Title：Template for Guidelines Governing Anti-Money Laundering and Countering Terrorism Financing of Securities Firms
Date：2019.07.11 (Amended)

This Template is adopted pursuant to the Money Laundering Control Act, the Counter-Terrorism Financing Act, the Regulations Governing Anti-Money Laundering of Financial Institutions, the Regulations Governing Internal Audit and Internal Control System of Anti-Money Laundering and Countering Terrorism Financing of Securities and Futures Business and Other Financial Institutions Designated by the Financial Supervisory Commission, and the Regulations Governing Reporting on the Properties or Property Interests and Locations of Designated Sanctioned Individuals or Entities by Financial Institutions.

A securities firm’s customer due diligence (CDD) measures shall be as follows:
1. A securities firm shall decline to establish a business relationship or carry out any transaction with a customer in any of the following circumstances:
A. The customer is suspected of using an anonymous account, an account in a fictitious name, a nominee, a shell entity, or a shell corporation.
B. The customer refuses to provide documents relating to the CDD measures, unless the customer's identity has been verified by a reliable and independent source.
C. A person acts on behalf of the customer, and it is difficult to check and verify the fact of authorization and identity-related information.
D. The customer uses forged or altered identification documents.
E. The customer provides only photocopies of the identification documents; provided, this does not apply to business for which a photocopy or image file of the identification document supplemented with other control measures are permissible under regulations.
F. Documents provided by the customer are suspicious or unclear, the customer refuses to provide other supporting documents, or the documents provided cannot be authenticated.
G. The customer delays inordinately in providing identification documents.
H. A counterparty to the business relationship is an individual, legal person, or organization that is sanctioned under the Counter-Terrorism Financing Act, or a terrorist or terrorist group identified or investigated by a foreign government or an international anti-money laundering organization; provided, this does not apply to payments made under subparagraphs 1 to 3 of paragraph 1, Article 6 of the Counter-Terrorism Financing Act.
I. Other unusual circumstances exist in the process of establishing a business relationship or conducting transactions and the customer fails to provide reasonable explanations.

2. CDD measures shall be conducted when:
A. Establishing business relations with any customer.
B. Carrying out any cash transaction (e.g. paying a settlement price in cash, or subscribing to a single fund and paying the price in cash at the counter) of NT$500,000 or more (including the foreign currency equivalent thereof).
C. There is a suspicion of money laundering or terrorism financing.
D. A securities firm has doubts about the veracity or adequacy of previously obtained customer identification data.
3. The CDD measures to be taken are as follows:
A. Identifying the customer and verifying the customer's identity using reliable, independent source documents, data or information, and retaining copies of the customer's identity documents or recording the relevant information thereon.
B. Verifying that any person purporting to act on behalf of the customer is so authorized, identifying and verifying the identity of that person using the method specified in the preceding item, and retaining copies of the person's identity documents or recording the relevant information thereon.
C. Taking reasonable measures to identify and verify the identity of the beneficial owner of a customer, including using reliable source data or information.
D. The CDD measures shall include learning about the purpose and intended nature of the business relationship and obtaining relevant information in view of the situation.
4. When the customer under the preceding subparagraph is an individual, at least the following information shall be obtained to identify the customer:
A. Full name.
B. Birth date.
C. Domicile or residential address.
D. Official identification document number.
E. Nationality.
F. If a foreign national, the purpose of the residence or transactions (e.g. tourism or work).
5. When establishing a business relationship with an individual customer who is identified as a high risk customer or as having any high risk factor under provisions relating to the assessment of risk of money laundering or terrorism financing by customers of securities firms, at least one of the following items of information shall be obtained:
A. Any name(s) or alias(es) previously used; examples of a name previously used include a name used before marriage or a name used before a name change.
B. Work address, post office box address, email address (if any).
C. Telephone or mobile phone number.
6. When the customer is a legal person, an organization, or a trustee, the securities firm shall, in accordance with subparagraph 3, understand the business nature of the customer or trust (including any trust-like legal arrangement) and obtain at

least the following information to identify the customer or the trust and verify its identity:
A.Name, legal form, and proof of existence of the customer or trust.
B. The charter or similar power documents that regulate and bind the legal person or trust, except for in any of the following circumstances:
a.A counterparty that is listed under item C of subparagraph 7 hereof, and is free of the circumstances in the proviso of subparagraph 3 of Point 4.
b. A customer that is an organization and acknowledges that it does not have a charter or similar power document.
C. Names and other necessary information of persons having a senior management position in the legal person, organization, or trustee (senior management personnel may including directors, supervisors, governors, general managers/presidents, chief financial officers, representatives, managers, partners, personnel with signing authority, or any natural person who is equivalent to any of the above senior management personnel. A securities firm shall use a risk-based approach to define the scope of senior management personnel.
D. Official identification number: e.g. government uniform ID number, tax code number, registration number.
E. The address of the registered office of the legal person, organization, or trustee, and if different, the address of its principal place of business.
F.The purpose of the dealings with the offshore legal person, organization, or trustee.
7. When the customer is a legal person, an organization, or a trustee, a securities firm shall, in accordance with item C of subparagraph 6 hereof, understand the ownership and control structure of the customer or the trust, and obtain the following information to identify the beneficial owners of the customer and take reasonable measures to verify the identity of such persons:
A. For legal persons or organizations:
a. The identity (e.g. the name, birth date, nationality, and identification document number) of the natural person(s) who ultimately have a controlling ownership interest. When a controlling ownership interest refers to directly or indirectly owning more than 25 percent of a firm's shares or capital, the securities firm may require the customer to provide a list of its shareholders or other documents to help finish the identification procedure.
b. When no natural person having control through ownership interest is identified, or when there is doubt about whether the natural person(s) with the controlling ownership interest are the beneficial owner(s) under the provisions in the preceding sub-item, a securities firm shall verify whether there is any natural person(s) exercising control of the customer through other means. When necessary, an undertaking by the customer may be obtained to verify the identity of the beneficial owner(s).

