. Employees shall also refrain from disclosing information and/or engaging in any act or omission that may cause damage to the Company's reputation, business operations, or interests.

2.1 Access Control

Directors, executives, and all employees shall strictly comply with the Company's information security and cybersecurity policies. They shall refrain from using confidential information without proper authorization and shall not access information or information assets beyond their assigned authority.

The Company shall establish access rights and access control measures for critical information to prevent unauthorized access to sensitive information.

System Administrators are responsible for managing and controlling access to information, including both direct access and access through information systems. They shall also establish, maintain, and manage user accounts and passwords to support user authentication, identity verification, and access monitoring for relevant information resources.

The use of personal devices to connect to the Company's information systems must comply with the Company's rules, regulations, security requirements, and applicable procedures.



During the employment period, employees shall not perform or omit any action that may cause damage to the Company as a result of false information, reports, records, or communications, regardless of the method used. Any employee who intentionally violates the Company's information security policies or security measures, resulting in damage to the Company, shall be subject to disciplinary action in accordance with the Company's regulations and may be subject to legal proceedings if such actions violate applicable laws.

IT personnel shall define and manage network access paths for Internet connectivity and ensure that all data transmission is conducted through appropriate security controls, such as firewalls or proxy servers.

Remote access to the Company's information systems shall only be permitted through a Virtual Private Network (VPN) to ensure that data transmitted over public networks is encrypted and protected. The use of VPN services must require user authentication and maintain access logs to enable traceability, monitoring, investigation, and review following security incidents.

2.2 Physical and Environmental Security

The Company shall implement appropriate physical and environmental protection measures for equipment and areas used to store critical information, including physical storage facilities and information systems, to prevent unauthorized access to sensitive information.

Employees shall use the Company's assets with due care and responsibility. Equipment provided by the Company must be properly maintained and kept in good working condition at all times. In the event of any damage or malfunction, employees shall contact the IT department for inspection and corrective action.

Employees are responsible for protecting the Company's assets from loss, damage, or misuse, even when such assets are not directly under their assigned responsibility.

Company assets shall not be used for any purposes other than legitimate business purposes unless specifically authorized by the Company. Any equipment that contains critical information or provides access to the Company's information systems must be protected against unauthorized use, such as by implementing password protection or configuring screen lock/screen saver settings when the equipment is unattended.

In the event that any equipment is lost or stolen, employees shall immediately notify the IT department so that appropriate information security measures can be considered and implemented.

The Company shall centrally manage and maintain information technology equipment to ensure that such equipment remains in good condition and is available for continuous and effective operation.

2.3 Information Classification

The Company shall classify information and determine the appropriate level of importance and confidentiality. This classification approach serves as a prudent and appropriate framework for managing and securing electronic documents. The Company has established processes and procedures for the handling and management of critical documents as follows:



2.3.1 Information Categories

- **Management Information:** Includes information related to policies, strategies, performance commitments, human resources, budgets, finance, and accounting.
- **Operational Information:** Refers to information used by each department to perform its specific operational duties and responsibilities.

2.3.2 Information Confidentiality Classification

- **Confidential:** Information whose full or partial disclosure may result in serious damage, significant impact, or adverse consequences to the Company or relevant parties.
- **Public:** Information that may be freely disclosed or distributed to the public.

2.3.3 Access Levels

- **Management Level:** Access to information shall be granted based on the individual's role, responsibilities, and the list of authorized personnel designated within the relevant department or business unit.
- **General User Level:** Users shall only be permitted to access information that has been authorized for their use or information that is intended for general users.
- **System Administrator Level or Legally Authorized Personnel:** Access shall be granted based on assigned access rights and shall be limited to the scope of duties and responsibilities required by their roles and applicable laws.

2.4 Data Backup

Critical information shall be securely stored, and appropriate emergency response procedures shall be established to ensure the effectiveness and practical implementation of data recovery capabilities in the event of an emergency or disaster.

System Administrators or designated personnel shall be responsible for performing data backups and verifying the accuracy, completeness, and integrity of backed-up data in accordance with the defined backup schedule and the Company's data backup and recovery policy.

In the event of any issue that results in an incomplete or unsuccessful backup process, a root cause analysis shall be conducted, and appropriate corrective actions shall be implemented.

3. User Account and Password Management

The Company shall implement strict access control measures for information and information processing facilities. Clear guidelines and criteria for granting access rights shall be established to ensure that access privileges are appropriate to users' roles, responsibilities, and business requirements.



Employees at all levels are responsible for understanding and strictly complying with this Policy, as well as recognizing the importance of system security. For example, software installation shall only be performed by authorized personnel who have been granted Administrator-level privileges.

Access to server control rooms shall be restricted exclusively to authorized personnel.

Access rights to information and information systems (such as internal business applications, Internet access, and centralized data storage areas) shall be granted only to the extent necessary for employees to perform their assigned duties. For example, employees may access work-related files within their own departments, while access to information belonging to other departments shall be restricted to designated shared areas only. All access rights must be approved in writing by authorized personnel before being granted.

