Template of Directions Governing Anti-Money Laundering, Combating the Financing of Terrorism and Counter Proliferation Financing for the Non-Life Insurance Sector

Approved and kept on file by the Financial Supervisory Commission, with official letter Jin Guan Bao Zong Zi No. 1140422169 dated August 11, 2025

Article 1

These directions are established in accordance with the "Money Laundering Control Act", the "Counter-Terrorism Financing Act", the "Regulations Governing Anti-Money Laundering of Financial Institutions" and the "Regulations Governing Implementation of Internal Control and Audit System for Anti-Money Laundering and Countering Terrorism Financing of An insurance company, Post Offices Engaging in Simple Life Insurance Business and Other Financial Institutions Designated by the Financial Supervisory Commission".

Article 2

The internal control system established by an insurance company, in accordance with the "Regulations Governing Implementation of Internal Control and Audit System for Anti-Money Laundering and Countering Terrorism Financing of An insurance company, Post Offices Engaging in Simple Life Insurance Business and Other Financial Institutions Designated by the Financial Supervisory Commission", for Anti-Money Laundering (AML) and Combating the Financing of Terrorism (CFT) and any subsequent amendment should be approved by its board of directors (council). The internal control system should contain the following particulars:

I. Policies and procedures for identifying, assessing, and managing the risk of money laundering and terrorism financing (ML/TF) established in accordance with the "Guidelines Governing Money Laundering and Terrorist Financing Risk Assessment and Relevant Prevention Program for Insurance Sector" (Appendix).
II. An AML/CFT program established in accordance with the above guidelines and based on ML and TF risk assessment results and business size to manage and mitigate identified risks, which also includes enhanced control measures for higher risk situations.
III. Standard operating procedures for monitoring compliance with AML/CFT regulations and for the implementation of AML/CFT program, which should be included in the self-inspection and internal audit system, and enhanced if necessary.

The identification, assessment and management of ML/TF risks provided in subparagraph 1 of last paragraph should at least cover the aspect of customers, geographic areas, and products, services, transactions or delivery channels, etc., and be conducted in accordance with the following provisions:

I. Make a risk assessment report,
II. Consider all risk factors to determine the level of overall risk, and appropriate measures to mitigate the risks,
III. Have a mechanism in place for updating risk assessment report periodically to ensure the update of risk profile,
IV. Submit the risk assessment report to the Financial Supervisory Commission (FSC) for recordation after it is completed or updated.

The AML/CFT programs provided in subparagraph 2 of paragraph 1 should include following policies, procedures and controls:

I. Verification of customer identity,

II. Name screening and watch list filtering of customers and related parties of a transaction,
III. Ongoing monitoring of transactions,
IV. Record keeping,
V. Reporting of currency transactions that reach a certain amount,
VI. Reporting of suspicious ML/TF/PF (Proliferation Financing) transactions and reporting in accordance with "Counter-Terrorism Financing Act".
VII. Appointment of a compliance officer at the management level to take charge of AML/CFT compliance matters,
VIII. Procedures for screening and hiring employees,
IX. An ongoing employee training program,
X. An independent audit function to test the effectiveness of AML/CFT system,
XI. Others required in AML/CFT related regulations or by the FSC.

An insurance company should establish a group-level AML/CFT program for implementation by branches (or subsidiaries) within the group. The AML/CFT program should include the policies, procedures and controls mentioned in the preceding paragraph, and in addition, the following particulars without violating the information confidentiality regulations of Taiwan and countries or jurisdictions at where the foreign branches (or subsidiaries) are located:
I. Policies and procedures for sharing information within the group required for the purposes of customer due diligence (CDD) and ML/TF risk management,
II. When necessary for AML/CFT purposes, group-level compliance, audit, and AML/CFT functions can be performed to obtain customer and transaction information as well as information on unusual transactions or activities and analysis from foreign branches (or subsidiaries), and when necessary, foreign branches (or subsidiaries) can access such information through group management functions,
III. Adequate safeguards on the confidentiality and use of information exchanged, including safeguard against information leakage.

An insurance company should ensure that its foreign branches (or subsidiaries) apply AML/CFT measures permitted by the laws and regulations of host countries or jurisdictions, and those measures should be consistent with those adopted by the head office (or parent company). Where the minimum requirements of the countries where its head office (or parent company) and branches (or subsidiaries) are located are different, the branch (or subsidiary) should choose to follow the criteria which are higher. However, in case there is any doubt regarding the determination of higher or lower criteria, the determination by the competent authority of the place at where the head office of the insurance company is located should prevail. If a foreign branch (or subsidiary) is unable to adopt the same criteria as the head office (or parent company) due to prohibitions from foreign laws and regulations, appropriate additional measures should be taken to manage the risks of ML/TF, and a report should be submitted to the FSC.

The branches or subsidiaries of foreign financial institutions operating in Taiwan should, in accordance with the "Guidelines Governing Money Laundering and Terrorist Financing Risk Assessment and Relevant Prevention Program for Insurance Sector", formulate policies, procedures for identifying, assessing, and managing ML/TF risks, as well as policies, procedures, and control mechanisms required for AML/CFT program. If the parent group has established regulations that are not lower than those required by Taiwan and do not violate Taiwan laws and regulations, the branches or subsidiaries operating in Taiwan may apply the regulations of the parent group.

For an insurance company that has established a board of directors (council), the board of directors (council) takes the ultimate responsibility for ensuring the establishment and maintenance of appropriate and effective AML/CFT internal controls. The board of directors (council) and senior management should understand the

company's ML/TF risks and the implementation of its AML/CFT program, and take measures to build a culture of AML/CFT compliance.

Article 3

The terms used in the template of directions are defined as follows:

I. A certain amount: "A certain amount" shall mean NTD 500,000 (or equivalent foreign currency),

II. Currency transaction: "Currency transaction" shall mean receiving cash or paying cash in a single transaction (including all transactions recorded on cash deposit or withdrawal vouchers for accounting purpose),

III. Establishing business relationship: "Establishing business relationship" shall mean that a person requests the insurance company to provide insurance or financial services and establish relationship that can continue for a duration, or that a person first approaches the insurance company as a potential customer and expects such relationship that may continue for a duration,

IV. Customer: "Customer" shall mean a person (including a natural person, a legal person, an entity or a trust) that establishes business relationship with the insurance company,

V. Beneficial owner: "Beneficial owner" shall mean the natural person(s) who ultimately owns or controls a customer, or the natural person on whose behalf a transaction is being conducted. It includes the natural person(s) who exercise ultimate effective control over a legal person or legal arrangement,

VI. Risk-based approach (RBA): "Risk-based approach" shall mean that an insurance company should identify, assess and understand the ML/TF risks that it is exposed to and take appropriate AML/CFT measures to effectively mitigate such risks. With such approach, an insurance company should take enhanced measures for higher risk scenarios while simplified measures may be taken for lower risk scenarios to effectively allocate resources and mitigate the identified ML/TF risks in the most appropriate and effective way.