c. Where no natural person is identified under (i) or (ii) above, a firm shall identify and take reasonable measures to verify the identity of the relevant senior management personnel.
B. For trustees: the identity of the settlor(s), the trustee(s), the trust supervisor, the trust beneficiaries, and any other person exercising ultimate effective control over the trust, or the identity of person(s) in equivalent or similar position.
C. Unless otherwise provided for in the proviso of subparagraph 3 of Point 4, or if the customer has issued bearer shares, a securities firm is not subject to the requirements of identifying and verifying the identity of beneficial owner(s) of a customer as set out in item C of subparagraph 3 if the customer or the person having a controlling ownership interest in the customer is:
a. An R.O.C government entity.
b. An enterprise owned by the R.O.C government.
c. A foreign government entity.
d. A public firm and its subsidiaries.
e. An entity listed on a stock exchange outside of the R.O.C. that is subject to regulatory disclosure requirements of its principal shareholders, and the subsidiaries of such entity.
f. A financial institution supervised by the R.O.C. government, and an investment vehicle managed by such institution.
g. A financial institution incorporated or established outside R.O.C. that is subject to and supervised for compliance with Anti-Money Laundering and Countering the Financing of Terrorism (AML/CFT) requirements consistent with standards set by the Financial Action Task Force on Money Laundering (FATF), and an investment vehicle managed by such institution. The securities firm shall retain the documentary evidence related to the aforesaid financial institution or investment vehicle (e.g. records of publicly disclosed audit information, the financial institution's anti-money laundering operational rules, records of searches for adverse information, statements by the financial institution).
h. Funds managed by R.O.C. government agencies.
i. An employee stock ownership trust or employee welfare savings trust.
D. Contractual stipulations may be adopted to provide for the handling of the following circumstances as follows:
a. The securities firm may refuse business dealings or terminate business relations at its sole discretion under the circumstances in item H of subparagraph 1.
b. For customers such as unwilling to coordinate with the routine review, refusing to provide beneficial owners or information about exercising the control over customers, or unwilling to explain the nature and purpose of the transaction and sources of the funds, and so on, the securities firm may temporarily suspend or terminate its business relationship with the customer.
8. Method for verifying the identity of a customer who establishes a business relationship with the securities firm, and of a person purporting to act on behalf of the customer, and of a beneficial owner thereof:

A. Verification by documents:
a. Individual:
b. Verification of identity or birth date: Obtain unexpired official identification documents with photos, e.g. national ID card, passport, Alien Resident Certificate, driver's license. If there is any doubt about the valid period of an above document, a certification or undertaking by an embassy or notary public shall be obtained. In addition, in the case of a beneficial owner, the securities firm need not require provision of the original identification document for verification, or the securities firm may, in accordance with its own operational procedures, ask the legal person, organization, or representative thereof, to issue a statement regarding the information of the beneficial owners, but it is required that at least a portion of the information specified in the statement be verifiable by other reliable documents or sources of information such as documents evidencing company registration or company annual reports.
c. Verification of address: Obtain the customer’s bills, reconciliation statements, or documents issued by the government.
B. Legal person, organization, or trustee: Obtain documents such as certified articles of incorporation, business license issued by the government, partnership agreement, trust instrument, certification of incumbency. If the trustee is a trust managed by a financial institution as stated in Article 5, paragraph 1 of the Money Laundering Control Act, the trust deed may be substituted by a written document issued by the financial institution. However, this does not apply if the country or area where the financial institution is located in falls within the circumstances in the proviso of subparagraph 3 of Point 4.
9. When necessary, verification may be carried out by means other than document verification. For example:
C. Contact the customer via phone or letter after the account has been opened.
D. Information provided by another financial institution.
E. Cross validate information provided by the customer with other reliable public information or paid database information.
Enhanced CDD shall be conducted for any customer who is identified as a high risk customer or as having any high risk factor under provisions relating to the assessment of risk of money laundering or terrorism financing by customers of securities firms. For example:
10. Obtain a reply letter which is signed by the customer himself/herself or by an authorized person of the customer, legal person, or organization, and which is in reply to a letter sent to the address provided by the customer, or make telephone inquiries.
11. Obtain supporting evidentiary materials regarding information on an individual's wealth and sources of fund.
12. Obtain supporting evidentiary materials on the sources and flow of fund of a legal person, organization, or trustee, such as a list of main suppliers, or a list of main customers.

13. Site visit.
14. Obtain information on past dealings of the securities firm, and notify the securities firm.

A securities firm shall not establish a business relationship or conduct occasional transactions with a customer before completing the CDD process. However, a securities firm institution that meets all of the following requirements may first obtain information on the identity of the customer and its beneficial owner(s) and complete the verification after the establishment of a business relationship:

15. Money laundering and terrorism financing risks are effectively managed, including adopting risk management procedures with respect to the circumstances under which a customer may utilize the business relationship to complete a transaction prior to verification.
16. It is necessary to do so to avoid interruption to the normal conduct of business with the customer.
17. Verification of the identities of the customer and its beneficial owner(s) will be completed as soon as reasonably practicable after the establishment of a business relationship. The business relationship must be terminated if verification cannot be completed within a reasonably practicable time limit, and the securities firm shall notify its customer in advance of this requirement.

If a securities firm allows a customer to establish a business relationship with it before the completion of CDD measures, it shall adopt relevant risk control measures, including:

18. Set a deadline for completion of the CDD measures.
19. Before completion of the CDD measures, the AML/CFT supervising officer of the business unit shall examine the dealings with the customer and report the CDD progress to the senior officer regularly.
20. Before the completion of the CDD measures, the number and types of the customer’s transactions shall be limited.
21. The securities firm shall use a risk-based approach to determine the risk level, and set the “reasonably practical time limit” in item C of the preceding subparagraph accordingly. Illustrative examples are as follows:

A. The CDD procedures shall be completed no later than 30 days after establishing a business relationship.
B. If the CDD procedures are not completed within 30 days after establishing a business relationship, the securities firm shall temporarily suspend the business relationship with the customer, and avoid conducting any further transaction.
C. If the CDD procedures are not completed within 120 days after establishing the business relationship, the securities firm shall terminate the business relationship with the customer.