In cases where temporary access to the Company's information systems or networks must be granted to external parties, such access shall require prior approval from authorized personnel. Access rights shall be revoked immediately upon the expiration of the approved access period.

User accounts within the Company's systems shall be reviewed and audited regularly to prevent unauthorized or inappropriate accounts from retaining access privileges, such as accounts belonging to former employees. The Company shall immediately revoke access rights when unauthorized, inappropriate, or inactive accounts are identified. Appropriate actions may include disabling user accounts, deleting accounts, resetting passwords, or other necessary measures.

Passwords shall be established in accordance with the Company's business requirements and current security conditions. The Company shall communicate password management requirements to all employees, including the protection of passwords and other authentication credentials used to access computer systems, Company information, or personal data. Such credentials must be kept strictly confidential, must not be disclosed to unauthorized persons, and must not be shared with others.

4. Computer Network and Data Transfer Management

4.1 Network Management

Employees shall acknowledge and comply with appropriate guidelines for the use of the Company's computer systems and networks, including information security procedures, to prevent the accidental disclosure of confidential information.

Employees are strictly prohibited from using the Company's assets or Internet resources for commercial purposes or personal benefit unless such use directly supports the Company's business objectives. Employees shall avoid accessing websites or sending and receiving emails that may pose cybersecurity risks or increase the likelihood of cyberattacks. In addition, the Company's computer resources and networks shall not be used for any illegal activities or activities that violate public morals, such as creating websites for unauthorized commercial purposes or distributing unlawful or unethical content.

Employees are strictly prohibited from accessing computer systems or information subject to access controls for the purpose of modifying, deleting, or copying information without proper authorization or legitimate access rights.

Employees shall not install any software or store any data on Company computers without prior authorization.



Employees shall not infringe upon the copyrights of the Company and/or any third parties that have authorized the Company to use computer software, whether such authorization is granted through contracts or any other means. Employees shall not reproduce, modify, publicly distribute, lease, or copy such software, regardless of whether such actions are intended for commercial gain or any other purpose.

The Company shall implement adequate and appropriate network security measures to protect its information technology infrastructure. Security software shall be installed to protect against external threats that may affect critical servers and client servers. Such security software shall be regularly and promptly updated to ensure continuous effectiveness and protection against emerging threats.

Access to the Company's network systems shall be subject to strict security controls to ensure system stability and protection. Network segmentation shall be implemented to clearly separate internal users from external users or third parties who connect with the Company. This approach helps reduce the risk of unauthorized access and enhances the Company's overall cybersecurity posture.

4.2 Data Transfer

Data transfer agreements shall be established to ensure that information is securely managed throughout the data transmission process. Such agreements shall address information security requirements and clearly define the responsibilities of all relevant parties. System Administrators shall be responsible for overseeing and ensuring that all data transfer activities maintain the three fundamental principles of information security, namely Confidentiality, Integrity, and Availability (CIA).

A Non-Disclosure Agreement (NDA) shall be signed between the Company and external parties to ensure that the Company's confidential information is not disclosed without appropriate authorization.

Company software shall not be provided or made available for use by any unauthorized third party, including suppliers, contractors, customers, or any other external parties, and shall not be used for personal purposes. In addition, employees are prohibited from using the Internet or Internet connections to transfer data, distribute inappropriate or illegal content, transmit obscene materials, or send and receive emails in a manner that violates applicable laws, copyright laws, the intent or objectives of the Company's Cybersecurity Policy, or any other relevant regulations.

The transmission, use, processing, storage, and destruction of critical information, including devices containing critical information, shall be performed through appropriate and secure procedures to prevent unauthorized access to such information.

System activity logs and records of critical systems shall be maintained for an appropriate retention period to comply with applicable laws, regulations, and requirements of relevant external authorities.

The Company shall establish proactive processes to prevent disruptions to information systems and respond to cybersecurity attacks in a timely manner. Such processes shall include rapid detection and mitigation measures, root cause analysis, and preventive actions to avoid recurrence of similar incidents.

The Company shall establish a clear complaint management process through which employees and stakeholders can submit complaints or concerns.



5. System Acquisition, Development, and Maintenance

The development of information systems shall follow a proper and reliable process covering all stages, including system design, development, testing, and deployment into the production environment. Development environments shall be segregated from production environments. The Company shall also emphasize secure system design principles to ensure that systems have adequate security controls in place and shall perform security assessments before systems are put into operation.

Any changes to information systems or related equipment shall be carried out through appropriate change management procedures and processes. Such processes shall include impact assessments and communication with relevant stakeholders. Adequate testing shall be performed to ensure system stability and reliability. All relevant documentation shall be updated and maintained to accurately reflect the implemented changes.

This policy will take effect from 20 August 2026 onwards.

.....
(Mr. Chompoo Glinpu)
CEO / Managing Director



SILAMAS GROUP

Head Office : 68 Moo 2, Sriwaeenoi Rd., Srisajorakhaenoi, Bangsaothong, Samutprakarn, 10570 THAILAND

Branch : 555 Moo 10, Nong-kham, Sriracha, Chonburi, 20230 THAILAND

Review and Revision History

Announcement No.	Date	Description
3/2026	20/8/2026	First issue