ONE GAME FOUNDATION LTD.

MANUAL ON PREVENTION OF MONEY LAUNDERING AND FINANCING OF TERRORISM (the "Manual")

Published on July 13, 2018

TABLE OF CONTENTS

1. INTRODUCTION 3

2. DEFINITIONS 6

3. BEST PRACTICES 9

3.1 General best practices 9

3.2. Internal policies, procedures and controls to prevent activities related to money laundering and financing of terrorism 9

3.3 Assessing risks and applying a risk-based approach 10

3.4 General principles for performance of customer due diligence measures 14

3.5 Identification and verification of customers' and agents' identities 17

3.6 Non-individual customers: Identification and verification of beneficial owners' identities 21

3.7 On-going monitoring of a business relationship 24

3.8 Simplified customer due diligence measures 26

3.9 Enhanced customer due diligence measures 26

3.10 Dealing with Politically Exposed Persons ("PEPs") or a family member or close associate of any such individual 29

3.11 Audit Function 31

3.12 Compliance Management 31

3.13 Training of employees 31

3.14 Record-Keeping 33

3.15 Filing a suspicious transaction report ("STR") 34

ANNEXES A & B 37

1. INTRODUCTION

1.1 This Manual contains the internal policies, procedures and controls for assessment and prevention of money laundering and terrorism financing by One Game Foundation Ltd. (Registration No. UEN 201810158R) a company incorporated in Singapore with its registered address at 68 Circular Road #02-01 Singapore 049422 (the "**Company**").

1.2 It is the policy of the Company to prohibit and actively prevent money laundering and any activity that facilitates money laundering or the funding of terrorist or criminal activities. The Company is currently **NOT** subject to any specific legislation relating to Anti-Money Laundering and Countering of Financing of Terrorism ("**specific AML/CFT legislation**"), but in the spirit of benchmarking itself against entities regulated by such specific AML/CFT legislation, the Company has chosen to implement similar AML/CFT processes and procedures to the extent applicable. The Company will not be applying AML/CFT processes and procedures to every aspect of its business but will limit it to the sale of its digital tokens and the use of the purchasers of the digital tokens. In other words, the AML/CFT processes and procedures in this Manual are **voluntary on the part of the Company**.

1.3 This Manual differs from the requirements imposed by specific AML/CFT legislation on other entities in that it does not contain any detailed processes and procedures for on-going monitoring. This Manual will only focus on the acceptance of customers who purchase the Company's products, in particular, its digital tokens. For entities subject to specific AML/CFT legislation, this would be the stage known as "on-boarding of new clients". The Company has determined that on-going monitoring is only necessary if the Company undertakes any transactions on behalf of its customers in the way that entities regulated under specific AML/CFT legislation would.

1.4 The Company has decided to adapt the requirements under Part VIA of the Accounting and Corporate Regulatory Authority ("**ACRA**") Act (Cap. 2A) (the "**ACRA Act**"), and Part II of the First Schedule of the Accounting and Corporate Regulatory Authority (Filing Agents and Qualified Individuals) Regulations 2015 (the "**2015 Regulations**"), and not the requirements applicable to banks and other financial institutions regulated by the Monetary Authority of Singapore ("**MAS**"). The Company is aware that a new law, the Payment Services Bill, had been the subject of a consultation paper by MAS which may apply to services related to virtual currencies, but at the time this Manual is being prepared (July 2018), this Payment Services Bill has not yet been brought into force.

1.5 The Manual will therefore be reviewed and updated on a regular basis to ensure appropriate policies, procedures and internal controls are in place to account for both changes in AML/CFT regulations applicable to the Company and changes in its business. These are policies, procedures and internal controls to be used and complied with by all directors, registered filing individuals, and employees of the Company.

1.4 What is money laundering?

1.4.1 Money laundering is a process carried out with the intention to conceal the benefits obtained from criminal activity so that they are made to appear to have originated from legitimate sources. In this process, money obtained through criminal activity or other criminal property, for example, money or money's worth, securities, tangible property and intangible property, are mixed with or exchanged for money originating from legitimate sources or other assets with no obvious link to their criminal origins.

1.4.2 Generally, the process of money laundering comprises three stages:

(a) Placement: this is the physical movement of the benefits (usually cash) from criminal conduct.

(b) Layering: this is the process of separating the benefits of criminal conduct from the illegitimate source through layers of financial transactions to disguise the audit trail.

(c) Integration: if the layering process is successful, the integration stage will place the laundered money and other benefits back into the economy so that they appear to be legitimate.

1.5 What is the financing of terrorism?

1.5.1 Terrorism seeks to influence, compel or intimidate governments or the general public through threats or violence, causing of damage to property or danger to life, creating of serious risks to public health or safety, or disrupting of important public services or infrastructure.

1.5.2 The funds required by terrorists to carry out terrorism acts are acquired from terrorism financing. Sources of terrorism financing may be legitimate or illegitimate. For example, they may be derived from criminal activities. They may also be derived from legitimate sources such as income from legitimate business operations belonging to terrorist organisations. The methods used by terrorist organisations to obtain, move, or conceal funds for their activities are similar to those used by criminal organisations to launder their funds.

1.5.3. Terrorist financing may not involve the proceeds of criminal conduct, but rather an attempt to conceal either the origin of the funds or their intended use, which could be for criminal purposes. Legitimate sources of funds are a key difference between terrorist financiers and traditional criminal organizations. Under the Terrorism (Suppression of Financing) Act ("**TSOFA**"), a terrorist is defined as anyone who commits, or attempts to commit, any terrorist act or participates in or facilitates the commission of any terrorist act. It also includes any person set out in the First Schedule to TSOFA. The First Schedule to TSOFA refers to specific individuals, all individuals and entities belonging to or associated with the Taliban in the Taliban List, and all individuals and entities belonging to or associated with the Al-Qaida organization in the Al-Qaida List. Sections 3 to 6 of the TSOFA expressly prohibit the following:

(a) provision and collection of property for terrorist acts

(b) provision of property or services for terrorist purposes

(c) use or possession of property for terrorist purposes

(d) dealing with property of terrorists or terrorist entity

1.6 The main scope of the Manual and the Steps taken by the Company

1.6.1. Perform customer KYC and due diligence ("**CDD**") measures and formally adopt the AML/CTF programme: Specific rules and procedures are set forth for the identification and performance of due diligence measures not only on a customer and any individual purporting to act on behalf of a customer, but on all the beneficial owners of the customer if it is an entity or legal arrangement and to pay particular attention if any persons involved are politically-exposed individuals.

1.6.2. Out-sourcing of AML/CFT checks: The Company has appointed an external and professional service provider to undertake the actual AML/CFT and Know-Your-Customer ("**KYC**") checks. Such checks are to follow the processes and procedures set out in this Manual.

1.6.3 Maintain all documents and records relating to each relevant matter and obtained through customer due diligence measures

1.6.4 Compliance management and review arrangements: The Company will carry out regular review, assessment and updates of the internal policies, procedures and controls to ensure that they are adequate and they manage the money laundering and financing of terrorism risks effectively.

1.6.5 Appoint an AML/CTF compliance officer

1.6.6 Training of personnel (if required by applicable laws): In a framework that encourages a culture of internal control and compliance with the Manual, the Company has circulated this Manual to all directors, registered filing individuals, and employees of the Company and if required by applicable law, will conduct training to ensure that the directors, registered filing individuals, and employees of the Company are regularly and appropriated trained on the laws and regulations relating to the prevention of money laundering and the financing of terrorism, and the Company's internal policies, procedures and controls for the prevention of money laundering and the financing of terrorism.

1.6.7 Design and adopt an AML/CTF risk awareness training programme (if required by applicable laws)

1.6.8 File a suspicious transaction report: When the Company or the compliance officer or senior management of the Company has suspicions that a customer is engaged in money laundering or the financing of terrorism, the Company is obliged to file a suspicious transaction report. However, the Company retains its rights not to disclose to anyone, including the customer, that a report has been filed nor disclose any information or other matter which is an item subject to legal privilege.

1.6.9 Establish procedures for responding to authority's feedback

2.

