

**Anti-Money Laundering / Counter-Terrorism
and Proliferation of Weapon of Mass Destruction Financing (AML/CTPF) Policy
Kiatnakin Phatra Financial Group**

As the Board of Directors, senior management and employees of Kiatnakin Phatra Financial Group (The Group) recognize the importance of Anti-Money Laundering / Counter-Terrorism and Proliferation of Weapon of Mass Destruction Financing or AML/CTPF, the Group has established the Policy as the core policy for the standard operation practices, with the following objectives:

- To serve as the Core Policy of the Group, namely Kiatnakin Bank Public Company Limited and companies in Kiatnakin Phatra Financial Group, which are required to comply with AML/CTPF laws.
- To serve as the operation guidelines to ensure that the Group's activities are in accordance with AML/CTPF laws and AML/CTPF global standards.
- To serve as the Core Policy for the Group's Business Ethics and Code of Conduct.

The elements of the policy can be divided into 11 sections, as follows:

Section 1 Role and Responsibilities

All employees that work with the Group's customers and partners are responsible for;

1. Complying with AML/CTPF laws, core and secondary AML/CTPF policies, code of business conduct, and related notices.
2. Attending AML/CTPF trainings as scheduled, and, once notified to participate in relevant training, it is imperative that employees provide strict cooperation in this matter.
3. Reporting suspicious transactions that may constitute money laundering.
4. Absolutely refraining from disclosing information on the conduct of customer due diligence or the reporting of transaction or the dissemination of any other information to AMLO, unless otherwise exempt under relevant laws.

Section 2 AML/CTPF Enterprise Risk Assessment

The Group has set out the guidelines of AML/CTPF risk assessment as follows;

1. AML/CTPF enterprise risk assessment results of the Group shall be prepared, and the measures and guidelines on risk reduction shall be prepared in written, which may be in forms of documents or reports.
2. Documents or reports on AML/CTPF enterprise risk assessment shall be deemed the most important policy and procedure of the Group, which shall be approved by the Bank's Board of Directors or its top management.
3. Guidelines for AML/CTPF enterprise risk assessment shall be at least considered based on the following principles;
 - 3.1 The AML/CTPF national risk assessment report has been widely publicized by AMLO should be mutually considered.

- 3.2 Risk factors such as risk factors regarding customers, areas or countries, products, services, nature of transactions, and service channels should be mutually considered.
- 3.3 Risk assessment should be conducted and summarized, and risk mitigation or reduction measures and methods should be specified.
4. The Group's AML/CTPF enterprise risk assessment shall be reviewed and revised on 5-year basis.
5. The Group's AML/CTPF enterprise risk assessment results or reports shall be submitted to AMLO upon request.

Section 3 Customer Acceptance Policy

The Group has set out customer acceptance guidelines as follows;

1. Know Your Customer (KYC) and Customer Due Diligence (CDD) needs to be carried out prior to any business relationship or transaction or acceptance of customer transactions.
2. Know Your Customer (KYC) and Customer Due Diligence (CDD) needs to be carried out prior to any business relationship or acceptance of customer transactions from time to time
3. Conducting Enhanced Due Diligence (EDD) for high-risk clients
4. Screening information of customers and ultimate beneficial owners with designated persons or sanctions lists (regarding terrorism and proliferation of weapon of mass destruction financing), watch lists (regarding money laundering and/or terrorism and proliferation of weapon of mass destruction financing), and any additional lists which will be further announced by AMLO, including additional lists under AML/CTPF laws as provided by external providers.
5. Evaluating client information and evidence of identification process to determine client risk levels prior to any business relationship or customer acceptance.
6. Senior management needs to consider and make the final decision to engage in any business relationship or accept customer transactions with high-risk customers.
7. Prohibited customers include:
 - Persons who have refused to provide required information or documentation, fail to provide sufficient information, fail to provide information regarding their identity, or KYC cannot be conducted.
 - Persons who use alias or conceal their true names, or provide false information to conceal themselves.
 - Financial institutions that are residents of countries or territories without being physically present in such countries or territories (also referred to as shell banks).
 - Correspondent banks that do not have any policies or measures on AML/CTPF, or the same fail to comply with global standards or international laws.
 - A person or group of persons or entity that triggers sanctions lists, as announced or provided by AMLO and international organizations.
 - Persons suspected of using the institution as a money laundering channel or using the transactions to finance terrorism and proliferation of weapon of mass destruction financing.

