PT Bank OCBC NISP, Tbk
Anti Money Laundering &
Counter Financing Terrorism

QUOTE OF ANTI MONEY LAUNDERING AND COUNTER FINANCING TERRORISM POLICY

I. INTRODUCTION

PT Bank OCBC NISP, Tbk ("Bank") is a public listed company incorporated under the provisions of The Company Act No. 40, year 2007. Bank officially became a Commercial Bank in 1967, Foreign Exchange Bank in 1990 and Public Company in Indonesia Stock Exchange since 1994.

The Financial Action Task Force (FATF), OJK (Financial Services Authority), and PPATK (Indonesian Financial Transaction Reports and Analysis Center/INTRAC) recommend all Financial Service Institution to establish Anti-Money Laundering and Prevention of Terrorism Financing regime by promoting a risk-based approach in accordance with AML-CFT regulations, National Risk Assessment & Sectoral Risk Assessment of AML-CFT in Indonesia. The Policy summarized by this Quote was established to protect Bank from the money laundering and criminal funding for terrorism.

Bank will verify its AML – CFT framework, goals and strategies on an periodical basis and maintain an effective program for the Bank's business that reflects the best practices for financial institution.

II. STRUCTURE AND POLICY

The Bank has active Supervisory Board under Compliance Director, and the implementation of AML – CFT Program handled by Division Head of AML – CFT and all the team members ("Division") which has been appointed by the Management. The Division is responsible for adherence to applicable AML – CFT Program derived from the INTRAC and OJK.

Bank has created a set of policy and procedures concerning general AML standards and principles. The governance ensures that the standards are implemented into day-to-day operational activities. All policy and procedures are published on accessible media so it can be accessed by all employees. They are subject to periodical review to ensure their conformity with recent and updated AML – CFT regulations.

The scope of this policy covers all aspects of Anti Money Laundering and Counter-Financing Terrorism Prevention, namely:

1. Active supervision of the Board of Directors and Board of Commissioners;
2. Policies and Procedures;
3. Internal Control;
4. Information Management System; and
5. Human Resources and Training

III. CUSTOMER DUE DILIGENCE

Bank has implemented know your customer (KYC) procedure to assure all kinds of customers are subject to identification and verification process. The KYC has been implemented in all branches

and business units. The goals are Bank has sufficient information and data about the customers profile, whom they deals with, and also the Ultimate Beneficial Owner (UBO). The procedures include mandatory documents requirements, enhanced due diligence for politically exposed persons (PEPs) and customers from high risk businessess or countries, name screening, and the ongoing monitoring and updating data of all existing customers. Bank also can apply Simplified Due Diligence on the customer onboarding process to payroll account and government institutions.

Bank shall refuse to open an account or has to close an existing account, if the following:

a) Cannot fix a reasonable belief that it knows the true identity of the customer and/or UBOs and/or the nature of business concerning the identification of the customers are not met;
b) Known and/or suspected the utilization of fake documents;
c) Assets that are known or suspected to be the proceeds of criminal activity;
d) Enter into business relationships with individuals or entities known or suspected to be a terrorist or a criminal organisation, or listed on sanction lists and/or weapon mass-destruction proliferation list;
e) Maintain anonymous accounts or accounts operate for shell banks.

IV. CORRESPONDENT BANKING

Bank has implemented procedures for correspondent banking. The procedures cover, but are not limited to:

a) Request to provide sufficient information to fully understand of the nature of its business, management and ownership structure, bank's regulation and supervision in the respondent's country, compliance to regulations and supervision including assessment of compliance of the respondent bank's AML-CFT program;
b) Risk-classification of correspondent banking relationships;
c) Obtaining senior officer approval of the establishment of new correspondent banking relationships;
d) Apply transaction monitoring and filtering on transactions.

Bank will not and shall refuse to open an account or establish business relationship for shell banks. Correspondent banks have to provide confirmation that they will not provide banking services to or engage in business with shell banks.

V. REGULATORY REPORTING

Bank has an obligation to report cash transaction with certain amount based on relevant regulation, suspicious transaction/activity, and international fund transfer. Suspicious transactions must be handled and escalated with approval of Compliance Director prior reporting to regulator.

VI. AML - CFT ENTITY RISK ASSESSMENT

The AML-CFT Entity Risk Assessment is prepared by conducting inherent risk assessment activities, establishing risk tolerance, formulating mitigation and risk control measures, residual risk

evaluation, applying a risk-based approach, and reviewing and evaluating approaches based on risk. Bank is required to use National Risk Assessment of Money Laundering & Terrorist Financing (NRA AML-CFT) and Sectoral Risk Assessment of Money Laundering & Terrorist Financing (SRA AML-CFT) published by PPATK & OJK as a reference to assess Bank's AML-CFT Entity Risk Assessment.

VII. SANCTIONS COMPLIANCE

Sanctions Compliance Implementation is important in banking activities. Bank OCBC NISP obligates to establish restrictions and controls on the movement of goods, services, and customers' funds were transacted through the products and services that provided by bank. Sanctions Compliance implementation goal is to keep Bank OCBC NISP from compliance risk, operational risk and reputational risk exposure. Bank OCBC NISP implements AML-CFT Sanctions procedure as a form of risk mitigation and guidance to relevan working units. The implementation based on OCBC Group and Sanctions regulations issued by the government / local jurisdictions, international institutions / multilateral and clearing countries.

VIII. FINANCIAL CONGLOMERATION

Bank as part of the financial conglomerate shall apply and monitor the implementation of the PPU APU program throughout the network of offices and subsidiaries or affiliated companies owned by the same controllers. These applications and monitoring include information exchange policies and procedures for CDD objectives and risk management for money laundering and terrorism financing. In carrying out the exchange of information, Financial Conglomeration shall have adequate provisions on information security, principally customer data

IX. RECORD RETENTION

Bank has to record all data and or information regarding customers documents and its financial transactions. Bank maintains customers documentations for minimum of 10 (ten) years. Bank will provide information and/or documents competent authorities as ordered by laws and regulations, when required.

X. TRAINING

Bank has implemented AML – CFT training program for all staff. Bank's training program is tailored to the operations and business unit to assure all staffs are aware of different patterns, methods, techniques, and typologies of money laundering or terrorist financing which may occur in daily operational activities. The training programs cover policy and procedures for the implementation of AML – CFT Program as well as roles and responsibilities of employees to assist in the eradication of money laundering or terrorist financing.

XI. INTERNAL CONTROL

Bank has an effective internal control system. Bank's AML – CFT Program is subject to independent control by Internal Audit function. The control demonstrates the adequacy of policy, procedures, internal monitoring, and responsibilities of working units associated with the implementation of AML – CFT Program.

The Quote is an integral part of Bank's Anti-Money Laundering and Counter Financing Terrorism Policy, and shall take effect from March 30, 2020.