Cybersecurity and Information Technology Policy

Amata VN Public Company Limited, its associates, subsidiaries, and affiliates (the Company) recognize that information is a valuable business asset that is collected, processed, and transmitted through computer systems and electronic devices. The Company has an open policy that allows employees to use computers and network systems to use applications and search for information independently under security measures. The Company pays attention to the systematic and effective supervision of information and cyber information in order to prevent risks and protect assets, including information, from all forms of cyber threats.

The Company has therefore established this policy to manage the use of computers, information, and network systems to be secure and efficient, with a focus on confidentiality, integrity, availability, and security according to the national and international cybersecurity and information technology standard framework, as well as relevant laws and regulations to oversee that information and information technology are used to support business operations appropriately, and the objectives and goals of the organization can be achieved continuously.

Definitions

Confidentiality refers to maintaining or reserving to prevent computer network systems, computer systems, information systems, information, data, or electronics from being accessed, used, or disclosed by unauthorized persons.

Integrity refers to taking steps to keep information or electronic data intact, accurate, and complete at the time of use, processing, transfer, or retention so that it is not altered, corrected, lost, or destroyed unlawfully or without authorization.

Availability refers to the management of an organization's information assets to be able to work efficiently, access them conveniently, quickly, or use them when needed.

Security refers to measures or actions that are taken to protect information assets and handle, mitigate risks, detect and respond to all forms of threats from both internal and external parties that aim to steal, destroy, damage, or interfere with the work that causes damage to the Company's business operations. The principles are as follows:

- Confidentiality: Protecting the confidentiality of information by preventing unauthorized access and disclosure of information, including personal information owned by the Company.
- Integrity: Ensuring that the Company's information must not be altered, modified, or destroyed by unauthorized persons.
- Availability: Ensuring that authorized users can access information and services quickly and reliably.
- Accountability: Identifying an individual's responsibilities, including liability and responsibility for the consequences of acting in that role.
- Authentication: Ensuring that access to computer systems and information must be completed only through a complete authentication process.
- Authorization: Ensuring that the grant of access to computer systems and information is at least privileged and in accordance with the need-to-know basis as permitted.
- Non-repudiation: Ensuring that the participants involved in the transaction cannot be denied as having nothing to do with the transaction taking place.

Data refers to information, messages, instructions, command sets, or anything else that is stored in the form of documents, printed materials, or electronic media that can be accessed, searched, or executed through various electronic network systems or electronic data processing technologies.

Information refers to the information of an organization that has been processed, analyzed, calculated, and interpreted to make it easy for users to understand, compare, and use in the operation of the organization. It has a variety of characteristics and forms. Common forms include:

- Information that is in electronic form, such as electronic documents, databases.
- Stored information that can be forwarded, removable, collaborative tools, etc.
- Information that is in printed documents, such as documents printed out.
- Information that individuals remember to use

Information technology refers to the application of computer technology and telecommunications and communication network equipment to locate, store, analyze, send, distribute, export, track, collect, and manage information of the organization.

Threat refers to any situation or event that may adversely affect the operations or property of an organization, individual, or other organization through unauthorized access to the system, destruction, disclosure, modification of information, and/or inability to provide the Services.

System refers to a network tool or device that connects data and transfers data over the Internet and intranet systems, both wired and wireless, as well as various electronic devices and telecommunications media that can operate or be used in the same way.

Asset refers to information, equipment, applications, services, or other information resources that support business operations and have economic value to the organization.

Practices

The Company establishes guidelines for the management of cybersecurity and information technology by strictly complying with the requirements for the use of computers and network systems of the organization in accordance with relevant laws, regulations, standards, and measures. The guidelines are as follows:

1) Identify, analyze, evaluate, and manage risks on cyber and information technology risks that align with the business context and cover risks posed by internal and external stakeholders throughout the supply chain.

2) Develop a strategic plan for cybersecurity and information technology risk management that is linked to the organization's vision, mission, objectives, and acceptable risk levels.

3) Establish cybersecurity and information technology plans or measures that cover identification of business environments and contexts, protection measures, detection, response, and recovery of damaged information systems and assets.

4) Oversee, protect, and manage the Company's information assets, premises, equipment, information systems, and computer networks to be safe and secure at all stages of the secure system/software development life cycle, including developing and maintaining them available and efficient at all times.

5) Protect the Company's information, its customers and partners who store, process, or transmit information technology from unauthorized access, transmission, correction, reproduction, modification, deletion, or destruction.

6) Provide technology systems to prevent cyber threats and cybersecurity, as well as information technology systems that are effective, resilient, and support essential functions.

7) Regularly examine vulnerability assessments, penetration tests, as well as establishing procedures and processes for the management of incidents that may affect cybersecurity and information technology.

8) Track, monitor, and detect abnormal events that may affect the continuity of business operations, as well as maintaining and monitoring network equipment and information systems to be effective and available at all times.

9) Control, limit the scope of the impact, and take corrective action in a timely manner, including improving the process to appropriately respond to incidents of security violations, be able to prevent, correct, and mitigate impacts on various business activities efficiently.

10) Continuously monitor and review the security status and activities that may affect the network and information systems of the organization, as well as preventive measures to maintain effective cybersecurity and information technology.

11) Perform rapid recovery or restoration of assets and information systems when damaged by data security breaches and cyber threats.

12) Provide support and cooperation with organizations from the private sector, the public sector, and civil society, both domestically and internationally, in preventing and maintaining cybersecurity and information technology.

