Anti-Money Laundering and Countering Terrorism Financing Policy of E.SUN Financial Holding Company and its Subsidiaries[1]

Approved on the 8th meeting of the 6th Term by the Board of Directors

Dated April 25, 2018

Chapter I General Principles

Article 1 Basis

To strengthen the anti-money laundering ("AML") and counter terrorism financing ("CFT") mechanisms of E.SUN Financial Holding Company (hereinafter called "the Company") and its subsidiaries, to establish the internal control and audit framework, and to maintain the reputation of the Company and its subsidiaries, the "Anti-Money Laundering and Countering Terrorism Financing Policy of E.SUN Financial Holding and Subsidiaries" (hereinafter referred to as "the Policy") has been formulated in accordance with Article 8, Paragraph 10 of the Implementation Rules of Internal Audit and Internal Control System of Financial Holding Companies and Banking Industries, Article 7 of the Directions Governing Internal Control System of Anti-Money Laundering and Countering Terrorism Financing of Banking Sector and Electronic Payment Institutions as well as Electronic Stored Value Card Issuers, Article 5 of the Directions Governing the Internal Control System for Anti-Money Laundering and Countering Terrorism Financing of the Securities and Futures Sector, Article 2 of Template of Directions Governing Anti -Money Laundering and Countering the Financing of Terrorism of Banks of the Bankers Association of the R.O.C., and Article 11 of the Template for Guidelines Governing Anti-Money Laundering and Countering Terrorism Financing of Securities Firms of the Taiwan Securities Association. The objective of the Policy is to establish consistent standards of internal control and code of conduct for the Company and its subsidiaries.

Article 2 Objectives

The Policy sets out the Company's overall AML/CTF framework. Its objectives are as follows:

(1) To comply with laws and regulations with regard to anti-money laundering and countering terrorism financing, relevant legislation promulgated by the authorities, and other related regulations.

(2) To mitigate the risk of the Company, its subsidiaries and their employees, products or services being used by customers for money laundering and terrorist financing.

(3) To strengthen employees' awareness on detection of money laundering, including acquisition of professional knowledge on prevention of money laundering, implementation of customer due diligence, appropriate document retention and transaction monitoring.

Article 3 Applicability

The Policy shall apply to the Company and "financial institutions" as defined in Article 5 of the Money Laundering Control Act of the Company's host country which are affiliated to the Company. Such "financial institutions" include foreign subsidiaries or branches (hereinafter referred to as "respective applicable entities") and their employees.

Article 4 Principle of application of stricter standard:

[1] "The Policy" is originally written in Chinese, this document is the translated version for reference purpose only. If there should be any discrepancy or contradiction in between, the original Chinese version will be prior.
(此英譯版本為參考，若與正式中文文件存有歧義，請以中文版為主)。

To the extent that the laws and regulations of host countries or jurisdictions so permit, foreign branches and subsidiaries shall implement AML/CTF measures that are consistent with those adopted by the head office (or parent company). Where the minimum requirements of the host countries of the Company and foreign branches and subsidiaries are different, the foreign branches and subsidiaries shall choose to comply with the higher standards. However, in case there is any doubt regarding the determination of higher or lower standards, the determination made by the competent authority of the Company's host country shall prevail. If the foreign branches and subsidiaries is not allowed to implement the measures of head office (or parent company) due to conflicting with foreign regulatory requirements, the bank should apply appropriate additional measures to manage ML/TF risks. In addition, such measures shall be reported to the dedicated AML unit or dedicated supervisor of the foreign branches and subsidiaries' local parent company or head office and filed with the competent authority of the place in which the Company is located, i.e. Financial Supervisory Commission (FSC).

Article 5 Organization and responsibilities

I. The Company shall deploy a sufficient number of individuals to be responsible for AML/CTF work; such individuals shall be solely responsible for the management and implementation of the Group's AML/CTF work, and shall be responsible for conducting the following:

(1) Formulation and implementation of group-wide AML/CTF policies;

(2) Establishment and management of group-wide AML/CTF risk appetite;

(3) Identification and assessment of group-wide AML/CTF risk;

(4) Planning of Group-wide AML/CTF information-sharing procedures and mechanisms;

(5) Assisting the respective applicable entities in the development and implementation of AML/CTF program;

(6) Supervising the respective applicable entities in implementation of AML/CTF program;

(7) Coordinating, managing and supporting the respective applicable entities on AML/CTF-related matters.