VII. Related parties of a transaction: "Related parties of a transaction" shall mean any third party, which is other than a company's customers, involved in a transaction.

Article 4

An insurance company should comply with following requirements when conducting CDD measures:

I. An insurance company should avoid establishing business relationship or processing transactions if any of following situations is identified:
   (i) A customer is suspected to use anonymous, fake name, figurehead, fictitious business or entity,
   (ii) A customer refuses to provide relevant documentations required for the purpose of CDD except that the company may verify the customer's identity by using reliable and independent source of information,
   (iii) In the case that any person acts on behalf of a customer, it is difficult to verify that the person purporting to act on behalf of the customer is so authorized and it is difficult to verify the identity of that person,
   (iv) Using counterfeit or altered identity documents,
   (v) Identification documents presented are photo copies except for the business that permits the use of photo copies or soft copies of identification documents coupled with other alternative measures under applicable regulations,
   (vi) Documents provided by the customer are suspicious or unclear, the customer refuses to provide other supporting documents, or the documents provided cannot be authenticated,
   (vii) A customer delays the providing of required customer identification documents in an unusual manner,
   (viii) The parties with whom the company establishes business relationship are designated individuals, legal person or entities sanctioned under the "Counter-Terrorism Financing Act" and terrorists or terrorist groups that are identified or investigated by a foreign government or an international organization. This requirement, however, does not apply to any payment made in accordance with paragraph 1 of Article 6 of the "Counter-Terrorism Financing Act",

(ix) Other unusual scenarios occur when the company establishes business relationship with or processes transactions for a customer and the customer fails to provide a reasonable explanation.

II. An insurance company should perform CDD when:
(i) Establishing business relationship with a customer,
(ii) Conducting cash receipt or payment in a single transaction of NTD 500,000 or more (including the foreign currency equivalent) (including all transactions recorded on cash deposit or withdrawal vouchers for accounting purpose),
(iii) Identifying a suspicious ML/TF/PF transaction,
(iv) There are doubts about the veracity or adequacy of previously obtained customer identification data.

III. An insurance company should take CDD measures as follows:
(i) Identifying the customer and verifying the customer identity using reliable, independent source documents, data or information, and retaining hard copies of customer identity documents or recording the relevant information thereon,
(ii) In the case that any person acts on behalf of a customer to conduct transactions, an insurance company should verify that the person purporting to act on behalf of the customer is so authorized. In addition, identify and verify the identity of that person in accordance with preceding Item, and retain photocopies of the agent's identity documents or record the relevant information thereon,
(iii) Identifying the beneficial owner of the customer, and taking reasonable measures to verify the identity of the beneficial owner, including using reliable source data or information,
(iv) CDD measures should include understanding and, as appropriate, obtaining information on the purpose and intended nature of the business relationship.

IV. For an individual customer, an insurance company should at least obtain the following information to identify the customer identity when applying the requirements under preceding subparagraph.
(i) Full name,
(ii) Date of birth,
(iii) Household registration or residential address,
(iv) Official identification document number,
(v) Nationality,
(vi) The purpose of insurance purchase of a foreign national.

V. For a customer that is a legal person, an entity or trustee of a trust, an insurance company, when applying the requirements under subparagraph 3, should understand the business nature of the customer or the trust, and obtain at least following information of the customer or the trust to identify and verify the customer identity:
(i) The name, legal form, and proof of existence of the customer or trust,
(ii) The articles of incorporation or similar powers that regulate and bind the legal person, entity or trust except in following circumstances:
    1. The objects and insurance products provided in item 3 and item 4 of subparagraph 6 without any circumstances provided in subparagraph 3 of paragraph 1 of Article 6
    2. It has been confirmed that the entity customer has no articles of incorporation or document of similar powers.
(iii) Information of persons holding the position of senior management (including directors, supervisors, members of council, chief executive officer, chief financial officer, authorized representatives, managers, partners, authorized signatories, or any natural person having equivalent aforementioned position, an insurance company should determine the scope of senior management position by applying a risk-based approach) in a legal person, an entity or trustee of a trust.
(iv) The address of the registered office of a legal person, an entity or a trustee, and the address of its principal place of business operations.

VI. For a customer that is a legal person, an entity or trustee of a trust, an insurance company, when applying

the requirements under item 3 of subparagraph 3, should understand the ownership and control structure of the customer, and identify the beneficial owners of the customer and take reasonable measures to verify the identity of such persons through following information:

(i) For a customer that is a legal person or an entity

1. The identity of the natural person(s) who ultimately has a controlling ownership (such as name, date of birth, nationality, and identification number, etc.) "Natural person(s) who ultimately has a controlling ownership" refers to any natural person(s) that directly or indirectly owns more than 25 percent of shares or capital of the legal person. In such case, an insurance company may request the customer to provide a shareholder register or other documents to support the identification of such person(s).
2. If no natural person is identified under the previous sub-item or there is doubt as to whether the natural person(s) with the controlling ownership is the beneficial owner(s), an insurance company should identify the natural person(s) exercising control of the customer through other means. If necessary, an insurance company may obtain a certification from the customer to identify the beneficial owner(s).
3. If no natural person is identified under the two sub-items above, an insurance company should identify the persons holding the position of senior management.

(ii) For a customer that is a trustee of a trust: an insurance company should identify the settlor, the trustee, the protector, the beneficiaries, and any other natural person exercising ultimate effective control over the trust, or the persons in equivalent or similar positions.