22.When a customer is a legal person, the securities firm shall ascertain whether it can issue bearer shares by examining the customer’s articles of incorporation, or asking the customer to issue an undertaking, or another means, and with respect to

any customer that has issued bearer shares, it shall adopt one of the following measures to ensure that the information on beneficial owners is kept updated.
A. Require the customer to require its bearer share holders who have ultimate controlling interest in the legal person to register their identities with the customer, and require the customer to notify the securities firm when the identity of a shareholder who has ultimate controlling interest in the legal person changes.
B. Require the customer, after every shareholder meeting, to give the securities firm updated information on its beneficial owner(s), and to provide information on shareholders who hold a certain percentage of bearer shares. However, the customer shall promptly notify the securities firm when the customer learns for any other reason about any change of identity of a shareholder who has ultimate controlling interest in the legal person.
23. When the securities firm conducts CDD, it shall use adequate risk management systems to determine whether the customer or any of its beneficial owner(s) or senior management personnel is currently or was once a politically exposed person at home or abroad or in an international organization:
A. If the customer or a beneficial owner of the customer is currently a politically exposed person abroad, the customer shall be directly deemed a high risk customer, and the enhanced CDD measures in Point 4, paragraph 1, subparagraph 1 shall be adopted.
B. If the customer or a beneficial owner is currently a politically exposed person at home or in an international organization, the securities firm shall evaluate the risks before establishing a business relationship with the customer, and shall reevaluate them every year subsequently. For a customer that has been recognized by the securities firm as a high risk customer, the enhanced CDD measures in Point 4, paragraph 1, subparagraph 1 shall be adopted.
C. If any senior management personnel of a customer is currently a politically exposed person at home or abroad or in an international organization, the securities firm shall consider the senior managing official’s influence over the customer to determine whether to adopt the enhanced CDD measures in Point 4, paragraph 1, subparagraph 1.
D. Regarding a politically exposed person at home or abroad or in an international organization who is not incumbent, the securities firm shall consider relevant risk factors and then evaluate the person’s influence, and determine through a risk-based approach whether the provisions in the preceding three items should be applied to the person.
E. The preceding four items also apply to family members and close associates of any politically exposed person. The scope of family members and close associates shall be determined as provided in the latter part of paragraph 4 of Article 7 of the Money Laundering Control Act.
F. When a beneficial owner or senior management personnel of a customer that is listed in sub-items a, b, c, or h of item C of subparagraph 7 is a politically exposed person, the provisions of items A to E of this subparagraph do not apply.

24. Other compliance matters in connection with CDD measures:
A. To establish business relations with a customer, or to conduct financial transactions exceeding a certain dollar amount with a walk-in customer, or when it suspects that a customer's documents are insufficient to establish positive identification, a securities firm shall use a government-issued identity document or another identification document to confirm the customer’s identity, and then record the result.
B. A securities firm shall adopt enhanced CDD measures for a customer that opens a brokerage account and conducts transactions via a professional intermediary.
C. A securities firm shall adopt enhanced CDD measures for a customer seeking personal wealth management services.
D. A securities firm shall adopt enhanced CDD measures for a customer that is blacklisted by another securities firm.
E. A securities firm shall use CDD procedures that enable it to identify non-face-to-face customers just as effectively as it identifies other customers, and must further have special and adequate measures to reduce risk.
F. When a business relationship is established over the Internet, the process shall be in accordance with relevant due diligence procedures which are adopted in accordance with the requirements of, and accepted for recordation by, the competent authority.
G. When a customer mandates or authorizes another to establish a business relationship, or when a securities firm does not discover a suspicion about a customer until after the securities firm has already established the business relationship with the customer, the securities firm must verify the situation by telephone or written correspondence, or by making a site visit.
H. When a customer establishes a business relations by mail correspondence, after the business relationship is established, the securities firm must send its return correspondence by registered mail to substantiate it.
I. If a securities firm discovers, without violating any law or regulation, or finds it necessary to assume, that funds flowing through a customer's account come from corruption or misuse of public assets, the securities firm shall refuse to handle the transactions or terminate the business relationship altogether.
J. When a securities firm is unable to complete CDD procedures for a customer, it shall consider reporting the suspicion of money laundering or terrorism financing related to the customer.
K. When a securities firm suspects that a customer or a transaction involves money laundering or terrorism financing, and the securities firm reasonably believes that carrying out CDD procedures may disclose information to the customer, it may refrain from performing the procedures and report the suspicion of money laundering or terrorism financing instead.
L. Other matters requiring attention in establishing business relationships shall without exception be handled in accordance with the internal operating rules and procedures of the securities firm.

25. The securities firm shall report suspicion of money laundering or terrorism financing in accordance with Article 10 of the Money Laundering Control Act when it establishes a business relationship or conducts a transaction with any counterparty specified in subparagraph 1, item H. If that counterparty is an individual, legal person, or organization that is sanctioned under the Counter-Terrorism Financing Act, the securities firm, from the day it comes to know so, shall refrain from doing any of the acts set out in Article 7, paragraph 1 of the Counter-Terrorism Financing Act, and shall carry out reporting procedures as set out in the Counter-Terrorism Financing Act (the reporting should be done in the format that is downloadable from the website of the Ministry of Justice Investigation Bureau [MJIB]). If any circumstance contemplated by subparagraph 2 or 3 of paragraph 1, Article 6 of the Counter-Terrorism Financing Act existed with respect to the securities firm before the aforesaid counterparty was sanctioned, the securities firm shall apply to the Ministry of Justice for permission in accordance with the Counter-Terrorism Financing Act.

A securities firm’s CDD measures shall include ongoing due diligence on customer identity, and shall be conducted in accordance with the following provisions:

1. A securities firm shall apply CDD measures to existing customers on the basis of materiality and risk, and conduct due diligence on existing relationships at appropriate times, taking into account whether and when CDD measures have previously been undertaken and the adequacy of data obtained. The aforesaid appropriate times shall at least include:

A. When the customer opens another new account or establishes a new business relationship.

B. When it is time for periodic review of the customer scheduled on the basis of materiality and risk.

C. When it becomes known that there is a material change to the customer's identity or background information.

2. A securities firm shall conduct ongoing due diligence on the business relationship to scrutinize transactions undertaken throughout the course of the relationship to ensure that the transactions being conducted are consistent with the securities firm's knowledge of the customer, its business and risk profile, including, where necessary, the source of funds.

3. A securities firm shall periodically review the adequacy of the information obtained in respect of customers and beneficial owners and ensure that the information is kept up to date, particular for higher risk categories of customers, whose reviews shall be conducted at least once every year, while the review frequency for other customers shall be determined by a risk-based approach.