II. The respective subsidiaries shall be staffed with an adequate number of AML/CTF personnel and resources appropriate to the size and risks of its business. The board of directors of the respective subsidiaries shall appoint a senior officer to act as the dedicated AML/CTF Responsible Officer and vest the person full authority in coordinating and supervising AML/CTF implementation and shall ensure that its AML/CTF personnel and the dedicated AML/CTF head does not have concurrent responsibilities that may have a conflict of interest with their AML/CTF responsibilities. Banking subsidiaries (including banking subsidiaries of such subsidiaries) shall, set up an independent, dedicated AML/CTF compliance unit under the president or the legal compliance unit or risk management unit of the head office; such AML/CTF compliance unit shall not handle businesses other than AML/CTF.

III. The dedicated responsible unit or dedicated AML/CTF Responsible Officer mentioned in the preceding subparagraph shall be in charge with the following duties:

(1) Supervising the planning and implementation of policies and procedures for identifying, assessing and monitoring ML/TF risks.

(2) Coordinating and supervising the institution's implementation of AML/CTF risk identification and assessment.

(3) Monitoring and controlling ML/TF related risks.

(4) Developing an AML/CTF program.

(5) Coordinating and supervising the implementation of the AML/CTF program.

(6) Confirming the Company is in compliance with AML/CTF related laws and regulations, including the relevant templates or self-regulatory rules formulated by the related financial services association and approved by the competent authorities.

(7) Supervising the reporting of suspicious ML/TF transactions and properties or property interests and location of designated individuals or legal entities sanctioned under Counter-Terrorism Financing Act to the Financial Intelligence Unit. The Investigation Bureau, Ministry of Justice is the Financial Intelligence Unit of the Company's host country.

IV. The responsible units or Responsible Officer in the foreign subsidiaries of the respective applicable entities shall be in charge of the aforesaid affairs, report to the respective dedicated responsible unit or dedicated Responsible Officer in their parent company.

V. The dedicated AML/CTF Responsible Officer mentioned in Subparagraph 2 hereof shall report to the board of directors and supervisors (board of supervisors) or the audit committee of the company concerned at least semi-annually, or whenever a major regulatory violation is discovered.

VI. The foreign business units of the respective applicable entities shall be staffed with an adequate number of AML/CTF personnel taking into consideration the size and risks of their business, and appoint an AML/CTF compliance head to take charge of the coordination and supervision of related compliance matters.

VII. The appointment of an AML/CTF compliance head by the foreign business unit of the respective applicable entities shall comply with the regulations of the host country and the requirements of the local competent authority. The AML/CTF compliance head shall be vested with full authority in AML/ CFT coordination and supervision, including reporting directly to the dedicated AML/CTF Responsible Officer mentioned in Subparagraph 2, and shall not hold other concurrent responsibilities, except compliance head. If the AML/CTF compliance head holds other concurrent responsibilities, the foreign business unit shall communicate the fact with the competent authority of the host country to confirm the holding of other concurrent posts not resulting in or potentially leading to the conflict of interest, and file a report on the matter to the competent financing authority of the Company's host country, i.e. the FSC.

Article 6 ML/TF risk appetite

I. The Company and the respective applicable entities shall set their risk appetite for ML/TF, and establish specifically with respect to the degree and type of their willingness to bear money-laundering and sanction risk, corresponding structures for management purposes.

II. The Company and the respective applicable entities shall monitor their risk limit on a regular basis. When risk approaches or exceeds the limit of the set risk appetite, improvement plan shall be formulated, along with relevant measures including restriction of business activity, and strengthened control procedures for risk mitigation.

III. The limit for ML/TF-related risks shall be inspected and approved by the Company’s business management unit (risk management) and board of directors on an annual basis.

Chapter II Anti-Money Laundering and Combating Terrorism Financing Matters

Article 7 Definition:

I. Money laundering:

(1) Money laundering under the Policy shall, in addition to that regulated by the Money Laundering Control Act of the Company's host country, include that as defined by respective international organizations and international conventions.