(iii) The requirements on identification and verification of beneficial owner's identity under item 3 of subparagraph 3 do not apply to a customer or a person having control over the customer when it is one of the following entities, unless the customer or the person meets the proviso in subparagraph 3 of paragraph 1 of article 6 or has issued bearer shares:

1. Taiwan government,
2. Taiwan government-owned enterprise,
3. Foreign government entity,
4. Taiwan public company and its subsidiary,
5. Entity listed on a stock exchange outside of Taiwan that is subject to regulatory disclosure requirements of its principal shareholders, and the subsidiaries of such entity,
6. Financial institution supervised by Taiwan government, and the investment tools managed by such financial institution,
7. Financial institution incorporated or established outside of Taiwan that is subject to and supervised for compliance with the AML/CFT requirements that are consistent with the standards set by the Financial Action Task Force (FATF), and investment tool managed by such institution. An insurance company should keep relevant documents and proof of the aforementioned financial institutions and investment tool (such as record of public information search, AML policies and procedures of the financial institution, record of negative news search, statements of the financial institution, etc.).
8. Fund administered by Taiwan government entity,
9. Employee Stock Ownership Trust, Employee Benefit Savings Trust.

(iv) When a customer buys property insurance, injury insurance, health insurance or insurance products without policy value reserve, the regulations governing identification and verification of beneficial owner's identity stipulated in item 3 of subparagraph 3 do not apply, unless the customer comes from a high-risk country or region where no effective AML/CFT operations is carried out, or the insurance company has sufficient evidences to suspect that the customer or transaction is associated with ML/TF.

VII. For customers who have established business relations with an insurance company, except as otherwise stipulated by law, the insurance company should, using reliable and independent sources of documents, data or information, carry out the verification of the identities of the customer, the agent and the beneficial

owner in the following ways, and keep copies of the identity proof documents or record them.

(i) Verification through documents,

1. Individual

(1) Verification of identity or date of birth: obtain an unexpired official identification document that bears a photograph of the individual (e.g. identification card, passport, residence card, driving license, etc.) If there is doubt as to the validity of such documents, the insurance company should obtain certification provided by an embassy official or a public notary. With respect to the identity or date of birth of the beneficial owners of an entity, the company may not obtain original copies of the aforementioned document for verification, or may, according to the company's internal operating procedures, request the legal person, the entity and its authorized representative to provide a certification that specifies the identification data of the beneficiary owners. Part of the data on such certification, however, should allow the insurance company to perform verification through the certificate of incorporation, annual report, or other reliable source documents or data.

(2) Verification of address: obtain bills, account statements, or official documents, etc. from the customer.

2. Legal person, organization or trustee of a trust

Obtain certified articles of incorporation, government-issued business license, partnership agreement, trust instrument, certification of incumbency, etc. If a trust is managed by a financial institution described in paragraph 1 of Article 5 of Money Laundering Control Act, a certification issued by the financial institution may substitute for the trust instrument of the trustee unless the country or region where the financial institution is located is high-risk country or region without effective AML/CFT operations or there is enough information to suspect the customer or transaction as being associated with ML/TF.

(ii) Verification through non documentary methods, for example:

1. Contacting the customer by telephone or letter after a business relationship has been established.
2. Checking references provided by other financial institutions.
3. Cross-checking information provided by the customer with other reliable public information or private database, etc.

VIII. For a customer identified by an insurance company as a high-risk customer in accordance with the company's relevant requirements on customer ML/TF risk assessment, the company should perform the following enhanced verification:

(i) Obtaining a reply, signed by the customer or the authorized signatory of the legal person or the entity, for a letter mailed to the address provided by the customer, or contacting the customer by telephone.

(ii) Obtaining evidence that supports an individual's sources of wealth and sources of funds.

(iii)Site visit.

(iv)Obtaining prior insurance reference.

IX. An insurance company is not allowed to establish business relationship with a customer before completing CDD. If following requirements are met, however, an insurance company may complete verification after the establishment of the business relationship following the obtaining of identification data of the customer and beneficial owner:

(i) The ML/TF risks are effectively managed. This includes that the insurance company should take risk control measures with respect to the scenario that a customer may take advantage of verifying identity after transaction completed.

(ii) It is essential not to interrupt the normal conduct of business with customers.

(iii)The insurance company ensures that verification of the identity of the customer and beneficial owner is carried out as soon as it is reasonably practicable. If the insurance company fails to complete the verification of identity of the customer and beneficial owner in a reasonably practicable timeframe, it should terminate the business relationship with the customer and inform the customer in advance.

X. If an insurance company permits the establishment of the business relationship with a customer before completing customer identity verification, the company should adopt relevant risk control measures, including:
   (i) Establishing a timeframe for the completion of customer identity verification.
   (ii) Before the completion of customer identity verification, chiefs of business operation units should periodically review the business relationship with the customer and regularly keep senior managers informed of the progress of customer identity verification.
   (iii) Limiting the number of transactions and types of transaction before the completion of customer identity verification.
   (iv) Before the completion of customer identity verification, keeping the customer from making payment to any third party unless following requirements are met:
      1. There is no suspicion of ML/TF.
      2. The customer is assessed as a low ML/TF risk customer.
      3. The transaction is approved by senior manager at the level determined on the basis of the company's internal consideration for risk.
      4. The names of recipients do not match with lists established for AML/CFT purposes.
   (v) If there is any doubt as to the authenticity, appropriateness or intention of the customer or beneficial owner, the exception provided in the previous item does not apply.
   (vi) The insurance company should determine the "reasonably practicable timeframe" provided in item 3 of the previous subparagraph based on a risk-based approach to the extent that timeframes are differentiated according to risk level. For example:
      1. An insurance company should complete customer identity verification no later than 30 business days after the establishment of business relationship.
      2. If customer identity verification remains uncompleted 30 days after the establishment of business relationship, the insurance company should suspend business relationship with the customer and refrain from carrying out further transactions (except to return funds to their sources, to the extent that this is possible).
      3. If customer identity verification remains uncompleted 120 days after the establishment of business relationship, the insurance company should terminate business relationship with the customer.

XI. For a customer that is a legal person, an insurance company should understand whether the customer is able to issue bearer shares by reviewing the article of incorporation or requesting a certification from the customer, and take one of the following measures to ensure the update of beneficial owners:
   (i) Requesting the customer to require bearer share holders who ultimately have a controlling ownership interest to notify the customer to record their identity, and requesting the customer to notify the insurance company immediately when the identity of such share holder change.
   (ii) Requesting the customer, after each shareholders' meeting, to update the information of beneficial owners and provide identification data of any shareholder that holds a certain percentage (or above) of bearer shares. The customer should notify the insurance company immediately if, through other means, it is aware that the identity of any shareholder who ultimately has a controlling ownership has changed.

