Regulations Governing Anti-Money Laundering and Countering the Financing of Terrorism for Enterprises Handling Virtual Currency Platform or Transaction

Article 1 These Regulations are enacted pursuant to Paragraph 2, Article 5 of the Money Laundering Control Act to which Paragraph 3 of Article 6, first part of Paragraph 4 of Article 7, Paragraph 3 of Article 8, Paragraph 3 of Article 9, and Paragraph 3 of Article 10 apply mutatis mutandis, and Paragraph 5, Article 7 of the Counter-Terrorism Financing Act.

Article 2 The terms as used in these Regulations are defined as follows:

1. "A enterprise handling virtual currency platform or transaction" (hereinafter referred to as the enterprise) refers to a business that engages in the following activities on behalf of others.
   (1) Exchange between virtual currencies and fiat currencies, such as New Taiwan Dollar (hereinafter referred to as NTD), foreign currencies, and currencies issued by Mainland China, Hong Kong, or Macao.
   (2) Exchange between one and more forms of virtual currencies.
   (3) Transfer of virtual currencies.
   (4) Safekeeping or administration of virtual currencies or instruments enabling control over virtual currencies.
   (5) Participation in and provision of financial services related to an issuer's offer or sale of virtual currencies.
2. "A virtual currency" refers to a digital representation of value with the use of cryptography and distributed ledger technology or other similar technology that can be digitally stored, exchanged, or transferred, and can be used for payment or investment purposes. However, virtual currencies do not include digital representations of NTD, foreign currencies, currencies issued by Mainland China, Hong Kong, or Macao, securities, and other financial assets issued in accordance with laws.
3. "The establishment of business relationship" refers to the acceptance of customer applications for registration or establishment of similar business transaction relationships.
4. "An occasional transaction" refers to a transaction involving activities specified in Subparagraph 1 with an individual that has not established a business relationship with the enterprise.
5. "The beneficial owner" shall mean the natural person(s) who ultimately owns or controls the customer or the natural person on whose behalf a transaction is being conducted, including those persons who exercise ultimate effective control over a legal person or arrangement.
6. "Risk-based approach" (RBA) shall mean the enterprise shall identify, assess and understand the money laundering and terrorist financing (hereinafter referred to as ML/TF) risks to which they are exposed and take appropriate anti-money laundering and countering terrorist

financing (hereinafter referred to as AML/CFT) measures commensurate with those risks in order to effectively mitigate them. Based on the RBA, the enterprise shall take enhanced measures for higher risk situations, and take relatively simplified measures for lower risk situations to allocate resources efficiently and use the most appropriate and effective approach to mitigate the identified ML/TF risks.

The term "the enterprise" used in Subparagraph 1 of the preceding paragraph refers to those registered domestically.

Where the financial institutions and designated nonfinancial businesses or professions specified in Article 5 of the Money Laundering Control Act engage in activities specified in the items in Subparagraph 1, Paragraph 1 herein, they shall execute businesses in accordance with the related AML/CFT regulations established by these central competent authorities governing target businesses and these Regulations shall not apply.

Article 3 The enterprise shall comply with the following provisions in undertaking customer due diligence (CDD) measures on customers:

1. The enterprise shall not accept anonymous accounts or accounts in fictitious names for establishing or maintaining business relationship.
2. The enterprise shall undertake CDD measures on customers when:
   (1) Establishing a business relationship with any customer;
   (2) Carrying out an occasional transaction equal to and above NTD$30,000 (including the foreign currency equivalent thereof), or multiple occasional transactions that are obviously related with a sum total more than NTD$30,000 (including the foreign currency equivalent thereof).
   (3) There is a suspicion of money laundering or terrorist financing; or
   (4) The enterprise has doubts about the veracity or adequacy of previously obtained customer identification data.
3. The CDD measures to be taken by the enterprise shall be as follows:
   (1) Identifying the customer and verifying the customer's identity using reliable, independent source documents, data or information.
   (2) 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 methods specified in the preceding item.
   (3) Identifying the identity of the beneficial owner of a customer and taking reasonable measures to verify the identity of the beneficial owner, including using data or information from a reliable source.

