CTBC Financial Holding Co., Ltd.
Anti-Money Laundering and Countering the Financing of Terrorism Policy

Chapter 1 General provisions

Article 1 Purpose

CTBC Financial Holding Co., Ltd. (the Company) establishes this Anti-Money Laundering and Countering the Financing of Terrorism Policy (the Policy) in accordance with subparagraph 2(11) of paragraph 1 and paragraph 10 of Article 8 of the Implementation Rules of Internal Audit and Internal Control System of Financial Holding Companies and Banking Industries. The Policy is established to provide internal control and behavior standards for the Company and its subsidiaries in order to prevent money laundering and terrorist financing; protect the reputation of the Company and its subsidiaries; ensure compliance with relevant domestic and foreign laws and regulations and with the regulatory requirements and guidance of international organizations; reduce the risk of transactions, products, or services provided by the Company or its subsidiaries being used to launder money or finance terrorism; assist governments in tracking the flow of funds of specific people; and investigate and prevent illegal or otherwise inappropriate transactions.

Article 2 Scope

The Policy applies to:

(a) any Company subsidiary, including foreign branches and subsidiaries, that is a financial institution as defined in Article 5 of the Money Laundering Control Act or that has anti-money laundering or countering the financing of terrorism (AML/CFT) obligations in the country or jurisdiction of its incorporation or registration (a Covered Member); and

(b) the Company and any Company subsidiary that does not meet the definition of a financial institution as described in paragraph (a) above.

Article 3 Applicability

In addition to complying with relevant laws and regulations and the self-regulatory requirements and guidelines templates of trade associations, Covered Members shall establish their own policies

and procedures in accordance with the Policy in order to satisfy relevant AML/CFT regulatory requirements.

If AML/CFT requirements in a country or jurisdiction where a foreign branch or subsidiary is registered differ from, but do not conflict with, the requirements of the Policy, the stricter requirements shall apply. In the event that local regulatory requirements conflict with those of the Policy, the foreign branch or subsidiary shall issue a report to the Chief Compliance Officer and AML/CFT Responsible Officer of its company and the parent company to seek their opinions, with a copy sent to the Company's Chief Compliance Officer, in order to resolve the conflict.

Articles 4, 5, and 6; paragraph 1 of Article 7; and Articles 8, 9, 10, 11, and 13 of the Policy shall not apply to the entities set forth in paragraph (b) of Article 2 hereof.

Chapter 2 AML/CFT requirements

Article 4 Internal control system

Covered Members shall establish AML/CFT internal control systems, which shall include:

(a) policies and procedures for identifying, assessing, and managing money laundering and terrorism financing (ML/TF) risks, including risk appetite;
(b) AML/CFT programs that take ML/TF risks and business size into consideration; and
(c) procedures for supervising the compliance of AML/CFT regulatory requirements and the implementation of AML/CFT programs.

The board of directors of each Covered Member has the ultimate responsibility for ensuring the establishment and maintenance of appropriate and effective AML/CFT internal controls. Each Covered Member's board of directors and senior management shall understand their company's ML/TF risks and implementation of the AML/CFT programs, and shall take measures to foster a strong AML/CFT culture.

Article 5 Group risk appetite and risk management

To effectively manage ML/TF risks, Covered Members shall:

(a) perform a regular enterprise-wide risk assessment (EWRA), in which residual risk is determined through the evaluation of inherent risks and controls, and submit the EWRA reports to the

Company's Compliance Department; and

(b) establish an action plan for improvement based on the EWRA results, and, until the improvement is completed, periodically report the action plan, its expected completion timeline, and execution progress to the Company's Compliance Department and the Covered Member's board of directors.

The implementation of the methodology guidelines for the abovementioned EWRAs, and any subsequent amendment thereto, is subject to the approval of the Company's president. To ensure that Covered Members apply consistent principles in their EWRAs, Covered Members shall perform their EWRAs in accordance with the methodology guidelines. In addition, for the purpose of monitoring the group's ML/TF risks, the timeline of an EWRA is determined after discussion between the Company's Compliance Department and the Covered Member's responsible unit.