XII. When conducting CDD, an insurance company should utilize proper risk management mechanisms to determine whether the customer, its beneficial owners or persons holding senior management position in the customer are or were politically exposed persons ("PEPs") entrusted by a domestic or foreign government or international organization.
   (i) If the customer or its beneficial owners are PEPs entrusted by a foreign government, the insurance company should treat such customer as a high-risk customer and take enhanced due diligence ("EDD") measures provided in the items of subparagraph 1 of paragraph 1 of Article 6.
   (ii) If the customer or its beneficial owners are PEPs entrusted by a domestic government or international organization, the insurance company should perform risk assessment when establishing business relationship with the customer and re-perform it in every subsequent year. For a customer treated by

the insurance company as a high-risk customer, the insurance company should take EDD measures provided in the items of subparagraph 1 of paragraph 1 of Article 6.

(iii) If the persons holding senior management position in the customer are PEPs entrusted by a domestic or foreign government or international organization, the insurance company should take into account the influence that such person exerts on the customer, to determine whether the customer is subject to EDD measures provided in the items of subparagraph 1 of paragraph 1 of Article 6.

(iv) For PEPs that had been entrusted by a domestic or foreign government or international organization, the insurance company should take into account relevant risk factors to assess their influence, and determine whether they are subject to the requirements under the 3 items above by applying a risk-based approach.

(v) The requirements under the 4 items above also apply to family members and close associates of PEPs. The scope of aforementioned family members and close associates should be determined in accordance with provisions in the last part of paragraph 4 of Article 8 of the Money Laundering Control Act.

(vi) The requirements under item 1 to item 5 of this subparagraph do not apply to the objects described in sub-item 1 to sub-item 3 and sub-item 8 of item 3 of subparagraph 8 when their beneficial owners or senior managers are PEPs.

XIII. Other requirements that an insurance company should comply with when conducting CDD.

(i) Directions for Underwriting Process

1. When an individual is applying for insurance, a sales representative of the insurance company should request the proposer and the insured to provide identification documents (identification card, passport, driver's license, or other supporting documents that can prove their identity) or record the relevant information thereon. When a legal person is applying for insurance, the legal person's certificate of registration, legitimate proof of the authority of the person purporting to act on behalf of the customer (such as a business license, other incorporation or license of registration, etc.).
2. An underwriter of the insurance company should review the application forms filled out by the applicant or the insured at the time of underwriting with due diligence to ensure that the CDD made on the parties hereof in the solicitation report is true. If necessary, an underwriter should request a survival investigation on the application case and attach relevant information for recordation. When a legal person is applying for insurance, the insurance company should take reasonable methods to understand the nature of its business, the beneficial owner and the control structure, and keep relevant documents and information.
3. In addition to identification card and license of registration, a second identification document may be requested for the CDD, if necessary. The second identification document should be identity-provable. A name list issued by organizations, schools or groups can also be used as a second identification documents if it can serve as confirmation of a customer's identity. If the customer refuses to provide a second identification documents, the application should be declined or be processed after the CDD is completed.
4. An insurance purchased by any person acting on behalf of a customer should follow item 2 of subparagraph 3 of this article.
5. For a non-face-to-face customer, an insurance company should perform CDD procedures that are as effective as those performed in the ordinary course of business and must include special and sufficient measures to mitigate the risks.
6. For a customer establishing business relationship with the insurance company through the Internet, the company should comply with the "Directions for Insurance Enterprises Engaging in Electronic Commerce Business".

(ii) Directions for Re-verification of Customer Information after Underwriting:

1. When a customer of a jumbo case (amount determined by individual insurance company) cancels a policy and asks for refund of premium paid, the insurance company should verify the identity and the motive of the customer to prevent ML/TF activities.

2. A policy change made by any person acting on behalf of a customer should follow item 2 of subparagraph 3 of this article.

(iii) Directions for Claims Payment:

1. When paying out insurance proceeds, an insurance company should review the payment flow if any suspicion arises. If the beneficiary demands to cancel "non-negotiable" remark off the check, the company should understand the motive, and makes adequate notes.
2. An insurance company should review whether the process of changing of beneficiary is normal and reasonable.
3. An insurance company should review whether there is a reasonable connection between the amount of insurance proceeds and the beneficiary's occupation or identity.
4. Claims application made by any person acting on behalf of a customer should follow item 2 of subparagraph 3 of this article.

(iv) For customers who fail to complete the relevant procedures for CDD, an insurance company should consider reporting any suspected ML/TF/PF transactions related to that customer.

(v) When an insurance company suspects that a customer or transaction may involve ML/TF/PF, and they reasonably believe that carrying out CDD procedures might disclose information to the customer, they may not carry out these procedures and instead report suspected ML/TF/PF activities.

XIV. In the case that a customer in a business relationship or transaction is in the situation described in item 8 of subparagraph 1, the insurance company concerned should report suspicious ML/TF/PF transaction in accordance with Article 13 of the Money Laundering Control Act. If such customer is a designated individual, legal person, or entity sanctioned under the Counter-Terrorism Financing Act, the insurance company is prohibited from the activities described in paragraph 1 of Article 7 of the Counter-Terrorism Financing Act since the date of knowledge, and should report in accordance with Article 12 of the Counter-Terrorism Financing Act. (The format can be downloaded from the website of the Investigation Bureau, Ministry of Justice (MJIB)). If the insurance company is involved in the situation described in the subparagraph 2 and 3 of paragraph 1 of Article 6 of the Counter-Terrorism Financing Act before aforementioned objects are listed as designated individuals, legal persons or entities sanctioned under the Counter-Terrorism Financing Act, the insurance company should obtain the approval in accordance with relevant regulations established under the Counter-Terrorism Financing Act.

XV. The provisions of the preceding paragraph should also apply in cases where a third party is appointed, entrusted, or otherwise designated by an individual, legal person or entity subject to sanctions, or where the third party holds or manages the property or interests in property of such individual, legal person or entity for other reasons.

