Information Technology and Cybersecurity

Policy and Guidelines

ศิครินทร์
SIKARIN

Sikarin Public Company Limited

Information Technology and Cybersecurity Policy and Guidelines
Sikarin Public Company Limited

Sikarin Public Company Limited (“Sikarin” or “the Company”) recognizes that Information and Communication Technology (ICT) is a critical infrastructure that supports the core business operations of the organization, including management, medical services, and communication with all stakeholders. The security and stability of information systems are central to maintaining the trust of service users, shareholders, partners, regulators, and the broader society.

Sikarin is committed to managing its ICT systems effectively, securely, and in a way that can handle risks across all dimensions. This includes ensuring data security, service continuity, protection against cyberattacks, and safeguarding personal data.

This policy defines the criteria, processes, and responsibilities for all sectors within the organization, from the Board of Directors, senior executives, the Sustainability Committee, to all employees, ensuring that Sikarin's ICT operations are safe, compliant with relevant laws, and capable of addressing complex cyber threats in the digital era effectively.

Scope of the Policy

This policy covers the management of ICT system security and risk across all areas of Sikarin, including data, resources, systems, and related networks.

Objectives

- To establish guidelines for securing ICT systems and communications.
- To prevent and mitigate risks associated with the use of ICT.
- To ensure that Sikarin’s operations comply with relevant standards and laws.

Roles and Responsibilities

Board of Directors

- Set the vision, direction, and framework for cyber security and information technology risk management policies in alignment with Sikarin's core strategy.
- Review and approve policies, as well as oversee the implementation to ensure effective execution.

- Supervise the comprehensive assessment of information technology and communication risks, covering both technical and strategic aspects.
- Promote Sikarin’s compliance with legal requirements, international standards, and best practices in information and cyber security.

Executives

- Responsible for driving the implementation of policies in various departments.
- Allocate appropriate resources, systems, and personnel to support information technology security management.
- Monitor and evaluate the effectiveness of risk control measures and regularly report to the Board.
- Foster the creation of a corporate culture where cyber security awareness is present at all organizational levels.

Relevant Departments

- Implement the information technology risk control measures outlined in the policies and practices.
- Develop and improve systems, processes, and technologies to enhance the security of information and systems.
- Coordinate to investigate, analyze, and manage any cyber security incidents that may arise.
- Prepare reports on information technology incidents and risks, presenting them to executives for consideration and remediation.
- Provide training and raise awareness among employees regarding cyber security and safe technology usage.

Employees

- Strictly adhere to the information and communication technology security policies and practices set by Sikarin.
- Use information systems, devices, and technologies carefully, avoiding violations of regulations or creating risks to the system.
- Participate in training and development programs related to cyber security provided by Sikarin.
- Immediately report any abnormal events or threats that could impact system security to the relevant departments.

Guidelines for maintaining security and controlling risks of information technology systems

The aim is to ensure that the organization can achieve its stated goals. By using information technology as a tool to support and effectively manage risks that may arise from the use of technology. Good information technology management requires a link between information technology management processes. Effective resources and information to support appropriate policies, strategies, organizational goals and risk management. Including reporting and monitoring operations. To ensure that the technology that Sikarin uses can help support the strategy and achieve business objectives and create competitive potential and add value to the organization. Sikarin must consider taking the following actions.

1. Information technology system security policy (IT Security Policy)

1.1. The Board of Directors and executives are responsible for ensuring that security policies are established in the information technology system in writing including the duty to consider and approve the said policy. Sikarin must communicate the said policy to create understanding and be able to follow it correctly, especially between the information technology department and business departments within Sikarin to ensure coordination and business operations according to the set goals.

1.2. Provide an evaluation of the effectiveness of the information technology security policy at least once a year or when there are changes that affect the security of Sikarin. The evaluation of Sikarin's performance can be done by Sikarin's internal information technology audit department (IT Audit) or external auditors to improve and correct shortcomings in the security of Sikarin's information technology systems.

