Objectives

The objectives of the Policy on the Implementation of Anti-Money Laundering, Counter-Terrorism Financing, and Prevention of Financing for the Proliferation of Weapons of Mass Destruction Programs are:

- To mitigate the risks associated with money laundering, terrorism financing, and the financing of the proliferation of weapons of mass destruction.
- To minimize the exploitation of the Bank as a medium for money laundering, terrorism financing, and the financing of the proliferation of weapons of mass destruction.

Implementation of AML, CFT, and CPF Programs includes:

1. Active Supervision by the Board of Directors and the Board of Commissioners.
    a. Active supervision by the Board of Directors shall at least include:
        - Proposing written policies and procedures regarding the implementation of AML, CFT, and CPF programs to the Board of Commissioners.
        - Ensuring the implementation of AML, CFT, and CPF programs is carried out in accordance with the established written policies and procedures.
        - Establishing a dedicated work unit and/or appointing an officer responsible for the implementation of AML, CFT, and CPF programs.
        - Supervising the compliance of work units in implementing AML, CFT, and CPF programs.

- Ensuring that the written policies and procedures regarding the implementation of AML, CFT, and CPF programs align with changes and developments in products, services, and technology in the financial services sector, as well as with the evolving methods of AML, CFT, and/or CPF.
- Ensuring that officers and/or employees, particularly those from related work units and new employees, have attended training related to the implementation of AML, CFT, and CPF programs at least 1 (once) a year.
- Ensuring discussions related to the implementation of AML, CFT, and CPF programs are included in the Board of Directors meetings.

In the event that there is a need based on the Bank's risk assessment of AML, CFT, and/or CPF, the activities, scale of business, complexity of business, business characteristics, and/or significant events or developments in the management and operations of the Bank, training related to the implementation of AML, CFT, and CPF programs may be conducted more than 1 (once) a year.

b. Active Supervision by the Board of Commissioners shall include, at a minimum:

- Ensuring the Bank has policies and procedures for implementing the AML, CFT, and CPF programs.
- Approving the policies and procedures for implementing the AML, CFT, and CPF programs as proposed by the Board of Directors.

- Evaluating the policies and procedures for implementing the AML, CFT, and CPF programs.
- Supervising the responsibilities of the Board of Directors in implementing the AML, CFT, and CPF programs.
- Ensuring discussions related to the implementation of the AML, CFT, and CPF programs are held in meetings of the Board of Directors and the Board of Commissioners.

2. Responsibilities for Implementing AML, CFT, and CPF Programs

Responsible Officer for the implementation of AML, CFT, and CPF programs.

a. The Bank must establish a compliance management structure for the implementation of AML, CFT, and CPF programs, including the appointment of compliance officers at the management level.

b. The Bank is required to form a dedicated work unit and/or appoint officers responsible for the implementation of AML, CFT, and CPF programs at both the head office and branch offices.

c. The appointment of responsible officers for the implementation of AML, CFT, and CPF programs shall be made according to the Bank's needs, based on the risk assessment of money laundering (ML), terrorism financing (TF), and/or proliferation financing (CPF), business activities, scale of operations, business

complexity, business characteristics, and/or significant events or developments in the Bank's management and operations.

d. The dedicated work unit and/or appointed officers, as referred to in point 2, shall be established as part of the Bank's organizational structure and shall report to the Board of Directors.

e. The responsibility for implementing AML, CFT, and CPF programs within banks, securities companies, investment managers, insurance companies, infrastructure financing companies, and technology-based joint funding institutions shall fall under one of the members of the Board of Directors overseeing compliance functions.

f. The Bank must ensure that the dedicated work unit and/or officers responsible for the implementation of AML, CFT, and CPF programs possess adequate expertise and have the authority to access all customer data and other relevant information.

3. Policies and Procedures

Banks are required to establish written policies and procedures for the implementation of Anti-Money Laundering (AML), Combating the Financing of Terrorism (CFT), and Countering the Financing of Proliferation of Weapons of Mass Destruction (CPF) programs, which may be supplemented with flowcharts and detailed explanations of each procedural stage depicted in these diagrams.

The policies and procedures for implementing AML, CFT, and CPF programs shall encompass the following:

a. Customer identification and verification.

b. Identification and verification of the Beneficial Owner.

c. Rejection of transactions and termination of business relationships.

d. Ongoing management of risks associated with AML, CFT, and CPF related to customers, countries, products, services, and distribution networks.

e. Maintenance of accurate records regarding transactions, documentation, Customer Due Diligence (CDD) processes, and the administration of policies and procedures.

f. Updating and monitoring.

g. Reporting to senior management, the Board of Directors, and the Board of Commissioners on the implementation of AML, CFT, and CPF policies and procedures.

h. Reporting to the Financial Transaction Reports and Analysis Center (PPATK).

i. AML, CFT, and CPF policies and procedures must take into account the potential misuse of information technology by perpetrators of money laundering, terrorist financing, and/or proliferation financing.

j. Specifically for Commercial Banks, the scope of AML, CFT, and CPF policies and procedures must include Cross-Border Correspondent Banking and Fund Transfers.

k. Banks are required to identify and assess the risks of AML, CFT, and/or CPF related to new product development and business practices, including new distribution mechanisms and the adoption or enhancement of technology for existing products.

4. Internal Control

The implementation of an effective and independent internal control system must be demonstrated through:

a. The presence of adequate policies, procedures, and internal monitoring mechanisms.

b. Clearly defined authority and responsibilities for work units involved in the implementation of AML, CFT, and CPF programs.

c. Independent audits to verify the effectiveness of AML, CFT, and CPF program implementation.

