Chang Hwa Commercial Bank, Ltd.
"Anti-Money Laundering and Countering the Financing of Terrorism Policy"

Article 1 (Objective, Authority and Application Scope)

The Policy is established in accordance with "Regulations Governing Internal Audit and Internal Control System of Anti-Money Laundering and Countering Terrorism Financing of Banking Business and Other Financial Institutions Designated by the Financial Supervisory Commission" for the purpose of anti-money laundering and countering the financing of terrorism (AML/CFT) as the basis for implementation.

The Policy applies to all units of Chang Hwa Commercial Bank (hereinafter "the Bank"), including management units based in the Head Office for all kinds of business of the Bank, domestic and foreign business units, and subsidiaries.

Article 2 (Organization Structure)

The board of directors of the Bank takes the ultimate responsibility for ensuring the establishment and maintenance of appropriate and effective AML/CFT internal controls. The board of directors and senior management should understand the Bank's money laundering and terrorist financing (ML/TF) risks and the implementation of AML/CFT programs, and take measures to form a strong AML/CFT culture.

The board of directors should appoint the Chief Compliance Officer to serve as AML/CFT responsible officer who is responsible for AML/CFT affairs and coordinating and monitoring the execution of the Policy. The responsible officer shall not take other duty which conflicts with the AML/CFT responsibilities.

The Bank should set up the AML/CFT Management Team to execute the AML/CFT affairs.

The instruction for the composition, operation, responsibilities and related matters of the AML/CFT Management Team shall be approved by the board of directors.

Article 3 (Risk Assessment)

The Bank should take related measures to identify and assess its ML/TF risks, and determine specific risk categories based on the risk identified, in order to control, mitigate or prevent such risks.

Such specific risk category should cover at least the following aspects: geographic areas, customers, products and services, transactions or delivery channels, etc. The Bank should analyze each risk category to determine detailed risk factors which apply.

I. Geographical risk: The Bank should identify geographic areas that are exposed to higher ML/TF risks.

II. Customer risk: The Bank should take an overall account of a customer's background, occupation, characteristics of social and economic activities, geographic areas, and an entity customer's organization type and structure, etc., to identify the customer's ML/TF risks.

III. Product and service, transaction or delivery channel risk:

i. The Bank should identify products, services, transactions or delivery channels that have higher ML/TF risk based on the nature of individual product, service, transaction or delivery channel.

ii. The Bank should, before launching a new product, service or business (including new payment method, applying new technology on existing or new product or service), perform ML/TF risk assessment and establish relevant risk management measures.

Article 4 (Level of customer risk and category rules)

The Bank shall establish more than two levels of customer risk and category rules as bases to determine the extent of customer due diligence and ongoing monitoring.

Based on the type of business relationship and considered associated risk factors, the Bank may formulate types of customers who should be directly identified as high risk or low

risk.

Article 5 (Time for risk assessment)

With respect to a new customer to establish business relation with the Bank, the Bank should determine risk level of the customer when establishing business relation.

With respect to an existing customer with a specific risk level, the Bank should re-assess customer risk in accordance with its related risk assessment rules. The points of time to re-assess the customer risk are as follows:

I. When the customer opens a new account or establishes a new business relation.

II. Time to conduct periodic review determined on the basis of the customer's materiality and risk.

III. When the Bank knows a material change occurs in the customer's identification and background information.

IV. When the Bank reports a suspicious ML/TF transaction or other events that may result in substantial change in customer risk profile occur.

Although the Bank performs customer risk assessment when establishing business relation with a customer, the Bank should conduct due diligence to existing customer on the basis of customer's materiality and risk level; and, after considering the sufficiency of the information obtained from the customer during the last due diligence, the Bank should review the existing business relationships at appropriate times and adjust the level of customer risk in a timely manner.

A bank should review periodically the sufficiency of the information for identifying customers and beneficial owners and ensure the update of such information. Especially for high-risk customers, they should be reviewed at least once a year.

Article 6 (Follow-up control measures)

The Bank should establish control measures according to the risks identified to

mitigate or prevent ML/TF risks. To manage and reduce ML/TF risks effectively, the Bank should determine to apply the following control measures based on risk profiles of the customer:

I. Conduct enhanced due diligence.

II. Obtain the approval of senior management, defined by the Bank considering internal risks, before first establishing a business relation or establishing a new business relation.