(2) Pursuant to Article 2 of the Money Laundering Control Act of the Company's host country, money laundering refers to the following actions:

1. Attempt to cover up or conceal the source of illegal/criminal gains, or attempt to transfer or alter specific illegal/criminal gains such as to enable others to evade criminal prosecution.

2. Disguise or conceal the nature, source, destination, location, ownership, right of disposal or other rights of specific illegal/criminal gains.

3. Accept, hold or use of specific illegal/criminal gains of others.

(3) Money laundering consists of the following three phases:

1. Placement

This is the earliest phase of money laundering; its purpose is to direct illegally-obtained cash into the financial system without raising the attention of financial institutions or law enforcement authorities. Skills for placement of cash include breaking down the sum of cash to be deposited with financial institutions to avoid triggering reporting requirements, and purchase of financial tools such as bank drafts before cashing them and then depositing the cash into financial institutions.

2. Layering

During this phase money laundering mainly consists of moving the funds within the financial system, through numerous and complex financial transactions or records to cover up the source of illegal gains, e.g., using the accounts in several banks to transfer funds.

3. Integration

Following complex layering transactions involving illegal gains such as to integrate them into the financial system, the purpose at this phase is to arrange additional transactions to give an image of obtaining funds in a lawful manner; the types of transaction include: sale and purchase of real estate and securities.

II. Terrorism financing:

(1) Terrorism financing under this Policy refers to the process of raising funds for terrorists in order for the latter to conduct terrorist activities.

(2) Terrorism financing often refers to transactions involving funds being owned by terrorists or have been or are intended to assist terrorist activities. In general the focus of AML systems is on handling of illegal gains. In other words the source of funds is the major focus in AML systems. However, with respect to terrorism financing, the focus is on the destination or ultimate usage of the funds. The funds may have lawful origins.

III. Beneficial owner: This is the natural person(s) who ultimately owns or controls a customer and/or the natural person on whose behalf a transaction is being conducted, including those persons who exercise ultimate effective control over a legal person or arrangement.

IV. Risk-based approach (RBA):

(1) This refers to the respective applicable entities being required to identify, assess and understand the money laundering and terrorist financing (ML/TF) risks to which they are exposed and take appropriate anti-money laundering and countering terrorist financing (AML/CTF) measures commensurate with those risks in order to effectively mitigate them. Using risk-based approach to undertake customer due diligence and continuous monitoring is universally recognized as the most effective AML/CTF means. The general principle of risk-based approach is: insofar as a customer is assessed as having greater ML/TF risk, the respective applicable entities shall immediately adopt enhanced measures to control and reduce such risk. If the risk is relatively minimal, simplified measures can be adopted. An advantage of risk-based approach is the ability prioritize, thus maximizing the efficiency of resource-allocation. Customers with the greatest risk can receive the greatest attention.

(2) For customers with greater ML/TF risk, enhanced customer due diligence procedure shall apply. This includes requirement for more information on the customer's identity, approval by a higher level of management, more frequent monitoring of transactions and regular review.

V. Shell banks: This refer to banks which do not have physical presence in their country of incorporation and approval, and which are not being affiliated with financial groups subject to effective merged supervision and control. Physical presence refers to implementation of meaningful planning and management in specific countries. Establishment of local agency institution or low-level personnel does not amount to physical presence.

Article 8 Customer due diligence measures

I. The respective applicable entities shall verify the customer’s identity in the following situations:

(1) When establishing business relations with the customer;

(2) When undertaking any temporary transactions of specific amount;

(3) When there is a suspicion of money laundering or terrorist financing;

(4) When they have doubts about the veracity or adequacy of previously obtained customer identification data.

II. The following measures shall be adopted when verifying the customer’s identity:

(1) Identify the customer and verify that customer’s identity using reliable, independent source documents, data or information. In addition, they shall retain copies of the customer’s identity documents or record the relevant information thereon.

(2) Verify that any person purporting to act on behalf of the customer (the representative) with respect to establishment of business relationship or undertaking a transaction is so authorized. They shall furthermore truly verify the fact of such authorization, and identify and verify the identity of the agent using reliable, independent source documents, data or information. In addition, they shall retain copies of the agent’s identity documents or record the relevant information thereon.