(4) Understanding, and in view of the situation, obtaining relevant information on the purpose and intended nature of the business relationship when undertaking CDD measures.

4. When the customer specified in the preceding subparagraph is a natural person, the enterprise shall obtain at least the following information on the customer to identify and verify the customer's identity:
   (1) Name.
   (2) Number of official identity document.
   (3) Date of birth.
   (4) Nationality.
   (5) Household registration or residence address.
5. When the customer specified in Subparagraph 3 is a legal person, an organization or a trustee, the enterprise shall understand the business nature of the customer or trust (including a legal arrangement similar to a trust) and obtain at least the following information to identify the customer or the trust and verify its identity:
   (1) Name, legal form, and proof of existence of the customer or trust.
   (2) The charter or similar power documents that regulate and bind the legal person or trust, except for any of the following circumstances:
      A. Customers/entities provided under Item (3) of Subparagraph 7 hereof without the situations specified in the proviso of Subparagraph 3 of Article 6 herein.
      B. The customer who is an organization is verified that it does not have a charter or similar power document.
   (3) Names of relevant persons having a senior management position in the customer.
   (4) The address of the registered office of the customer, and if different, the address of its principal place of business.
6. When the customer is a legal person, the enterprise shall understand whether the customer is able to issue bearer shares and apply appropriate measures for customers who have issued bearer shares to ensure their beneficial owners are kept up-to-date.
7. When the customer specified in Item (3) of Subparagraph 3 is a legal person, an organization or a trustee, the enterprise shall 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:
   (1) For legal persons and organizations:
      A. The identity of the natural person(s) who ultimately has a controlling ownership interest in the legal person. A controlling ownership interest refers to owning directly and/or indirectly more than 25 percent of the legal person's shares or capital; the enterprise may ask the customer to provide its list of shareholders or other documents to assist in

the identification of persons holding controlling ownership interest.

B. To the extent where no natural person exerting control through ownership interests is identified under the preceding sub-item or that there is doubt as to whether the person(s) with the controlling ownership interest are the beneficial owner(s), the identity of the natural person(s) (if any) exercising control of the customer through other means.

C. Where no natural person is identified under Sub-item A or B above, the enterprise shall identify the identity of a natural person who holds the position of senior managing official.

(2) For trustees: the identity of the settlor(s), the trustee(s), the trust supervisor, the beneficiaries, and any other natural person(s) exercising ultimate effective control over the trust, or the identity of person(s) in equivalent or similar position.

(3) Unless otherwise provided for in the proviso of Subparagraph 3 of Article 6 or where the customer has issued bearer shares, the enterprise is not subject to the requirements of identifying and verifying the identity of beneficial owner(s) of a customer set out under Item (3) of Subparagraph 3 hereof, provided the customer or the person having a controlling ownership interest in the customer is:

A. a R.O.C government entity;

B. an enterprise owned by the R.O.C government;

C. a foreign government entity;

D. a public company and its subsidiaries;

E. an entity listed on a stock exchange outside 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 established outside R.O.C. that is subject to and supervised for compliance with 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;

H. a fund administered by a R.O.C. government entity; or

I. an employee stock ownership trust or an employee savings trust.

8. The enterprise shall perform CDD measures by itself. However, if it is otherwise permitted by laws or regulations that the enterprise 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 enterprise relying on the third party shall still bear the ultimate responsibility for CDD measures and comply with the following provisions:

(1) The enterprise shall be able to immediately obtain the necessary CDD information.
(2) The enterprise shall take adequate steps to satisfy itself that copies of identification data and other relevant documentation relating to CDD requirements will be made available from the third party upon request without delay.
(3) The enterprise 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) The enterprise shall make sure that the jurisdiction where the third party it relies on has AML/CFT regulations in place consistent with the standards set out by the FATF.