Article 5

The CDD measures conducted by an insurance company should include ongoing customer identity verification and should be conducted in accordance with the following provisions:

I. An insurance company should conduct CDD measures to the existing customers based on their materiality and risk level. After considering the time point of the previous CDD and the adequacy of the obtained information, the insurance company should review the existing business relationships at an appropriate time. The above-mentioned appropriate time should at least include:

(i) When a customer increases the sum assured unusually or enters new business relationships with the insurance company.

(ii) When it is time for periodic review of the customer information scheduled on the basis of materiality and risk level.

(iii) When it becomes known that there is a major change to customer's identity and background information.

II. An insurance company should scrutinize transactions undertaken throughout the course of the relationship with customers to ensure that the transactions being conducted are consistent with the company's

knowledge of the customers, their business and risk profile, including where necessary, the source of funds.

III. An insurance company should periodically review the sufficiency of the information used to identify customer and beneficial owners and ensure the update of such information. High-risk customers, especially, should be subject to at least annual review. For other customers, the insurance company should determine the frequency of review by applying a risk-based approach.

IV. When conducting CDD measures, an insurance company may rely on the customer identification data previously obtained and kept, and is not required to conduct such measures each time when the customer conducts a transaction. If the insurance company has doubts about the veracity and adequacy of previously obtained customer identification data, identifies a suspicious ML/TF/PF transaction, or there is major change in the way of transaction of the customer that is inconsistent with its business profile, the insurance company should re-conduct CDD measures in accordance with the requirements of Article 4.

Article 6

An insurance company should determine the extent to which it conducts CDD and ongoing due diligence measures described in subparagraph 3 of Article 4 and the preceding Article by applying a risk-based approach, including:

I. For higher risk situations, the insurance company should take enhanced CDD and ongoing due diligence measures, which should at least include following additional enhanced measures:
   (i) Before establishing or adding new business relationship, the insurance company should obtain the approval of certain level senior management, determined according to the company's internal consideration of risk.
   (ii) The insurance company should take reasonable measures to understand the source of wealth and source of funds of the customer. The source of funds refers to the original source that generates such funds (e.g. salary, income from investment, disposal of real estate, etc.).
   (iii)The insurance company should conduct enhanced ongoing monitoring of the business relationship.

II. For customers from high ML/TF risk jurisdictions, the insurance company should apply enhanced measures proportionate to the risks.

III. For lower risk situations, the insurance company may take simplified measures commensurate with the lower risk factors. Simplified measures, however, should not be permitted in one of the following situations:
   (i) Customers are from high ML/TF risk countries or regions that have not implemented effective measures to prevent ML/TF, which include but are not limited to the jurisdictions, published by international anti-money laundering organizations and notified by the FSC, that have serious deficiencies in AML/CFT, and other jurisdictions that fail to comply with or completely comply with the recommendations of such international anti-money laundering organizations.
   (ii) The insurance company has sufficient reason to suspect the customers or transactions may be involved in ML/TF.

An insurance company may take following simplified due diligence measures:

I. Lowering the frequency of updating customer identification data.

II. Lowering the extent to which the insurance company conducts ongoing monitoring, and using a reasonable threshold amount as the basis for reviewing transactions.

III. The insurance company is not required to collect specific information or take special measures to understand the purpose and the nature of the business relationship if these can be inferred from the transaction types or existing business relationship.

An insurance company should conduct CDD measures to the existing customers based on their materiality

and risk level. After considering the time point of the previous CDD and the adequacy of the obtained information, the insurance company should review the existing business relationships at an appropriate time

Article 7

An insurance company should perform CDD measures by itself. Even if regulatory requirements or the FSC otherwise permits the insurance company to reply on third-parties to identify and verify the identity of customer, the person on behalf of the customer, the beneficial owners of the customer, or the purpose or nature of business relationship, the ultimate responsibility for CDD measures should still remain with the insurance company, which should be required to:

I. Obtain immediately the necessary information concerning CDD measures.
II. Take measures that are in line with its own needs to ensure that the third parties it relies on will provide the customer identification information or copies of other relevant documents required for CDD in accordance with the company's requirements without delay.
III. Ensure that the third parties it relies on are subject to regulations, supervision or monitoring, and have appropriate measures in place to comply with the relevant regulations for CDD and maintaining records.
IV. Confirm the location of the third party it relies on, and ensure that its AML/CFT regulations are consistent with the standards set by the FATF.

Article 8

An insurance company's mechanism for name screening on customers and related parties of a transaction should be conducted as follows:

I. The insurance company should establish policies and procedures for name screening on customers and related parties of a transaction, by applying a risk-based approach, to detect, match, and filter whether the customers, persons holding senior management position of the customers, beneficial owners of the customers, or related parties of the transaction are designated individuals, legal persons or entities sanctioned under Counter-Terrorism Financing Act, or terrorists or terrorist groups identified or investigated by foreign governments or international organizations. In the case of true match, the company should undertake the measures provided in subparagraph 14 of Article 4.
II. The policies and procedures for name screening on customers and related parties of a transaction should include at least the logic of matching and filtering, the operating procedure for name screening, and the standard of review, and should be documented.
III. The insurance company should record the result of name screening, and keep such record in accordance with the requirements for retention period of Article 13.
IV. The name screening mechanism should be subject to testing, including:
    (i) Whether the sanction list and threshold setting are determined by applying a risk-based approach.
    (ii) Whether the data input in the corresponding system data fields is correct and complete.
    (iii)The logic of matching and filtering.
    (iv)Model validation.
    (v) Whether data output is correct and complete.
V. The insurance company should determine whether such mechanism continues to appropriately reflect the risk identified and update the mechanism at proper time.

Article 9

An insurance company's ongoing monitoring on transactions should be conducted in accordance with the following regulations:

I. The insurance company should integrate customer information data and transaction data throughout the company step-by-step by information systems for enquiries made by the head office (branches) for the purpose of AML/CFT, in order to enhance its capacity of transaction monitoring. With respect to the

customer data requested or enquired by each business unit, the insurance company should establish internal control procedures and ensure the confidentiality of the data.

II. The insurance company should establish policies and procedures for ongoing monitoring of transactions by applying a risk-based approach and use information systems to assist the identification of suspicious ML/TF/PF transactions.

III. The insurance company should review its policies and procedures for ongoing monitoring of transactions and update periodically to take into account regulatory requirements on AML/CFT, customer profiles, the size and complexity of business, the trend and information related to ML/TF obtained from internal or external sources, the result of internal risk assessment, etc.