(3) Verify the identity of the beneficial owner of the customer and take reasonable measures to verify the identity of the beneficial owner, including using relevant data or information from a reliable source.

(4) Understand and, depending on the situation, obtain relevant information of the purpose and intended nature of the business relationship when undertaking (customer due diligence) CDD measures.

III. When the customer is a legal person, they shall understand whether the customer is able to issue bearer shares and apply appropriate measures for customers who have issued bearer shares to ensure their beneficial owners are kept up-to-date.

IV. When the customer is a legal person, an organization or a trustee, they shall understand the ownership and control structure of the customer or the trust, and identify the beneficial owners of the customer and take reasonable measures to verify the identity of such persons.

V. If an applicable entity forms a suspicion of money laundering or terrorist financing and reasonably believes that performing CDD procedure will tip off the customer, it is permitted not to pursue that procedure and file a suspicious transaction report (STR) instead.

Article 9 Ongoing review of customer's identity:

I. The respective applicable entities shall conduct ongoing due diligence on the business relationship with the customer to scrutinize transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with their knowledge of the customer, its business and risk profile, including, where necessary, the source of funds.

II. The respective applicable entities shall review periodically the sufficiency of the information for identifying customers and beneficial owners based on their importance and risk level, and ensure that such information is updated. In particular, high-risk customers shall be reviewed at least once annually.

III. The respective applicable entities can rely on existing customer records to undertake identification and verification without the need to repeatedly identify and verify the identity of an existing customer when carrying out transactions. However, the respective applicable entities shall conduct CDD measures again in accordance with Article 8 when they have doubts about the veracity or adequacy of the records, when there is a suspicion of ML/TF in relation to such customers, or when there is a material change in the way that such customers' transactions are conducted or their accounts are operated, which is not consistent with the customer's business profile.

Article 10 Customer acceptance procedure and refusal to establish business relationship or transaction:

I. The respective applicable entities shall formulate customer acceptance procedure in order to identify the type of customers with high ML/TF risks. They shall also refuse to establish business relationship or undertake transactions with the type of customers with excessive ML/TF risk.

II. When verifying the customer's identity, insofar as the subject of establishment of business relationship is under sanction or a terrorist, or where there are irregularities such as unclear identity, or provision of false information or concealment of information, they shall refuse to establish such relationship or undertake transactions.

III. When establishing business relationship with customers, the respective applicable entities shall state in relevant contractual documents such as master agreements that if such customers are involved in ML and TF, or refuse to cooperate with their CDD, or provide false information or conceal information, they can suspend such customers' transactions or temporarily suspend or terminate their business relationship with such customers.

Article 11 Timing of strengthening CDD measures and ongoing review mechanism:

I. The Company shall provide a list of ML/TF risk ratings based on countries to specify countries or jurisdictions with extremely high and high ML/TF risks. Formulation of such list shall take the level of aggressiveness of the respective countries against money laundering and terrorism financing into consideration, including but not limited to those in which the competent authority in the Company's host country, i.e., the FSC has forwarded publication by international organizations on AML/CTF as countries or jurisdictions with serious deficiencies in their AML/CTF regimes, and other countries or jurisdictions that do not or insufficiently comply with the recommendations of international organizations on AML/CTF.

II. If any transaction involves countries or jurisdictions with extremely high ML/TF risk, e.g., the source of remittance or the beneficiary is from such countries or jurisdictions, the respective applicable entities are forbidden to undertake such transaction in principle.

III. The respective applicable entities shall strengthen their measures for verification of customer's identity or ongoing review on the following type of customers:

(1) They are high-risk customers;

(2) The customers or their beneficial owners are from countries or jurisdictions with extremely high ML/TF risk;

(3) Other circumstances in which the respective applicable entities are of the opinion that there is a need to strengthen customer identity verification or ongoing review measures.

