Information Security Policy

and Responsible Development of Artificial Intelligence Technology

Teka Construction Public Company Limited

Teka Construction Public Company Limited recognizes the importance of managing information security and developing Artificial Intelligence (AI) technology safely and ethically to support the changes in the digital age and create sustainable value for the business and all stakeholders. Therefore, the Board of Directors has approved a policy on responsible information security and AI development to provide guidance for all relevant parties in their operations.

Translation

1. Scope of Policy

This Information Security and Responsible Artificial Intelligence Development Policy applies to all levels of company personnel, including permanent and temporary employees, managers, partners, and related parties who are assigned or authorized to access company data or technology systems. This policy covers the storage, use, and protection of all types of company data, including financial data, business operations data, and personal data of customers, partners, employees, and all stakeholders, as well as the ethical and secure development and use of Artificial Intelligence (AI) technology.

2. Objectives

• To prevent data leakage, unauthorized access, and cyberattacks that may cause damage to the company's data and technology systems.

• To ensure that the company's AI development and use are secure, transparent, fair, and do not create negative impacts on any stakeholders.

• To ensure that information security and AI operations comply with relevant laws, regulations, and standards, such as the Personal Data Protection Act (PDPA) and the principles of good governance as outlined in the company's code of ethics and corporate governance principles.

• To build confidence in the company's transparency and reliability in managing data and using technology responsibly.

• To ensure that information security and AI management aligns with the Sustainable Development Goals (SDGs) and enhances the company's long-term competitiveness.

3. Duties and Responsibilities

In order to ensure effective information security management and artificial intelligence technology development across all levels of the organization, and in alignment with the company's business direction, the duties and responsibilities of relevant departments and individuals are defined as follows:

3.1 Board of Directors

• Approve and oversee information security policies and the responsible development of artificial intelligence technology in alignment with the company's strategic goals and governance guidelines.

• Provide strategic advice to senior management to promote technological sustainability and risk prevention.

3.2 Senior Management

• Allocate sufficient and appropriate resources, such as personnel, budget, and technology, for information security and AI operations.

• Monitor progress of operations and threat management, including regular system audits and security assessments.

• Support the development of ethical AI management processes and ensure that AI development aligns with company guidelines.

Translation

• Promote knowledge, understanding, and awareness among employees and partners, emphasizing the importance of information security and the ethical use of AI.

• Report key information security operations and challenges periodically to the company board or relevant sub-committees.

3.3 Relevant Agencies

• Develop a secure and compliant system for storing and managing AI-related information and data.

• Conduct cybersecurity threat monitoring and develop appropriate response plans.

• Coordinate with management and relevant external agencies in managing risks and disputes.

• Monitor technology trends and threats related to information security and AI to recommend up-to-date development guidelines.

• Train relevant personnel to understand the systems and tools related to security management.

3.4 Employees

• Adhere to company policies, practices, and measures regarding information security and AI.

• Use company data and technology appropriately, avoiding actions that may lead to damage or infringement of rights.

• Report any cyber threats, data breaches, or inappropriate AI use to supervisors.

• Participate in information security and AI-related training or activities to enhance knowledge and awareness of their critical role.

4. Policies and measures

• All personnel must comply with the specified information security policies and measures. They must protect the company's confidential information, customers, partners, and employees from leakage or unauthorized use.

Translation

• Do not use or disclose internal company information for personal gain or third parties. without approval

• Data access is appropriately managed and controlled. Using a modern security system that complies with relevant standards.

• All personnel must use the Company's technology systems and equipment for work purposes only. Do not use it in a way that may cause damage or safety risks.

• Do not install any software or programs on Company equipment without permission. To prevent the risk of malware or computer viruses.

• The development and use of AI must be done responsibly. Taking into account transparency, fairness and not creating negative impacts on stakeholders.

• People must avoid using AI in ways that create bias or discrimination. And the impact of AI on data privacy must be assessed.

• AI usage must be regularly monitored and evaluated. To ensure compliance with relevant ethical principles and laws.

• The company has strict measures to prevent cyber threats, such as regular system inspections. Data encryption and developing response plans in the event of unexpected events.

• Personnel are responsible for reporting incidents involving threats or violations of system security as soon as they are discovered.

• All personnel have a duty to follow the specified measures and guidelines. Including participating in related training To develop knowledge and understanding of information security and AI.

Translation

• Promote personnel to be conscientious and careful in using the company's information and technology.

• Management of personal information must be in accordance with relevant laws. There are measures to protect the privacy (Privacy) of information in every process.

• The company is committed to following international standards in information and technology management.

• Training, workshops and workshops The content will cover principles of data security and ethical use of AI. Protection against cyber threats and safe management of personal information Training content will be designed to be in line with the job description and needs of the organization. So that personnel can apply them to the work process appropriately.

• Stakeholders can report violations of the information security policy and the development of artificial intelligence technology through the Whistle Blowing channel. The company maintains the information of whistleblowers confidential according to the whistle blowing policy.

1. Directly responsible supervisor or

2. Send an electronic letter to your supervisor. or internal audit office or personnel department or

3. Send by post to the Chairman of the Audit Committee. or directors of the company

4. Notify via https://investor.tekacon.com/th/corporate-governance/whistleblowing

• If it is found that there has been a wrongdoing or violation of the policy. The company will take appropriate punishment according to company discipline. To create transparent

Translation

operating standards Support the development of safe and ethical technology. as well as maintaining the confidence of stakeholders

• The Company requires continuous review and improvement of its information security policy and responsible development of artificial intelligence technology. At least once a year or when there are changes in laws, regulations, or related practices. To ensure that such policies remain appropriate and effective in responding to business and technological changes.

Approved by resolution of the Board of Directors meeting No. 4/2026 on November 4, 2026.
This shall be effective from November 5, 2026 onwards.

Signed .....

(Mr. Poonsawat Phoaprapat)

Acting Chairman of the Board

Translation