IV. Policies and procedures for ongoing monitoring of transactions should include at least complete and documented monitoring types, setting of parameters, amount thresholds, alerts and operation procedures of monitoring, the reviewing procedures for monitored cases and reporting standards, and should be documented.

V. The mechanism provided in last subparagraph should be subject to testing, including:
   (i) Internal control procedure: review the roles and responsibilities of persons or business units related to the mechanism for monitoring accounts and transactions.
   (ii) Whether the data input in the corresponding system data fields is correct and complete.
   (iii) The logic of detection scenario.
   (iv) Model validation.
   (v) Data input.

VI. In the cases where the insurance company identifies or has reasonable grounds to suspect customers, or the funds, assets or intended or performed transactions of the customers are related to ML/TF, regardless of the amount, value, or whether transactions are completed, the insurance company should perform enhanced review of the customer identity.

VII. The characteristics of suspicious ML/TF/PF transactions provided in the Annex are not exhaustive. The insurance company should select or develop suitable types of red flag transactions based on its size of assets, geographic areas, business profile, customer base profile, characteristics of transactions, and the company's internal ML/TF risk assessment or information of daily transactions, to identify red flag transactions of potential ML/TF/PF.

VIII. For red flag transactions identified in accordance with last subparagraph, the insurance company should determine whether such transactions are reasonable (e.g. whether such transactions are apparently incommensurate with the identity, income, or scale of business of the customer, unrelated to the customer's business profile, do not match the customer's business model, no reasonable economic purpose, no reasonable explanation, no reasonable purpose, or unclear source of funds or explanation) and keep review records. If the insurance company determines such transaction is not a suspicious ML/TF/PF transaction, the company should record the reason for the decision. If the company determines such transaction is suspicious ML/TF /PF transaction, in addition to performing CDD measures and retaining relevant documentations, the company should report to the MJIB without any delay after such reporting is approved by the Responsible Officer. The reporting should be completed no later than two business days after the approval is obtained. The same applies to transactions which are not completed.

IX. With respect to the characteristics of suspicious ML/TF/PF transactions, the insurance company should determine the ones that are required to be monitored with the assistance of related information systems by applying a risk-based approach. For those that are monitored without the assistance of information systems, the company should also, by other means, assist employees to determine whether transactions are suspicious ML/TF/PF transactions when they are conducted by customers. The assistance of information system cannot completely replace the judgment of employees. The insurance company is still required to strengthen employee training to allow employees capable of identifying suspicious ML/TF/PF transactions.

Procedures for reporting of suspicious ML/TF/PF transactions:

I. When an employee of a business unit identifies any abnormal transaction, the employee should immediately report such transaction to a supervisory officer.
II. The supervisory officer should determine as soon as possible whether such transaction is subject to reporting requirements. If it is determined that such transaction should be reported, the supervisory officer should immediately request the employee who identifies the abnormal transaction to complete the form for reporting (The format can be downloaded from the website of the MJIB), the completed form for reporting should then be submitted to the Responsible Unit.
III. After the report is submitted by the Responsible Unit and approved by the Responsible Officer, the insurance company should file the report to the MJIB without any delay. The reporting should be completed no later than two business days after the approval is obtained. The same applies to transactions which are not completed.
IV. If the reporting mentioned above is an apparently significant and urgent case, the insurance company should report to the MJIB by fax or other feasible means as soon as possible and then immediately submit the hard copy of the report. The company is not required to submit the hard copy of the report if the MJIB confirms the receipt of such report by sending a fax reply. In such cases, the company should retain the fax reply.

Requirements on the confidentiality of reporting data and information are as follows:

I. Employee at all levels should keep the reporting of suspicious ML/TF/PF transactions confidential and should not disclose such information. The insurance company should provide employees trainings or materials on how to avoid the disclosure of such information in the interaction with customers and in daily operation.
II. All documents related to such reporting should be classified as confidential. In the cases of any disclosure, the insurance company should take measures in accordance with relevant requirements.
III. Employees of the Responsible Unit, compliance officers or internal auditors may be allowed to timely obtain customer identification data and transaction record for work-related purposes, to the extent that requirements on confidentiality are met.

The insurance company should record the operation of its ongoing monitoring of transactions and keep such record in accordance with the requirements on retention period stipulated in Article 13.

.

Article 10

Before launching new products or services with policy value reserves or cash value, or engaging in new types of business (including new payment mechanisms and the application of new technologies to existing or new products or services), an insurance company should conduct ML/TF risk assessment of the product, and establish corresponding risk management measures to reduce the identified risks.

Article 11

An insurance company should comply with following requirements on currency transactions above a certain amount:

I. The insurance company should verify customer identity and retain relevant records.
II. The insurance company's customer identity verification measures should comply with following requirements:
    (i) Verify customer identity with the identification documents or the passport provided by the customer, and record the name, date of birth, address, telephone number, account number of the transaction account, transaction amount, and identification number of the customer. However, if it can be confirmed that the customer is the account holder himself/herself, the identity verification is then not required. Nevertheless, it should be noted in the transaction record that it was a transaction made by the account holder.

(ii) If a transaction is processed by a person acting on behalf of the customer, the insurance company should verify the person's identity with the identification documents or the passport provided by the person, and record the name, date of birth, address, telephone number, account number of the transaction account, transaction amount, and identification number of the person.

III. Except for the situations described in paragraph 2 of this article, the insurance company should report such transactions within 5 business days after the completion of transactions in the way of media reporting to the MJIB (the format can be downloaded from the website of the MJIB). In case where the company fails to complete media reporting with a justified reason, it may submit a hard copy of the report (the format can be downloaded from the website of the MJIB) after obtaining the approval from the MJIB.

IV. The insurance company should retain the reporting data and relevant documentations submitted to the MJIB in accordance with the requirements of Article 13.

An insurance company is not required to file a report on any of the following cash transactions above a certain amount with the MJIB, provided the insurance company verifies the identity of the customer and keeps the transaction records thereof:

I. Deposits into the accounts opened by government agencies, state-owned enterprises, institutions acting with governmental power (within the scope of mandate), public and private schools, public enterprises and government funds established under laws.

II. Transactions and fund arrangements between financial institutions. Notwithstanding the foregoing, payables to another financial institution's customer paid through an inter-bank deposit account, such as a customer cashing the check issued by another financial institution, should be handled as required, provided the cash transaction of the same customer exceeds a certain amount.