Article 12 Enhanced or simplified CDD measures and ongoing review mechanism:

The measures for verification of customer identity and ongoing review mechanism shall be conducted on a risk-based approach (RBA):

(1) Insofar as a customer is involved in circumstances provided in Article 11, Paragraph 3, enhanced CDD or ongoing review measures shall be conducted, including adopting at least the following additional enhanced measures:

1. Obtaining approval from senior management officer before establishing or entering a new business relationship;

2. Conducting enhanced CDD measures;

3. Conducting enhanced ongoing monitoring of the business relationship, e.g., increasing the frequency of customer review and implementing enhanced monitoring mechanism.

(2) For lower risk circumstances, simplified CDD measures which shall be commensurate with the lower risk factors may be applied. However simplified CDD measures are not allowed in any of the following circumstances:

1. The customer comes from an extremely high or high ML/TF risk country or jurisdiction with;

2. There is a suspicion of ML/TF in relation to the customer or the transaction.

Article 13 Customer risk assessment:

I. The respective applicable entities shall conduct verification, assessment and management of customers' ML/TF risk, based on which they shall set at least 3 risk ratings namely high, medium and low risk. The level of approval and respective procedures shall be determined in accordance with customers' risk ratings.

II. Specific risk assessment factors shall at least include indicators such as jurisdiction, the customer and its product and service, transaction or payment channel risk:

(1) Jurisdiction risk: Countries that are exposed to higher ML/TF risk shall be identified by the respective applicable entities.

(2) Customer risk: The respective applicable entities shall take an overall account of the customer's background, occupation, characteristics of social and economic activities, countries, channel through which a business relationship is established with the customer and in the case of an entity customer, its organization type and structure, etc., to identify the customer's ML/TF risk.

(3) Product and service, transaction or payment channel risk: The respective applicable entities shall identify the nature of individual products and services, transactions or payment channels that have higher ML/TF risk that may bring greater ML/TF risk.

III. The respective applicable entities and their employees shall not disclose to outside parties information relating to their customers' risk rating. The above shall not apply if such disclosure is in cooperation with statutory AML/CTF matters.

IV. The respective applicable entities shall update customer information regularly and re-assess the risk nature.

Article 14 Name screening procedure:

I. The respective applicable entities shall establish policies and procedures for name screening, based on a risk-based approach, to detect, match and filter whether customers, or the senior management officers, beneficial owners or connected parties of the customers are sanctioned individuals, legal persons or organizations, or terrorists/terrorist groups identified or investigated by a foreign government or an international organization.

II. The procedure for name screening on customers, counterparties and relevant parties of a transaction that established by the respective applicable entities shall at least include matching and filtering logics, the operation procedure for name screening and the standard of review, and should be documented.

III. The lists used for name screening shall be announced by the Company separately. The respective applicable entities may add additional lists depends on local regulatory requirements and actual need.

Article 15 Politically Exposed Persons (PEPs):

I. Politically Exposed Persons (PEPs) are individuals who currently or previously hold important public appointments and who possess significant power in policy-making, action or allocation of government resources. By reason for their appointment and status, PEPs are inevitably subject to corruption risk. If a PEP comes from a country where corruption among public officials and private individuals is rampant, such a risk will undoubtedly increase. In addition, if such country does not possess appropriate AML/CTF standard, the risk of corruption will be even more serious. In the circumstances, the respective applicable entities are required to determine whether a customer, the beneficial owners or senior management officers are PEPs.

II. When verifying customer's identity, the respective applicable entities shall determine whether a customer, the beneficial owners or senior management officers are individuals who are or were politically exposed persons("PEPS") entrusted by a foreign government or an international organization:

(1) For a customer or the beneficial owner thereof determined to be a current PEP of a foreign government, the respective applicable entities shall treat the customer directly as a high-risk customer, and adopt enhanced CDD measures under Subparagraph 1, Paragraph 1 of Article 12.

(2) For a customer or the beneficial owner thereof determined to be a current PEP of the domestic government or an international organization, the respective applicable entities shall assess the PEP's risks when establishing business relationship with the PEP and conduct annual review thereafter. Insofar as business relationship with a customer is determined to be of high risk, the respective applicable entities shall adopt enhanced CDD measures under Subparagraph 1, Paragraph 1 of Article 12.

(3) Where a senior management officer of a customer is determined to be a current PEP of the domestic government, a foreign government or an international organization, the respective applicable entities shall determine whether to apply the enhanced CDD measures under Subparagraph 1, Paragraph 1 of Article 12 considering the officer's influence on the customer.