DEFINITIONS

Definitions of Terms Used in the Manual	
agent (in relation to a customer)	a person appointed by the customer to act on the customer's behalf in any business relationship.
beneficial owner (in relation to a customer)	(a) an individual who ultimately owns or controls (whether through direct or indirect ownership or control) more than 25% of the shares or voting rights of the customer; or (b) otherwise exercises control over the management of the customer.
business relationship (in the context of a relationship between the Company and a customer)	a business, professional or commercial relationship between the Company and its customer. It may be a formal or an informal arrangement, and includes an occasional or a one-time transaction. For the purposes of this Manual, the business relationship generally refers to the one-time sale of a product by the Company to the customer.
company	a company incorporated pursuant to the Companies Act or pursuant to any corresponding written law.
foreign company	a company incorporated outside Singapore.
compliance management arrangements	carrying out regular reviews, assessments and updates of the adequacy of internal policies, procedures and controls to ensure that money laundering and financing of terrorism and proliferation risks are mitigated effectively. Examples of areas that may be reviewed are: (a) whether there are areas of weakness in the registered FA where appropriate risk-sensitive checks may not be being carried out in accordance with Part II of the First Schedule of the Regulations; (b) whether correct and updated records are kept; and (c) whether there are any new products, services or procedures that may be used for money laundering and financing of terrorism and which must be catered for.
connected party	(a) in relation to a legal person (other than a partnership), means any director or any natural person having executive authority (eg: Chief Executive Officers, Managing Directors etc.) in the legal person; (b) in relation to a legal person that is in a partnership, means any partner or manager*; and (c) in relation to a legal arrangement, means any natural person having executive authority in the legal arrangement.

	* *Manager in relation to a LLP, means any person (whether or not a partner of the LLP) who is concerned in or takes part in the management of the LLP. (whether or not his particulars or consent to act are lodged with the Registrar as required under s23(2) of the LLP Act).*
Customer or customer	any person who enters into a business relationship with the Company.
director	has the same meaning provided in section 4 of the Companies Act, that is, a director includes any person occupying the position of a director of a corporation by whatever name called and includes the person in accordance with whose directions or instructions the directors of a corporation are accustomed to act and an alternate and substitute director. It should be noted that all directors will be subject to the legal obligations of directorship in the Companies Act.
Financial Action Task Force ("FATF")	means the intergovernmental body which develops and promotes policies and international standards to protect the global financial system against money laundering, terrorism financing and proliferation financing. The FATF has issued 40 Recommendations, 11 Immediate Outcomes and Interpretive Notes for combating money laundering, terrorism financing and proliferation financing.
internal communication	means having procedures in place to alert the relevant persons working for the Company to: (a) how criminals may make use of the Company to launder money or fund terrorism or proliferation, so as to enable them to take appropriate action to prevent and to report it; and (b) Updates on guidance and news issued by authorities in Singapore.
limited partnership	a limited partnership registered under the Limited Partnerships Act. A "limited liability partnership" is defined as limited liability partnership registered under the Limited Liability Partnerships Act.
politically exposed person ("PEP")	an individual who: (a) is or has been entrusted with any prominent public function in Singapore (domestic PEPs) or in a country or territory outside Singapore (foreign PEPs). In this context, "prominent public function" includes the role held by a head of state, head of government, government minister, senior civil or public servant, senior judicial or military official, senior executive of a state-owned corporation, senior political party official,

	or a member of the legislature but excludes the role held by middle-ranking or more junior officials; or (b) is or has been entrusted with any prominent public function by an international organisation (PEPs of international organisations). In this context, "prominent public function" includes the role held by a director, deputy director, member of the board and member of the senior management of an international organisation, but excludes the role held by middle-ranking or more junior officials.
close associate of a PEP	a natural person who is closely connected to a PEP, either socially or professionally. This includes: (a) an immediate family member (spouse, child, adopted child, step child, sibling or parent) of a PEP; or (b) a natural person that the PEP may have significant influence over due to the level of exposure to the PEP.
suspicious transaction report or STR	a report by which a person — (a) discloses, under section 39(1) of the Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act (Cap. 65A), any knowledge or suspicion referred to in that provision, or the information or other matter on which that knowledge or suspicion is based, to a Suspicious Transaction Reporting Officer; or (b) informs, under section 8(1) of the Terrorism (Suppression of Financing) Act (Cap. 325), a police officer or Commercial Affairs Officer, of any fact or information referred to in that provision.
suspicious transaction reporting officer	has the same meaning as in section 2(1) of the Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act.
Digital token	means a digital and virtual token, in which encryption techniques are used to regulate the generation of the token or units of it, and to verify the transfer of the token. Such a digital token is not currency or legal tender issued by any central bank nor does it confer any interest in the ownership of, or debt relating to, any asset or property.

3. BEST PRACTICES

3.1 General best practices

3.1.1 The Company will comply with the following general best practices in the conduct of its token sale(s) and related activities:

(a) exercise due diligence, and conduct its business, in such a manner as to guard against the facilitation of money laundering and the financing of terrorism and proliferation; and

(b) assist and cooperate with the relevant law enforcement authorities in preventing money laundering and the financing of terrorism and proliferation.

3.2. Internal **policies, procedures and controls to prevent activities related to money laundering and financing of terrorism**

Requirement for internal policies, procedures and controls

3.2.1 The Company has developed and implemented anti money laundering and counter financing of terrorism risk management internal policies, procedures and controls ("**IPPCs**"). These IPPCs serve to discharge the responsibility of the Company for the prevention of activities related to money laundering and financing of terrorism and proliferation, and provide a framework of directions to its registered qualified individuals and employees for such prevention. The IPPCs should be effective in mitigating the risks faced by the Company and reflective of the Company's operation(s).

The internal policies, procedures and controls required

3.2.2 The Company has established and maintained appropriate and risk-sensitive internal policies, procedures and controls concerning all of the following matters:

(a) CDD measures (including simplified and enhanced) and on-going monitoring (including enhanced on-going monitoring);

(b) appropriate compliance management arrangements including monitoring, carrying out regular review assessment, updates and the internal communication of the IPPCs to ensure that they are adequate and they manage the money laundering and financing of terrorism risks effectively;

(c) making of suspicious transaction reports;

(d) risk assessment and management;

(e) appointment of a professional, third party service provider to conduct the CDD measures;

(f) appointment of an internal AML/CTF compliance offer;

(g) responding to the relevant authority's feedback as and when enquired and

(h) only if required by applicable laws, training of directors, and employees of the Company.

3.2.3 The IPPCs in paragraph 3.2.2 include those which:

(a) provide for the identification and scrutiny of complex or unusually large transactions; unusual patterns of transactions which have no apparent economic or visible lawful purpose; unusual patterns of transactions which are not related to the business activities of the customer for which the entity was originally set up to conduct; and any other activity which the Company regards as particularly likely by its nature to be related to money laundering or the financing of terrorism;

(b) specify the taking of additional measures, where appropriate and necessary, to prevent the development of new products and new business practices, including new delivery mechanisms, for money laundering and the financing of terrorism and proliferation; and the use of new or developing technologies, for both new and pre-existing products, for money laundering and the financing of terrorism; and

(c) determine whether a customer, connected party, beneficial owner, or agent is a PEP.

3.2.4 Senior management shall be actively involved in the approval process of the Company's anti money laundering and counter financing of terrorism IPPCs.

3.3 Assessing risks and applying a risk-based approach

Situations in which the Company is required to apply a risk-based approach

3.3.1 The Company will take reasonable steps to identify and assess its money laundering and financing of terrorism risks and apply a risk-based approach in:

(a) establishing IPPCs in relation to the risks faced by the Company in order to prevent activities related to money laundering and the financing of terrorism. The IPPC should be effective in mitigating the money laundering and the financing of terrorism risks faced by their business operations;

(b) identifying and verifying the identity of the beneficial owners of its customers and other connected parties;

(c) performing CDD (including screening and risk assessments) on existing and new customers and other connected parties, and determine the extent of CDD ranging from simplified to enhanced CDD where appropriate to mitigate the money laundering and the financing of terrorism risks assessed for their customers and services offered;

(d) determining whether to perform enhanced CDD or the extent of enhanced CDD to be performed for: (i) domestic PEPs, including their immediate family

members and close associates; (ii) PEPs of international organisations, including their immediate family members and close associates; or (iii) PEPs who have stepped down from their prominent public functions, taking into consideration the level of influence such persons may continue to exercise after stepping down from their prominent public functions, including their immediate family members and close associates. If the business relationship presents a high risk for money laundering or the financing of terrorism, enhanced CDD must be performed;

(e) understanding the risks of money laundering and the financing of terrorism in the countries or territories that a third party that the Company wishes to rely on operates in, if applicable; and

(f) determining the frequency of performing on-going monitoring of business relationships, depending on the level of risks.