4.A securities firm can rely on existing customer records from its previously conducted CDD procedures to undertake identification and verification. Therefore,

a securities firm is allowed to carry out transactions without repeatedly identifying and verifying the identity of an existing customer. However, a securities firm shall conduct CDD measures again in accordance with Point 2 if it has doubts about the veracity or adequacy of the records, or there is a suspicion of money laundering in relation to that customer, or there is a material change in the way that the customer's transactions or account are operated, which is not consistent with the customer's business profile.

A securities firm shall determine the extent of applying CDD and ongoing due diligence monitoring measures using a risk-based approach (RBA), including:
1. For higher risk circumstances, a securities firm institution shall perform enhanced CDD or ongoing due diligence measures by adopting additionally at least the following enhanced measures:
A. Before establishing or entering a new business relationship, the securities firm shall obtain the approval of senior management at a level of approval authorization based on internal risk considerations.
B. A securities firm shall take reasonable measures to understand the sources of the customer's wealth and funds. The sources of funds means the real sources of the funds; for example, salary and wages, investment income, and real estate transactions.
C. A securities firm shall conduct enhanced ongoing monitoring of the business dealings and relationship.
2. For customers from countries or regions with high risks of money laundering or terrorism financing, a securities firm shall conduct enhanced CDD measures consistent with the risks identified.
3. For lower risk circumstances, a securities firm may apply simplified CDD measures, which shall be commensurate with the lower risk factors. However simplified CDD measures are not allowed in any of the following circumstances:
A. Where the customers are from or in countries or jurisdictions known to have inadequate AML/CFT regimes, including but not limited to those which are designated by international organizations on AML/CFT as countries or regions with serious deficiencies in their AML/CFT regime, and other countries or regions that do not or insufficiently comply with the recommendations of international organizations on AML/CFT as forwarded by the Financial Supervisory Commission (FSC).
B. Where there is a suspicion of money laundering or terrorist financing in relation to the customer or the transaction.
Simplified CDD measures that a securities firm may take are as follows:
1. Lower the frequency of customer identity information updates.
2. Lower the level of ongoing monitoring, and set a reasonable monetary amount threshold as the basis of examining transactions.

3. When the purpose and nature of the type of transactions or the established business relationship can be inferred from the transactions or relationship themselves, the securities firm is not required to further collect specific information or carry out special measures to examine the purpose and nature of the business dealings and relationship.

A securities firm shall perform its own CDD operations. However if it is otherwise permitted by laws and regulations or the FSC that a securities firm may rely on third parties to perform the identification and verification of the identities of customers, agents, and beneficial owners or the purpose and intended nature of the business relationship, the securities firm relying on the third party shall still bear the ultimate responsibility for CDD measures and comply with the following provisions:

1. A securities firm relying on a third party shall be able to immediately obtain the necessary CDD information.
2. A securities firm shall take adequate steps to ensure that identification data and other relevant documentation relating to the CDD requirements will be made available from the third party upon request without delay.
3. A securities firm shall ensure that the third party it relies on is regulated, supervised or monitored, and has appropriate measures in place for compliance with CDD and record-keeping requirements.
4. A securities firm shall ensure that the jurisdiction where the third party it relies on is based has AML/CFT regulations in place that are consistent with the standards set out by the FATF.

A securities firm's watch list filtering mechanisms for customers and transaction-related counterparties shall be handled in accordance with the following provisions:

1. A securities firm shall establish policies and procedures for watch list filtering, using a risk-based approach, to detect, match, and filter whether customers, or the senior managerial officers, beneficial owners or trading counterparties of customers are individuals, legal persons or organizations sanctioned under the Counter-Terrorism Financing Act or terrorists or terrorist groups identified or investigated by a foreign government or an international organization. If so, the securities firm shall take the measures under Point 2, subparagraph 15.
2. The policies and procedures for customer and transaction counterparty watch list filtering shall include at least matching and filtering logics, implementation procedures and evaluation standards, and shall be documented.
3. A securities firm shall document its name and account filtering operations and maintain the records for a time period in accordance with Point 10.
4. The filtering mechanism shall be tested, including testing for the following:

A. Whether the sanctions list and threshold settings are based on the risk-based approach.
B. Correctness and completeness of data input and corresponding fields in the system.
C. Logic of matching and screening.
D. Model validation.
E. Correctness and completeness of data output.
5. Based on the test results, confirm whether the filtering mechanism can still adequately reflects risks, and modify the mechanism in a timely manner.

A securities firm’s ongoing monitoring of account and transaction shall be in accordance with the following provisions:
1. A securities firm shall progressively make use of information systems to integrate the basic information and transaction information of the entire company’s customers so that the head office and branches may carry out inquiries for the purpose of prevention of money laundering and countering terrorism financing, so as to strengthen its ability to monitor accounts and transactions. A securities firm shall also establish internal control procedures for requests and inquiries as to customer information made by various units and shall exercise care to ensure the confidentiality of the information.
2. A securities firm shall establish policies and procedures for account and transaction monitoring using a risk-based approach, and use the information system to assist in the detection of suspicious money laundering or terrorism financing transactions.
3. A securities firm shall review its policies and procedures for account and transaction monitoring based on AML/CFT laws and regulations, the nature of customers, business size and complexity, money laundering and terrorism financing trends and related information gathered from internal and external sources, and its internal risk assessment results, and update those policies and procedures periodically.
4. A securities firm's policies and procedures for account and transaction monitoring shall include at least complete money laundering and terrorism financing monitoring indicators, parameter settings, monetary threshold amounts, alerts and monitoring operations, and investigation procedures and reporting standards for monitored cases, and shall be documented.
5. The mechanism of the preceding subparagraph shall be tested, including testing for the following:
A. Internal control process: examine the roles and responsibilities of personnel or units relating to the account and transaction monitoring mechanism.
B. Correctness and completeness of data input and corresponding fields in the system
C. Detection scenario logic.

