King's Town Bank Anti-Money Laundering and Countering Terrorism Financing Policy

Article 1: Purpose

To strengthen the Group's overall anti-money laundering and countering terrorism financing mechanism, the Bank has hereby formulated the "King's Town Bank Anti-Money Laundering and Countering Terrorism Financing Policy" (hereinafter "the Policy") for compliance by the Bank and its subsidiaries.

Article 2: Applicable Subjects

The applicable subjects of this Policy are the Bank and its subsidiaries that meet the definition of "financial institution" stipulated in Article 5, Paragraph 1 of the Money Laundering Control Act (hereinafter "subsidiaries") and all of their employees.

The Bank's other affiliated enterprises that do not fall under the definition of "financial institution" in the preceding Paragraph must also refer to this Policy or handle the matters according to the anti-money laundering and countering terrorism financing regulations formulated by the competent authorities of the industry to which they belong.

Article 3: Money Laundering and Terrorist Financing Risk Identification, Assessment, and Management

The Bank and its subsidiaries shall refer to the relevant risk prevention plan regulations or templates developed by the industry's competent authorities or the industry association to which they belong, as well as develop and review relevant plans, methods, and control measures for identifying, assessing, and managing money laundering and terrorist financing risks on a regular basis.

The Bank and its subsidiaries must designate the responsible units to conduct risk assessments and implement measures to prevent money laundering and terrorist financing. These measures allow the management to gain a clear understanding of the overall money laundering and terrorist financing risks they may face. Based on this understanding, the management can determine which mechanisms to establish, develop appropriate mitigation measures, and revise prevention plans in a timely manner. The institution's risk assessment report shall be submitted to the Bank's board of directors, and the risk assessment report must be delivered to the competent authority for inspection.

The Bank should conduct a money laundering and terrorist financing risk assessment of the product and establish corresponding risk management measures to reduce the identified risks before launching a new product or service or handling a new type of business.

Article 4: Anti-Money Laundering and Countering Terrorism Financing Plan

The Bank shall develop a Group-wide Anti-Money Laundering and Counter-Terrorism Financing Plan based on relevant laws and regulations, the results of money laundering and terrorist financing risk assessments, and the business operation scale. However, the subsidiaries may adjust the contents included in the preceding Plan based on the nature of their business as long as they do not violate the law.

To revise this Policy and the standard operating procedures for its implementation, the Bank and its subsidiaries must refer to the Group-level Anti-Money Laundering and Countering Terrorism Financing Plan, as well as the guidelines governing anti-money laundering and counter-terrorism financing templates developed by the industry associations to which the Bank and its various businesses belong. The Policy shall be included in the self-inspection and internal audit items and strengthened when necessary to supervise and control compliance with the anti-money laundering and countering terrorism financing-related laws and regulations.

Article 5: Information Sharing

The Bank and its subsidiaries may share information to prevent money laundering and combat terrorist financing, provided that it complies with the data protection regulations of the Bank and its subsidiaries. However, the exchanged information shall be kept confidential, and appropriate security protection measures must be taken as stipulated in the information-sharing procedure for compliance.

Article 6: Anti-Money Laundering and Countering Terrorism Financing Culture

The board of directors of the Bank and its subsidiaries are ultimately responsible for ensuring the establishment and maintenance of appropriate and effective anti-money laundering and countering terrorism financing internal control systems. The board of directors and senior management must understand the money laundering and terrorist financing risks and the anti-money laundering and countering terrorism financing mechanism operations and take measures to create a culture that values anti-money laundering and countering terrorism financing.

Article 7: Customer Identity Confirmation and Due Diligence

The Bank and its subsidiaries shall identify and verify customers using a risk-based approach pursuant to relevant laws and regulations. Customer identification and verification measures must at least include:

I. Appropriate risk management mechanisms must be adopted to verify whether customers, their beneficial owners, and senior management are current or former important political figures in domestic and foreign governments or international organizations. The scope, verification, and risk assessment of important political figures, their family members, and persons with close ties must also be performed.

II. The Bank shall review the identity information of existing customers based on their importance and risk level, inspect the information obtained to identify the customer and the beneficial owner and ensure that the information is updated, especially for high-risk customers. Simplified measures may be adopted for low-risk situations, and the degree of simplification shall be proportional to the low-risk factors.

III. The Bank must understand the purpose and nature of the business relationship with the customer and obtain relevant information to ensure that the transactions executed are consistent with the customer and its business and risks depending on the circumstances. When necessary, the Bank must also identify the source of the customer's funds.

IV. The Bank shall re-verify the customer's identity if it has any doubts about the authenticity or appropriateness of the customer's information, if the customer is suspected of money laundering or terrorist financing transactions, or if there is a significant change in the way the customer's transactions or account are operated that is inconsistent with the customer's business characteristics.

V. The Bank shall temporarily suspend transactions or terminate business relationships with customers who refuse to cooperate with the review; refuse to provide information about the beneficial owner or person in control of the customer; or refuse to cooperate with an explanation of the nature, purpose, or source of funds of the transaction.

VI. The Bank shall not perform the customer identification procedures if it suspects that the customer or transaction may be involved in money laundering or terrorist financing and if it is reasonable to believe that performing the procedures may reveal information to the customer. Instead, the Bank shall report the transaction

as a suspected money laundering or terrorist financing transaction case.

