O-Bank Co., Ltd. Artificial Intelligence Technology Application Policy

Amended by the 10th Board of Directors in its 2nd Meeting on June 24, 2026

Article 1 (Purpose and Basis)

In accordance with the "Guidelines for Artificial Intelligence (AI) Applications in the Financial Industry" and the "Directions for Financial Institutions Engaging in the Application of Artificial Intelligence (AI) Technology", this Policy is hereby established to facilitate the development of Artificial Intelligence (AI) within the Bank and to strengthen the protection of client assets and risk management in the application of AI technology across banking operations.

In view of the increasing application of AI in financial services—which enhances financial market efficiency, reduces costs, improves customer experience, strengthens risk management, facilitates compliance, prevents financial crime, defends against cybersecurity incidents, and promotes sustainable development—this Policy serves as a definitive framework for all personnel within the Bank’s organization to follow.

Article 2 (Definitions of Artificial Intelligence)

Artificial Intelligence (AI) as referenced in this Policy shall include Generative AI.

1. Artificial Intelligence (AI): Refers to technologies that learn from large-scale datasets and utilize machine learning or associated modeling algorithms to mimic human learning, cognitive, and behavioral patterns. These capabilities include, but are not limited to, perception, prediction, decision-making, planning, reasoning, and communication.
2. Generative AI: Refers to related technologies that learn from large-scale datasets to generate content that simulates human intellectual creativity. Such content forms include, but are not limited to, text, images, audio, photographs, video, and source code.

Article 3 (Scope of Application)

When applying Artificial Intelligence (AI) technology to client asset protection and risk management operations, the Bank shall conduct assessments in accordance with the risk assessment criteria and procedures authorized by the President. Based on the assessment results, it shall be determined which of the following scenarios apply:

1. Interactions with consumers[1].
2. Provision of financial product recommendations.
3. Provision of customer services.
4. Material impact on clients' financial transaction rights and interests.
5. Significant impact[2] on the Bank's business operations.

The aforementioned risk assessment criteria and procedures shall be separately established by relevant units, senior executives, or personnel designated by the President.

Article 4 (Principles and Considerations for the Use of Artificial Intelligence)

1. Protection of Privacy and Customer Rights
   (1) The Bank shall strictly comply with financial regulations and other statutory requirements regarding cybersecurity, personal data protection, and intellectual property rights, as well as all relevant data usage rules.
   (2) When interacting with consumers, the Bank shall inform or disclose the specific target populations, applicable scenarios, or designated purposes of such interactions or automated financial services. Consumers shall be given the autonomy to choose whether to utilize the service, and shall be informed of alternative options, except where otherwise provided by applicable laws and regulations.
   (3) The Bank is strictly prohibited from developing or deploying AI

[1] Consumer: Refers to an individual or entity that accepts financial products or services provided by a financial services provider. However, this term excludes the following: (i) Institutional professional investors; and (ii) Natural or legal persons meeting specific financial capacity or professional expertise criteria.

[2] Significant impact on the Bank's business operations: Refers to the explanations regarding the conditions of "materiality" set forth in Article 4, Paragraph 5 of the "Regulations Governing Internal Operating Systems and Procedures for the Outsourcing of Financial Institution Operations."

systems that are manipulative or deceptive, or that exploit individual vulnerabilities to distort behavior. Furthermore, the use of AI for social scoring or unauthorized real-time remote biometric identification surveillance is strictly banned, thereby safeguarding clients' personality rights and behavioral autonomy.

2. Ensuring System Robustness and Security
   (1) Throughout the processes of data processing, storage, transmission, and usage, the Bank shall diligently protect the data privacy of both individuals and the organization, and implement appropriate protective measures to ensure system robustness and data security. This includes deploying relevant security technologies to prevent, detect, and respond to various security threats and attacks—such as hacking and malware—thereby preventing data breaches or unauthorized access.

3. Implementing Transparency and Explainability
   (1) When utilizing Artificial Intelligence (AI) technology to interact with consumers, the Bank shall explicitly inform them that the interaction is executed automatically through the aforementioned technology.
   (2) During the model training phase of AI technology, the Bank shall ensure security when selecting relevant tools such as models or algorithms, and shall adopt effective measures to enhance model explainability and training quality. These actions aim to prevent the generation of inappropriate information, thereby improving the accuracy and reliability of the overall AI outputs or generated content.
   (3) Where financial transactions are involved, the Bank shall understand how decisions are made and enhance the explainability of the models to ensure the effective management and oversight of AI operations.

4. Ensuring Fairness
   (1) Throughout the stages of algorithm design, development, data collection, training data selection, processing, model construction,

generation, optimization, and subsequent application to financial services, the Bank shall implement anti-discrimination measures to comply with the Principle of Treating Customers Fairly in the Financial Services Industry.

(2) When addressing issues of unfairness or bias in AI as mentioned in the preceding paragraph, the Bank shall evaluate whether to include parameters of customers' personal attributes (such as name, nationality, ethnicity, place of birth, residence, or age), medical conditions, or physiological characteristics in the algorithmic decision-making process. Furthermore, the Bank shall assess risks from cybersecurity, legal compliance, and risk management perspectives, and proceed in accordance with internal procedures.

5. Establishing Governance Structure and Accountability Mechanisms

(1) The Bank shall foster internal knowledge regarding Artificial Intelligence (AI) technology and shall designate senior executives or a committee to be responsible for establishing AI-related oversight, management, and internal governance frameworks.

