Shanghai Rural Commercial Bank Co., Ltd.
Key Points of the Responsible Artificial Intelligence Policy
(2026 Edition)

I. Purpose

To adapt to FinTech development trends and the innovative application of artificial intelligence (AI) models, further standardize the model management of Shanghai Rural Commercial Bank (hereinafter referred to as "SHRCB" or "the Bank") and elevate its model management capabilities, the Bank has formulated measures such as the *Measures for Model Management of SHRCB*, the *Regulations on Model Verification Management of SHRCB*, and the *Measures for the Management of Data Security of SHRCB,* in alignment with its digital transformation strategy and practical conditions.

II. Management Structure

The Bank has established the Model Management Committee under the Senior Management level as its specialized body for model review. The Committee is primarily responsible for conducting model reviews within its scope of responsibilities, undertaking decision-making and approval on model-related matters, and hearing reports on model management work, among other duties.

The Bank has established a Three Lines of Defense mechanism for model risk management. Model owners serve as the First Line of

Defense for the Bank's model risk management, and are responsible for tasks including model development, optimization, and retirement. The Risk Management Department of the Head Office serves as the Second Line of Defense for the Bank's model risk management, and is responsible for tasks including classification and grading management of models and their effectiveness assessment. The Audit Department of the Head Office serves as the Third Line of Defense for the Bank's model risk management, and is responsible for conducting independent and objective audit supervision and evaluation of the Bank's model management.

III. Management Requirements

1. Model Classification and Grading Management

The Bank implements classified and graded management of models based on management requirements, model application scenarios, and the degree of reliance placed on models in approval decisions. Model categories and classification standards are uniformly formulated and maintained by the Risk Management Department of the Head Office.

2. Model Lifecycle Management

The Bank implements unified management over the development and application of AI models, establishes an admission mechanism for externally sourced models and algorithm products, and proactively manages the model research and development process, to ensure that model algorithms are verifiable, auditable, and traceable.

The Bank explicitly stipulates that prior to deployment, information systems and model algorithms must undergo rigorous review. This scrutiny assesses the rationality, legitimacy, and interpretability of data and model usage, as well as the impact of data utilization on the legitimate rights and interests of relevant subjects, potential ethical and moral risks, and the efficacy of preventative and control measures, thereby eradicating major tech ethics risks at the source.

When conducting business using AI technology, the Bank shall provide explanations and disclosure information regarding the impact of data on decision-making outcomes, monitor automated processing and system operating results in real time, and establish risk mitigation measures for AI applications, including formulating alternative plans for exiting AI applications, and developing contingency plans and conducting drills to address security threats.

Following model deployment, model owners shall continuously monitor the models and comprehensively assess their effectiveness. If material issues are identified during monitoring and an impact assessment determines that continued use of the model would result in material adverse impacts, the models shall be optimized or retired.

3. Data Security and Intellectual Property Protection

Model owners shall, in accordance with the *Measures for the*

Management of Confidentiality of SHRCB, strictly implement the confidentiality management system for all model-related materials, and strictly control the scope of access on a need-to-know basis.

The Bank establishes a comprehensive cybersecurity defense system adaptable to on-premises environments, cloud environments, and distributed architectures, deploys a variety of security equipment and software, including firewalls, intrusion detection, malicious code detection, desktop management, web application firewalls, web page anti-tampering, data loss prevention, and operation and maintenance bastion hosts, thereby minimizing the risk of data breach incidents to the greatest extent possible.

Model owners shall, in accordance with the *Measures for the Management of Intellectual Property Rights of SHRCB*, properly implement relevant intellectual property protection for eligible models.