Information Technology Security Policy

THAICOM PLC.

May 24, 2021

Thaicom Public Company Limited
(Company Registration No. 0107536000897)
63/21, Rattanatibet Road
Nonthaburi 11000, Thailand.
www.thaicom.net, www.ipstar.com
Tel. (66 2) 596 5060
Fax. (66 2) 591 0705

THAICOM

THAICOM Public Company Limited

Information Technology Security Policy

Thaicom Public Company Limited and its subsidiaries (Company) recognize the importance of information technology security for the Company's business operations and therefore have issued an Information Technology Security Policy in order to protect information or reduce risk from threats, which may adversely affect the Company's business. This Information Technology Security Policy (Policy) refers to the Cybersecurity Act and international standards or guidelines.

Scope

This Policy covers the prevention of threats, the cybersecurity of the Company's information technology systems which are sited either in or outside the Company's premises, and the cybersecurity of any cloud system that the Company procures or uses. It also covers the usage of information technology systems by any user of the Company and its subsidiaries.

Principles and guidelines for cybersecurity

The Company embraces the "Zero Trust" principles, which assume that a cybersecurity incident may occur at any time and therefore is unavoidable. Accordingly, to mitigate risk and its impact, it is required to limit access to systems and resources on a "least privilege" or "need-to-use" basis and to continuously monitor resource accesses for suspicious activity.

Work structure and responsibilities

The Company appoints a committee to take care of information technology, which consists of the head of important business units, with the Chief Executive Officer (CEO) as the Chairman and the head of information technology as the secretary. The committee oversees the operation of information technology and its effectiveness, and manages cybersecurity risk and its impact to be in line with the Company's strategies.

Thaicom Public Company Limited
(Company Registration No. 0107536000897)
63/21, Rattanatibet Road
Nonthaburi 11000, Thailand.
www.thaicom.net, www.ipstar.com
Tel. (66 2) 596 5060
Fax. (66 2) 591 0705

Role	Responsibilities
Chief Executive Officer (CEO)	Set out overall strategies, follow up and oversee the execution of Information Technology Security Policy, and approve any guidelines concerning information system.
Head of Information Technology	Design and develop policies and guidelines concerning the security of information technology so as to be most secure and beneficial for the Company.
Head of business unit, and all management levels	Explain to the staff any policy or guidelines concerning the security of information technology, take care of, advise, and warn the staff, as well as report on any improper action.
All staff	Study and strictly follow the policies and guidelines concerning the security of information technology, fully cooperate with the Company in monitoring for improper or potentially dangerous usage of the information technology, and immediately inform the Company of such usage.
Staff with job functions related to outside personnel	Control the outside personnel so that any policy or guidelines concerning the security of information technology are strictly followed.
Internal Audit	As needed, arrange audit plan to audit the management and operation of the security of information technology.

Policy

The Company shall set up policies and guidelines which are in line with related laws and the following principles:

1. Privilege and control of access to systems and resources

Access rights to systems and resources shall be based solely on the roles and responsibilities. Hence, there shall be a management system for tightly controlling the access to the location, system, equipment, data, and resources in order to prevent any unauthorized access. As a minimum, the following guidelines shall be applied:

1) Create an asset inventory and specify ownership of assets
2) Make use of the Multi-Factor Authentication technique to control the access to systems or data
3) Apply cryptography and key management technique
4) Emphasize and manage the physical and environmental security

Thaicom Public Company Limited
(Company Registration No. 0107536000897)
63/21, Rattanatibet Road
Nonthaburi 11000, Thailand.
www.thaicom.net, www.ipstar.com
Tel. (66 2) 596 5060
Fax. (66 2) 591 0705

2. Management of the monitoring for improper or potentially dangerous usage of the information technology

The monitoring for the improper or potentially dangerous usage of information technology shall be thorough and consistent with the following guidelines as a minimum:

1) Review of account and privilege and related risks
2) Network zoning, micro-segmentation of the application layer, and application-aware firewall
3) Network security management by hunting for network intrusions
4) Information security incident management
5) Systems acquisition, development and maintenance with consideration for security and the management of vulnerabilities

3. Management of business continuity

The management of business continuity shall consider the plan to respond to cyber-attacks and regularly review the Company's compliance with related laws and regulations.

4. Review and changes of Policy

The Company may review this Policy from time to time to ensure that it remains in adherence to laws, any significant business changes, and any suggestions and opinions from other organizations. The Company shall explicitly announce an updated Policy through appropriate channels.

This Policy was announced on May 24, 2021.

(Mr. Prasert Bunsumpun)
Chairman of the Board of Directors
Thaicom Public Company Limited

Thaicom Public Company Limited
(Company Registration No. 0107536000897)
63/21, Rattanatibet Road
Nonthaburi 11000, Thailand.
www.thaicom.net, www.ipstar.com
Tel. (66 2) 596 5060
Fax. (66 2) 591 0705