8. Regular and continuous review of customer information needs to be conducted until a relationship with the customer is terminated.
9. Transaction movements need to be tracked continuously until a relationship with the customer is terminated.
10. Transaction reporting needs to be carried out in accordance with AML/CTPF laws. Once suspicious transactions that may constitute money laundering and terrorism financing are detected, AMLO needs to be notified immediately.
11. The client's risk levels on money laundering and terrorism financing need to be reviewed in accordance with the results of customer information review and customer transaction monitoring.

Section 4 AML/CTPF Risk Management for Customers

The Group recognizes the importance of AML/CTPF risk management for customers in order to prevent the Bank and companies in the Group's operations from being used as a tool or channel for money laundering and terrorism financing. The AML/CTPF risk management is as follows:

- Internal risk management for products and services, and service channels
- Customer AML/CTPF risk management
- Ongoing AML/CTPF risk management

Section 5 AML/CFT Management Information Technology Systems

The Group is committed to establishing an effective information technology system to monitor and verify customer information as a tool to ensure that the AML/CTPF policy is realized including AML/CTPF high-risk lists that administrated and announced by international organizations, where the database has been provided by external providers for the purpose of compliance with the global standards.

Section 6 AML/CTPF Reporting Requirements

The Group has policies and procedures that require the reporting of customer transactions and/or suspicious activities as stipulated by AML/CTPF laws. The reporting guidelines are as follows:

- Reports of cash transactions
- Reports of asset transactions
- Reports of money transfer and electronic payments
- Reports of suspicious transactions
- Any other reports which will be further announced by AMLO in the future.

Section 7 AML/CTPF Record-keeping Obligations

The Group has policies that require the retention of customer information in accordance with AML/CFT laws. The guidelines are as follows:

- The information on Know Your Customer (KYC) and Customer Due Diligence (CDD) of customer will be kept for 10 years from the date of termination of relations or in compliance with the period which will be provided by laws or further announced.
- The information on transaction reports shall be kept for 5 years from the date of transactions or information recording or in compliance with the period which will be enforced by relevant laws or further announcement.

Section 8 The Internal Audit Function

The Group has established the Office of Internal Audit is acting independently to inspect operations and to assess the effectiveness of AML/CTPF measures within the organization, particularly for business operations and the Information Technology system supporting operations at least 1 audit shall be conducted to assess AML/CTPF performances. The audit results will be reported directly to relevant committees, or senior executive.

Section 9 Personnel Selection and AML/CTPF Training

All new employees shall not involved in money laundering, terrorism, and proliferation of weapon of mass destruction financing. All new employees shall attend AML/CTPF training with the result of "Pass" for its post test prior to positioning as the Group's employees, provided that the training experience shall be recorded as an evidence. All existing employees shall attend AML/CTPF training at least once 1 year.

Section 10 Information Disclosure on AML/CTPF

To comply with AML laws and AML/CTPF laws, the Group has specified the guidelines for information disclosure on AML/CTPF as follows;

- The Group is prohibited to disclose or perform any action to make customers know suspicious transaction reports, or submit any other information relating to customers to AMLO.
- The Group is able to mutually or interactively use/ share/ send within the Group information for fulfilling the objectives of Customer Due Diligence and AML/CTPF risk management.

Section 11 Policy Review

The Group's policy shall be reviewed and contains updated subject matter and in compliance with AML/CTPF laws. The review, revision, and amendment of the Policy must be approved by the Bank's Board of Directors or top management.