9. The enterprise shall not establish business relationship with a customer or conduct occasional transactions with a value of more than NTD$30,000 before completing the CDD measures.
10. Where the enterprise is unable to complete the required CDD process on a customer, it shall consider filing a suspicious transaction report on money laundering or terrorist financing (STR) in relation to the customer.
11. If the enterprise forms a suspicion of money laundering or terrorist financing and reasonably believes that performing the CDD process will tip-off the customer, it is permitted not to pursue that process and file an STR instead.

Article 4 If there exists any of the following situations in the CDD process, the enterprise shall decline to establish business relationship or carry out any transaction with the customer:

1. The customer is suspected of opening an anonymous account or using a fake name, a nominee, a shell company or legal persons/organization to establish a business relationship;
2. The customer refuses to provide the required documents for identifying and verifying its identity;
3. Where any person acts on behalf of a customer for establishing business relationship or conducting a transaction and it is difficult to check and verify the fact of authorization and identity-related information;
4. The customer uses forged or altered identification documents;
5. Documents provided by the customer are suspicious or unclear, and the customer refuses to provide other supporting documents or documents provided by the customer cannot be verified;
6. The customer procrastinates in providing identification documents in an unusual manner;
7. The customer is an individual, a legal person or an organization sanctioned under the Counter-Terrorism Financing Act, or a terrorist or terrorist group identified or investigated by a foreign government or an international organization, except for payments made under

Subparagraphs 1 to 3, Paragraph 1, Article 6 of the Counter-Terrorism Financing Act; or

8. Other unusual circumstances exist in the process of establishing business relationship or conducting transaction and the customer fails to provide reasonable explanations.

Article 5 The CDD measures of the enterprise shall include ongoing customer due diligence and comply with the following provisions:

1. The enterprise shall apply CDD requirements to existing customers on the basis of materiality and risk, and conduct due diligence on such existing relationships at appropriate times, taking into account whether and when CDD measures have previously been undertaken and the adequacy of data obtained. The aforementioned appropriate times shall include at least:
   (1) When the customer enters new business relationships with the enterprise;
   (2) When it is time for periodic review of the customer scheduled on the basis of materiality and risk; and
   (3) When it becomes known that there is a material change to customer's identity and background information.
2. The enterprise shall conduct ongoing due diligence on the business relationship to scrutinize transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the institution's knowledge of the customer, its business and risk profile, including, where necessary, the source of funds.
3. The enterprise shall periodically review the existing customer records to ensure that documents, data or information of the customer and its beneficial owner(s) collected under the CDD process are adequate and kept up-to-date, particularly for high-risk customers, whose reviews shall be conducted at least once every year.
4. The enterprise may rely on existing customer records to undertake identification and verification without the need to repeatedly identify and verify the identity of an existing customer when carrying out transactions. However, the enterprise shall conduct CDD measures again in accordance with Article 3 when it has doubts about the veracity or adequacy of the records, where there is a suspicion of ML/TF in relation to that customer, or where there is a material change in the way that the customer's transaction is conducted or the customer's account is operated, which is not consistent with the customer's business profile.

Article 6 The enterprise shall determine the extent of applying CDD and ongoing due diligence measures under Subparagraph 3 of Article 3 and the preceding article based on a risk-based approach (RBA):

1. For higher risk circumstances, the enterprise shall perform enhanced CDD or ongoing due diligence measures, including adopting at least the following additional enhanced measures:
   (1) Obtaining the approval of senior management of the enterprise before establishing or entering a new business relationship;
   (2) Taking reasonable measures to understand the sources of wealth and the source of funds of the customer; the aforementioned source of funds refers to the substantial source from which the funds generate; and
   (3) Conducting enhanced ongoing monitoring of the business relationship.
2. For customers from high ML/TF risk countries or regions, the enterprise shall conduct enhanced CDD measures commensurate with the risks identified.
3. For lower risk circumstances, the enterprise 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:
   (1) Where the customers are from or in countries and jurisdictions known to have inadequate AML/CFT regimes, including but not limited to those which 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; or
   (2) Where there is a suspicion of ML/TF in relation to the customer or the transaction.

