

## **O-Bank Anti-Money Laundering and Countering the Financing of Terrorism Policy**

### **Article 1 Purpose**

To prevent money laundering and the financing of terrorism (ML/FT) crime, this Policy is hereby adopted in accordance with relevant regulations prescribed by the competent authority.

### **Article 2 Identification, assessment, and management of ML/FT risks**

O-Bank shall identify, assess, and manage ML/FT risks, and shall adopt documented risk assessment procedures.

The identification, assessment, and management of ML/FT risks referred to in the preceding paragraph shall be implemented in accordance with the following provisions.

1. The Bank shall take appropriate measures to adopt concrete risk assessment factors. These shall include, at the very least, customers, geographic areas, products and services, transactions, and payment delivery channels, and the Bank shall further analyze each risk category to determine detailed risk factors.
2. The Bank shall establish procedures for periodic, comprehensive ML/FT risk assessments based on following risk factors.
  - (1) The nature, scale, diversity and complexity of business.
  - (2) Target markets.
  - (3) Number and scale of banking transactions.
  - (4) Managed data related to high risk profiles.
  - (5) Businesses and products.
  - (6) The examination report results of internal audits and financial supervisory regulatory.
  - (7) Other information obtained from internal database and external sources.
3. The Bank shall produce risk assessment reports.
4. The report shall consider all risk factors to determine the level of overall risk, and appropriate measures to mitigate the risks.
5. The Bank shall have a mechanism in place for updating risk assessment reports to ensure that risk data are kept up-to-date.
6. When a risk assessment report is completed or updated, it shall be submitted to the FSC for recordation.

### **Article 3 AML/CFT program**

In order to manage and mitigate identified risks, and to adopt enhanced control measures for higher risk cases, the Bank shall adopt a group-level AML/CFT program

based on related legislative provisions, the results of ML/FT risk assessments, the scope of its businesses, and the distribution of its all branches and subsidiaries.

The Bank's foreign branches and subsidiaries shall adopt AML/CFT procedures in accordance with this policies and procedures, the group-level AML/CFT program, and host-jurisdiction AML/CFT legislation. Where the minimum requirements of the countries where its headquarters and branches or subsidiaries are located are different, a branch or subsidiary shall choose to abide by whichever criteria are more stringent.

In drafting O-Bank Co. Ltd.'s Policy and Procedures for its implementation, the Bank shall refer to the group-level AML/CFT program as well as AML/CFT model guidelines adopted by the Trade Association for each of the Bank's various products of business, and shall also include their contents among the matters requiring attention to the Bank's self-inspections and internal audits. When necessary, the Bank shall take enhanced measures in order to monitor and control compliance with AML/CFT legislation.

#### **Article 4 Sharing information within the group**

Provided that the information confidentiality regulations of the ROC or of host countries or jurisdictions where domestic, foreign branches and subsidiaries are located are not violated, foreign branches and subsidiaries may share information for the purpose of preventing ML/FT criminal activity, but they shall maintain the confidentiality of exchanged information and take appropriate security protection measures, and they shall adopt written procedures for sharing of information within the group.

#### **Article 5 Customer due diligence and ongoing due diligence on customer identity**

The Bank, acting in accordance with applicable legislation, shall carry out customer due diligence based on risk-based approach (RBA) and ongoing due diligence, and shall adopt documented and profiled procedures for customer due diligence and ongoing due diligence on customer identity.

The aforementioned continuous customer due diligence review should cover both face-to-face and non-face-to-face customers. The process of confirming customer identities and conducting ongoing due diligence should include document authentication and, if necessary, independent communication with the customers.

The Bank shall take different control measures for high-risk customers and customers with high-risk factors in order to effectively manage and mitigate identified risks, while in low-risk scenarios the Bank may take simplified measures to a degree commensurate with low-risk factors identified.

In the case of customers holding prominent political positions (PEP customers) or originating from countries with elevated risks of money laundering and terrorism financing or other risk factors that, upon comprehensive assessment, are determined as high-risk customers, an escalation to a higher approval level should be warranted. In the process of carrying out customer due diligence, if the Bank discovers a situation where it is required by law to decline to establish business relationship or suspend any transaction with the customer, the Bank shall apply legal compliance.

