Cathay Financial Holdings (Cathay FHC) and Subsidiaries'

Artificial Intelligence (AI) Governance Policy

Approved by the board of directors on 15th August, 2024

Responsible Unit: Data & AI Development Department

Article 1 Objectives

Cathay Financial Holdings (hereinafter referred to as "Cathay FHC") and its subsidiaries (hereinafter collectively referred to as "the Group") have established this Policy to develop responsible artificial intelligence (AI), effectively manage the related risks associated with the Group's use of AI. This Policy also aims to protect consumer privacy and customer rights while taking into account social fairness and ecological responsibility.

Article 2 Scope of Application

This Policy applies to all AI-related activities within the Group, covering any phase of the AI lifecycle utilized by Cathay FHC, its subsidiaries, or through inter-company collaborations within the Group. Exceptions to this Policy are only applicable where explicitly stipulated by law.

Article 3 Definitions

I. Subsidiaries: Financial subsidiaries directly or indirectly controlled by Cathay FHC, excluding foreign subsidiaries or branches, unless otherwise required by law.

II. Artificial intelligence (AI): refers to the technology that simulates human learning, thinking, and response patterns through large-scale data learning, utilizing machine learning or related modeling algorithms for tasks such as perception, prediction, decision-making, planning, reasoning, and communication.

III. Generative AI: Refers to AI that can generate content that resembles content created by human intelligence in the form of but are not limited to, articles, images, audio, video, and code.

IV. AI Governance: Refers to the management measures of the use of AI, including but not limited to the frameworks and standards for AI research, development, and application to comply with laws and regulations and to ensure information security, fairness, and respect for human rights, while fostering innovation and trust.

V. AI lifecycle: Refers to the four stages of AI utilization: "system planning and design," "data collection and input," "model building and validation," and "system deployment and monitoring." The first three stages are collectively referred to as "implementation," the fourth stage as "usage," and all four stages together as "application."

Article 4 Six Governance Principles

In developing AI-related technologies and establishing information security control measures, the Group should consider both consumer rights and social responsibilities, and each company should practice AI governance in accordance with the following principles:

I. Establishing Governance and Accountability Mechanisms:

(1) The Group commits to the spirit of responsible innovation by taking on internal and external responsibilities associated with AI use. This includes setting up an internal governance structure, as well as an oversight and accountability mechanism to protect consumer privacy and information security while fostering a culture of responsible AI development.

(2) The Group shall establish a risk management mechanism that makes decisions and provides oversight based on risk assessments. This includes implementing management measures across all stages of the AI lifecycle and conducting regular reviews to continuously improve the effectiveness of the risk management mechanism.

(3) Relevant units or personnel will receive the necessary training and resources to develop sufficient knowledge and skills for AI implementation, use, and management, enabling them to adapt to the rapid development and changes in AI technology. It is also recommended that management gain a clear understanding of AI usage.

(4) When adopting AI products or services from third-party vendors, it is essential to assess whether the vendor possesses the necessary knowledge, expertise, and experience. An oversight mechanism should be established, responsibilities clearly defined, and an exit strategy put in place. All procedures should be carried out in accordance with relevant internal management guidelines.

II. Emphasis on Fairness and Human-Centered Values

(1) The use of AI should be rooted in the principles of fairness and inclusive finance, be consistent with human-centered values, and ensure that humans

remain in control. It should support human autonomy, respect fundamental human rights, and allow for human oversight. Efforts should be made to minimize unfair outcomes caused by algorithmic bias.

(2) Ensure that decisions made using AI are rational and strive to avoid bias as much as possible to prevent discriminatory outcomes against certain groups.

(3) When implementing generative AI, assessments must be made to determine whether it introduces bias or unfairness toward certain groups. If third-party generative AI is used and the fairness of the training process, data, or algorithm is not fully understood, relevant personnel must conduct an objective and professional risk assessment to manage potential risks.