Article 7 Where the enterprise serves as the originating party of virtual currency transfers, it shall comply with the following provisions:
1. The enterprise shall obtain required and accurate information on the customer transferring the virtual currency (hereinafter referred to as the originator) and required information on the customer receiving the virtual currency (hereinafter referred to as the beneficiary). It shall hold previously acquired information in accordance with Article 10, and submit the aforementioned information immediately and securely to the enterprise serving as the beneficiary party. Law enforcement authorities should be able to compel immediate production or such information and the enterprise shall respond accordingly.
2. The required information of the aforementioned originator and beneficiary specified in the preceding subparagraph includes:
   (1) Information of the originator shall include the name of the originator, information on the wallet used for transferring the virtual currency, and one of the following information of the originator:

A. Number of official identity document.
B. Address.
C. Date and place of birth.

(2) Information of the beneficiary shall include the name of the beneficiary and information on the wallet used for receiving the virtual currency.

3. Where the enterprise fails to conduct the transfer in accordance with the two preceding subparagraphs, it is not allowed to process the virtual currency transfer.

Where the enterprise serves as the beneficiary party of virtual currency transfers, it shall comply with the following provisions:

1. Take reasonable measures to identify virtual currency transfers that lack the required information specified in Subparagraph 2 of the preceding paragraph.
2. Have risk-based policies and procedures for determining when to execute, reject, or suspend a virtual currency transfer that lacks the required information specified in Subparagraph 2 of the preceding paragraph and the appropriate follow-up actions.
3. Maintain the information on the originator and beneficiary in accordance with Article 10.

When the enterprise transfers virtual currencies, it shall verify that the transaction counterparty (originating party or beneficiary party) is subject to and supervised for compliance with AML/CFT requirements consistent with standards set by the Financial Action Task Force on Money Laundering (FATF).

Article 8 The enterprise shall establish policies and procedures for watch list filtering, based on a risk-based approach, to detect, match and filter whether customers, beneficial owners or connected parties of the 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.

The enterprise shall document its name and account filtering operations and maintain the records for a time period in accordance with Article 10.

Article 9 When conducting CDD measures, the enterprise shall put in place risk management systems to determine whether a customer and its beneficial owner is a person who is or has been entrusted with a prominent function by a domestic government, a foreign government, or an international organization (referred to as politically exposed persons (PEPs) hereunder):

1. For a customer or the beneficial owner thereof determined to be a current PEP of a foreign government, the enterprise shall treat the customer

directly as a high-risk customer, and adopt enhanced CDD measures under Subparagraph 1 of Article 6.

2. For a customer or the beneficial owner thereof determined to be a current PEP of the domestic government or an international organization, the enterprise shall assess the PEP's risks when establishing business relationship with the PEP and conduct annual review thereafter. In case of higher risk business relationship with such customers, the enterprise shall adopt enhanced CDD measures under Subparagraph 1 of Article 6.
3. For a PEP who is no longer entrusted with a prominent public function by the domestic government, a foreign government or an international organization, the enterprise shall assess the influence that the individual could still exercise by considering relevant risk factors and determine whether to apply the provisions of the two preceding subparagraphs based on the RBA.
4. The three preceding subparagraphs shall apply to family members and close associates of PEPs.

The scope of PEPs, their family members and close associates mentioned in the preceding paragraphs will be determined by the regulations stipulated in the latter part of Paragraph 4, Article 7 of the Money Laundering Control Act.

Provisions of the first paragraph do not apply when the beneficial owner of a customer specified under sub-items (A) to (C) and (H) of Item (3), Subparagraph 7 of Article 3 is a PEP.

Article 10 The enterprise shall keep records on all business relations and transactions with its customers in hard copy or electronic form and in accordance with the following provisions:

1. The enterprise shall maintain all necessary records on domestic and international transactions for at least five years or a longer period as otherwise required by law.
2. The enterprise shall keep all the following information for at least five years or a longer period as otherwise required by law after the business relationship is ended, or after the date of the occasional transactions:
   (1) All records obtained through CDD measures, such as copies or records of passports, identity cards, driving licenses or other similar official identification documents.
   (2) Contract document files.
   (3) Business correspondence, including information on the background and purpose obtained from inquiries to complex, unusual large transactions and the results of any analysis undertaken.