III. Payments collected under a collection service (excluding payments deposited in designated stock subscription accounts) where the payment notice expressly bears the name and identification card number of the counterparty (including the code which enables tracking of counterparty's identity), and type and amount of transaction. Nevertheless, the duplicate copy of the payment notice should be kept as the transaction record.

Article 12

When an insurance company reports properties or property interests and locations of designated individuals, legal persons or entities sanctioned under Article 7 of the Counter-Terrorism Financing Act, the company should comply with the following provisions:

I. The insurance company should, after learning the case, complete a report in the format required by the MJIB. After obtaining the approval on the report from the company's Responsible Officer, the company should submit the report to the MJIB in the manner required by the MJIB without any delay. The report should be submitted no later than 2 business days after being approved.

II. If the reporting mentioned above is an apparently significant and urgent case, the insurance company should conduct the reporting to the MJIB by fax or other feasible means as soon as possible and then submit the make-up report in the format and manner required by the MJIB. The company is not required to submit the make-up report if the MJIB confirms the receipt of such report by sending a fax reply in its prescribed format. In such cases, the company should retain the fax reply sent by the MJIB.

III. The insurance company should produce an annual report as of December 31 every year (the "settlement record date") in the format required by MJIB. The report should state all properties or property interests of designated sanctioned individuals, legal entities or groups managed or held by the insurance company as of the settlement record date and the report should be submitted to the MJIB for reference before March 31 the following year.

The reporting records, transaction documents and annual reports mentioned in the preceding paragraph should be handled in accordance with Article 13.

Article 13

An insurance company should keep records on customers and transactions with hard copies or electronic data in accordance with following requirements:

I. The insurance company should maintain, for at least five years, all necessary records on transactions, both domestic and international. However, in case where laws otherwise provide a longer period for record-keeping, the company should comply with such laws. The aforementioned necessary records include:
   (i) The name or policy number of each party involved in a transaction.
   (ii) Date of transaction.
   (iii) Currency type and amount of transaction.
   (iv) The methods of paying in or paying out, such as cash, check, etc.
   (v) Destination of funds.

II. For currency transactions above a certain amount, the insurance company should keep relevant records on the verification and reporting of such transactions for at least 5 years in the original manner. The insurance company should, based on its own considerations and in accordance with the principle of uniformity across the entire company, select a method for recording the customer verification procedures.

III. For the reporting of suspicious ML/TF/PF transactions, the company should keep relevant records of reporting for at least 5 years in the original manner.

IV. The insurance company should keep following information for at least 5 years after the business relationship is ended. However, in case where laws otherwise provide a longer period for record-keeping, the company should comply with such laws:
   (i) All records obtained through the CDD measures, e.g. copies or records of official identification documents like passports, identity cards, driving licenses or similar documents.
   (ii) Archives of contract documents.
   (iii) Business information, including the information of the background or purpose of complex, unusual transactions obtained from enquiries, and the result of any analysis undertaken.

V. The records kept by the insurance company should be sufficient to permit reconstruction of individual transactions so as to provide evidence for the determination of criminal activity.

VI. The insurance company should ensure that it can rapidly provide transaction records, the CDD information, and relevant information, etc. to competent authorities upon appropriate authority.

Article 14

Other matters that require attention:

I. An insurance company should pay attention when a customer or sales staff is suspected of circumventing the requirements of the Money Laundering Control Act (such as the same proposer or the insured separately purchases jumbo insurance), and should ensure that its motives are understood.

II. The insurance company should review its internal control measures annually (the intervals can be set by each company according to their own circumstances) to see if it is adequate to prevent ML/TF behaviors. If there is any deficiency in the operation of each unit, it should be promptly improved.

III. The insurance company should pay attention on confidentiality when investigating any staff member (employee) suspected of involvement in ML/TF.

Article 15

Responsible Unit and the Responsible Officer:

I. An insurance company should deploy adequate and sufficient AML/CFT officers and resources according to its size and risks, etc. The board of directors (council) should appoint a senior officer to serve as the AML/CFT Responsible Officer, who should be sufficiently authorized to coordinate and supervise AML/CFT affairs. The company should ensure that such officers and the Responsible Officer do not take other responsibility which conflicts with their AML/CFT responsibilities.

II. The Responsible Unit and the Responsible Office described in last subparagraph are in charge of

following affairs:

(i) Supervising the identification, assessment, and monitoring of ML/TF risks, as well as the planning and implementation of relevant policies and procedures.

(ii) Coordinating and supervising the implementation of the company-wide ML/TF risk identification and assessment.

(iii) Monitoring risks related to ML/TF.

(iv) Developing AML/CFT programs.

(v) Coordinating and supervising the implementation of AML/CFT programs.

(vi) Ensuring the compliance with relevant AML/CFT regulatory requirements, including relevant templates or self-regulatory rules established by associations of the industry and approved by the FSC for references.

(vii) Supervising the reporting of suspicious ML/TF/PF transactions and properties or property interests and locations of designated objects under the Counter-Terrorism Financing Act to the MJIB.

(viii) Other issues related to AML/CFT.

III. The Responsible Officer described in the subparagraph 1 should report to the board of directors (council) and the inspectors (supervisors, board of supervisors) or the audit committee at least every six months. If any significant violation of laws is discovered, the Responsible Officer should immediately report to the board of directors (council) and the inspectors (supervisor, board of supervisors) or the audit committee without any delay.

IV. The overseas business units of an insurance company should, based on comprehensive consideration of the number of branches, business scale and risks in the region where they are located, deploy adequate AML/CFT personnel, and appoint one person as the supervisor to be responsible for coordinating and supervising the implementation of AML/CFT laws.

V. The establishment of the AML/CFT supervisor in the overseas business units of an insurance company should comply with the local laws and regulations and the requirements of the local authorities. It should also possess sufficient authority to coordinate and supervise AML/CFT efforts, including the ability to report directly to the Responsible Officer described in subparagraph 1. In addition, apart from being the compliance supervisor, this supervisor should be a full-time position. If he/she holds other positions concurrently, it should be communicated to the local authorities to confirm that the concurrent positions do not pose any conflict of duties and it should be reported to the FSC for recordation.