13) Provide communication and promote awareness on cybersecurity and information technology to employees, suppliers, partners, and relevant stakeholders.

14) Provide channels for whistleblowing and receiving complaints, a complaint handling process, whistleblower protection, and performance notification for internal and external stakeholders affected by the Company's business operations in a systematic and fair manner.

Duties and Responsibilities

To ensure that cybersecurity and information technology policies are implemented throughout the organization and that clear oversight is in place, the Company sets forth the following responsibilities of individuals or departments within the organization:

Board of Directors

1) Consider approving and reviewing current cybersecurity and information technology policies and measures to be appropriate to the environment and risk factors by reviewing them at least once a year.

2) Supervise business operations to be in line with relevant laws, rules, regulations, policies, and guidelines, as well as encourage concrete implementation of this policy.

3) Supervise and encourage management to assess cybersecurity and information technology risks and allocate resources to ensure appropriate and adequate risk control effectiveness.

4) Consider reports on risks and performance in accordance with cybersecurity and information technology policies and measures, and make useful recommendations to management for development and improvement.

5) Consider urgent issues related to cybersecurity and information technology to ensure timely action.

6) Encourage and support executives to recognize and prioritize cybersecurity and information technology and cultivate a corporate culture.

Executives

1) Provide rules, procedures, and preventive measures appropriate to the context of each company and in accordance with the policies, procedures, and laws of the countries in which the Company conducts business.

2) Establish an organizational structure with responsible individuals and clear responsibilities and roles while allocating appropriate and adequate resources.

3) Establish cybersecurity and information technology strategies and plans, including business continuity management.

4) Provide the development and review of adequate and effective risk management, internal control, and internal audit systems on cybersecurity and information technology.

5) Monitor, supervise, manage, and support employees, suppliers, business partners, and key stakeholders to comply with relevant laws, policies, measures, and procedures, as well as developing and improving practices to be more effective.

6) Act as a good role model by avoiding any activity that may lead to situations or suggestions that could result in policy violations.

7) Encourage subordinates at all levels to recognize the importance of policy compliance and cultivate it as a corporate culture.

8) Create and promote awareness and understanding of cybersecurity and information technology by communicating to employees and relevant stakeholders on an ongoing basis.

9) Consider the report on the performance of the policy before presenting it to the Board of Directors.

10) Provide channels for whistleblowing and receiving complaints about violations of cybersecurity and information technology policies, including complaint handling processes and protection measures for whistleblowers, complainants, witnesses, and information reporters.

Departments or Individuals Responsible for Cybersecurity and Information Technology

1) Establish relevant procedures and measures to prevent potential cybersecurity and information technology violations.

2) Establish a clear information disclosure and reporting process for cybersecurity and information technology.

3) Assess and manage cybersecurity and information technology risks that cover threats, vulnerabilities, likelihood, and impact on assets, organizational personnel, and related external entities, as well as guidelines on prevention and mitigation.

4) Develop internal control, risk management, and policy compliance monitoring to be effective and concise, as well as informing and following up with relevant departments for regular improvement and correction.

5) Follow up, inspect, collect, and store reports on cybersecurity and information technology, and disclose information in accordance with requirements of the regulatory authorities.

6) Regularly report information about risks or threats on cybersecurity and information technology to management and report immediately in the event of an abnormality.

7) Coordinate and integrate cooperation with relevant individuals, agencies, or stakeholders to jointly establish measures, management, and mechanisms for control, response, and problem solving.

8) Communicate and train to raise awareness about cybersecurity and information technology to employees and relevant stakeholders on an ongoing basis.

9) Provide initial suggestions on the implementation of the policy, as well as coordinate or discuss with other relevant departments to ensure that the suggestions are correct, complete, and clear.

10) Report the results of the policy compliance to the Board of Directors, executives, or relevant agencies.

11) Review cybersecurity and information technology policies in accordance with relevant laws, regulations, practices, and standards.

<u>Employees</u>

1) Learn, understand, and comply with laws, rules, regulations, policies, and guidelines, including relevant standards.

2) When someone is found to have committed an offense or committed an act that violates this policy, the information or complaint must be reported through the Company's whistleblowing channels.

Communication and Training

The Company provides communication of cybersecurity and information technology policies through appropriate training, orientation, meetings, or activities in various forms that are appropriate for the directors, executives, employees, subsidiaries, associates, other companies over which the Company has control, business representatives, and suppliers, as well as relevant stakeholders, and evaluates their effectiveness and makes continuous improvements.

Whistleblowing

Those who see an action that qualifies as a violation of this policy must complain or report it according to the procedures of the whistleblowing policy. The complainant or whistleblower will be protected, and the information will be kept confidential without impacting their position or compensation, both during the investigation and after the completion of the process.

Penalty

The cybersecurity and information technology policy is considered part of the discipline of the work. Directors, executives, and employees who do not comply must be investigated and considered for disciplinary action in accordance with the Company's regulations, charters, and related laws. This may include dismissal. In the event of an investigation, all employees must fully cooperate with internal and external agencies.

In the meantime, the Company will not demote, punish, or adversely affect directors, executives, and employees who reject actions intended to violate this policy, even if such actions cause the Company to lose business opportunities.

Therefore, this notification is announced for acknowledgment and thorough observance.

Announced on February 25, 2025.

- Signature -

(Dr. Apichart Chinwanno)

Chairman of the Board of Directors