3.3.2 The Company will take the following steps in applying a risk-based approach:

(a) identify the money laundering and the financing of terrorism and proliferation risks faced by the Company;

(b) assess the risks identified according to various categories, for example, customers (including their layers of structures, scale of activities), and countries or territories where the customers are from or in; before determining the level of overall risk and the appropriate types and extents of controls to be designed and implemented. For example, a risk assessment may lead to a classification of different levels of risk, for example, higher, medium and lower risk;

(c) design different extent of controls (for example, different extent of CDD measures for different categories of customers) to mitigate the assessed risks. For example, enhanced CDD measures needed to mitigate higher levels of risk, and simplified due diligence measures needed to mitigate lower levels of risk;

(d) monitor the implementation of these controls and enhance them if necessary; and

(e) document the risk assessment, keep it up to date and provide the riskassessment information to government authorities in Singapore if required

<u>Customer risk identification and assessment</u>

3.3.3 In identifying and assessing its risks with respect to a customer, the Company will screen the customer for adverse information and against other relevant sources on combatting money laundering and financing of terrorism for the purposes of determining if there are any money laundering or financing of terrorism risks in relation to the customer. When identifying the ML/TF risks, the Company will consider:

(a) the customer profiles including the type of customer and their source of funds, whether the customers domiciled in a foreign country, the nature and purpose

of the business relationship between the Company and the customers, and whether any of the customers are likely to be PEPs;

(b) the "designated services" that the Company provides and the methods of service delivery, against the customer's requests for services;

(c) whether the Customers conduct their transactions using physical cash;

(d) the criminal threat environment and possible vulnerabilities of the Company; and

(e) the foreign jurisdictions in which the Company provides the services.

The Company shall conduct screening and assess the risks of the customer before it establishes a business relationship. The results of the screening performed should be documented accordingly. Please refer to paragraphs 3.5 to 3.6 for the screening requirements in relation to individuals and corporate bodies.

3.3.3(A) *ML/TF risk indicators:* the Company has the following suggested list of ML/TF risk indicators and treatment/actions that is not exhaustive and is only to serve as a guide when considering the ML/TF risks that might apply to the Company:

(a) the customer provides insufficient, incomplete or suspicious information or information that cannot be verified;

(b) use of proxies, unverifiable IP address or geographical location, disposable email address or mobile number, ever changing devices used to conduct transactions;

(c) customers or transactions in high risk locations (e.g. prescribed foreign countries and the application of sanctions laws);

(d) Unusual patterns of transaction activity (e.g. volumes, velocity, structuring to avoid detection/reporting obligations, source, destination);

(e) Transactions involving known blacklisted addresses such as 'darknet' market place transactions and tumblers;

(f) Ransom-ware;

(g) Transactions in higher risk or anonymous digital currencies; and

(h) Employee collusion

3.3.4 *Higher risks* **-** These may be circumstances where the risks of money laundering or the financing of terrorism are higher and enhanced controls, including enhanced CDD measures and enhanced on-going monitoring may have to be performed. If the customer is unable to provide an adequate, satisfactory and credible explanation in response to an enquiry, further enquiry will be required. Where responses are not credible, or the Company's suspicions are not adequately allayed by the responses, the Company shall have the right to not accept any further instructions from the

customer, terminate the existing business relationship and consider whether to file a suspicious transaction report. Examples of higher risk factors include but are not limited to the following:

Customer risk factors

(a) non-resident customer and customer who has no address or multiple addresses;

(b) legal persons or arrangements that are personal asset holding vehicles and incorporated in jurisdictions that do not have a public list of its shareholders;

(c) companies that have unaccounted use of nominee shareholders or bearer shares;

(d) businesses that are cash-intensive;

(e) the ownership structure of the customer appears unusual or excessively complex given the nature of its business;

(f) the customer has criminal convictions involving fraud or dishonesty;

(g) the customer, beneficial owner, or agent who is a PEP or a family member or close associate of any such individual;

(h) the customer does not have up-to-date company accounts;

(i) the customer who asks for short-cuts and unexplained speed in completing the transaction;

(j) the customer is overly secretive or evasive (e.g. of who the beneficial owner is, or the source of funds);

(k) the customer shows unwillingness to provide evidence of identification or provides unsatisfactory evidence of identification of himself or his beneficial owners, connected parties, or both;

(l) the customer is actively avoiding personal contact without good reason; and

(m) where there are difficulties in obtaining details of the customer's beneficial owners, connected parties or both.

Country/ territory risk factors

(a) countries or territories identified by credible sources, such as mutual evaluation or detailed assessment reports or published follow up reports, as not having adequate anti-money laundering or counter financing of terrorism systems;

(b) countries or territories subject to sanctions, embargoes or similar measures issued by, for example, the United Nations;

(c) countries or territories identified by credible sources as having significant levels of corruption or other criminal activity; and

(d) countries or territories identified by credible sources as providing funding or support for terrorist activities or that have designated terrorist organisations operating within their territories.

Services/ transactions risk factors

(a) anonymous transactions (which may include cash);

(b) payments are made by the customer in actual cash (in the form of notes and coins) which would usually not be accepted anyway;

(c) payments received from un-associated third parties for the services or transactions provided;

(d) the customer asks the Company to undertake any transaction that relates to, any country or jurisdiction in relation to which the FATF has called for countermeasures or enhanced CDD measures, for example, to receive payment for the Company's products from a bank in such a jurisdiction;

(e) unusually high levels of assets or unusually large transactions in relation to what might reasonably be expected of customers with a similar profile;

(f) requests by the customer for payments to third parties without substantiating reason or corresponding transaction (such payments may be refunds for the proceeds of a token sale);

(g) abandoned transactions with no concern for the fee level;

(h) an absence of documentation to support the customer's story, previous transactions or company activities;

(i) unexplained use of express trusts;

(j) unexplained delegation of authority by the customer through the use of powers of attorney, mixed boards and representative offices;

(k) in the case of express trusts, an unexplained relationship between a settlor and beneficiaries with a vested right, other beneficiaries and persons who are the object of a power; and

(l) in the case of an express trust, an unexplained (where explanation is warranted) nature of classes of beneficiaries and classes within an expression of wishes.

3.3.5 *Lower risks* - There are circumstances where the risk of money laundering or the financing of terrorism may be lower, and where reduced controls including simplified

CDD measures may be allowed to be performed. Examples of potentially lower risk situations include but are not limited to the following:

Customer risk factors

(a) the customer is a financial institution which is subjected to money laundering and the financing of terrorism obligations; and

(b) the customer is a public company listed on a stock exchange and subject to disclosure requirements which impose requirements to ensure adequate transparency of beneficial ownership.

Country/ territory risk factors

(a) countries or territories identified by credible sources, such as mutual evaluation or detailed assessment reports, as having adequate anti-money laundering or counter terrorism financing systems, and

(b) countries or territories identified by credible sources as having a low level of corruption or other criminal activity.

Mitigating the risks through development of controls

3.3.6 After the risks have been identified and assessed, the Company will ensure that an appropriate extent of control is put in place to reduce these risks and prevent its services from being used for money laundering or the financing of terrorism. Some examples of controls for mitigating the risks are:

(a) applying different extent of CDD measures, for example, enhanced, normal or simplified CDD for different levels of risks;

(b) applying different extent of identification and verification measures for beneficial owners or connected parties;

(c) obtaining additional information, for example, source of wealth, source of funds etc on higher-risk customers including PEP, or a family member or close associate of such an individual; and

(d) applying different extent of on-going monitoring of the transactions of customers with whom there is a business relationship.

Monitoring the implementation of and enhancing the effectiveness of controls

3.3.7 The Company will have some means of monitoring and reviewing whether its controls are working effectively and if not, where these controls need to be enhanced. Some examples of situations which may be considered in deciding whether these controls should be enhanced are:

(a) uncharacteristic transactions which are not in keeping with the customer's profile and business;

(b) when Singapore regulatory authorities announce trends in money-laundering and financing of terrorism and proliferation, or changes or enhancements to anti-money laundering and financing of terrorism and proliferation measures; and

(c) when credible sources highlight trends and cases pertaining to money-laundering and financing of terrorism and proliferation.

Documenting the risk assessment

3.3.8 The Company will document its risk assessments (including information regarding each risk revision for every customer).

3.4 *General principles for performance of customer due diligence measures*

Requirements of customer due diligence

3.4.1 The Company will comply with the following requirements in performing CDD measures:

(a) identify its customers and agents, if any and verify their identities on the basis of documents, data or information obtained from a reliable and independent source;

(b) if the customer is an entity or legal arrangement, identify whether there is a beneficial owner, and take reasonable measures on a risk-sensitive basis to verify the beneficial owner's identity;

(c) determine whether a customer and beneficial owner is a PEP, or a family member or close associate of any such individual; and

(d) obtain information on the purpose and the intended nature of the business relationship.