If the Company, a Covered Member, or another subsidiary fails to satisfy any of the following group ML/TF risk appetite guidelines, it shall devise and implement measures for improvement and report on the implementation status of these measures to the boards of directors of itself and the Company until the improvement is completed:

(a) Do not intentionally violate applicable AML/CFT regulatory or self-regulatory requirements.
(b) Maintain a rating of at least "fair" for each control factor[1].
(c) Maintain a residual risk level of no higher than "medium" on the Company's internal risk map[2].

The inherent risk of a Covered Member is divided into five levels: high, medium high, medium, medium low, and low. To ensure no significant difference exists between the inherent risk assessment and national risk assessment (NRA) results of each Covered Member, before assessing its own inherent risk, each Covered Member shall take the latest NRA results into consideration and determine whether any modification to the EWRA methodology is necessary in accordance with the NRA results.

Article 6 Customer due diligence

Covered Members shall establish and implement risk-based customer due diligence (CDD) procedures including but not limited to the following:

(a) Identifying and verifying customer identities through reliable, independently sourced documents, data, and information. Situations requiring such CDD include but are not limited to:
    (1) establishing a business relationship with a customer;

[1] Control effectiveness comprises five levels: very poor, poor, fair, good, and very good.
[2] Residual risk comprises five levels: high, medium high, medium, medium low, and low.

(2) conducting a currency transaction of NT$500,000 or more (or foreign currency equivalent);
(3) conducting a cross-border remittance of NT$30,000 or more (or foreign currency equivalent);
(4) identifying a suspected ML/TF transaction; and
(5) questioning the veracity or adequacy of previously obtained customer identification data.

(b) Taking reasonable measures to identify and verify the identities of beneficial owners. In the case that a customer is an entity, an organization, or the trustee of a trust, an understanding is gained of the customer's ownership and control structure.

(c) Performing the ongoing monitoring of existing customer business relationships. Situations requiring such ongoing monitoring include but are not limited to when:
(1) a customer opens a new account or establishes a new business relationship;
(2) a periodic review is due in accordance with a customer's materiality and risk level; and
(3) a material change is known to have occurred in a customer's identity or background information.

(d) Carefully reviewing transactions in a business relationship with a customer to ensure related transactions are commensurate with the customer's background, business, and risk. A Covered Member shall also, when necessary, gain an understanding of the customer's source of funds.

Article 7 Name screening

Covered Members shall establish name-screening procedures for the customers and related parties involved in transactions. Specifically, Covered Members shall apply a risk-based approach in order to detect, match, and filter customers, people who hold a senior management position in a customer, beneficial owners of a customer, or related parties of a transaction who are designated individuals or entities sanctioned under the Counter-Terrorism Financing Act or are a terrorist or terrorist group member identified or investigated by a foreign government or international organization. The procedures for name screening shall include and document, at a minimum, the logic of matching and filtering, the name-screening operating procedure, and review standards.

For compliance by the Company and its subsidiaries, including Covered Members, with paragraph 1 of Article 7 of the Counter-Terrorism Financing Act, guidelines and procedures are established regarding matters such as the scope of applicability, the parties subject to screening, and when screening is required. The implementation of these guidelines and procedures, and any subsequent amendment thereto, is subject to the approval of the Company's president. Except for those subsidiaries that, due to their business nature or limited size, may directly implement the guidelines released by the Company, subsidiaries shall establish their own guidelines or incorporate the guidelines released by the Company into their existing internal regulations.

Article 8 Ongoing monitoring of accounts or transactions

Covered Members shall perform the ongoing monitoring of accounts and transactions, including but not limited to the following:

(a) establishing policies and procedures for the ongoing monitoring of accounts and transactions by applying a risk-based approach and using information systems to facilitate the detection of suspicious transactions;

(b) periodically reviewing and updating the policies and procedures described in paragraph (a) to take into account customer profiles, business size and complexity, ML/TF-related trends and information obtained from internal and external sources and internal risk assessment results;

(c) in policies and procedures for the ongoing monitoring of accounts and transactions, include and document complete monitoring scenarios, parameters, monetary thresholds, operating processes for early warnings and monitoring them, and inspection processes and reporting standards for monitoring cases; and

(d) in the monitoring scenarios mentioned in paragraph (c), include red flags defined by relevant trade associations, in accordance with its business nature, and add related red flags by referring to the Covered Member ML/TF risk assessments and daily transaction information.