D. Model validation.
E. Data output.
6. The securities firm shall further examine the customer’s identity when the securities firm discovers or has reasonable grounds to suspect that its customer, customer’s funds, assets, or transactions that it plans to conduct or already has conducted are related to money laundering or terrorism financing regardless of the monetary amount or value, or whether the transaction is completed.
7. Suspicious types of transactions suggesting money laundering and terrorism financing are listed in the Appendix. However, the appendix may not be exhaustive. A securities firm shall choose or develop types of transactions that should be watch-listed by the securities firm as possible money laundering or terrorism financing activities based on the securities firm's own asset scale, geographical distribution, business characteristics, the natures and transaction characteristics of its customer groups, and the securities firm's internal risk assessment of money laundering and terrorism financing or information on normal transaction activities.
8. The securities firm shall determine the reasonableness of identified watch-listed transactions under the preceding subparagraph on a case-by-case basis, and shall complete the investigation process as quickly as possible to determine whether a given transaction is suspected of involving money laundering or terrorism financing and retain records of the investigation. (The determination of reasonableness may include determining whether there are situations such as transactions that are out of keeping with a customer’s identity, income level, or business scale, or transactions that are not related to the nature of a customer’s business, a customer’s business model, or have no reasonable economic purpose, use, or explanation, or an unclear or inadequately explained source of funds.) When a transaction is examined and determined not to be suspected of money laundering or terrorism financing, the reasons for the exclusion shall be recorded and analyzed. When the investigation has resulted in a determination that a transaction is suspected of money laundering or terrorism financing, then regardless of the amount of the transaction, the securities firm shall submit a report, in a format prescribed by the MJIB, for approval by the chief AML/CFT officer, and after such approval shall immediately file the report with the MJIB. The report shall be filed within 2 business days following the date of said approval. The same shall apply even if the transaction is not completed.
9. A securities firm shall identify via a risk-based approach which suspicious types of transactions suggesting money laundering and terrorism financing as listed in the Appendix require the firm to establish an information system to aid in their monitoring. Regarding types of transactions that are not included for monitoring by that information system, the securities firm shall also use other methods to help its employees identify suspicious types of transactions suggesting money laundering and terrorism financing. The information system cannot completely replace employee’s judgement. The securities firm shall continue to strengthen the

training of its employees so that its employees are able to identify suspicious types of transactions suggesting money laundering and terrorism financing.
10. A securities firm shall document its ongoing execution of monitoring of accounts and transactions, and maintain the records for a time period in accordance with Point 10.

Report of suspicious transactions suggesting money laundering and terrorism financing :
1. A case handler in any unit who discovers an unusual transaction shall immediately report it to the AML/CFT supervising officer.
2. Upon receipt of such a report, the supervising officer shall promptly decide if it is indeed a matter that should be reported. If it is determined that the matter should be reported, the supervising officer shall instruct the case handler to fill out a report form immediately (the reporting should be done in the format that is downloadable from the website of the MJIB).
3. After the report form has been approved by the supervising officer of the unit and forwarded to and approved by the chief AML/CFT officer, the report shall immediately be filed with the MJIB. The report shall be filed within 2 business days following the date of said approval. Within 15 days after the end of each fiscal year, the categories of suspicious types of transactions suggesting money laundering or terrorism financing and the quantities of suspicious transactions therein shall be submitted to the competent authority for review and copies also forwarded to the Taiwan Stock Exchange and Taiwan Securities Association.
4. If the suspected money laundering or terrorism financing transaction represents an obviously serious or urgent case, the securities firm shall promptly report to the MJIB by fax or other feasible method, and then immediately submit the written materials. However, if the securities firm has received an acknowledgment of receipt (format downloadable from the MJIB website) from the MJIB by fax need not submit the written materials to the MJIB. The firm shall preserve the acknowledgement of receipt.
Data confidentiality
1. Employees at all levels shall diligently maintain confidentiality, and prevent any disclosure of any reported data or information. The securities firm shall provide its employees with training or instructional materials to prevent information disclosure during interactions or normal operations between its employees and customers.
2. Documents relating to reported matters shall be treated as confidential documents. If confidential information is disclosed in any case, the securities firm shall take corresponding measures under applicable provisions.
3. AML/CFT personnel, regulatory compliance personnel, and internal audit personnel, for purposes of carrying out their duties, should be able to promptly

access customer information and transaction records, but such individuals are nevertheless still required to diligently maintain confidentiality.

When the securities firm files a report on the properties or property interests and locations of designated sanctioned individuals or entities pursuant to Article 7 of the Counter-Terrorism Financing Act, it shall comply with the following provisions:
1. After learning of the case, the unit-in-charge at the head office shall submit the report for approval by the chief AML/CFT officer, and then immediately file the report with the MJIB, in a format and manner prescribed by the MJIB. The report shall be filed within 2 business days following the date of said approval.
2. In the event of an obviously significant and urgent case, the securities firm shall make a prompt report to the MJIB as soon as possible by fax or by other available means and afterwards file a make-up report in a format (downloadable from the MJIB website) and manner prescribed by the MJIB. However, such a make-up report is not required if the MJIB has confirmed the receipt of report by sending a reply in a prescribed format by fax. The securities firm shall retain the faxed reply from the MJIB.
3. The securities firm shall prepare an annual report as of 31 December (the "cut-off date") every year, in a format (downloadable from the MJIB website) prescribed by the MJIB. The report shall state all properties or property interests of designated sanctioned individuals, legal entities or groups managed or held by the securities firm as of the cut-off date under Article 7 of the Counter-Terrorism Financing Act and the report shall be submitted to the MJIB for recordation by 31 March the following year.
The reporting records, transaction documents and annual reports mentioned in the preceding paragraph shall be retained in their original forms for 5 years.