When customer due diligence measures have to be performed

3.4.2 The Company will perform CDD measures when:

(a) it sells digital tokens to customers in exchange for virtual currencies or fiat currencies;

(b) it suspects that there is money laundering or financing of terrorism; or

(c) it doubts the veracity or adequacy of documents, data or information previously obtained for the purposes of identification or verification.

3.4.3 Generally, the Company will complete the verification of the identity of a customer, beneficial owner and agent before the establishment of a business relationship which is generally the sale of the digital tokens. For clarification, in the particular case of the sale of the digital tokens, the Company has appointed an external and professional

service provider to undertake the actual AML/CFT and KYC checks. However, if it is essential not to interrupt the normal conduct of business (for example, a deadline for the completion of the token sale) and the risks of money laundering or financing of terrorism or proliferation may be effectively managed by the Company, then this verification may take place after the establishment of the business relationship, provided that it is completed within 14 calendar days after the establishment of the business relationship. If CDD cannot be completed by the end of 1 month from the completion of the token sale, the Company may as part of the AML/KYC process, terminate the business relationship with the customer by refunding the customer the proceeds of the token sale. Where the token sale has been completed, the customer may be screened in the manner set out in paragraph 3.4.5.

3.4.5 The Company may at its discretion conduct a periodic screening of its customers to ascertain if any of them may have been sanctioned or otherwise be the subject of adverse reports since the time they had bought the Company's products.

Inability to perform customer due diligence measures

3.4.8 Where the Company is unable to perform or complete any CDD measures in relation to a customer (including simplified or enhanced CDD measure) or does not receive a satisfactory response to any inquiry in relation to any information required as part of those CDD measures, it will:

(a) not establish a business relationship with the customer;

(b) terminate any existing business relationship with the customer; and

(c) consider whether it is required to file a suspicious transaction report under section 39(1) of the Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act ("**CDSA**") and section 8 or 10 of TSOFA.

3.4.9 Please refer to **Annex A** for a list of indicators that the Company may take note of in deciding whether a disclosure should be made.

Reliance on identification and verification already performed

3.4.10 The Company need not repeatedly identify and verify the identity of a customer or its beneficial owner, if the Company sells another product to that customer;

3.4.11 The Company shall rely on the identification and verification measures that it has already performed, subject to its on-going monitoring procedures, unless it has doubts about the veracity of the information obtained. Examples of situations that may lead to the Company having doubts may be where there is a suspicion of money laundering or financing of terrorism in relation to a particular customer.

3.4.12 If it is an existing customer, the Company will perform the CDD based on its assessment of the materiality and risks of money laundering and the financing of terrorism, taking into account: -

(a) any previous CDD measures performed in relation to the customer;

(b) the time when any CDD measures were last performed in relation to the customer; and

(c) the adequacy of the data, documents or information obtained from any previous CDD measures performed in relation to the customer.

3.4.13 The Company may consider waiving the full customer identity checks for the following categories of existing customers:

(a) existing customers who have been in contact with the Company for the last 5 years and who provided some formal identification on first contact provided that there are no suspicions of money laundering and financing of terrorism and the Company is satisfied that the original identification documents were adequate. A note confirming this will be signed by the directors or senior management of the Company and attached to the file; and

(b) existing customers who have been in regular contact with the Company for the last 5 years and who have not on those occasions provided formal identification on first contact provided that there are no suspicions of money laundering and financing of terrorism and the law practice is satisfied that it knows the customer. A note confirming this will be signed by the directors or senior management of the Company and attached to the file. The note shall include details of the length of time the Company has known the customer and nature of the referral to the Company (for example, through a friend, business acquaintance or customer).

<u>Reliance on third parties to perform customer due diligence measures</u>

3.4.14 From time to time, the Company may rely on a third party to perform any CDD measures, including simplified and enhanced CDD measures apart from ongoing CDD on the business relationship with the customer during the course of business relationship. For the avoidance of doubt, such third party does not refer to the professional third-party service provider appointed under paragraph 1.6.5 of this Manual. The Company will first have to be satisfied that the following requirements are met:

(a) the third party it intends to rely on is also subject to and supervised for compliance with anti-money laundering and counter financing of terrorism and proliferation requirements, and for the recording and reporting of transactions suspected of involving money laundering or the financing of terrorism, consistent with the FATF Recommendations, and that the third party has adequate measures in place to comply with those requirements;

(b) the Company takes appropriate steps to identify, assess and understand the risks of money laundering and the financing of terrorism and proliferation in the countries or territories that the third party operates in;

(c) the third party is able and willing to provide, without delay, upon the Company's request, any document obtained by the third party with respect to the CDD measures performed for the Company; and

(d) if CDD measures are performed by a third party for the Company, the Company will immediately obtain the necessary information about the customer from that third party.

3.4.15 The Company remains ultimately responsible for compliance with its legal obligations under Part II of the First Schedule of the Regulations, notwithstanding its use of a third party to perform CDD.

3.5 Identification and verification of customers' and agents' identities

The persons who the Company shall identify and verify

3.5.1 The Company will establish the identity of each customer, connected party and its agent, if any. For this purpose, the Company may, but is not required to refer to the Customer Acceptance Checklist at Annex B. The Company may rely on the checklists or other process employed by its service provider appointed under paragraph 1.6.5 of this Manual.

Requirements for identification and verification of customers

3.5.2 For the opening of bank accounts or as required by specific AML/CFT legislation, identifying a customer or agent is usually a two-part process. First, the Company will identify the customer or agent by obtaining and recording information about the customer, and second, he shall verify the information using reliable and independent source documents, data or information, so as to ensure that the information obtained and recorded is authentic. A national registration identity card (in the case of a Singaporean) or a passport (in the case of a foreigner) is considered a reliable and independent source document. However, where the customer or agent is unable to produce original documents for verification for good reason, the Company may consider accepting documents that are certified to be true copies by qualified persons such as lawyers or notaries. **However, the Company will not verify identification documents received electronically, unless required by applicable laws.** This is because the Company is not subject to any specific AML/CFT legislation at this point in time that requires the Customer to actually have sight of original documents, and unless required by applicable laws, will accept scanned or electronic copies of documents for the purposes of its AML/CFT and KYC checks.

3.5.3 The Company will also keep copies of all documents used in verifying the customer's identity.

3.5.4 Where the customer is a Singapore Government entity, the Company shall only be required to obtain information to confirm that the customer is a Singapore Government entity as asserted.

Identification and verification of customers who are individuals

3.5.5 The Company will obtain and record at least the following information to identify a customer who is an individual:

(a) full name, including any alias;

(b) photo identification;

(c) residential address and telephone number and other contact information (eg: electronic mailing address);

(d) date of birth; and

(e) nationality/ dual nationalities (where applicable).

3.5.6 If the customer is a sole proprietor, the Company shall also obtain and record the above information in relation to the sole proprietor.

3.5.7 For purposes of verification, the Company shall ask to see photo identification documents of the customer. Examples of photo identification documents include identity cards, passports, driving licences or any document issued by a state government. Where feasible, the residential address is to be verified by means of a utility bill or bank statement addressed to the customer (whose name is reflected in the photo identification document) at that residential address. Screening on the customer will then by completed by checks using databases such as World-Check, World Compliance or Dow Jones Factiva, and other databases of the various government agencies, FIUs, central banks, other authorities in charge of supervision on financial markets.

Identification and verification of customers who are not individuals

3.5.8 The Company will ascertain the identity the customer, and verify the customer's identity, respectively, through the following information below. Screening of the customer will also be done using the databases referred to in paragraph 3.5.8:

(a) full name;

(b) incorporation number or registration number (in the case of a customer that is a body corporate or unincorporate);

(c) address of place of business or registered office address and telephone number;

(d) the date of incorporation or registration (as the case may be);

(e) the place of incorporation or registration (as the case may be);

(f) The documents that prove the existence of the customer;

(g) The documents that regulate and bind the customer, such as the constitution of a company if the customer is a company, or the trust deed of an express trust if the customer is an express trust; and

(h) The individuals in the senior management of the customer.

3.5.9 If the customer is a sole proprietorship, partnership, limited partnership, limited liability partnership, or a company incorporated in Singapore, **the Company will obtain and record a profile of the entity from ACRA database which is generally sufficient to establish the existence of the customer and that it is incorporated/registered in Singapore, the name and legal form of the customer, the identities of all the persons having executive authority in the customer, the address of the registered office and the address of the principal place of business**. The Company may also obtain from the customer the documents that regulate and bind the customer (such as the constitution of a company, if the customer is a company, or the trust deed of an express trust, if the customer is an express trust).

