



Generative Artificial Intelligence Policy

Krungthai Card Public Company Limited

(Public Version)

Generative Artificial Intelligence Policy

Krungthai Card Public Company Limited

Krungthai Card Public Company Limited and its subsidiaries (“the Company” or “KTC”) recognize the role and importance of emerging technologies, particularly Generative Artificial Intelligence (“Generative AI”), which plays a significant role in social and technological change. Generative AI can also be used to support business operations, improve efficiency and agility, and enhance customer and employee experiences. At the same time, the use of such technology may involve risks that need to be appropriately managed. The Company has therefore established this Policy as a framework for governing the use of Generative AI and managing related risks and impacts in an appropriate, secure, and responsible manner, in compliance with applicable laws, regulations, and requirements, while giving due consideration to information security and data privacy.

Objective

- 1) To establish a framework for managing risks and impacts from the use of Generative AI, including control measures to identify, assess, and mitigate such risks.
- 2) To provide guidelines for the safe and responsible use of Generative AI within the Company, in accordance with applicable laws, ethical principles, and relevant standards, and to protect the Company’s information, customer data, and personal data from unauthorized access, disclosure, or use.

Scope

This Policy covers the management of risks from the use of Generative AI, with a focus on protecting the Company’s information and customer data from unauthorized access, modification, or use, as well as risks from products, services, or solutions provided by third parties, including vendors, suppliers, and outsourcing service providers, that use Generative AI.

Guidelines

1. Risk Management and Security

The Company requires appropriate assessment and management of risks that may arise from the use of Generative AI, including risks related to data, cybersecurity, vulnerabilities, and potential impacts on the Company, customers, and stakeholders. The Company shall review the risk assessment on a regular basis or upon any significant changes and shall conduct security testing and assessments of relevant systems, as appropriate, to ensure that the use of Generative AI complies with applicable internal policies and external requirements.

2. Approval and Control of Use

The use of Generative AI shall be subject to the Company's prescribed review and approval process, which shall consider security, privacy, risk management, potential business impacts, and compliance with applicable laws, regulations, and relevant standards.

The Company permits the use of only systems or tools that have been formally approved and shall establish appropriate access controls based on users' roles and responsibilities.

For products, services, or systems provided by third parties that use Generative AI, an assessment must be conducted in accordance with relevant policies. Where appropriate, the Company shall also consider including contractual requirements relating to the use of Generative AI.

3. Data Privacy and Security Protection

The Company places importance on the appropriate control and protection of data submitted to and generated by Generative AI, taking into consideration the classification and sensitivity of the data. The Company shall define categories of data that are prohibited from being submitted to Generative AI, including actual personal data, financial information that has not been authorized for disclosure, and confidential business information. Data submitted to Generative AI shall be limited to what is necessary for the intended purpose and shall be subject to appropriate security measures throughout the data lifecycle.

4. Use and Review of Outputs

The use of Generative AI is intended to support work performance. Users should have sufficient knowledge or expertise in the relevant subject matter and shall ensure that Generative AI outputs are reviewed by a subject matter expert or their supervisor, as appropriate, before use. Generative AI outputs shall be treated as supporting information and not as final results. Users shall be aware of the limitations and risks of Generative AI and shall consider the confidentiality, accuracy, and objectivity of the information. Users are also responsible for carefully reviewing and correcting outputs that may contain bias, inaccurate conclusions, or conclusions that are unreasonable or unsupported.

5. Incident Response and Disciplinary Actions

The Company requires any actual or suspected data leakage involving Generative AI or other AI tools to be reported immediately. This includes cases where Confidential or Restricted data is submitted to the system, or access rights are granted to employees or other individuals without authorization. The Company shall suspend or revoke the relevant access rights and investigate the incident to establish the facts and determine the appropriate action in accordance with applicable internal rules and regulations.

6. Training and Awareness

The Company shall provide employees with ongoing training and awareness programs on the risks associated with the use of AI systems or tools, as well as safe use practices. Employees who use Generative AI or create work with Generative AI shall complete training on relevant policies and guidelines. Employees who are authorized to use Generative AI shall read, understand, and acknowledge the terms of use under this Policy prior to using Generative AI, with such acknowledgment retained as evidence.

Policy Review

This Policy shall be reviewed at least annually or when there are significant changes that may affect its implementation, including changes in laws, regulations, business operations, technology, or emerging AI-related risks.

This Policy has been approved by the Board of Directors and shall be effective from the date of approval.