1.3. In cases where Sikarin uses information technology services from outside service providers (Outsource), Sikarin must establish a policy to support the use of such services, which must cover methods for selecting and considering the qualifications of service providers and having regulations regarding the use of services to reduce the risk of accessing property information inappropriately Including requirements regarding data confidentiality. and do not disclose important information.

1.4. Sikarin must have measures in place to ensure that it can control the operations of external service providers in accordance with the established agreements which can check the operational process and have a plan in place. If an event occurs that may affect the security of the information system

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

Must be consistent with Sikarin's overall risk management policy (Enterprise Risk Management) and cover the following matters:

2.1. Defining duties and responsibilities in managing and managing information technology risks.

2.2. Identifying IT-related risks

2.3. assessment that covers the likelihood or frequency of risks occurring and the impacts that will occur on prioritizing risk management.

2.4. Determining methods or tools to manage and manage risks to a level acceptable to the organization.

2.5. Setting risk level indicators (IT risk indicator) includes arranging for tracking and reporting of indicator results. said to those responsible to be able to manage and Manage risks appropriately and keep up with events.

3. Guidelines for controlling information technology system risks

3.1. Maintaining accuracy and security in operations related to information systems at least must cover the following matters

1) Define operating procedures related to information technology systems to ensure operations. It is correct and safe in writing for employees to follow. Computers can operate correctly and in accordance with the information system security policy.
2) Receiving - sending information (Information transfer) both inside and outside the organization. Must maintain the security of information transmitted through the computer network by protecting it from alteration or damage the data and malicious programs (malware) that are sent through communication channels. There is protection for confidential or important information sent in the form of attachment files and automatic forwarding of electronic mail outside the organization. By encrypting data to use in transmitting information.
3) Companies must have measures to prevent and detect threats from malicious programs (Malware) by installing anti- Malware programs to cover both processors and computers as well as improving protection programs. to be current and be able to fix the information technology system so that it can return to normal use. In addition, Sikarin must have a system or process for protection to reduce the risk of website imitation (Phishing).
4) Companies must require backup of critical business data. Operating system Application Complete computer system and set data recovery goals (Recovery Point Objective: RPO) , such as the type of data and the most recent data set that can be recovered. Sikarin must store backup media off-site for safety. If the work location is damaged, the backup data and data recovery process must be tested at least once a year. Sikarin must also prevent damage to the backed-up data.

Backup Sikarin must specify at least the following procedures:

□Data that must be backed up and backup frequency

□Type of media used to record data (media)

□Amount that must be reserved (copy)

□Steps and methods for backing up data

□Where and how to store data storage media

□Data recovery process in case of data loss

5) Store and record various evidence (logs) of accessing the information technology system to be complete and sufficient for inspection. It must at least cover access to and use of the information system (application log), file usage, and internet use via Sikarin's internal computer network.

6) Control and limit software installation rights on work systems In order for the operating system to be accurate and complete and reliable Including performing penetration tests on important work systems connected to external networks before installing them on Sikarin's work systems. To properly detect potential vulnerabilities (technical vulnerability management) of the software to be reinstalled. In the case of installing additional features on the old work system, Sikarin must consider testing if the new feature has an impact on the work system that is already in use.

3.2. Controlling access to information systems and data (access control) to prevent intrusion and unauthorized access. Must at least cover the following matters.

1) 1) Controlling access to systems and information. Sikarin must determine the right to access the system and data appropriately according to the needs and responsibilities of the user. To prevent data leakage and unauthorized modification of the database. It requires users to verify their identity by specifying a username and password in order to access information according to their specified rights. and record system access by all types of user accounts.