3.5.10 If the customer is a foreign entity, the Company will obtain and record the same particulars as required for a Singapore entity. If the Company is unable to obtain the foreign entity's incorporation or registration documents from a body which regulates the foreign entity in its foreign jurisdiction for purposes of verification of the foreign entity's identity, it shall have the foreign entity's identity verified independently by a person/body responsible in that foreign country for the regulation of companies or by another professional or by other reasonable means. The Company may also refer to the following link for a non-exhaustive list of foreign regulators of companies and refer to it to obtain relevant information about foreign companies: http://www.ecrforum.org/worldwide-registers/. If the Company is satisfied that there is little or no risk of money laundering or terrorist financing or such risk is low and it has no suspicions of the same, it may obtain information on the identity of the customer from (i) a structure chart (of the entity) provided by the customer directly or (ii) information available on the customer's website or (iii) information available from the customer's annual reports or (iv) information from any publicly known source that is reliable. A "foreign company" is defined as a company incorporated outside Singapore.

3.5.11 If the customer is a trust, the Company will ascertain the identity and particulars of each trustee (trustees must be identified in accordance with their categorisation, natural person or company or other legal entity) and the nature of the trust. In cases that the Company acts as a trustee of the express trust governed by Singapore law, it shall perform the following CDD measures: -

(a) obtain and maintain adequate, accurate and current information on the identities of the settlor, each trustee, the protector (if any) and each beneficiary or class of beneficiaries of the trust, and of any other individual exercising effective control over the trust;

(b) obtain and maintain basic information on every other regulated agent of, or service provider to, the trust, including any investment adviser or manager, accountant or tax adviser;

(c) maintain the above information for at least 5 years after the Company's involvement with the trust ceases;

(d) ensure that the information is kept accurate and as up-to-date as possible, and is updated on a timely basis;

(e) subject to any rule of law relating to a trustee's duty of confidentiality, the Company will, when forming a business relationship with any person referred to in the following sub-paragraphs in the Company's capacity as a trustee, disclose to that person the Company's status as such trustee:

a. a financial institution as defined in section 27A(6) of the Monetary Authority of Singapore Act (Cap. 186), read with section 27A(7) of that Act;

b. a casino operator as defined in section 2(1) of the Casino Control Act (Cap. 33A);

c. a licensed estate agent as defined in section 3(1) of the Estate Agents Act (Cap. 95A);

d. a dealer in precious stones or precious metals as defined in regulation 2 of the Corruption, Drug Trafficking and Other Serious Crimes (Cash Transaction Reports) Regulations 2014 (G.N. No. S 692/2014);

e. a legal practitioner,

f. a foreign lawyer registered under section 36P of the Legal Profession Act;

g. a notary public as defined in section 2 of the Notaries Public Act (Cap. 208); or

h. a public accountant as defined in section 2 of the Accountants Act (Cap. 2).

3.5.12 If the customer is an attorney, the Company will identify both the principal and the attorney. The Company will cease or refuse to act for a customer who gives a power of attorney in favour of any person without any apparent reason and refuses to explain why a power of attorney is given and/or is reluctant to provide the identity documents of the attorney.

3.5.13 If the customer is a Singapore charity, club or a society, the Company will check that the registration number for the charity or society or club is correct. For charities, the Company will check with the Commissioner for Charity and for societies, the Registrar of Societies, and shall obtain the names of all trustees and officers of the charity, club or society before permitting the customer to purchase any product.

3.5.14 If the customer is a foreign charity, club and society, the Company will obtain the same particulars as required for a Singapore charity, club and society. If the Company is unable to obtain the foreign charity's, club's or society's registration number from a body in a foreign country equivalent to the Commissioner for Charity or the Registrar of Societies, the Company may have the foreign charity's, club's or society's identity verified independently by a person/body responsible in that foreign country for the regulation of charities, clubs and societies or by another professional or by other reasonable means.

3.5.15 If the customer is a Singapore co-operative society, the Company will check the registration particulars of the co-operative or check the same with the Registrar of

Co-operative Societies, and obtain the names of the members of the committee of management and officers of the cooperative before permitting the customer to purchase any product.

3.5.16 If the customer is a management corporation ("**MCST**"), the Company will obtain the names of all officers of the Management Council of the MCST before accepting the retainer.

3.5.17 If the customer is an estate, the Company must have sight of the death certificate and if applicable, the original will or a certified true copy of the will of the deceased. The Company will obtain the relevant identity documents to establish the identities of the executors or administrators of the deceased estate and where applicable, the original or certified true copy of the letters of administration or probate.

Identification and verification of agents

3.5.18 Where the customer appoints one or more persons to act on his behalf as an agent in establishing a business relationship with the Company, or if the customer is not an individual, the Company will obtain and record the following information of the agent:

(a) full name, including any alias;

(b) identity card, birth certificate or passport number, in the case of an agent who is an individual;

(c) incorporation number or registration number, in the case of an agent that is a body corporate or unincorporate;

(d) residential address or address of place of business or registered office address and telephone number;

(e) date of birth, incorporation or registration (as the case may be); and

(f) nationality or place of incorporation or registration (as the case may be).

3.5.19 The Company will also verify the authority of the agent to act on behalf of the customer. This may be done by obtaining the following information, for example, (i) the appropriate documentary evidence that the customer has appointed the agent to act on his behalf; or (ii) a summary of the oral instructions given to the agent by the customer.

Obtaining information on the purpose and the intended nature of the business relationship

3.5.20 The Company only intends to apply this Manual to purchasers of its products, including digital tokens but if any customer intends to enter into a business relationship beyond that of a purchaser with the Company, the Company may require from such customer:

(a) details of the customer's business or employment;

(b) the nature and purpose of the relationship between the customer and its beneficial owners; and

(c) the anticipated level, frequency and nature of transactions that are to be performed by the Company for the customer throughout the business relationship.

3.6 Non-individual customers: Identification and verification of beneficial owners' identities

Requirements for identification and verification of beneficial owners

3.6.1 The Company will inquire if there is any beneficial owner in relation to a customer that is not an individual (natural person). Where it becomes aware pursuant to the inquiry or otherwise that there is one or more beneficial owner in relation to the customer, the Company will take reasonable measures, based on risk, to obtain sufficient information to identify and verify the identity of every beneficial owner. In addition, if the customer is a body corporate or unincorporate or a legal arrangement, the Company will take reasonable measures to understand the ownership and control structure of the body corporate or unincorporate, or the legal arrangement, as the case may be.

3.6.2 The Company will identify and take reasonable measures to verify the identity of each beneficial owner of the customer, through the following information:

(a) the identity of each individual (if any) who has a controlling ownership interest in the customer;

(b) if there is any doubt as to whether an individual who has a controlling ownership interest in the customer is a beneficial owner of the customer, or if there is no individual who has a controlling ownership interest in the customer, the identity of each individual (if any) who has control of the customer through other means; or

(c) if there is no individual who has a controlling ownership interest in the customer or who has control of the customer through other means, the identity of each individual in the senior management of the customer.

3.6.3 If there is no individual who has a controlling ownership interest in the customer or who has control of the customer through other means, the Company will ascertain and take reasonable measures to verify the identity of each individual in the senior management of the customer, such as a chief executive officer (CEO), chief financial officer (CFO), managing or executive director, or president. If the customer is an express trust, the Company will ascertain and take reasonable measures to verify the identity of the settlor, each trustee, the protector (if any) and each beneficiary or class of beneficiaries of the trust, and any other individual exercising effective control over the customer (including through a chain of control or ownership)

3.6.4 The requirement to verify the identity of beneficial owners of a customer is different from the requirement to verify the identity of individual customers. After the beneficial owners have been identified, it is not necessary for verification of their identity to be

done on the basis of documents, data or information obtained from reliable and independent sources. The Company may decide, based on risk, whether it is reasonable to obtain information provided by its customers about their beneficial owners, for example, an undertaking or a declaration from its customers, and take reasonable measures to verify the identity of the beneficial owner by, for example, researching publicly available information on the beneficial owner such as the business profile obtained from ACRA, or from a body in a foreign country equivalent to ACRA or arranging a face-to-face meeting with the beneficial owner, to corroborate the undertaking or declaration provided by the customer.

