

Anti-Money Laundering Policy

Jeonbuk Bank

This Anti-Money Laundering (AML) Policy was established to ensure compliance with relevant AML regulations. Accordingly, it reflects current laws in force such as the Act on Reporting and Use of Certain Financial Transaction Information, the Act on the Proceeds of Crime, the Anti-Terrorism Financing Act, and the Anti-Money Laundering/Combating Financing Terrorism (hereinafter referred to as “AML/CFT”) regulations promulgated by the Korea Financial Intelligence Unit (“KoFIU”).

Jeonbuk Bank operates an AML program throughout its business sites, including overseas subsidiaries, to comply with this Policy. The program stipulates all business procedures and controls required for employees to perform their AML obligations.

1. Anti-Money Laundering Laws

Korea’s AML system has the following structure:

- Suspicious Transaction Report (STR): If a financial institution suspects that transactions are related to money laundering or terrorist financing, then it shall report it to KoFIU.
- Currency Transaction Report (CTR): A financial institution shall file a Currency Transaction Report (CTR) for each transaction in Korean currency of more than 10 million Korean won to KoFIU.
- Customer Due Diligence (CDD): A financial institution shall take reasonable care of customers to identify and verify the customer’s identity as well as obtain information on the transaction purpose and identify the beneficial owner to guard against financial transactions or services being used for illegal acts.

2. Internal Policies

Jeonbuk Bank has established all policies and procedures necessary to comply with the current AML-related laws in force in Korea, and documented them as guidelines or manuals. In addition, Jeonbuk Bank provides regular training programs for its employees.

3. Customer Due Diligence (CDD)

When opening a new account, if a customer makes a one-time financial transaction of more than 10 million won (or more than US\$10,000), or if a customer electronically transfers more than 1 million won (or more than US\$ 1,000), or when money laundering is suspected, a different level of customer due diligence shall be carried out based on the level of risk associated with money laundering. For high-risk customers, we identify and verify the beneficial owners to collect additional information and to ascertain the nature and purpose of the transaction. Documents, data, and information collected

through customer due diligence and verification and customer information shall be managed for the periodic review described below, and comparison of such information.

For customers who uses non-face-to-face services, we collect information on contact verification, name, English name, ID number, address, contact information, job information, transaction purpose, fund source and beneficial owner to conduct customer due diligence.

4. Transaction Monitoring

We operate an anti-money laundering system equipped with the following functions to effectively monitor abnormal transactions and transaction patterns:

- Reviewing and comparing customer profiles and peer group profiles
- Reviewing and comparing transaction information based on standardized previous money laundering cases
- Measuring and evaluating money laundering risk based on customer and transaction information
- Analyzing financial transaction patterns based on information on the customer, account, and transactions.

Abnormal transactions identified through the AML system and verified to be suspicious through the internal procedures shall be reported to the head of KoFIU.

5. Suspicious Transaction Report (STR)

If a financial institution suspects that transactions are related to money laundering or terrorist financing, then it shall report it to KoFIU.

6. Currency Transaction Report (CTR)

A financial institution shall file a Currency Transaction Report (CTR) for each transaction (receipt or payment) in Korean currency of more than 10 million to KoFIU within 30 days.

7. Politically Exposed Persons (PEP)

With respect to persons who had or have political/ social influence in a foreign country, or their family members and closely related persons, we shall collect additional information about their families and related entities in addition to the ordinary customer due diligence and other verification procedures. Files of the PEP shall be reviewed and approved by the compliance officer of the Bank.

8. Due Diligence System to Prevent Terrorist Financing (Watch List Filtering)

- If a person whose financial transaction is restricted by an announcement of the Financial Services

Commission (FSC) relating to the financing of terrorism engages in a financial transaction after obtaining a permit for financial transaction from the FSC, he/she shall be subjected to enhanced customer due diligence and obtain approval from the compliance officer of the Bank.

- Establishing or maintaining business relationships with terrorists or terrorist organizations designated by the United Nations shall be prohibited.

- Establishing or maintaining business relationships with persons on the OFAC sanctions list and EU sanctions list shall be prohibited.

- Establishment of business relationships with persons related to higher-risk countries and non-compliance countries announced by the Financial Action Task Force (FATF) shall require enhanced customer due diligence and approval from the compliance officer.

9. Record Keeping

All internal and external reports and related information, including information on customer due diligence and verification, financial transaction and suspicious transaction reports, etc., shall be retained for at least five years.

10. Training

Employee training on the AML system shall be provided at least once per year with the recording of training details such as training dates, participants, and content of training. Training programs may be provided for each position or duty of the employee. In particular, tellers who provide customer services and employees responsible for reporting suspicious transactions shall attend the AML Information Systems User Training Program.

11. Independent Audit

Audits on AML shall be conducted periodically, and other details for audit shall be as follows:

- Department in Headquarters: Once per year

- Branches: Regular on-site audits, irregular written audit or monitoring audits

The audit results shall be reported to the Board of Directors, and the scope of audit, procedures, violations and instructions shall be recorded.

12. Establishing Anti-Money Laundering Procedures for New Products, etc.

Departments related to product and service development shall assess the risks in accordance with the "Anti-Money Laundering (AML) Checklist" to reduce the risk of money laundering associated with new products and services before the launch of new products and services, and ensure that the compliance department evaluates the assessment results.

The compliance department shall perform the following tasks while assessing risks, report the results to

the compliance officer, and register the risk level of the product in the AML system:

- Reviewing and deliberating money laundering risk assessment result of new products and services
- Reviewing and deliberating money laundering risk assessment results according to new financial techniques

Level of risks shall be classified into low, medium, and high risk according to the risk assessment results.

13. Customer Due Diligence for Overseas Branches and Subsidiaries

The same customer due diligence standards that apply to domestic branches shall apply to all transactions occurring at overseas branches or subsidiaries. The Bank shall take special care to ensure that overseas branches or subsidiaries located in countries that do not or insufficiently comply with FATF recommendations can fully comply with AML/CFT standards. In the event of a conflict between domestic law and foreign/local law regarding AML regulations applicable to overseas branches or subsidiaries, the higher standards shall apply to the extent permitted by foreign/local laws and regulations.