3. Transaction records maintained by the enterprise shall be sufficient to reconstruct individual transactions so as to provide, if necessary, evidence of criminal activity.
4. The enterprise shall ensure that transaction records and CDD information will be available swiftly to the competent authorities when such requests are made with appropriate authority.

Article 11 The enterprise shall report cash transactions with an amount equal to or above NTD$500,000 (including its equivalent in foreign currencies and currencies issued by Mainland China, Hong Kong, or Macao) to the Investigation Bureau, Ministry of Justice within five (5) business days of the transaction.

The data reported to the Investigation Bureau, Ministry of Justice and relevant transaction records in the preceding paragraph shall be kept in accordance with the preceding article.

Article 12 The enterprise shall comply with the following provisions for ongoing monitoring of transactions:
1. The enterprise shall establish policies and procedures for transaction monitoring based on a risk-based approach and utilize information system to assist in the detection of suspicious ML/TF transactions. The enterprise shall review its policies and procedures for transaction monitoring on a regular basis.
2. The policies and procedures for transaction monitoring in the preceding subparagraph shall include at least complete monitoring indicators, parameters setting, threshold amounts, alerts and operation procedures of monitoring, the reviewing procedures for monitored cases, and reporting standards, and shall be documented.
3. The enterprise shall document its operation of ongoing transaction monitoring and maintain the records for a time period in accordance with Article 10.

The enterprise shall file suspicious ML/TF transaction reports in accordance with following provisions:
1. For a transaction that exhibits the monitoring indicators or other irregularities set out under Subparagraph 2 of the preceding paragraph, the enterprise shall complete the review process as quickly as possible to determine whether the transaction is suspected of involving ML/TF activity, and shall retain records.
2. Where the review has resulted in a determination that a transaction is suspected of involving ML or TF activity, regardless of the amount of the transaction, the enterprise shall promptly file an STR with the Investigation Bureau, Ministry of Justice in a format prescribed by the Bureau after the report has been approved by the responsible compliance officer at the enterprise. The report shall be filed within

two (2) business days of said approval. The same shall apply to attempted transactions.

3. For obviously significant suspicious ML/TF transactions of an urgent nature, the enterprise shall file a report as soon as possible to the Investigation Bureau, Ministry of Justice by fax or other feasible means.
4. The enterprise shall keep the data reported to the Investigation Bureau, Ministry of Justice and relevant transaction records in accordance with Article 10.

Article 13 When the enterprise files a report under Paragraph 3, Article 7 of the Counter-Terrorism Financing Act, it shall comply with the following provisions:

1. After learning of the case, the enterprise shall submit the report for approval by the responsible compliance officer, and then promptly file the report with the Investigation Bureau, Ministry of Justice in the format and manner prescribed by the Bureau. The report shall be filed within two (2) business days following the date of approval.
2. In the event of an obviously significant and urgent case, the enterprise shall file a report as soon as possible to the Investigation Bureau, Ministry of Justice by fax or other feasible means.

The reporting records and related relevant transaction certificates mentioned in the preceding paragraph shall be maintained in accordance with Article 10.

Article 14 The enterprise shall take appropriate measures to identify, assess, and understand its ML/TF risks. The measures shall at least cover the customers, countries or geographic areas, products, services, transactions or delivery channels and be processed in accordance with the following provisions:

1. A risk assessment report shall be documented every two years;
2. The risk assessment shall consider all risk factors to determine the level of overall risk, and appropriate measures to mitigate the risks;
3. Keeping the risk assessment up-to-date; and
4. The risk assessment report shall be provided upon the request of the Financial Supervisory Commission (hereinafter referred to as the “FSC”).