3.6.5 The Company may require the customer to provide a list of its beneficial owners, duly signed by one of the customer's directors (if a company), partner (if a partnership) or in any other case, a member of the customer's management team. The Company shall keep the documentation of the CDD performed in the identification of the beneficial owner(s) and ensure that it is available upon request by government authorities in Singapore.

Situations where inquiry into the existence of beneficial owners is not required

3.6.6 The Company need not inquire if there exists any beneficial owner in relation to a customer that is:

(a) a Singapore government entity, that is, a ministry or department of the Government of Singapore, an organ of state or a statutory board in Singapore;

(b) a foreign government entity;

(c) an entity listed on the Singapore Exchange;

(d) an entity listed on a stock exchange outside Singapore which is regulated by an authority of a country or territory other than Singapore regulating the provision of financial services;

(e) a Singapore financial institution, as defined in section 27A(6), read with section 27A(7), of the Monetary Authority of Singapore Act;

(f) a financial institution incorporated or established outside Singapore that is subject to and supervised for compliance with requirements for the prevention of money laundering and the financing of terrorism consistent with the standards set by the FATF;

(g) an investment vehicle, the managers of which are Singapore financial institutions or financial institutions incorporated or established outside Singapore, and subject to and supervised for compliance with requirements for the prevention of money laundering and the financing of terrorism consistent with standards set by the FATF;

(h) a public company that is commonly regarded as a multi-national company, with offices in more than 2 countries, and whose head office is regulated by a government authority in that jurisdiction.

unless the Company has doubts about the veracity of the information obtained in performing CDD measures or suspects that that the customer is carrying out or facilitating money laundering or the financing of terrorism or proliferation.

3.6.7 The Company shall keep a record in writing of the basis for its determination that a customer falls within (a) to (g) above.

Identifying the "beneficial owner"

3.6.8 For a customer that is a body corporate, the Company will identify the beneficial owners by:

(a) identifying the natural persons (whether acting alone or together) who ultimately own all the assets or undertakings of the body corporate or the individuals described in paragraph 3.6.10 below;

(b) to the extent that there is doubt under (a) as to whether the natural persons who ultimately own the body corporate are the beneficial owners or where no natural persons ultimately own the body corporate, identifying the natural persons (if any) who ultimately control the body corporate or have ultimate effective control over the body corporate; and

(c) where no natural persons are identified under (a) or (b), identifying the natural persons having executive authority in the body corporate, or in equivalent or similar positions.

3.6.9 For a customer that is a legal arrangement, that is, an express trust or similar arrangement, the Company will identify the beneficial owners:

(a) of the express trusts, by identifying the settlor, the trustee(s), the protector (if any), the beneficiaries or class of beneficiaries, and any other natural person exercising ultimate ownership, ultimate control or ultimate effective control over the trust (including through a chain of control/ownership or both) corporate or the individuals described in paragraph 3.6.11 below; and

(b) for other types of legal arrangements, identifying persons in equivalent or similar positions as those described under (a).

Identification and verification of beneficial owners of different customers

3.6.10 As for customers who are bodies corporate or legal arrangements the beneficial owner of these customers is:

(a) where the individuals who benefit from the body corporate or legal arrangement have been determined, any individual who benefits from at least 25% of the property of the body corporate or the legal arrangement;

(b) where the individuals who benefit from the body corporate or legal arrangement have yet to be determined, the class of persons in whose main interests the body corporate or legal arrangement is set up or operates; or

(c) an individual who controls at least 25% of the property of the body corporate or legal arrangement.

3.6.11 As for customers who are trusts, the beneficial owner:

(a) of a trust includes any individual who is entitled to a vested interest in at least 25% of the capital of the trust property. “Vested interest” is defined as an interest that a person is currently entitled to, without any pre-conditions needing to be fulfilled;

(b) of a trust includes any individual who has control over the trust. “Control” is defined as a power whether exercisable alone, jointly with another person or with the consent of another person under the trust instrument or by law: to dispose of, advance, lend, invest, pay or apply trust property; vary the trust; add or remove a person as a beneficiary to or from a class of beneficiaries; appoint or remove trustees; or direct, withhold consent to or veto the exercise of any of the above powers; or

(c) of a trust other than one which is set up or which operates entirely for the benefit of individuals falling within (a), includes the class of persons in whose main interest the trust is set up or operates, and the class must be described.

3.6.12 For customers who are estates of deceased persons, the beneficial owner of an estate is any executor, administrator or personal representative until the administration of the estate is complete.

3.7 On-going monitoring of a business relationship

Requirement of on-going monitoring

3.7.1 As the Company is not subject to any specific AML/CFT legislation, there is no requirement to conduct on-going monitoring of every customer who has purchased a product (including a digital token) from the Company. However, if the customer does have a business relationship with the Company that goes beyond the sale of a product, on-going monitoring may be required. If customers who have purchased digital tokens are using such tokens on platforms operated by the Company, the Company will only perform on-going monitoring on such customers if they are PEPs at the time of purchase or if they subsequently become PEPs or if it comes to the knowledge of the Company that such token purchasers are conducting suspicious transactions, or in circumstances in which enhanced customer due diligence measures are, in the opinion of the Company, required. “On-going monitoring” is defined as:

(a) a periodic screening of token purchasers who are using the tokens on the Company’s digital platforms, such screening to be performed once every year.
(b) scrutiny of transactions undertaken throughout the course of the relationship (including, where necessary, the source of funds) to ensure that the

transactions are consistent with the Company's knowledge of the customer, its business and risk profile;

(c) keeping the documents, data or information obtained in the course of performing CDD measures (including simplified and enhanced CDD measures) up-to-date;

(d) determining the appropriate frequency on when on-going monitoring must be conducted using a risk based approach;

(e) reviewing every business relationship based on risk assessment; and

(f) taking appropriate after-action review.

The extent of on-going monitoring

3.7.2 The Company will determine the extent to which on-going monitoring must be conducted using a risk-based approach. Therefore, when dealing with high-risk customers and PEP, for example, the extent of on-going monitoring must be enhanced.

3.7.3 On-going CDD does not require the Company to (i) suspend or terminate a business relationship until CDD data, documents and information have been updated so long as it is satisfied that it knows who its customer is; (ii) perform the whole CDD process again every few years; and (iii) conduct random checks of files.

3.7.4 If the Company has reasonable grounds, based on on-going CDD, or otherwise, for suspecting that the business relationship with the customer involves engagement in money laundering or the financing of terrorism, the Company will file a suspicious transaction report with either or both of the following (as the case may be):

(a) a Suspicious Transaction Reporting Officer, if the customer may be engaged in money laundering; and/or

(b) a police officer or Commercial Affairs Officer, if the customer may be engaged in financing of terrorism.

3.7.5 If the Company suspects that a customer may be engaged in money laundering or the financing of terrorism and it has reasonable grounds to believe that the performance of any CDD measures will tip-off the customer, the Company shall: -

(a) not need to perform those CDD measures; but

(b) instead file a suspicious transaction report with either or both of the following (as the case may be):

(i) a Suspicious Transaction Reporting Officer, if the customer may be engaged in money laundering; and/or

(ii) a police officer or Commercial Affairs Officer, if the customer may be engaged in financing of terrorism.

3.7.6 The Company shall conduct the relevant due diligence measures when:

(a) there is a material change in the nature of the business relationship with the customer;

(b) the Company becomes aware that it may lack adequate identification information on a customer; or

(c) the Company becomes aware that there may be changes in the ownership or constitution of the customer.

3.8 Simplified customer due diligence measures

3.8.1 The Company may perform simplified CDD measures to effectively identify and verify a customer, beneficial owner and agent if:

(a) it is of the view that the risks of money laundering and the financing of terrorism financing are low, for example, if the customer or its beneficial owner falls into the categories listed in paragraph 3.5.4 and paragraph 3.6.6;

(b) the assessment of low risk is supported by an adequate analysis of risks by the Company, taking into account any information that may be identified using objectively reliable and independent source documents, data or information.

(c) the simplified CDD measures are commensurate with the levels of risk identified, based on the risk factors identified by the Company.

3.8.2 Where the Company performs simplified CDD measures, it may document the details of its risk assessment including when it was done, and the nature of the simplified CDD measures.

3.8.3 Examples of simplified CDD measures that the Company may perform are:

(a) verifying the identity of the customer, beneficial owner and agent after the establishment of the business relationship;

(b) taking fewer measures to identify and verify the identity of a beneficial owner;

(c) reducing the frequency of on-going monitoring (if applicable); and

(d) not obtaining specific information to understand the purpose and intended nature of the business relationship but inferring it from the available facts and circumstances.