2) 2) Establishing measures to ensure the physical and environmental security of information assets. Sikarin must arrange space for placing important information assets such as server rooms. computer center etc. To be safe and prevent unauthorized persons from accessing the said area. Safety from natural disasters must be taken into account and threats from humans and is secretive and prevents disclosure of information and details Area restricted to the public. Sikarin must determine the right to enter and exit restricted areas for only those with relevant duties and a tight access control system and Sikarin must record information on entering and exiting the server room or computer center Including the need to provide security, such as having a CCTV system fingerprint scanner fire alarm equipment Fire extinguisher or automatic fire extinguishing system Backup power system.

3.3. Data Security

Sikarin must have processes in place to maintain data security that is adequate to prevent unauthorized persons from accessing it or can change and edit information or use the information for illegal purposes.

1) Sikarin must specify what information is important or confidential and classify information according to level of confidentiality and importance. So important information is protected at an appropriate level according to the level of confidentiality.

2) Set access rights to sensitive or confidential information to prevent unauthorized access and modification. Change of information by someone who does not have rights or permission.

3) Transmission of important data over public networks Companies must encrypt data. To prevent access or change data in accordance with and appropriate to the level of risk that may occur.

4) Storing sensitive or confidential information Companies must maintain data security by: Encrypt data That can prevent the misuse of important information in the event of a data leak and is consistent with the level of risk that may occur with sensitive information.

3.4. Monitoring and checking for abnormalities and vulnerabilities in information systems Companies must conduct a vulnerability assessment. with every important work system at least once a year.

3.5. Maintaining the availability of information systems and management of events that may affect Information system security

1) Sikarin must have management of events that may affect the security of the information system (information security incident management) by covering at least the following matters:

- Written response plan in the event of an incident that may affect the security of the information system (Incident response plan).
- Evaluate incidents or weaknesses in information system security. To consider the severity of the incident and its impact on the security of the information system.
- Arrange for individuals or agencies to perform the duty of reporting the following events:

Report Immediately when an Incident Occurs	During the Editing Process	The Problem was Solved and the Cause Ended
1. Date and time of the event 2. Crime scene agency/system Details and causes of the incident that occurred 3. Expected impacts 4. Name of contact person/coordinator of Sikarin to provide information.	1. Date and time of the event 2. Crime scene agency/system details and causes of the incident that occurred 3. Impacts expected to occur by assessing the value of damages that may occur to customers and Sikarin 4. Troubleshooting and time period for correction	1. Data and time of the event 2. Crime scene agency/system details and causes of the incident 3. Expected impacts by estimating the amount of damage that may occur to customers and Sikarin. 4. Troubleshooting actions 5. Troubleshooting results and resolution time

Report Immediately when an Incident Occurs	During the Editing Process	The Problem was Solved and the Cause Ended
	5. Progress in resolving the problem	6. Future prevention guidelines and collecting evidence to identify causes and solutions.
Report without delay when you know. The event has been initially verified.	Report within the next 2 business days after the incident is known and verified.	Report when the incident is resolved or the problem is resolved within 15 days.

2) Sikarin must establish business continuity management in information systems (Information security of business continuity management).

- Prioritize disaster recovery according to potential impacts. Including the relationship of each work system. and determining the time for returning to normal operation of the work system.
- Procedures for solving problems or responding to events in each situation that arises.
- The person who is responsible and has decision-making authority includes the designation of responsible officials who can work in each situation, including the names and telephone numbers of all involved persons.
- Identify necessary resources for critical work systems that need to be used, such as center details, backup computer, location, map, computer model, systems used in work, various information and records. There must be an information system that is ready-to-use condition.
- Sikarin must communicate the IT continuity plan to relevant officials to acknowledge it and create a common understanding. To be able to act correctly when an incident occurs.
- Test compliance with the IT continuity plan at least once a year. The test must be conducted in a situation that is consistent with the nature, scope, and complexity of Sikarin's business operations. It is a possible situation and consistent with the current situation of Sikarin.

This Information Technology and Cyber Security Policy and Guidelines is the 3rd revision and is effective from 16 January 2025 onwards by the resolution of the Board of Directors at the meeting No. 1/2025 on 15 January 2025.

....

Mr. Seni Chittakasaem

Chairman