(4) For a PEP who is no longer entrusted with a prominent public function by the domestic government, a foreign government or an international organization, the respective applicable entities shall assess the influence that the individual could still exercise after considering relevant risk factors and determine whether to apply the provisions of the preceding three sub-paragraphs.

(5) The preceding four sub-paragraphs apply to family members and close associates of PEPs.

III. The respective applicable entities shall establish corresponding implementation procedures for PEPs, their family members and close associates in terms of scope, review and risk assessment.

Article 16 Ongoing due diligence of accounts and transactions;

I. The respective applicable entities shall use a database to consolidate basic information and transaction information on all customers for the purpose of AML/CTF inquiries so as to strengthen capability of account and transaction monitoring. The respective applicable entities shall also establish internal control procedures for requests and inquiries regarding customer information, ensuring confidentiality of the information.

II. The respective applicable entities shall establish policies and procedures for account and transaction monitoring based on a risk-based approach and utilize information systems to assist in the detection of suspicious ML/TF transactions.

III. The respective applicable entities shall review their policies and procedures for account and transaction monitoring based on AML/CTF regulations, nature of customers, business scale and complexity, ML/TF trends and related information gathered from internal and external sources, and their internal risk assessment results, and update those policies and procedures periodically.

IV. The policies and procedures for account and transaction monitoring of the respective applicable entities shall be documented and at least include complete ML/TF monitoring scenarios, parameters setting, threshold amounts, alerts and operation procedures of monitoring, the reviewing procedures for monitored cases and reporting standards.

V. Complete ML/TF monitoring scenarios mentioned in the preceding subparagraph shall, based on the business nature of the respective applicable entities, include the suspicious scenarios published by the competent authorities and relevant associations, and add additional monitoring scenarios in respect to the ML/TF risk assessment or daily transaction information of the respective applicable entities.

Article 17 Correspondent banking business:

I. The respective applicable entities shall implement the following measures for cross-border correspondent banking and other similar transactions:

(1) Gather sufficient publicly-available information to fully understand the nature of the correspondent bank's business and to determine its reputation and quality of management, including whether it has complied with AML/CTF regulations and whether it has been investigated or received regulatory action in connection with money laundering or terrorist financing (ML/TF);

(2) Assess whether the institutional client (respondent bank) has adequate AML/CTF controls;

(3) Obtain approval from senior management officers before establishing relationships with an institutional client (respondent bank);

(4) Document the respective AML/CTF responsibilities of each party;

II. The respective applicable entities shall confirm that the institutional client (respondent bank) are not involved in payable-through accounts when handling cross-border correspondent banking business.

III. The respective applicable entities are prohibited from entering into or maintaining correspondent relationship with shell banks and shall be required to satisfy themselves that respondent financial institutions do not permit their accounts to be used by shell banks;

IV. For the institutional client (respondent bank) that is unable to provide the aforementioned information upon the request of the respective applicable entities, the respective applicable entities may decline the correspondent bank's application to open an account, suspend transactions with the correspondent bank, file a suspicious ML/TF transaction report or terminate business relationship ;

V. The aforementioned provisions shall also apply when the institutional client (respondent bank) is a foreign branch or subsidiary of the Bank.

Article 18 Filing currency transaction report (CTR):

I. The respective applicable entities shall establish in accordance with local laws and regulations, procedure for filing transaction report above certain amounts such as to enable them to file with Financial Intelligence Unit for transactions above designated amounts.

II. Filing of transaction reports for transactions involving designated amounts by the respective applicable entities, and the scope and mode of such reports shall be pursuant to relevant regulations promulgated by local competent authorities.

Article 19 Filing suspicious ML/TF transaction report (STR):

I. The respective applicable entities shall establish STR procedure. For transactions which are deemed suspicious they shall in addition to verifying the customer's identity and retain transaction record, file report with Financial Intelligence Unit regardless of the amount involved.

II. Suspicious transactions referred to in the preceding paragraph shall be reported to Financial Intelligence Unit whether or not they are completed.

III. The respective applicable entities and their employees are, in addition to requirements by the law, prohibited from disclosing to others except for the Company and the respective applicable entities information on STR or relevant matters.