5. Implementation of AML, CFT, and CPF Programs in Branch Networks and Subsidiaries

The implementation of AML, CFT, and CPF programs in branch networks and subsidiaries includes:

a. Financial conglomerates are required to implement AML, CFT, and CPF programs across all branch networks and subsidiaries, both domestically and internationally, and to monitor their execution:

- Policies and procedures for information exchange aimed at CDD and risk management related to AML, CFT, and / or CPF.
- Adequate provisions to ensure the security and confidentiality of exchanged information, including measures to prevent breaches of anti-tipping off regulations.

b. All branch networks and subsidiaries, both domestically and internationally, are mandated to implement AML, CFT, and CPF policies and procedures.

c. Banks that are parent companies of Financial Conglomerates are responsible for ensuring that the Financial Conglomerate has implemented AML, CFT, and CPF programs across all branch networks and subsidiaries, both domestically and internationally. This includes the obligation for all member banks of the Financial Conglomerate to conduct risk assessments and implement appropriate risk mitigation measures.

d. If the regulations on AML, CFT, and CPF in the country where a branch or subsidiary is located are stricter than those stipulated by the Financial Services Authority (OJK) regulations, the branch or subsidiary must comply with the local authority's regulations.

e. If the country where a branch or subsidiary is located has not yet complied with FATF Recommendations, or if the country's AML, CFT, and CPF standards are more lenient than those stipulated by the OJK regulations, the branch or subsidiary

must implement the AML, CFT, and CPF programs as specified in the OJK regulations.

f. If the implementation of AML, CFT, and CPF programs in accordance with OJK regulations results in a breach of the prevailing laws in the country where a branch or subsidiary is located, the bank's foreign office must inform the bank's headquarters or the parent company of the Financial Conglomerate.

g. The bank's headquarters or the Financial Conglomerate, through its parent company, must implement adequate additional measures to manage the risks of AML, CFT, and / or CPF and inform the OJK.

6. Management Information System

a. Banks are required to have an information system capable of identifying, analyzing, monitoring, and effectively reporting on the transaction characteristics or patterns of behavior exhibited by customers.

b. If the bank is a subsidiary within a Financial Conglomerate, it may utilize the information system owned by the financial conglomerate's parent company or other entities within the financial conglomerate for the integrated implementation of AML, CFT, and CPF prevention programs.

c. Banks must maintain an integrated customer profile (single customer identification file), comprising at least information on Individual Prospective

Customers, Corporate Prospective Customers, and other Legal Entity Prospective Customers.

d. Banks must maintain profiles of politically exposed persons (PEPs) related to individual PEPs, corporate PEPs, and other legal entity PEPs.

e. The Bank's information system must consider information technology factors that could potentially be exploited by perpetrators of AML, CFT, and/or CPF.

7. Human Resources and Training

In order to prevent the Bank from being used as a medium or destination for AML, CFT, and/or CPF involving internal parties of the Bank, the Bank is required to:

a. Conduct screening procedures to ensure high standards in the recruitment of new employees (per-employee screening), both permanent and temporary employees, including senior officials, experts, from the lowest level up to 1 (one) level below the Board of Directors and Board of Commissioners.

b. Introduce and monitor employee profiles (know your employee), both permanent and temporary employees, including experts, from the lowest level up to the Board of Directors and Board of Commissioners.

c. The Bank must provide training on AML, CFT, and/or CPF to officials and/or employees as needed, which is continuous and periodic, at least once a year.

d. Training according to the Bank's needs based on the risk assessment of AML, CFT, and/or CPF, activities, business scale, business complexity, business

characteristics, and/or significant events or developments in the Bank's management and operations, training on AML, CFT, and CPF for officials and/or employees may be conducted more than 1 (once).

8. Reporting

Reporting to the Financial Services Authority regarding:

a. Individual assessments, risks, AML, CFT, and/or CPF that have been prepared individually, for the first time no later than 12 (twelve) months from the enactment of this Financial Services Authority Regulation.

b. Updates on individual assessments of AML, CFT, and/or CPF risks submitted annually no later than the end of June.

c. Policies and procedures for implementing AML, CFT, and CPF within 6 (six) months from the enactment of this Financial Services Authority Regulation.

d. Annual update plan reports submitted no later than the end of December before the data update period.

e. Implementation report of data updates submitted annually no later than the end of January after the last data update period.

f. Immediate blocking report with attached blocking minutes, no later than 3 (three) working days from the Bank receiving List of Suspected Terrorists and Terrorist Organizations (DTTOT) and CPF.

g. Nil report in case no identity match and other related information regarding Customers found in the DTTOT no later than 3 (three) working days from the Bank receiving DTTOT and CPF.

h. Submission of reports to the Financial Services Authority must be directed to the Head of Supervision Unit through the electronic system managed by the Financial Services Authority.

i. If the electronic system used for reporting is not yet available or encounters disruption, the Bank must submit documents physically or via email to the Financial Services Authority addressed to the Head of Supervision Unit.

j. If the reporting date falls on a holiday, the report shall be submitted on the next working day.

k. In case of changes to policies and procedures, and/or data update plan reports submitted to the Financial Services Authority, the Bank must submit such changes no later than 7 (seven) working days from the date the changes are made.

9. Supervision and Monitoring

In conducting supervision and monitoring of AML, CFT, and CPF programs, OJK has the authority to:

a. Supervise and monitor the implementation of AML, CFT, and CPF programs directly and indirectly.

b. Request relevant data and/or information from Banks for the purpose of supervising and monitoring compliance with the implementation of AML, CFT, and CPF programs by Banks.

c. Instruct Banks to block specific accounts.