III. Protection of Customer Privacy and Interests

(1) To protect financial consumers, the use of AI must comply with personal data protection regulations. This involves clearly informing consumers about the use of AI, respecting and safeguarding their privacy, managing and utilizing customer data responsibly, and adhering to the principle of data minimization. Attention should be paid to the risks of data leakage associated with the use of AI.

(2) When delivering financial services through AI, customers should be informed that the service is AI-driven. Customers should also be informed of any available alternatives in order to respect the customer's right to optionality.

(3) Alternatives should be evaluated based on their risks, costs, and technical feasibility. If no alternatives are offered, further consideration should be given to providing remedial measures for customers.

(4) Provide channels for customer redress in the event of adverse effects resulting from the use of AI.

IV. Ensuring System Robustness and Security

(1) To enhance information and communication security, AI resilience and data quality should be maintained and continuously improved to ensure the robustness and security of AI systems to prevent harm to consumers or the financial system.

(2) When AI developed or operated by third parties is used to provide financial services, appropriate risk management and oversight of those third parties should be in place. Appropriate controls measures must be in place to mitigate risks arising from improper operations or human error by third parties.

(3) Establish judgment metrics and thresholds for assessing the robustness of AI in use and implement evaluations and risk prevention measures. Contingency procedures or plans should be in place to effectively address unexpected or adverse effects. The concept of robustness should include stability, accuracy, and reproducibility.

(4) Follow relevant information security control protocols and establish appropriate security protection or control measures to prevent the AI in use from being exposed to security threats and attacks.

(5) Assess, plan, and review the security of data environments related to AI.

(6) If AI requires data transmission with other companies within the Group or external entities, appropriate data transmission risk assessments must be conducted to manage exposure levels. Follow relevant data transmission platform management protocols, retain transmission records, and ensure the security of data transmission.

V. Ensuring Transparency and Explainability

(1) To ensure information disclosure, when using AI, attention should be paid to its operational transparency and explainability. When AI is used to interact with consumers, appropriate disclosure should be made. However, if the use of AI is related to anti-money laundering, information security, fraud detection, etc., or if it involves the Group's trade secrets, to avoid other risks arising from excessive disclosure, the necessity and extent of disclosure to parties other than the competent authorities should be carefully controlled.

(2) Common principles of AI transparency should be evaluated, such as the level, timing, and form of explanation provided to customers. This will enhance customer protection and comply with the principles of treating customers fairly.

(3) Common principles of AI explainability should be evaluated, including the level of explainability and the person to which relevant information is provided. The level of explainability should correspond to the significance of the AI application. When using AI developed in-house, by third parties, or operated by third parties, it is important to ensure that relevant personnel understand the operation, prediction, or decision-making processes of the AI in order to manage the AI system and control risks effectively.

VI. Promoting Sustainable Development

(1) In aligning the use of AI with sustainable development, the development and implementation of AI should be guided by sustainability principles to ensure

that social equity and ecological responsibility are prioritized.

(2) Employees should receive appropriate education and training to enhance their understanding of AI. This training should include awareness of energy conservation, reduction of excessive resource consumption, and support for disadvantaged groups in terms of digital resources. This training should help employees adapt to AI-driven changes, protect their employment rights, and support the organization's commitment to sustainable development.

Article 5 Responsible Unit

The Data & AI Development Department is the responsible unit for this Policy. This department is responsible for the overall planning of AI governance-related strategies for the Group. It is also responsible for establishing the internal management framework, AI governance-related management regulations, and risk assessment methodologies for Cathay FHC. The responsible unit shall regularly report to the Cathay FHC Data and AI Governance Committee on the above matters. Additionally, the responsible unit is responsible for overseeing the development, implementation, and risk assessment methodologies of AI across the subsidiaries.

Article 6 Supplementary Provisions

Any matters not addressed by this Policy shall be handled in accordance with relevant internal and external regulations and guidelines.

Article 7 Implementation

The Policy shall take effect upon approval by the board of directors. Amendments or abolishment shall follow the same procedure.