VII. When the Bank verifies the identity of a customer, if some relevant laws and regulations require the Bank to refuse to establish a business relationship, transaction, or service, the Bank shall comply with such laws and regulations.

Article 8: Customer and Transaction Counterparty's Name and Title Verification

The Bank and its subsidiaries shall conduct name and title verification on customers, senior management personnel of customers, beneficial owners, and related parties to the transaction based on the risk-based approach and relevant laws and regulations; and formulate customer and transaction counterparty name and title verification procedures for compliance.

The scope of the name and title verification in the preceding paragraph shall include whether it is an important political person; a person or entity subject to economic sanctions; a terrorist or organization identified by a foreign government or international anti-money laundering organization; or an individual, legal person, or entity designated for sanctions under the Counter-Terrorist Financing Act.

Article 9: Ongoing Account and Transaction Monitoring

The Bank and its subsidiaries shall establish account and transaction monitoring policies and procedures based on a risk-based approach. These policies and procedures shall at least include the following: complete monitoring types, parameter settings, amount thresholds, early warning cases, implementation procedures for monitoring operations, review procedures for monitoring cases and reporting standards. The Bank shall also employ information systems to assist in identifying suspected money laundering or terrorist financing transactions and formulate ongoing account and transaction monitoring procedures for compliance.

The Bank shall develop the money laundering or terrorist financing transaction risk indicators that are in line with the Bank's situation based on its asset scale, geographical distribution, business characteristics, customer nature, and transaction characteristics with reference to the internal money laundering and terrorist financing risk assessment or daily transaction information. The goal is to identify potential money laundering or terrorist financing alert transactions. (For example, a customer frequently transfers funds between multiple different customer accounts, and the amount reaches a certain level. Multiple deposits exceeding a certain amount or a certain number of deposits are intensively deposited into a deposit account and then transferred quickly.) If the Bank discovers or has reasonable grounds to suspect that

a customer, the customer's funds, assets, or their intended/completed transactions are related to money laundering or terrorist financing, the Bank shall conduct further identity checks on the customer, regardless of the amount or value of the transaction or whether the transaction has been completed. If the Bank determines that there is a suspected money laundering or terrorist financing transaction, it shall report the transaction to the Financial Intelligence Unit in addition to verifying the customer's identity and keeping records of the transaction regardless of the amount of the transaction or whether the transaction has been completed.

Article 10: Record Preservation

The Bank and its subsidiaries shall preserve all records obtained from verifying customer identity, records and vouchers of customer transactions, and records and vouchers of reports on cash transactions exceeding a certain amount and suspected money laundering or terrorist financing transactions for at least five years according to the relevant laws and regulations.

Article 11: Transaction Reporting

The Bank shall report cash transactions exceeding a certain amount to the Financial Intelligence Unit based on the risk-based approach. The scope and method of reporting shall conform to the relevant regulations promulgated by the competent authority. If it is determined that there is a suspected money laundering or terrorist financing transaction, the Bank shall, in addition to verifying the customer's identity and preserving records of the transaction, report the transaction to the Financial Intelligence Unit regardless of the amount of the transaction or whether the transaction has been completed. The Bank shall also keep the report confidential according to the regulations and formulate written procedures for reporting large-value cash transactions and suspicious transactions for compliance.

Article 12: Country or Region Risk Assessments and Measures for Money Laundering and Terrorist Financing Risks

The Bank shall establish a risk assessment mechanism for money laundering and terrorist financing risk countries or regions based on the risk-based approach. The assessment items shall include, but are not limited to, countries or regions with serious deficiencies in anti-money laundering and combating terrorist financing as officially issued by the Financial Action Task Force (FATF) and forwarded by the Financial Supervisory Commission, and other countries or regions that do not comply or do not fully follow the FATF recommendations. The Bank shall also develop written procedures for assessing the risk of money laundering and terrorist financing in countries or regions to ensure compliance.

Article 13: Employee Recruitment and Education & Training

The Bank and its subsidiaries shall establish a prudent and appropriate employee selection and appointment procedure and arrange training courses on the Money Laundering Control Act and the legal responsibilities of financial professionals according to the relevant laws and regulations or business needs. The organizer, training content, and training hours of the training courses shall comply with the laws and regulations.

Article 14: Dedicated Unit Personnel and Internal Audit

The appointment of the chief AML/CFT compliance officer, the personnel of dedicated AML/CFT unit and the AML/CFT supervisors of business units under the command of the anti-money laundering and countering terrorism financing supervisors of the Bank and its subsidiaries shall meet the standards specified by law.

The Bank's audit units shall formulate audit items according to the relevant laws and regulations as well as the internal control measures and conduct regular audits.

Article 15: Statement on Internal Control for AML/CFT

The chairman, general manager, chief auditor, and the chief AML/CFT compliance officer of the Bank and its subsidiaries shall jointly issue an Statement on Internal Control for AML/CFT, which shall be submitted to the board of directors for approval. The content of the Statement on Internal Control for AML/CFT shall be disclosed on the company's website within three months after the end of each fiscal year, and an official notice shall be filed on the website designated by the competent authority.

Article 16: Other Related Requirements

Matters not addressed in this Policy shall be governed by the relevant regulations.

Article 17: Implementation and Amendment

This Policy shall enter into force and be implemented after approval by the board of directors, and the same shall apply to its amendments.

Formulated 12-25-2023