The securities firm shall process currency transactions of a certain amount or more in accordance with the following provisions:
1. A "currency transaction of a certain amount or more" means any single transaction involving receipt or payment of cash (this includes any transaction booked as cash for accounting purposes) or currency exchange transaction of NT$500,000 or more.
2. If a securities firm, when handling related business (e.g. bond trading or, directly or as an agent, handling margin trading, short selling, or other transactions), discovers a currency transaction of a certain amount or more, it shall verify the identity of the customer and shall preserve the related records and vouchers.
3. Measures for verifying customer identity shall be handled in accordance with the following provisions:

A. A firm shall verify the identity of its customer on the basis of the documentary proof of identity or passport provided thereby, and shall record the customer's name, date of birth (year/month/day), address, telephone, trading account number, transaction amount, and identity document number. If the customer can be verified as the owner of the transaction account, further identity verification is not required, but the transaction record should specify that the transaction is carried out by the account owner him/her/itself.
B. If a transaction is processed by an agent, based on the identification document or passport provided by the agent, the firm shall record the agent's name, date of birth (year/month/day), address, telephone, trading account number, transaction amount, and identity document number.
C. For occasional transactions, the customer’s identity shall be verified in accordance with Point 2, subparagraph 3 of this Template.
4. For any currency transaction of a certain amount or more, a securities firm shall file a report using electronic media (in the format downloadable from the MJIB website) with the MJIB within 5 business days after the transaction is completed. If the securities firm, for a legitimate reason, is unable to file the report by electronic media, it may file the report in writing (in the format downloadable from the MJIB website).
5. For a currency transaction of a certain amount or more, the requirement of reporting to the MJIB may be exempted in cases in which a currency transaction of a certain amount or more arises from a receipt or payment under relevant laws or regulations or contractual relationships, to or from a government agency, government owned enterprise, institution exercising public power (within the scope authorized), public or private school, public utility, or fund duly established by the government, but the securities firm shall still verify the customer's identity and preserve relevant transaction records and vouchers. Nonetheless, if a firm discovers that any above transaction is a suspected money laundering or terrorism financing transaction, it shall follow the provisions of Article 10 of the Money Laundering Control Act and of Article 7, paragraph 3 of the Counter-Terrorism Financing Act.

A securities firm shall keep records on all business relationships and transactions with its customers in hardcopy or electronic form in accordance with the following provisions:
1. A firm shall maintain all necessary records on transactions, both domestic and international, for at least 5 years, or for a longer period if required by law. The above necessary records include:
A. Name and account number of parties to transactions.
B. Date of transactions.
C. Type of currency and monetary amount.

2. For large currency transactions of a certain amount or more, the originals of the verification records and records and vouchers in connection with reports filed shall be kept for 5 years. The securities firm shall select a single method for recording customer verification procedures, in accordance with the principle that the entire company should adopt a consistent system.
3. For reports about suspected money laundering and terrorism financing transactions, report-related records and transaction vouchers shall be preserved in the original for 5 years. For any transaction suspected of involving money laundering, the firm shall preserve the transaction records and vouchers in a special-purpose book for reference. In a case duly under investigation pursuant to law, relevant transaction records and vouchers may not be destroyed before the case is closed, even where the time period for their preservation lapses.
4. A firm shall keep all the following information for at least five years after the business relationship or occasional transaction ends, or for a longer period if required by law:
A. All records obtained through CDD measures, such as copies or records of official identification documents like passports, identity cards, driving licenses or similar documents.
B. Account files.
C. Business correspondence, including inquiries to establish the background and purpose of complex, unusual large transactions and the results of any analysis undertaken.
5. Transaction records maintained by a securities firm shall be sufficient to permit reconstruction of individual transaction so as to provide, if necessary, evidence for prosecution of criminal activity.
6. A securities firm shall ensure that transaction records and CDD information will be available swiftly to the competent authorities when such requests are made with appropriate authority.

The AML/CFT internal control system established by a securities firm under Article 4 of the Regulations Governing Internal Audit and Internal Control System of Anti-Money Laundering and Countering Terrorism Financing of Securities and Futures Business and Other Financial Institutions Designated by the Financial Supervisory Commission, and any amendments thereto, shall be adopted by its board of directors, and shall include the following items:
1. Policies and procedures adopted to identify, evaluate, and manage the risks of money laundering and terrorism financing in accordance with the Guidelines Governing Money Laundering and Terrorist Financing Risk Assessment and Relevant Prevention Program Development by the Securities Sector (see Attachment).
2. AML/CFT programs adopted based on the above Guidelines, the results of risk assessment, and the securities firm's business scale, to manage and reduce

identified risks. Regarding higher risks, the firm shall adopt enhanced measures for control and management.
3. Standard operational procedures to supervise, control, and manage compliance with AML/CFT regulations and the execution of AML/CFT measures, which shall be included in the self-audit and internal audit systems, and enhanced when necessary.
The identification, evaluation, and management of the risks of money laundering and terrorism financing in subparagraph 1 of the preceding paragraph shall at least cover aspects such as customer, area, products and services, and transaction or payment methods, and shall be conducted in accordance with the following provisions:
1. Prepare a risk assessment report.
2. Consider all risk factors to determine the overall risk level and appropriate measures for reducing the risks.
3. Establish a mechanism for updating risk assessment reports to ensure that the risk data is kept up to date.
4. Submit risk assessment reports for recordation by the competent authority when the reports are finished or updated.
The AML/CFT program in paragraph 1, subparagraph 2 shall include the following policies, procedures, and control and management mechanisms:
1. CDD measures
2. Filtering the names of customers and parties relating to transactions.
3. Ongoing monitoring of accounts and transactions
4. Records retention.
5. Reporting currency transactions of a certain amount or more.
6. Reporting suspected money laundering or terrorism financing transactions, and filing reports pursuant to the Counter-Terrorism Financing Act.
7. Designating compliance matters for which the chief AML/CFT officer is responsible.
8. Employee selection and appointment procedures.
9. Ongoing employee training plans.
10. Function for independent auditing of the effectiveness of the AML/CFT system.
11. Other matters provided by applicable AML/CFT regulations and by the competent authority.
A securities firm that has any branch offices (or subsidiaries) shall establish a group-level AML/CFT program, and implement the program in its branch offices (or subsidiaries). In addition to the policies, procedures, and control and management mechanisms in the preceding subparagraphs, the following matters shall also be specified in accordance with the data confidentiality laws and regulations of Taiwan and of the jurisdictions where its foreign branch offices (or subsidiaries) are located:

1. The policies and procedures for sharing of information within the group that is required for the purpose of CDD measures and management of risks of money laundering and terrorism financing.
2. For AML/CFT purposes, when necessary, the securities firm may require its branch offices (or subsidiaries) to provide information on customers, accounts, and transactions, as required for group-level legal and regulatory compliance, audit, and AML/CFT functions. This shall include information and analysis of unusual transactions or activities. When necessary, the securities firm may also enable its branches (or subsidiaries) to receive the above information through group-level management functions.
3. The security and protection of the use and confidentiality of exchanged information, including security and protection measures against unauthorized disclosure of information.
To the extent permitted by the laws and regulations of the jurisdictions where the securities firm's foreign branch offices (or subsidiaries) are located, the firm shall ensure that its foreign branches and subsidiaries comply with the same strict AML/CFT measures as used in the head office (or parent company). Where the minimum requirements of the jurisdictions where its head office (or parent company) and branches (or subsidiaries) are located are different, the branch (or subsidiary) shall choose to follow the criteria which are higher. However, if there is any doubt regarding the determination of higher or lower criteria, the determination by the competent authorities of the place in which the head office (or parent company) of the firm is located shall prevail. If it 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 risks of money laundering and terrorist financing, and a report shall be made to the Securities and Futures Bureau, Financial Supervising Commission.
The policies and procedures adopted by a Taiwan branch or subsidiary of a foreign financial institution group to identify, evaluate and manage the risks of money laundering and terrorism financing in accordance with the Guidelines Governing Money Laundering and Terrorist Financing Risk Assessment and Relevant Prevention Program Development by the Securities Sector, and the AML/CFT programs adopted based on such Guidelines, as required in subparagraphs 1 and 2 of paragraph 1, must include policies, procedures, and control and management mechanisms. If the parent group has established policies and procedures no less strict than, and not in violation of, the laws and regulations of Taiwan, the Taiwan branch or subsidiary may apply the policies and procedures of the parent group.
The board of directors of the securities firm shall bear ultimate responsibility for establishing and maintaining appropriate and effective AML/CFT internal control. The board of directors and senior management shall understand the securities firm's AML/CFT risks, and the operation of the AML/CFT program, and adopt measures to create an organizational culture that emphasizes prevention of money laundering and countering of terrorism financing.

The securities firm shall arrange adequate AML/CFT personnel and resources according to its scale and risks, and the board of directors shall appoint one senior officer to be the chief AML/CFT officer. The firm shall give the chief AML/CFT officer adequate authorities of office to coordinate and supervise AML/CFT operations, and shall ensure that the personnel and officer do not concurrently hold any position involving a conflict of interest with their AML/CFT duties.
The chief AML/CFT officer in the preceding paragraph is responsible for the following matters:
1. Supervise planning and execution of the policies and procedures for identification, assessment, and monitoring of money laundering and terrorism financing risks.
2. Coordinate and supervise the execution of comprehensive identification and assessment of money laundering and terrorism financing.
3. Monitor risks relating to money laundering and terrorism financing.
4. Develop AML/CFT programs.
5. Coordinate and supervise the execution of AML/CFT programs.
6. Ensure compliance with applicable AML/CFT laws and regulations, including all relevant model guidelines or self-regulatory rules that are adopted by the financial industry professional association that the securities firm belongs to and approved for recordation by the competent authority.
7. Supervise the reporting of suspected money laundering or terrorism financing transactions to the MJIB and the reporting of assets and property interests of counterparties designated by the Counter-Terrorism Financing Act and their locations.
The chief AML/CFT officer under paragraph 1 shall report to the board of directors and supervisors (or the audit committee) at least every 6 months. When any material violations of law or regulation is found, the chief AML/CFT officer shall promptly report to the board of directors and supervisors (or the audit committee).
A foreign business unit of a securities firm shall take the number of its local subsidiaries, business scale, and risks into overall consideration to arrange adequate AML/CFT?personnel, and appoint a person to be the officer responsible for coordinating and supervising AML/CFT matters.
The arrangement of the AML/CFT supervising officer by the securities firm’s foreign business unit shall be in compliance with the laws and regulations, and requirements of the competent authority, of the host jurisdiction. The supervising officer shall have adequate authorities of office to coordinate and supervise AML/CFT matters, including the ability to communicate directly the chief AML/CFT officer of paragraph 1. He or she shall be full-time in the position of AML/CFT supervising officer, with the exception that he or she may concurrently hold the position of chief compliance officer. If the AML/CFT supervising officer

concurrently holds any other position, the foreign business unit shall communicate with the local competent authority to ensure that there is no likelihood of a conflict of interest, and report to the competent authority for recordation.

The securities firm’s domestic and foreign business units shall assign a member of the senior management to be the AML/CFT supervising officer, and the AML/CFT supervising officer shall be responsible for supervising matters relating the implementation of the AML/CFT operations of his/her business unit. A business unit shall conduct self-assessment in accordance with the Regulations Governing the Establishment of Internal Control Systems by Service Enterprises in Securities and Futures Markets.

The securities firm's internal audit unit shall audit the following matters in accordance with regulations, and issue an audit opinion:

1. Whether the money laundering and terrorism financing risk assessment and the AML/CFT programs meet related statutory and regulatory requirements and are implemented faithfully.
2. The effectiveness of the AML/CFT programs.

The powers and duties of the internal audit unit of the securities firm shall be as follows:

1. The internal audit unit shall conduct periodic audits in accordance with the internal control measures adopted and other relevant provisions, and carry out testing of the effectiveness of the AML/CFT program and the quality of risk management in the company's operations, departments, and branches (or subsidiaries).
2. The audit method shall encompass independent transaction tests, including screening relevant transactions involving products, customers, and regions that the securities firm has assessed as high-risk, and verifying that the securities firm is effectively implementing the applicable AML/CFT provisions.
3. The internal audit unit, when it discovers any deficiencies in the implementation of the management measures by any unit, shall regularly report such cases to the chief AML/CFT officer in writing, and such cases shall be provided for reference in the employee in-service training programs of the firm.
4. If any deliberate concealment or non-disclosure of any material violation is discovered, appropriate sanctions shall be imposed by the unit with authority to do so.

The securities firm’s general manager shall supervise all units in scrupulously assessing and reviewing the implementation of the AML/CFT internal control system. An AML/CFT internal control system statement shall be jointly signed by the chairman of the board, the general manager, the chief internal audit officer, and the chief AML/CFT officer, and shall be submitted to the board of directors for approval. The content of the statement shall be disclosed on the securities firm’s website, and shall be publicly announced and filed on the website

designated by the competent authority within 3 months after the end of every fiscal year.
For a Taiwan branch office of a foreign securities firm, the responsible person of the Taiwan branch office, who is authorized by the board of directors of the head office, will be responsible for the matters relating to the board of directors or supervisors provided in this Template. The statement of the preceding paragraph shall be jointly signed and submitted by the responsible person of the Taiwan branch office who is authorized by the board of directors of the head office, the chief AML/CFT officer, and the chief internal audit officer in the Taiwan area.