III. Increase the frequency of customer due diligence.

IV. Conduct enhanced ongoing monitoring of the business relationship.

The Bank may take simplified measures in a lower risk situation. However, when confirming the customer identity and conducting ongoing monitoring, simplified measures of confirming the customer identity should not be taken in one of the following situations:

I. Customers are from high ML/TF risk countries or jurisdictions, which include but are not limited to the countries or jurisdictions, published by international anti-money laundering organizations and notified by Financial Supervisory Commission (hereinafter "FSC"), that have serious deficiencies in AML/CFT, and other countries or jurisdictions that fail to comply with or completely comply with the recommendations of such organizations.

II. The Bank has sufficient reason to suspect the customers or transactions may be involved in ML/TF.

Article 7 (Mechanism of ML/TF risk assessment)

The Bank should establish a mechanism of periodic enterprise-wide ML/TF risk assessment and generate a risk assessment report to enable senior management to timely and effectively understand the bank's overall ML/TF risks, determine necessary mechanisms to be established, and develop appropriate mitigation measures.

The Bank should build the mechanism of ML/TF risk assessment based on following indicators:

I. The nature, scale, diversity and complexity of businesses.

II. Target market.

III. Volumes and sizes of banking transactions.

IV. Management data and reports related to high risks.

V. Businesses and products, including the channels and manners used to provide businesses and products to customers and the way to conduct customer due diligence.

VI. The examination results of internal audit and the supervisory authority.

When the Bank performs the enterprise-wide ML/TF risk assessment described previously, in addition to considering the indicators mentioned above, the information obtained from other internal and external sources is recommended as supporting information. For example:

I. Management reports provided by the Bank's business management units.

II. Relevant AML/CFT reports published by international anti-money laundering organizations and other countries.

III. Information of ML/TF risk released by the Competent Authorities.

The Bank’s enterprise-wide ML/TF risk assessment results should be used as a basis to develop AML/CFT programs. The Bank should allocate appropriate headcounts and resources based on risk assessment results and take effective countermeasures to prevent or mitigate risks.

If the Bank faces a material incident, has material development in management and operation, or confronts relevant new threats, it should re-perform the assessment.

The Bank should file the risk assessment report to FSC after completing or updating such report.

Article 8 (Internal control systems)

The Bank should build an enterprise-wide AML/CFT mechanism and compliance management of related laws and regulations, including the management scheme of

identifying, measuring and monitoring ML/TF risks, and establish AML/CFT programs in accordance with the related laws and regulations enacted by Competent Authority and based on the Policy, risk assessment result and scale of business. Periodically review is required.

On condition that the regulatory requirements on data confidentiality of R.O.C. and jurisdictions where the Bank has any foreign branch (and subsidiary) are met, the Bank should set up related rules for following matters:

I. Internally share information required for the purposes of confirming the customer identity and ML/TF risk management.

II. For the AML/CFT purposes, based on compliance, audit and AML functions, the Bank may request domestic and foreign business units and subsidiaries to provide information regarding customers, accounts and transactions when necessary. This should include information and analysis of transactions or activities which appear unusual. Similarly, business units and subsidiaries may receive such information from these functions when necessary for AML/CFT purposes.

III. Safeguard the confidentiality and use of information exchanged, including safeguards to prevent tipping-off.

Article 9 (Duty of confidentiality)

The Bank should not disclose the information of customer's risk level to its customers or personnel unrelated to AML/CFT obligations.

Regarding matters of suspicious ML/TF transaction reporting and/or reporting of TF sanctioned individual, all staff should keep them confidential and should not leak out at will. The documents related to matters of such reporting should be treated as confidential documents, and the case of leakage should be handled in accordance with the Money Laundering Control Act, Counter-Terrorism Financing Act, or relevant regulations.

Article 10 (Establish the Guidelines)

To carry out the implementation of the Policy, the Bank should establish the "Guidelines Governing Anti-Money Laundering and Countering the Financing of Terrorism"

and execute it after obtaining the approval from the board of directors. In the case of amendment, the requirements of this Article also apply.

Article 11 (Implementation and amendment)

The Policy should be implemented after approved by the board of directors. In the case of amendment, the requirements of this Article also apply.