Article 15 The enterprise shall establish internal audit and internal control system for AML/CFT operations based on its ML/TF risks and business size. The system and any subsequent amendments thereto shall be approved by the board of directors. The content of the system shall include the following matters:

1. The operation and control procedures for AML/CFT.
2. Appoint an AML/CFT compliance officer at the management level for coordinating and supervising AML/CFT operations.

3. Establish screening procedures to ensure high standards when hiring employees and ongoing employee training programs, including examining whether the prospective employee has character integrity and the professional knowledge required to perform his/her duty, and regularly organizing or participating in on-the-job training for AML/CFT operations.
4. Prepare and periodically update the ML/TF risk assessment report.
5. An independent audit function to test the effectiveness of AML/CFT system; and
6. Other matters required by the AML/CFT regulations and the FSC.

The policies, controls, and procedures established in the system in the preceding paragraph shall be approved by the senior management, to enable the enterprise to manage and mitigate ML/TF risks that have been identified either by the country or the enterprise. The enterprise shall monitor the implementation of those controls and enhance them if necessary. It shall also take enhanced measures to manage and mitigate the risks where higher risks are identified.

The AML/CFT compliance officer specified in Subparagraph 2 of Paragraph 1 shall meet one of the following qualification requirements within three (3) months after appointment, and the enterprise shall establish relevant control mechanisms to ensure compliance with the provisions hereof:
1. Having served as a legal compliance officer or AML/CFT compliance officer staffed under laws and regulations, on a full-time basis for at least three (3) years;
2. Having attended at least 24 hours of courses offered by institutions recognized by the FSC, passed the exams, and received completion certificates therefor; or
3. Having received an AML/CFT professional certificate issued by an international or a domestic institution recognized by the FSC.

The enterprise shall implement on-the-job training in accordance with Subparagraph 3, Paragraph 1 of the following provisions:
1. The AML/CFT compliance officer specified in Subparagraph 2, Paragraph 1 shall annually attend at least 12 hours of training on AML/CFT. The training shall cover at least newly amended laws and regulations, trends and typologies of ML/TF risks. If the person has obtained an AML/CFT professional certificate issued by an international or a domestic institution recognized by the FSC in a current year, the certificate may be used to substitute the training hours for the year.
2. The enterprise shall annually arrange appropriate hours and contents of orientation and on-the-job training on AML/CFT for its directors, supervisors, president, legal compliance officers, internal auditors, and

business personnel in view of the nature of its business, to familiarize them with their AML/CFT duties and equip them with the professional knowhow to perform their duties.

The enterprise shall conduct an independent audit on the following matters and submit audit opinions for the audit functions specified in Subparagraph 5, Paragraph 1:

1. Whether the ML/TF risk assessment and the AML/CFT policies, controls, and procedures meet the regulatory requirements and are implemented; and
2. The effectiveness of the AML/CFT policies, controls, and procedures.

Article 16 The enterprise shall conduct ML/TF risk assessments before launching new products, new services or new business practices. It shall also establish appropriate risk management measures to mitigate identified risks.

Article 17 The enterprise shall complete the AML compliance statement in accordance with the documents, information, and procedures specified by the FSC. Where the FSC orders the enterprise to provide supplementary information in the process for filing the statement and the enterprise fails to provide within the specified period, the statement shall be deemed as incomplete throughout the process.

For the implementation of internal audit and internal control system of AML/CFT of the enterprise, the FSC may, at any time, appoint a designee or entrust an appropriate institution to conduct an inspection using risk-based approach. The inspection includes on-site and off-site inspections. Where necessary, the enterprise may be required to entrust the professionals and technologists to conduct an inspection for the aforementioned implementation and submit a report to the FSC. The expenses shall be borne by the inspected entity.

When the FSC conducts the inspection in the preceding paragraph, the enterprise shall provide the AML-related books, documents, electronic data files, or other relevant materials. The aforementioned materials, whether stored in hard copy, electronic file, e-mail, or any other form, shall be provided, and the enterprise shall not circumvent, reject or obstruct the inspection for any reason.

Article 18 These Regulations shall become effective on July 1, 2021 except for Article 7 for which the effective date shall be specified by the FSC.