IV. Filing of STR by the respective applicable entities and the scope and mode of the STR shall be pursuant to relevant regulations promulgated by local competent authorities.

V. If a foreign branch or subsidiary discovers transactions suspected to be involved in ML/TF, it is not required to lodge report with the justice department of the Company's host country. However it shall still be required to comply with local laws and regulations.

Article 20 ML/TF risk assessment for new products, services or businesses:

The respective applicable entities shall establish ML/TF risk assessment procedure for new products, services or businesses. Prior to launching such new products, services or businesses, they shall conduct ML/TF risk assessment. They shall also establish corresponding risk management measures to reduce any risk identified.

Article 21 Record keeping:

I. The respective applicable entities shall establish procedure for retention of records or files (including without limitation files or information obtained from CDD, account-opening documents, relevant transaction records, transaction monitoring records and filing information) relating AML/CTF work process for future inspection and inquiry. Such records or files shall also serve as evidence in AML/CTF matters.

II. The respective applicable entities shall keep records on all business relations and transactions with its customers in hard copy or electronic form and in accordance with the following provisions:

(1) For domestic and international transactions all necessary records shall be retained for at least five years; the respective applicable entities shall comply with local laws and regulations insofar as they prescribe a longer period for retention of such records.

(2) The respective applicable entities shall keep all the following information for at least five years or a longer period as otherwise required by law after the business relationship is ended or temporary transaction is completed. The respective applicable entities shall comply with local laws and regulations insofar as they prescribe a longer period for retention of such records:

1. All records obtained with respect to verification of customer's identity.

2. Account files (including e-payment accounts and the accounts of electronic stored value card holders) or contract files.

3. Business correspondence, including information on the background and purpose obtained from inquiries to complex, unusual large transactions and the results of any analysis undertaken.

III. Transaction records maintained by the respective applicable entities must be sufficient to reconstruct individual transactions so as to provide, if necessary, evidence of criminal activity.

IV. The respective applicable entities shall ensure that transaction records and CDD information will be available promptly to the competent authorities when such requests are made with appropriate authority.

Article 22 Information Sharing:

I. To assist the respective applicable entities under the Company in conducting CDD procedure, as well as to achieve the Company's objective of managing AML/CTF risk, the Company shall establish at Group level, information sharing procedure and mechanism for the purposes of AML/CTF, including the scope of information sharing and mode of utilization of such information for use by the respective applicable entities insofar as it is within the scope of AML/CTF such as to enable them to conduct regular review of customer information, strengthened ongoing due diligence and adopt other necessary measures.

II. The Company may collect and summarize the regulations, procedures, or successful examples from the respective applicable entities and share the information among the other applicable entities in order to enhance the skills and performance of countering money laundering and combating the financing of terrorism.

Article 23 Employee's recruitment and training:

I. The respective applicable entities shall establish prudent and appropriate procedures for employee screening and hiring, including examining whether the prospective employee has character integrity and the professional knowledge required to perform his or her duty.

II. The respective applicable entities shall arrange for newly-recruited employees to undergo training on AML laws and regulations and legal responsibilities of financial staff, in order for such employees to understand the rules and regulations.

III. Appointment by the respective applicable entities of dedicated AML/CTF Responsible Officer, responsible staff and AML/CTF supervisor of business units (hereinafter called "AML/CTF supervisor") shall be in compliance with requirements of laws and regulations for qualifications. In addition the respective applicable entities shall formulate relevant control mechanism for such appointments.

IV. The respective applicable entities' dedicated AML/CTF Responsible Officer, responsible staff and AML/CTF supervisor of business units shall participate in annual AML/CTF training. The unit holding such training, training contents and training hours shall be in compliance with statutory requirements.

V. The respective applicable entities shall, pursuant to requirements of laws and regulations and business needs, conduct regular training or awareness education on their staff in order for such staff to understand relevant AML/CTF regulations, the scope of their responsibility, work procedures and relevant measures with which they shall be in compliance.

VI. The respective applicable entities shall arrange appropriate hours of orientation and on-the-job training of suitable contents on AML/CTF annually, taking into consideration the nature of their business for their directors, supervisors, president, legal compliance personnel, internal auditors, and business personnel such that they are familiar with their AML/CTF duties and are equipped with the professional know-how to perform their duties.