The securities firm shall ensure that it establishes high-standard employee selection and appointment procedures, including review of the integrity of character of employees and the professional knowhow required to perform their duties.
A securities firm's chief AML/CFT officer, AML/CFT personnel, and the AML/CFT supervising officer of a domestic business unit shall meet one of the following requirements within 3 months after his/her appointment, and the securities firm shall establish related mechanisms for control and management to ensure compliance with regulations:
1. Has been a full-time legal compliance or AML/CFT personnel for at least 3 years.
2. The chief AML/CFT officer and AML/CFT personnel shall attend at least 24 hours of courses held by institutions designated by the competent authority, and pass the investigation and obtain a certificate of completion for such courses. The AML/CFT supervising officer and personnel of a domestic business unit shall attend at least 12 hours of courses held by institutions designated by the competent authority, and pass the examination and obtain a certificate of completion for such courses. However, a chief compliance officer who concurrently serves as chief AML/CFT officer or compliance personnel who concurrently serve as AML/CFT personnel are deemed to meet the qualification requirements in this subparagraph after they have attended 12 hours of AML/CFT educational training offered by institutions recognized by the competent authority.
3. Obtain domestic or international AML/CFT professional certification held by institutions designated by the competent authority.
A securities firm’s chief AML/CFT officer and personnel or the AML/CFT supervising officer of a domestic business unit shall attend at least 12 hours of AML/CFT educational training held by an internal or external unit agreed by the AML/CFT officer. The content of the training shall cover at least newly amended laws and regulations, and trends and patterns of money laundering and terrorism financing risks. If in the current year a person has obtained a domestic or international AML/CFT professional certification issued by an institution

recognized by the competent authority, it may be used to offset his or her training hours for the year.

A foreign business unit's supervising AML/CFT officer and the chief AML/CFT officer and AML/CFT personnel shall have expertise in money laundering prevention, be well informed in relevant local laws and regulations, and attend not less than 12 hours of AML/CFT educational training offered by foreign competent authorities or relevant institutions every year. If no such training is available, the officers and personnel may attend AML/CFT courses offered by internal or external training units agreed to by the chief AML/CFT officer.

Appropriate content and hours of AML/CFT orientation and training shall be arranged for the securities firm’s directors, supervisors, general manager, compliance personnel, internal audit personnel, and business personnel according to the nature of their job duties, to familiarize them with their AML/CFT duties and equip them with the professional knowhow to carry out those duties.

When any of the follow circumstances exists with respect to an employee, the securities firm shall conduct sample checks of the business matters handled by that employee, and may as necessary request assistance from its internal audit unit:

1. The employee leads an extravagant lifestyle that is inconsistent with his or her level of income.
2. The employee has arranged for leave, but cancels the leave without reason.

Pre-employment and on-the-job training may be conducted as follows:

1. Pre-employment training: The training for new employees shall include a certain number of hours of training courses relating to AML/CFT laws and regulations and financial services personnel’s legal responsibilities, so as to familiarize new employees with relevant provisions and responsibilities.
2. On-the-job training:

A. Preliminary legal awareness training: After the Money Laundering Control Act and the Counter-Terrorism Financing Act enter into force or are amended, the securities firm shall act as quickly as possible to conduct legal awareness training. Personnel shall be familiarized with the Money Laundering Control Act, the Counter-Terrorism Financing Act, and related laws and regulations, and the securities firm's compliance measures shall be explained to them. The dedicated AML/CFT unit be responsible for planning and designing of the training, after which, employee training unit will be responsible for conducting the training.

B. Ongoing on-the-job training:

a. The employee training department shall offer regular annual training courses for study by employees, so as to improve employee’s judgment, ensure that AML/CFT functions are effectively performed, and prevent employees from violating laws. Courses relating to this training may be arranged in other suitable professional training classes.

b. In addition to instructors trained by the securities firm, academics and experts may also be hired as necessary to teach AML/CFT training programs.

c. In addition to introducing related laws and regulations, the courses shall also discuss actual case histories so that employees can understand the characteristics and types of money laundering and terrorism financing, and can spot transactions suspected of money laundering and terrorism financing.
d. The dedicated AML/CFT unit shall periodically check up on employees' attendance at training, and shall see to it that employees who have not attended training participate in relevant training in accordance with actual needs.
e. In addition to internal on-the-job training, the securities firm may also selectively send employees to attend training courses held by external training institutions.
3. Lectures on specific topics: To enhance employees' understanding of AML/CFT laws and regulations, the firm can arrange lectures on specific topics by academics and experts.

Other matters for attention:
1. If any of the following circumstances arises with respect to a customer, the securities firm personnel shall decline to serve the customer, and report to his or her immediate supervisor.
A. The customer insists not to provide relevant data when informed that the law requires the customer to provide relevant data to verify his/her/its identity.
B. Any individual or organization coerces or attempts to coerce the personnel not to keep files of transaction records or statements.
C. The customer attempts to persuade the personnel to waive the information provision requirements for such transactions.
D. The customer inquires about the possibility of avoiding reporting requirements.
E. The customer is eager to explain that the source of their funds is legal or that they are not laundering money.
F. The customer insists that a transaction must be completed immediately without a reasonable explanation.
G. The customer's description is clearly different from the actual transaction.
H. The customer attempts to offer benefits to the personnel to achieve the purpose of receiving services from the securities firms.

When the competent authority or auditors engaged by it carry out an audit under Article 8 of the Regulations Governing Internal Audit and Internal Control System of Anti-Money Laundering and Countering Terrorism Financing of Securities and Futures Business and Other Financial Institutions Designated by the Financial Supervisory Commission, the securities firm shall, when and as required, present relevant account books, documents, electronic data files, or other relevant materials. The aforesaid materials shall be provided regardless of their means of storage, whether hard copies, electronic files, emails, or any other form or means

of storage whatsoever, and the securities firm may not evade, refuse, or obstruct the audit for any reason.

This Template, and any amendments hereto, shall be enforced after it has been passed by the Board of Directors of the Taiwan Securities Association and submitted to the competent authority for recordation.