#### **Article 6 Name screening on customers and related parties of a transaction**

The Bank, acting in accordance with RBA and applicable legislations, shall carry out name screening on customers, and customers' senior superiors, beneficial owners, and transaction counterparties, and record in documented profiles according to model guidelines.

The scope of the name screening referred to in the preceding paragraph shall confirm whether a screened entity is automatically deemed a high-risk customer if the screened entity is a politically exposed persons ("PEPs"), is under economic sanctions, or recognized as a terrorist or a terrorist organization by a foreign government or anti-money laundering organization, or is an individual, a legal person, or an organization sanctioned under the "Counter-Terrorism Financing Act."

#### **Article 7 Ongoing monitoring of accounts and transactions**

The Bank, acting in accordance with RBA and applicable legislation, shall enhance ongoing monitoring of accounts and transactions, and record in documented profiles according to model guidelines.

#### **Article 8 Customer risk assessment factors and risk ratings**

According to assessments based on RBA referred to in Article 5 to Article 7 of O-Bank Co. Ltd.'s Policy, the risk assessment factors shall include, at the very least, geographic areas, products and services, transactions, and payment delivery channels, as set out in Article 2, paragraph 2, subparagraph 1 of O-Bank Co Ltd.'s Policy.

The risk ratings adopted by the Bank shall have at least three risk levels to serve as the bases for enhanced customer due diligence and ongoing monitoring.

The Bank shall not disclose a customer's level of risk to the customer or any party that is unrelated to the Bank's charge of its AML/CFT obligation units.

#### **Article 9 Currency Transaction Reports (CTR)**

The Bank shall act in accordance with applicable legislation by reporting CTR above a certain amount as well as suspected money laundering or terrorist financing

transactions, and shall record in documented profiles.

#### **Article 10 Exclusions for insurance agents**

When the Bank solicits beneficial insurance business on behalf of contracted insurance agents, it may be not applicable to ongoing customer due diligence set out in Article 5 of O-Bank Co. Ltd.'s Policy, the provisions governing name screening set in Article 6 herein, and provisions governing ongoing monitoring of transactions set out in Article 7 herein. The above does not apply, however, underwrite or claim settlement operations on behalf of insurance agents.

#### **Article 11 Records retention**

The Bank shall act in accordance with applicable legislation by retaining the following types of information on record for at least five years: all records obtained during the customer due diligence process; records of all business relationship and transactions with its customers; and records of CTR above a certain amount as well as suspicious money laundering or terrorist financing transactions. Transaction records retained by the Bank shall be sufficient to permit reconstruction of individual transactions so as to provide, if necessary, evidence of a criminal activity.

The Bank shall ensure that transaction records and customer due diligence information are provided promptly to the competent authorities when requests are made with appropriate authority.

#### **Article 12 Supervisory management of cross-border correspondent banking**

The Bank shall act in accordance with applicable legislation in cross-border correspondent banking and other similar business, and shall record in documented profiles of supervisory management.

#### **Article 13 Management of ML/FT risks of new products**

Before launching new products, new service, or new business, the Bank shall perform an ML/FT risk assessment and establish relevant risk management measures to mitigate the risks identified.

#### **Article 14 Employee hiring and training**

The Bank shall establish prudent and appropriate procedures for employee screening and hiring. Its chief AML/CFT officer and other AML/CFT personnel shall possess all statutory qualification requirements, and shall participate in on-the-job training in accordance with applicable legislative provisions.

**Article 15 AML/CFT responsible unit and audit monitoring**

The Bank shall set up a AML/CFT responsible unit and appoint responsible officer in accordance with legal requirements.

Each of the Bank's domestic and foreign business units shall also appoint a senior manager to supervise AML/CFT duties among business units.

The Bank's internal auditors shall determine audit programs and carry out periodically in accordance with applicable legal provisions and its internal control measures.

**Article 16 Statement of the AML/CFT internal control system**

The Bank's chairperson, president, chief auditor, and full-time chief AML/CFT officer shall jointly issue a statement of the AML/CFT internal control systems, and submit it to the Board of Directors for approval, disclosed on the Bank's website within three months after the end of each fiscal year, and publicly announced and reported via competent authority's website.

**Article 17 Other provisions**

Any matters not set forth herein shall be governed by law and applicable regulations.

**Article 18 Implementation and revisions**

This Policy shall be implemented after adoption by the Board of Directors. It shall further be reviewed each year, and the preceding shall also apply to any revisions.