



Responsible Artificial Intelligence Policy

Our Commitment

KBank is committed to developing and using Artificial Intelligence (AI) responsibly to create sustainable value for customers, employees, shareholders, business partners, and society. The Bank has established an AI governance and risk management framework based on Responsible AI Principles to ensure that AI is developed, deployed, and used within acceptable risk levels while complying with applicable laws, regulations, and internationally recognized standards.

Our Responsible AI framework is guided by the following principles:

1. Reliable Outcomes
2. Ethical and Lawful Use
3. Safety and Security
4. Accountability and Explainability
5. Respect for Privacy
6. Fairness and Freedom from Bias

KBank expects all directors, management, employees, and relevant third parties involved in the development, deployment, or use of AI to adhere to the following commitments.

1. Respect Data Privacy

We respect individuals' privacy and ensure that AI systems are developed and used in compliance with Thailand's Personal Data Protection Act (PDPA) and KBank's internal privacy governance framework. Personal data shall be collected, processed, and protected responsibly throughout the AI lifecycle.

2. Protect Cybersecurity

We safeguard AI systems and support infrastructure by implementing appropriate cybersecurity standards and controls to protect against unauthorized access, cyber threats, and other security risks.

3. Promote Fairness and Mitigate Bias

We seek to prevent unfair bias and discriminatory outcomes by incorporating appropriate risk assessments, testing, monitoring, and governance throughout the design, development, deployment, and operation of AI systems.



4. Maintain Human Oversight

We ensure appropriate human oversight for AI systems ("Human-in-the-loop" or "Human-over-the-loop"), particularly where AI may significantly affect individuals, customers, or society. Human intervention remains available to review, validate, override, or discontinue AI-assisted decisions when necessary.

5. Ensure Transparency and Explainability

We promote transparency by establishing governance, assurance, and audit processes that support the explainability, trustworthiness, and responsible use of AI systems. AI-generated outputs should be understandable to an appropriate extent based on the nature and level of risk.

6. Establish Accountability

We recognize that AI is a decision-support tool and does not replace human responsibility. Users are responsible for reviewing, validating, and applying their professional judgment before acting on AI-generated outputs. Accountability for decisions and outcomes always remains with the designated human decision-maker, while AI governance and risk relevant units oversee compliance, risk management, and the responsible use of AI across the organization.

7. Define Appropriate AI Boundaries

We define clear boundaries for AI use through a structured approval process covering Use Case, Objective, Exit Criteria, and Risk Assessment under the AI Criticality framework, evaluating the permitted scope based on potential adverse impact before deployment. Ongoing monitoring ensures AI is not used beyond the approved scope or scaled to production without approval from the relevant governing bodies.

8. Promote Environmentally Responsible AI

We strive to minimize the environmental impact of AI by improving the efficiency of AI infrastructure, optimizing computing resources, and encouraging the use of energy-efficient AI models and technologies. We also support collaboration with industry and academic partners to advance sustainable AI practices.

9. Prohibit Unacceptable AI Practices

In line with KBank's Responsible AI Principles particularly Ethical & Lawful Use and Fair and Unbiased, which align with the EU AI Act, we ensure AI is used only for its approved purpose, within its defined scope and acceptable risk level. AI must not be used for manipulative or deceptive practices, exploitation of vulnerable individuals or groups, unlawful social scoring, unauthorized biometric surveillance, or in ways that violate fundamental rights, privacy, equality, or result in discriminatory treatment.