(2) The Bank shall assign appropriate units or personnel to handle the promotion and management of AI, implement AI talent development initiatives, provide adequate training resources, and ensure that personnel involved in AI operations possess the specialized knowledge corresponding to their duties.

(3) Personnel responsible for utilizing Generative AI technology shall have a clear understanding of how Generative AI technology operates and how it formulates responses.

(4) The Bank shall assign appropriate units or personnel to participate in the decision-making processes of AI systems, including monitoring and final approvals. Such units or personnel shall be granted the authority to intervene, modify, or terminate system operations when necessary, ensuring that AI system risks remain within a controllable range.

(5) In the event of damages resulting from the use of AI, incident

reporting shall be conducted in accordance with the Bank's internal regulations[3]. The Bank shall implement responsive measures including investigation, remediation, and incident logging, while rigorously carrying out damage assessments and determining legal liability.

The designation of the aforementioned units, senior executives, or personnel shall be separately authorized and determined by the President.

6. Promoting Sustainable Development
   (1) In alignment with the Bank's sustainable finance strategies and implementation directions, the Bank shall appropriately incorporate comprehensive sustainability metrics based on international sustainable development goals and its own self-defined sustainability principles. This incorporation aims to leverage Artificial Intelligence (AI) to facilitate the execution of the aforementioned sustainability targets (e.g., the application of AI in promoting financial inclusion).
   (2) Whether developing AI internally or collaborating through outsourcing, the Bank shall prioritize the selection of technologies or infrastructures with a low ecological footprint, thereby minimizing the energy consumption derived from the utilization of AI.

Article 5 (Oversight and Management of Artificial Intelligence Use)

1. Where the Bank develops or optimizes AI technologies in-house, necessary technical documentation and related records shall be retained. This includes critical data, models, or algorithms recorded during the design, development, and implementation processes by developers that may influence decision-making, thereby ensuring auditability when necessary.

[3] Internal regulations: Refers to the "Directions for Information Security Incident Management," the "Directions for Operational Risk Event Data Collection," and other internal regulations related to incident reporting.

2. Where third-party AI technologies are utilized, the Bank shall perform due diligence, assessments, and continuous monitoring to ensure that third-party vendors maintain their own audit trails of AI computations, facilitating subsequent verification and audits.
3. When introducing third-party AI technologies, the Bank shall require vendors to provide relevant information and shall clearly define the scopes of liability to prevent any associated adverse impacts.

Article 6 (Risk Management Mechanisms)

1. Prior to utilizing Artificial Intelligence (AI) to provide financial services, the business unit applying the technology shall conduct an assessment focusing on data governance methodologies, cybersecurity, oversight mechanisms, consumer rights protection, and contingency measures for unexpected incidents. The assessment shall clearly define the authorized scope of application, capability limitations, and control points to prevent misuse or unintended use. The contents of such assessments shall be submitted in advance to the Bank's cybersecurity, legal compliance, and risk management units for their review and input.
2. The Bank's utilization of AI shall be guided by a risk-based approach. Commensurate with its scale of operations, the Bank shall establish appropriate risk management and periodic review mechanisms to continuously monitor whether the AI is applied within the designated authorized scope. Depending on the size, characteristics, or scope of the associated risks, an independent third party with AI expertise may be engaged to issue an objective and professional assessment and control report. The report shall encompass data quality, model quality, system security, as well as fairness, sustainable development, transparency, and explainability. Strategies and measures shall be adjusted and improved based on the assessment results. Similarly, when utilizing Generative AI, the Bank remains responsible for evaluating and controlling the risks associated with its generated outputs.

Article 7 (Outsourcing of Operations)

Where any Artificial Intelligence (AI) operations involving business items listed on the Bank's business license or involving customer information are outsourced, such outsourcing shall be handled in strict accordance with the "Regulations Governing Internal Operating Systems and Procedures for the Outsourcing of Financial Institution Operations."

Article 8 (Internal Control)

Units utilizing Artificial Intelligence (AI) technology that meet the aforementioned criteria shall incorporate the contents of this Policy into their internal control systems, and shall periodically review and verify the effectiveness of such internal controls.

Article 9 (Supplementary Provisions)

Any matters not explicitly covered herein shall be governed by and handled in accordance with the laws and regulations of the competent authorities as well as the relevant internal regulations of the Bank.

Article 10 (Implementation and Amendment)

This Policy, and any amendments hereto, shall become effective upon approval by the Board of Directors.

Matters regarding the application of Artificial Intelligence (AI) technology covered under this Policy through to its termination shall be determined by the authorized executives set forth in the Bank's Table of Delegation of Authority, or by department-level heads authorized by the President.

Revision History:

Version	Approval Date	Revision Description	Responsible Unit	Approval Authority
V1	May 2, 2025	New Issuance	Strategic Planning Department	Approved by the 9th Board of Directors in its 18th Meeting on May 2, 2025.
V2	Feb 4, 2026	Amended Articles 3 and 4, and made minor textual refinements pursuant to Government Directive No. 1140001939. Effective February 5, 2026, the Responsible Unit was changed to the Digital Strategy Department.	Strategic Planning Department	Amended by the 9th Board of Directors in its 24th Meeting on February 4, 2026.
V3	June 24, 2026	Incorporated relevant clauses in alignment with the Responsible AI Governance Framework released in the 2026 S&P Global CSA.	Digital Strategy Department	Amended by the 10th Board of Directors in its 2nd Meeting on June 24, 2026.