Article 24 Institutional ML/TF risk assessment:

I. The respective applicable entities shall establish a mechanism of periodic institutional ML/TF risk assessment and generate a risk assessment report to enable senior management to timely and effectively understand their overall ML/TF risks, determine necessary mechanisms to be established, and develop appropriate mitigation measures.

II. The respective applicable institutional ML/TF risk assessment results shall be used as a basis to develop AML/CTF programs. The respective applicable entities shall allocate appropriate head counts and resources based on such results and take effective countermeasures to prevent or mitigate risks.

III. Specific risk categories of such ML/TF risk assessment work shall cover at least geographic areas, customers, products, services, transactions or payment channels, etc. The respective applicable entities shall furthermore analyze each risk category to determine detailed risk factors.

IV. If a material change occurs to an applicable entity, e.g. a material incident, material development in management and operation, or relevant new threats, it shall re-perform the assessment.

Article 25 ML/TF risk prevention plan:

I. The respective subsidiaries (including their subsidiaries) shall formulate, based on the results obtained from analysis of risk assessment, ML/TF risk prevention plan.

II. To ensure that the annual prevention plans devised by the respective subsidiaries can be effectively executed, the Company's Chief Risk Officer shall report the results of the aforesaid annual prevention plans to the board of directors of the Company at least once a year.

Article 26 Implementation and statement of internal AML/CTF control system:

I. The domestic and foreign business units of the respective applicable entities shall each appoint a senior manager to act as the supervisor to take charge of supervising AML/CTF related matters.

II. The internal audit unit of the respective applicable entities shall conduct audit on the following matters and submit audit opinions on:

(1) Whether the ML/TF risk assessment and the AML/CTF program meet the regulatory requirements and are implemented; and

(2) The effectiveness of AML/CTF program.

III. The president of the Company shall oversee the respective units to prudently assess review the implementation of internal control system for AML/CTF; The chairman, president, general auditor and dedicated AML/CTF Responsible Officer of the respective local subsidiaries shall jointly issue a statement on internal control for AML/CTF, which shall be submitted to the board of directors for approval and disclosed on the website of the respective local subsidiaries within three (3) months after the end of each fiscal year, and filed via a website designated by the competent financial authority of the Company's host country, i.e., the FSC.

Article 27 Ultimate responsibility for internal control:

I. The board of directors of the Company bears the ultimate responsibility of ensuring the establishment and maintenance of appropriate and effective AML/CTF internal controls.

II. The board of directors and senior management shall understand the Company's ML/TF risks and the operation of its AML/CTF program, and adopt measures to create a culture of AML/CTF compliance.

Chapter III Supplementary Provisions

Article 28 Rewards and penalties:

I. A reward shall be given for any discovery or prevention of money laundering transactions or terrorism financing or prevention of damage to the reputation of the Company and the respective applicable entities consequent upon the implementation of statutory or regulatory requirements, this Policy or relevant internal regulations of the respective applicable entities. Failure to comply with the implementation of relevant regulations thereby causing damage to the reputation of the Company and respective applicable entities shall also be penalized.

II. With regard to matters pertaining to the aforesaid rewards and penalties, the respective applicable entities shall incorporate them into corresponding regulations for rewards and penalties.

Article 29 Interpretation and application:

I. The Company delegates the authority for interpretation or final adjudication on doubts against the applicability or contents of the Policy to its Chief Risk Officer.

II. The respective applicable entities shall, in addition to complying with the Policy by establishing relevant internal regulations, also comply with the Money Laundering Control Act and Counter-Terrorism Financing Act and other related laws, relevant rules or guidelines promulgated by the competent authorities, self-discipline rules or template guidelines announced by industry associations, such as to truly implement the requirements of AML/CTF regulations.

Article 30 Review and assessment:

The Policy shall be reviewed on a yearly basis so as to reflect applicable policies and legislation, international standards, and the latest system management technology and business developments to ensure its effectiveness against money laundering and terrorism financing.

Article 31 Approval level:

The Policy shall become effective upon approval of the Board of Directors.