FFHC Anti-Money Laundering and Countering Terrorism Financing Policy

Article 1. Purpose

This Policy is a consistent set of anti-money laundering and anti-terrorism financing guidelines established to maintain financial stability, combat criminal and terrorism financing activities, strengthen anti-money laundering and countering terrorism financing mechanisms, and prevent facilitating money laundering and terrorism financing activities through the provision of financial products or services of the company.

Article 2. Suitable for:

This Policy is applicable for business entities in conformity with Article 5 of the Money Laundering Control Act, which shall include branches and investment businesses both at home and overseas (hereafter referred to as FFHC Subsidiaries).
Investment businesses in the preceding paragraph refer to subsidiaries with more than 50% voting interest or that have contributed more than 50% of share capital in the investee company or that have directly or indirectly elected or appointed more than 50% of directors of the investee company.

Article 3. Commitment

To increase the depth of implementing anti-money laundering and countering terrorism financing of the group, First Financial Holding Co., Ltd. (FFHC; hereafter referred to as the Company) is committed to ensuring that all business entities of the group will establish a culture of anti-money laundering and countering terrorism financing. The Company shall allocate the manpower and resources required for executing operations related to anti-money laundering and countering terrorism financing.

Article 4. Scope of compliance

When handling matters related to anti-money laundering and countering terrorism financing, the entities of the group shall adhere to related laws and regulations enforced by competent authorities of Taiwan and overseas, as well as this Policy. Each business entity of the group shall ensure that its overseas branches implement anti-money laundering and countering terrorism financing measures consistent with those of the parent company, provided that it complies with local laws and regulations. This provision shall not apply to entities based overseas, where higher regulatory standard is adopted and one that shall prevail, or where the regulatory provision prohibits the entity from doing so.

Article 5. Principle of compliance

Each business entity of the group shall comply with the following principles when executing matters related to anti-money laundering and countering terrorism financing:

I. Risk-based orientation: The entity shall adopt risk-oriented management method and establish standard operating procedures for risk identification, assessment, and management, which shall be used to classify risks associated with customers, region, products and services, transaction or payment channels of the entity. A risk management mechanism shall be adopted accordingly and its validity checked on a regular basis.

II. Customer identity confirmation: The entity shall implement customer know-how, prudently assess customer and customer interaction principles, and formulate necessary internal regulations; if a customer is a corporation or trustee, the entity shall identify the customer's beneficiary and take reasonable authentication measures. Unless elsewhere regulated by law, each entity may not establish business relationships with the customer or conduct temporary transaction prior to completing the confirmation of customer's identity.

III. Customer due diligence: The entity shall establish policies and procedures for the verification of the names and titles of customers and parties relating to transactions. For "non-face-to-face" customers, the entity shall adopt customer verification procedures with the same effects as those used for "face-to-face" customers and implement special and adequate measures. The entity shall also use or establish a database of names of suspicious individuals and a search engine system to compare customers with individuals on the list (including individuals under economic sanctions, individuals, legal entities, or organizations sanctioned by the Ministry of Justice in accordance with the Terrorism Financing Control Act, or terrorists or terrorist groups identified or investigated by a foreign government or international organization) to verify the veracity of customer identity information. Following the company's risk assessment mechanism and internal control system, the entity shall implement different customer ID confirmation measures and continuous review mechanisms according to the risk assessment results (risk levels) of customers.

IV. Ongoing monitoring of accounts or transaction: The entity shall use IT system to integrate the basic information and transaction records of all customers and develop policies and procedures for ongoing monitoring of accounts or transaction. The aforementioned policy and procedures shall be regularly reviewed and updated.

V. Transaction reporting: Currency transactions equal to or above the applicable designated threshold and suspicious transactions identified through ongoing monitoring of accounts or transaction that should be reported, they shall be reported to the designated supervisor by the department head at the head office for approval, and then submitted to the competent authority. Overseas entities and investment businesses may report the said transactions to the competent authority in accordance with local laws and internal regulations.

VI. Data retention: The entity shall retain any customer transaction documents, confirmations and regulatory filings in accordance with law. Such items shall be kept for a minimum of five years and all filings shall be sufficient to reestablish individual transactions and readily available when requested upon by the competent authority.

Article 6. Responsible unit/head

Unless elsewhere regulated by law, the business entities of the company shall establish a unit responsible for anti-money laundering and countering terrorism financing, and shall allocate adequate manpower and resources depending on the size and risks involved. The board shall appoint a head as the designated supervisor and grant him or her with the necessary authority to execute anti-money laundering and combating terrorism financing. The designated supervisor shall report to the board and supervisors or audit committee semiannually. Any major violations discovered shall be reported to the board and supervisors or audit committee.

Article 7. Employee hiring and training

The business entities of the group shall establish prudent and appropriate recruiting procedures for staff, including an examination of his/her integrity and necessary expertise for performing his/her duties. In addition to acquiring necessary certificates, employees shall at least participate in education and training for a fixed number of hours every year.

Article 8. Establishment and implementation of internal control systems

The business entities of the group shall adopt three lines of defense to ensure accurate implementation of anti-money laundering and combating terrorism financing and establish internal control systems that shall cover at least the following matters:

I. Policies and procedures for the identification, assessment, and management of money laundering and terrorism financing risks.

II. Anti-money laundering and combating terrorism financing plans based on the risk assessment results and size of business to manage and reduce the risks identified, and adopt reinforcement control measures for high-risk items.

III. Standard operating procedures for monitoring and control of compliance with anti-money laundering and combating terrorism financing regulations and executing anti-money laundering and combating terrorism financing plans, which shall be included in self-assessments and internal audits and shall be improved when necessary.

IV. The entity is advised to regularly appoint foreign consultants to conduct independent identification and verification to verify the effectiveness of the AML/CFT framework, procedures, and operating system.

The business entities of the group shall appoint senior managers as supervisory managers to each of their domestic and overseas business units who supervise internal execution of anti-money laundering and combating terrorism financing matters, and shall be subject to self-assessments in accordance with regulations or incorporated in internal control self-assessment operations. Internal auditing units shall organize inspections in compliance with regulations to ensure the legality and validity of the anti-money laundering and combating terrorism financing plans.

Article 9. Politically exposed persons

Where a customer, or its person in charge, beneficial owner, or senior manager of a company of the Group is a current or former politically exposed person (PEP) of a domestic or foreign government or international organization, the customer shall be directly regarded as a high-risk customer. In addition to enhanced verification of customer identity, the entity shall conduct at least the following enhanced measures and conduct at least one customer review each year.

I. Approval from the manager from the level above the original authorization level must be obtained before customers may open new accounts or engage in new business dealings.

II. Reasonable measures shall be taken to establish the customer's motivation for establishing business transactions, source of wealth, and source of funds (e.g., salary, investment income, purchase and sale of real estate property, etc.). The same shall apply to users of type 3 electronic payment accounts.

III. Enhanced ongoing monitoring shall be conducted on the business relationship.

Regulations in the preceding paragraph also apply to PEPs' family members and close associates.