Article 9 Addressing and reporting suspected ML/TF activities

Covered Members shall establish a mechanism for handling suspected ML/TF activities, including but not limited to declining to conduct, or taking other appropriate action in response to, transactions that raise certain ML/TF red flags. In addition, if a transaction meets certain regulatory reporting standards, including but not limited to currency transactions above a certain amount and transactions or funds that are reasonably suspected of involving or that may involve criminal or terrorism financing activities, the Covered Member involved shall immediately report the transaction to the designated competent authorities and agencies.

Article 10 Record keeping

Every Covered Member shall establish a record-keeping procedure for retaining relevant AML/CFT records and documents, including but not limited to documents or information obtained from CDD, account opening documentation, relevant transaction records, reporting information, name screening, and the ongoing monitoring of accounts and transactions, and shall set an appropriate

period of retention according to applicable regulatory requirements and business needs for the purposes of future validation and enquiries and evidence regarding the fulfillment of AML/CFT obligations.

Article 11 Information sharing

To establish group-wide ML/TF red flags applicable across all its subsidiaries and to assist Covered Members in monitoring transactions and investigating suspicious transactions, the Company and each Covered Member shall, as long as any and all applicable laws and regulations have been or will be complied with and information confidentiality is ensured, share group watch lists and other relevant information for AML/CFT purposes. This information sharing, however, shall not violate the law against "disclos[ing] or deliver[ing] documents, pictures, information or objects relating to reported transactions suspected of violating provisions under Articles 14 and 15, or to suspected offences described in Articles 14 and 15", as set forth in paragraph 2 of Article 17 of the Money Laundering Control Act.

The implementation of the guidelines for information-sharing described in the previous paragraph, and any subsequent amendment thereto, is subject to the approval of the Company's president.

Article 12 Training

The Company and its subsidiaries, including Covered Members, shall, according to their business needs and as required by relevant laws and regulations, conduct AML/CFT training or designate personnel to attend such training in order to increase personnel's AML/CFT awareness and ensure that relevant operating processes and internal controls are implemented effectively.

The guidelines regarding training recipients, topics, methods, and hours, including any subsequent amendment thereto, are subject to the approval of the Company's president.

Article 13 Other requirements

In addition to the abovementioned requirements, for the purpose of effective AML/CFT practices, each Covered Member shall:

(a) designate an appropriate responsible officer in charge of the coordination and supervision of

the implementation of AML/CFT requirements;

(b) ensure it has properly established AML/CFT operations and internal controls; and

(c) fulfill other obligations as required by the competent authorities.

Chapter 3 Supplemental provisions

Article 14 Internal auditing

The Company and its Covered Members' internal audit units shall conduct audits in accordance with the Implementation Rules of Internal Audit and Internal Control System of Financial Holding Companies and Banking Industries, the Money Laundering Control Act, the Counter-Terrorism Financing Act, and other applicable laws and regulations in order to ensure the efficacy of the Company's AML/CFT internal control systems.

Article 15 Incentives and penalties

Employees shall be rewarded for effectively implementing relevant regulatory requirements, the Policy, and other internal regulations such that an ML transaction or TF activity is identified or prevented or that damage to the reputation of the Company or a subsidiary, including a Covered Member, is avoided. Employees shall be punished for non-compliance with relevant requirements that results in damage to the reputation of the Company or a subsidiary, including a Covered Member. The conditions of incentives and penalties and related requirements are stipulated by the internal regulations set by the HR units of the Company and its subsidiaries, including Covered Members.

Article 16 Explanation of the policy

The Company's Chief Compliance Officer is authorized to provide explanations and judgments in response to any question regarding the content and applicability of the Policy.

Article 17 Effectiveness and amendment

This Policy, and any amendment hereto, shall take effect upon being approved by the Company's Board of Directors and announced by its Chief Compliance Officer.