Article 16

The implementation, audit, and statement of the AML/CFT internal control system:

I. The domestic and overseas business units of an insurance company should appoint senior managers to serve as the AML/CFT supervisors who are responsible for supervising the implementation of AML/CFT-related matters in their respective units, and are responsible for conducting self-inspections in accordance with relevant regulations.

II. Internal audit unit of the insurance company should conduct the following audits in accordance with the regulations and submit the audit opinions:

(i) Whether ML/TF risk assessment and AML/CFT programs meet regulatory requirements and are implemented.

(ii) The effectiveness of AML/CFT programs.

III. Responsibilities of internal audit unit of the insurance company:

(i) Determining the items subject to audit according to internal control measures and relevant regulations, conducting periodic audit, and testing the effectiveness of AML/CFT programs and the quality of risk management of the company's operations, business units and branches (subsidiaries).

(ii) The auditing methods should cover independent transaction testing, which include selecting transactions related to high-risk products, customers, and geographic areas assessed by the insurance company to verify that the company has effectively implemented relevant AML/CFT regulations.

(iii) In case any deficiencies in the implementation of this management measure are discovered, regular reports should be submitted to the Responsible Officer for review, and these reports should also serve as a reference for on-the-job training for the employees.

(iv) If the internal audit personnel discover major violations but deliberately conceal them and fail to disclose them, the relevant responsible department of the head office should handle the situation appropriately.

IV. The insurance company's chief executive officer should supervise each unit to the extent that the implementation of AML/CFT internal control system is assessed and reviewed by each unit in a prudent manner. The chairman of the board (chairman of the council), chief executive officer, chief auditor (audit personnel), and AML/CFT Responsible Officer should jointly issue a statement for AML/CFT internal control system and submit to board of directors (council) for approval. Within 3 months after the end of each fiscal year, the insurance company should disclose the statement of internal control system on the website of the insurance industry and publish the statement through a website designated by the FSC.

V. The matters related to the board of directors or supervisors of a foreign insurance company's branch in Taiwan should be handled by the personnel authorized by the parent company. The statement mentioned in the previous subparagraph should be issued by the person in charge of the branch company in Taiwan, the AML/CFT Responsible Officer, and the person in charge of the company's audit operation in Taiwan region, who are all authorized by the parent company.

Article 17

Employee hiring and training:

I. An insurance company should establish highly effective procedures for employee screening and hiring, including reviewing whether a candidate has decent personality and professional knowledge required for the job.

II. The insurance company's AML/CFT Responsible Officer, AML/CFT officers, and domestic business unit supervisory officers should meet one of following requirements within 3 months after the appointment. The insurance company should establish relevant control mechanism to ensure the compliance of such requirements:

(i) Possessing at least 3-year experience as a compliance officer or AML/CFT officer.

(ii) The insurance company's AML/CFT Responsible Officer and AML/CFT officers should attend at least 24-hour training classes provided by an institution recognized by the FSC and obtain a certificate of completion after passing an exam. Domestic business unit supervisory officers should attend at least 12-hour training classes provided by an institution recognized by the FSC and obtain a certificate of completion after passing an exam. However, if the Chief Compliance Officer also serves as the AML/CFT Responsible Officer, or if compliance officers also act as the AML/CFT officers, then after they have completed the 12-hour AML/CFT education and training provided by an institution recognized by the FSC, they will be regarded as meeting the qualification requirements stipulated in this item.

(iii) Obtaining a domestic or international AML/CFT professional certificate issued by an institution recognized by the FSC.

III. The insurance company's AML/CFT Responsible Officer, AML/CFT officers, and domestic business unit supervisory officers, described in the preceding subparagraph should attend at least 12-hour AML/CFT trainings each year provided by the company or external training institutions agreed by the AML/CFT Responsible Officer. Such trainings should at least cover new updates on regulatory requirements, and ML/TF trends and types. Those who obtain domestic or international AML/CFT professional certificates issued by an institution recognized by the FSC in the year may be exempt from satisfying the requirements on training hour for the same year.

IV. The supervisory officers, AML/CFT officers and personnel of the overseas business units of the insurance company should possess professional knowledge in AML and be familiar with the relevant local laws and

regulations. They should also attend AML/CFT education and training courses organized by foreign regulatory authorities or relevant units for at least 12 hours each year. If no such education and training courses are organized by foreign regulatory authorities or relevant units, these personnel may participate in training courses offered by internal or external training institutions with the approval from the AML/CFT Responsible Officer as described in subparagraph 1 of Article 15.

V. The insurance company should arrange AML/CFT trainings each year that have appropriate contents and training hours determined according to the business and job nature for its directors (council members), supervisors, chief executive officer, compliance officers, internal auditors, sales representatives and other personnel engaged in AML/CFT matters, to allow them to understand their AML/CFT duties and have the expertise required for such duties.

VI. The insurance company should incorporate courses on AML/CFT into the on-the-job training programs for its all internal and external staff. This will enable all employees to understand the relationship between relevant laws and regulations on AML/CFT and the practical operations. The company may also hire scholars and experts from the Ministry of Justice, the FSC, universities, or other institutions as lecturers if needed.

VII. When the employees of the insurance company go abroad for further studies or business matters, they should take the opportunity to learn about the specific AML/CFT measures taken by the foreign insurance industry. If there are any foreign practices that can be referred to and adopted by the company, they may be given special rewards.

Article 18

In case where customers of an insurance company are in one of the following circumstances, the insurance company's employees should decline the customers' requests in a euphemistic manner and report to direct managers:

I. Insisting on not providing relevant information for identity verification when being told it is mandatory according to regulatory requirements.

II. Attempting to persuade employees not to collect data that is required to complete the transaction.

III. Enquiring the possibility of avoiding being reported.

IV. Eager to explain the source of fund is clean or the transaction is not for money laundering purpose.

V. Attempting to provide interest or benefits to sales representatives to obtain certain services from the insurance company.

Article 19

An insurance company should, in its cooperation promotion, joint marketing activities, and in the contracts with insurance agents or insurance brokers, stipulate that they should abide by the regulations on AML/CFT, and cooperate with the insurance company in the collection or verification of customer identity information. The insurance company should fully request and confirm with their insurance agents and brokers that they need to cooperate in taking AML/CFT measures when conducting customer solicitation.

Article 20

This template should be implemented after it is approved by council of the Non-Life Insurance Association and reported to the FSC for recordation. In the case of amendment, the same conditions and requirements apply.