288/2568

12 May 2020

Saksiam Leasing Public Company Limited
Cybersecurity Policy

Saksiam Leasing Public Company Limited recognizes the importance and is fully aware of managing security risks arising from cyber threats. In order to efficiently manage potential risks, the Company has established the Cyber Security Policy as follows:

1. Definitions

- **Cyber Security:** Any processes and actions, such as prevention, response, risk mitigation, strict enforcement, vigilance, attention to usage, and maintenance of computer systems and information containing critical systems and data, to protect them from any attempts of unauthorized access for the purpose of theft, destruction, or interference with operations that may cause damage to business operations.
- **Cyber Threat:** Any unlawful action or operation utilizing a computer, computer system, or undesirable program with the intent to harm a computer system, computer data, or other related data, which would cause damage or impact the operation of the computer, computer system, or other related data.
- **Cyber:** Data and communications resulting from the provision of services or the application of computer networks, the Internet, or telecommunication networks, including the normal provision of satellite services and similar interconnected general network systems.
- **Company:** Saksiam Leasing Public Company Limited.
- **External Party**: Individuals or juristic persons conducting business or providing services who may be granted access to the Company' s information and information processing equipment, such as consultants, service providers, system development or equipment procurement contractors, and operational contractors for the Company.

2. Objectives

1. To establish guidelines and principles for cyber security management.
2. To build knowledge and understanding among employees to ensure correctly and appropriately comply with policy, standards, operational procedures, recommendations, and relevant laws.
3. To prevent the Company's computer systems and information from being intruded, stolen, destroyed, interfered with, or subjected to any form of theft that may cause damage to business operations.

3. Cyber Threat Risk Governance

1. The Company shall define the roles, duties, and responsibilities of relevant parties in governing cyber threat risks to ensure the Company has security standards capable of identifying, preventing, detecting, responding to, and recovering from incidents to resume normal operations. This supports the Company in maintaining adequate capabilities appropriate for the volume and complexity of the Company's operational systems.
2. The Company shall designate a unit or responsible personnel with the duty to assess, monitor, prevent, and respond to cyber threats, and report cyber threat risk information to the Executive Committee and the Risk Management Committee. The Company may consider appointing specific employees responsible for responding to and handling abnormal cyber incidents in a timely manner to mitigate the impact.
3. The Company shall provide education on potential cyber threats to ensure employees have the knowledge, understanding, and awareness of the necessity for security, and comprehend the subsequent impacts if an incident occurs. This includes communicating guidelines for preventing and responding to cyber threat incidents.
4. The Company shall establish clear coordination channels between internal and external units to efficiently determine guidelines for responding to and resolving security incidents.

4. Cyber Threat Risk Management

The Company shall establish an information technology security policy that covers cyber threat risk identification, prevention, detection, response, and recovery, including continuously reviewing and updating cyber threat information to keep pace with changes, as follows:

1. **Identification:** The Company shall identify which operational processes and information assets are at risk of cyberattacks and require security protection to appropriately manage cyber threat risks affecting the Company's systems, assets, and data.
2. **Prevention:** The Company shall implement appropriate preventive measures to limit the impact of cyber threat incidents. This covers access control, training and awareness-building for employees and related parties, data security, and various security measures encompassing processes, practices, and technologies. Furthermore, the Company shall regularly maintain equipment and software related to electronic systems to ensure continuous operations.
3. **Detection:** The Company shall establish processes for continuous monitoring, surveillance, and detection of cyber threat incidents, and alert on any abnormalities. This includes monitoring cyber threat incidents occurring both internally and externally, and analyzing the weaknesses or vulnerabilities of the threats that occur to be used as supporting information for reviewing guidelines to prevent future risks and impacts.

4. **Response:** The Company shall define a response plan for cyber threat incidents and problem-solving guidelines, including formulating a Business Continuity Plan (BCP) that covers cases where the impact or damage from cyber threats causes operational disruptions. This ensures the continuous maintenance of security levels and service provision. The Company shall also analyze the root causes and detect evidence of the occurring threats, and establish communication processes with customers and stakeholders to ensure a correct and aligned understanding of the Company's situation.
5. **Recovery:** The Company shall establish plans and processes to restore systems to normal operations within a specified timeframe. This includes reviewing and updating the plan to reflect current situations and incorporating lessons learned from cyber threat incidents into the review of the recovery plan and processes to enhance efficiency and prevent recurring problems and impacts in the future.

5. Policy Review

The cyber security policy shall be reviewed and presented to the Board of Directors for approval at least once a year.

6. Enforcement

In the event that the Cybersecurity Act B.E. 2562 is amended or any additional details are announced that explicitly conflict with or contradict this policy, or may cause the Company or related parties to violate the said Act, the amended and/or relevant announcements or regulations of the Act shall prevail and replace the explicitly conflicting or contradicting parts.

This Cyber Security Policy was approved by the Board of Directors in Meeting No. 3/2020 on May 12, 2020.

Announced on May 12, 2020.
(Mr. Siwaphong Boonsalee)
Managing Director

Remark: The Board of Directors' Meeting No. 8/2568 on November 11, 2025, reviewed and found the policy still appropriate without changes, therefore, the original version is to be used.