3.9 Enhanced customer due diligence measures

<u>Situations in which enhanced customer due diligence measures have to be performed</u>

3.9.1 The Company will perform enhanced CDD measures and enhanced on-going monitoring in the following situations:

(a) where the risks of money laundering and the financing of terrorism are raised.

(b) in respect of all complex or unusually large transactions or unusual patterns of transactions that have no apparent or visible economic or lawful purpose;

(c) when it proposes to have a business relationship, or has established a business relationship, with any person from or in countries or territories outside Singapore known to have inadequate measures for the prevention of money laundering or the financing of terrorism (as determined by it, or as notified to it by the CE);

(d) for other categories of customers or other transactions which it considers may present a high risk of money laundering or the financing of terrorism;

(e) if the customer is from or in, or the transaction relates to, any country or jurisdiction in relation to which the FATF has called for countermeasures including enhanced CDD measures to be performed, as may be notified by the CE;

(f) If the customer is from or in any country or jurisdiction known to have inadequate measures to prevent money laundering and the financing of terrorism, as determined by the Company or as notified by the CE;

(g) If the Company suspects that the customer is engaged in, or the transaction involves, money laundering or the financing of terrorism.

(h) for dealing with customers who are not physically present for identification purposes; and

(i) where it proposes to have a business relationship with a PEP.

3.9.2 In determining whether a customer is from a country or territory in paragraph 3.9.1(c) paragraph 3.9.1(e), paragraph3.9.1(f) or in determining whether a customer is high risk under paragraph 3.9.1(a), the Company may consider the following FATF's website link of high risk and non-cooperative countries:

http://www.fatf-gafi.org/topics/high-riskandnon-cooperativejurisdictions/ or
http://www.fatf-gafi.org/countries/#high-risk

3.9.3 the Company shall also screen a customer against the lists of individual and entities known or suspected to be related to terrorists or terrorist organisations:

(a) the lists of individual and entities known or suspected to be related to terrorists or terrorist organisations (UNSCRs 1267/ 1989 Al-Qaida list);

(b) UNSCRs 1988 Taliban list, and all other persons identified in the First Schedule of the TSOFA;

(c) who are known or suspected to be involved in the proliferation of weapons of mass destruction and its financing to Iran (UN 1737 list) and the Democratic People's Republic of Korea (UN 1718 list); or

(d) any other listing promulgated by MAS or ACRA.

3.9.4 the Company may refer to the following link to MAS' website on targeted financial sanctions and subscribe to MAS' website to receive alerts to changes to the lists:

http://www.mas.gov.sg/Regulations-and-Financial-Stability/Anti-Money-Laundering-Countering-The-Financing-Of-Terrorism-And-Targeted-Financial-Sanctions/Targeted-Financial-Sanctions/Lists-of-Designated-Individuals-and-Entities.aspx

3.9.5 In addition, the Company may obtain more information about terrorist designation and the legislation for countering of terrorism, and sign up to the Inter-Ministry Committee on Terrorist Designation website at:

http://www.mha.gov.sg/Pages/Inter-Ministerial-Committee---Terrorist-Designation-%28IMC-TD%29-.aspx

3.9.6 The Company may also refer to the following links in determining whether the customer is from or in any country or jurisdiction known to have inadequate measures to prevent money laundering and the financing of terrorism:

(a) The list established and maintained by the Committee pursuant to resolutions 1267 (1999) and 1989 (2011) with respect to individuals, groups, undertakings and other entities associated with Al-Qaida:

http://www.un.org/sc/committees/1267/aq_sanctions_list.shtml

(b) The list established and maintained by the Committee established pursuant to resolution 1988 (2011) with respect to individuals, entities, groups, or undertakings:

http://www.un.org/sc/committees/1988/list.shtml

Enhanced customer due diligence measures

3.9.7 the Company will perform the following enhanced measures in situations as described under 3.9.1:

(a) obtain the approval of the senior management which is the director of the Company who supervises the file or another director/managing director of the Company who is not involved with the particular file, before:

(i) in the case of a new customer, establishing a business relationship with the customer; or

(ii) in the case of an existing customer, continuing a business relationship with the customer;

(b) take reasonable measures to establish the source of wealth, and the source of funds of the customer, and if the customer is an entity or a legal arrangement, of the beneficial owner of the customer; and

(c) conduct enhanced ongoing monitoring of the business relationship with the customer.

If enhanced CDD measures have to be performed by the foreign branch or foreign subsidiary of the Company and senior management approval is required, the Company shall determine whether the approval should be given by the senior management of that foreign branch or subsidiary.

Dealing with non-face-to-face customers

3.9.8 Where a customer has not been physically present for identification purposes, the Company will take specific and adequate measures to compensate for the higher risk, including performing one or more of the following:

(a) ensuring that the customer's identity is established by additional documents, data or information;

(b) implementing supplementary measures to verify or certify the documents supplied; or

(c) ensuring that the first payment to the Company for the services rendered is carried out through an account opened in the customer's name with a Singapore financial institution.

3.9.9 Examples of the measures to mitigate the increased risk (due to not being able to have face-to-face contact when establishing a business relationship) that the Company may perform are:

(a) have telephone contact with the customer at a residential or business number that can be verified independently;

(b) confirmation of the customer's salary details by requiring the presentation of recent bank statements; or

(c) certification of the customer's identification documents by requiring statutory declaration, or documents certified by notaries public.

3.10 Dealing with Politically Exposed Persons ("PEPs") or a family member or close associate of any such individual

3.10.1 A PEP is an individual who is or has been entrusted with a prominent public function. Due to their position and influence, many PEPs are in positions that can be potentially abused for the purpose of committing money laundering and related predicate offences, including corruption and bribery, as well as conducting activity relating to terrorism financing.

3.10.2 When considering whether to establish or continue a business relationship with a PEP, the Company will focus on the level of money laundering and terrorism financing risk associated with the particular PEP through appropriate CDD measures. The Company will also have sufficient controls in place to mitigate this risk.

Determining whether an individual is a PEP

3.10.3 The Company will establish and maintain risk-sensitive internal policies, procedures and controls to determine whether a customer, connected party, agent, beneficial owner is a PEP, an immediate family member of a PEP or a close associate of a PEP when conducting CDD on their customers.

3.10.4 To determine if a customer/agent/connected party/beneficial owner is a PEP, the Company will ensure that the CDD information is up to date so that they can monitor the business relationship for a change in PEP status. To do that, the Company may use the internet and media as sources for determining, monitoring, verification of information in relation to PEP. The Company may also subscribe to commercial databases to help it in identifying a PEP. Alternatively, self-declaration by a customer of their PEP status can also be accepted. However, the Company will not solely rely on such self-declarations (which may be false) and will engage the customers and obtain information pertinent to the different elements of the PEP definition. The Company may refer to the FATF guidance paper on PEPs: http://www.fatf-gafi.org/documents/documents/peps-r12-r22.html

Performance of enhanced CDD measures and enhanced on-going monitoring when dealing with PEPs

3.10.5 After determining whether an individual is a PEP, an immediate family member or close associate of a PEP, the Company will adopt a risk-sensitive approach in determining whether to perform enhanced CDD measures and the extent of such measures to be performed for any or all of the following:

(a) a domestic PEP, or his immediate family member or close associate;

(b) a PEP of an international organisation, or his immediate family member or close associate; or

(c) a PEP who has stepped down from his prominent public function, taking into consideration the level of influence that the person may continue to exercise after stepping down from such prominent public function, or his immediate family member or close associate.

3.10.6 If the Company is satisfied that the individuals in paragraph 3.10.2 do not present a high risk, the Company may decide not to perform enhanced CDD measures and enhanced on-going monitoring for these individuals. If the Company has reason to suspect that a customer is a politically-exposed individual or a family member or close associate of any such individual, the Company will conduct some form of electronic verification, such as an Internet based search engine (including social media) or alternatively an electronic search conducted through a reputable international electronic identify verification provider. However, if it is satisfied that

these persons present a high risk, then the Company may perform enhanced CDD measures and enhanced on-going monitoring for these individuals.

3.10.7 In addition, if the customer is a foreign PEP or family member or close associate of any such individual, the Company will perform enhanced customer measures and enhanced on-going monitoring for these individuals.

3.10.8 The requirements for enhanced CDD measures and enhanced on-going monitoring include but are not limited to the following:

(a) inquiring into the background and purpose of any transaction that the Company is engaged to carry out;

(b) identifying and if appropriate, obtain information on the purpose and intended nature of the business relationship with the customer;

(c) identifying and if appropriate, obtain information concerning the retaining, and transaction and/or advice that the Company is proposing to act for the customer on;

(d) obtaining approval from its senior management for establishing the proposed business relationship. The objective is that senior management is aware of the proposed business relationships with PEPs and that the Company does not undertake business relationships with them without proper controls.

(e) take reasonable measures to establish the source of wealth and source of funds which are involved in the proposed business relationship. The source of wealth refers to the origin of the PEP's entire body of wealth/total assets, and how the PEP came to acquire such wealth. The source of funds refers to the origin of the particular funds which are the subject of the business relationship between the PEP and the Company. The information required for the source of funds should not be limited to knowing which financial institution the funds are from, but should also establish a provenance or reason for it having been acquired. The Company may rely on publicly disclosed assets or rely on self-declarations of the PEP. However, when relying on self-declarations, any inability to verify the information should be taken into account in establishing the actual value of the wealth or funds. The Company may also rely on information sources such as publicly available property registers, land registers, asset disclosure registers, company registers, past transactions and other sources of information about legal and beneficial ownership where available. Internet and social media searches may also be relied on to reveal useful information about a customer's source of wealth or funds. Possible sources of wealth or funds include a PEP's current income, sources of wealth or funds obtained from his current and previous positions, business undertakings and family estates;

(f) conduct enhanced on-going monitoring on the business relationship entered into, which means on-going monitoring that is enhanced in terms of frequency over the course of the business relationship in question; and

(g) keep a record in writing of its findings.

Dealing with other high-risk situations

3.10.9 The Company may in assessing the risks involved in these situations, take into account examples such as the type of customer, the type of service or transaction that the customer expects the Company to perform, and the geographic area of operation of the customer's business. The Company may give particular attention to business relationships and transactions with persons from or in countries that have inadequate anti-money laundering or financing of terrorism measures.

3.9.10 If the Company is satisfied that there is high risk, it shall perform enhanced CDD measures and enhanced on-going of its customers.

3.11 Audit Function (optional)

The Company may but is not required to have these IPPC reviewed by its internal or external auditors.

3.12 Compliance Management

Requirements of compliance management

3.12.1 The Company will:

(a) have internal communications procedures to communicate its internal policies, procedures and controls described at paragraph 3.2;

(b) develop compliance management arrangements;

(c) appoint an employee or officer in a management position as one of its compliance officers in relation to anti-money laundering and countering the financing of terrorism and proliferation measures; and

(d) ensure that the compliance officer, as well as any other persons appointed to assist him, is suitably trained, qualified, and has adequate resources and timely access to all customer records and other relevant information which he requires to discharge his functions.

3.13 Training of employees

Training of employees

3.13.1 The Company will:

(a) ensure that its partners, directors and employees are familiar with the laws for the prevention of money laundering and financing of terrorism; and

(b) ensure that its employees are trained on its internal policies, procedures and controls for the prevention of money laundering and financing of terrorism,

including the roles and responsibilities of employees and legal practitioners in relation thereto.

3.13.2 The Company may consider screening individuals whom it may wish to hire as its employees to ascertain if:

(a) whether the individual has been convicted in Singapore of any offence involving fraud or dishonesty punishable with imprisonment for 3 months or more; and

(b) whether the individual is an undischarged bankrupt in Singapore;

Scope of training

3.13.3 The Company will ensure that its employees are trained and aware of the laws for the prevention of money laundering and financing of terrorism and proliferation, including the ACRA Act and 2015 Regulations, the CDSA and the TSOFA, and other legislation concerning the prevention of money laundering or financing of terrorism and proliferation.

3.13.4 Training of employees may also cover the following areas:

(a) recognition of and dealing with suspicious activities and transactions;

(b) the impact that money laundering and financing of terrorism may have on the Company, its business, customers and employees;

(c) the money laundering and financing of terrorism and proliferation risks that the Company faces, given the nature of its business and services;

(d) the changing behaviour and practices of money launderers and those financing terrorism and proliferation;

(e) the internal policies, procedures and controls that have been put in place by the Company to identify, reduce and manage money laundering and financing of terrorism and proliferation risks;

(f) different CDD measures, and, on-going monitoring measures; and

(g) effective ways of determining whether customers are PEPs and to understand, assess and handle the potential risks associated with PEPs. Training may use real-life case studies and examples and input and analysis from experienced and trained employees.

Frequency of training

3.13.5 The frequency of training should be sufficient to maintain the knowledge and competence of employees to apply CDD measures appropriately. For avoidance of doubt, employees will at least be trained on an annual basis.

3.14 Record-Keeping

The records that are required to be kept

3.14.1 The Company will keep the records of all CDD information (including screening results and risk assessment), and the supporting records in respect of a business relationship which is the subject to any CDD measures or on-going monitoring. These records should be sufficient to permit a reconstruction of individual transactions. In addition to the documents provided by customers, in the case of cryptocurrencies transferred to the Company, the Company should also keep screenshots of the transactions as reflected on the relevant blockchain or public ledger.

3.14.2 Examples of records to be kept are:

(a) A copy of the information and evidence of the customer's and agent's identity (including that of any beneficial owner in relation to the customer. These include but not limited to:
   (i) copies of all documents used in establishing and verifying the customer's, beneficial owner's and agent's identity;
   (ii) the agent's authority to enter into a business relationship on behalf of a customer;
   (iii) information on the purpose and intended nature of the business relationship;
   (iv) written records of the basis of the Company's determination that a customer falls into the categories for which inquiry into the existence of beneficial owner is not required;
   (v) documents of the Company's basis for being satisfied that a third party it is relying on to perform CDD has met the relevant requirements;
   (vi) the Company's risk assessment where it performs simplified CDD measures and the nature of the simplified CDD measures;
   (vii) written records of the Company's findings with regard to a PEP;
   (viii) written records of the Company's findings with regard to other high risk customers or transactions; and

(b) other relevant supporting records.

Duration of time for the keeping of records

3.14.3 The above records above will be kept by the Company throughout the duration of a business relationship and for an additional period of at least 5 years beginning on the date on which a business relationship ends.

Format for the keeping of records

3.14.4 The Company has the discretion to keep the records by:
(a) by way of original documents;
(b) by way of good photocopies of original documents;
(c) on microfiche; and
(d) in computerised or electronic form including a scanned form.

Sufficiency of document and records

3.14.5 The Company will take reasonable steps to ensure that the documents and records kept in relation to a relevant matter are sufficient to substantially permit a reconstruction of the relevant matter and if required, to provide evidence for the prosecution of an offence relating to the relevant matter

Documents and records to be made available

3.14.6 The Company will keep the above information to be readily available for examination upon request by government authorities in Singapore.

3.15 Filing a suspicious transaction report ("STR")

Reporting of suspicious transactions

3.15.1 The Company will have procedures in place to report suspicious transactions. STRs should be first reported to a designated person in the Company so that the Company can streamline the STRs to be reported and avoid any frivolous or unwarranted STRs that waste the time and resources of the authorities. The minimum areas to be covered in the procedures shall include:

(a) Persons within the Company to whom an employee has to report an STR (compliance officer or a member of the senior management of the Company);
(b) Avenues to report suspicious transactions (for example, whether email or in hard copy);
(c) Information required to be in a STR; and
(d) Timeliness of the STR

3.15.2 The Company will name a person in senior management or a director to whom an STR is to be escalated if there is no response to the employee's STR at first instance.

Requirement to consider whether a suspicious transaction report must be filed

3.15.3 Where the Company is unable to apply CDD measures in relation to a customer, it shall consider whether it is required to make a disclosure under section 39(1) of the CDSA and section 8 or 10 of the TSOFA.

3.15.4 If any of the Company's officers or employees knows or has reasonable grounds to suspect that any property of a customer may be connected to money laundering or financing of terrorism or proliferation, he must promptly alert the compliance officer or a member of the senior management of the Company. The compliance officer or senior management of the Company should consider making a suspicious transaction report to the Suspicious Transaction Reporting Office of the Commercial Affairs Department (CAD). The STR should be lodged without delay and should not exceed 15 business days of the case being detected, unless the circumstances are exceptional or extraordinary.

3.15.5 A suspicious transaction report may be made in writing addressed to Head, Suspicious Transaction Reporting Office, CAD, or via email to STRO@spf.gov.sg, or via the STR On-Line Lodging System. More details are available on CAD's website:

http://www.police.gov.sg/about-us/organisational-structure/specialist-staff-departments/commercial-affairs-department/aml-cft/suspicious-transaction-reporting-office/suspicious-transaction-reporting#content

3.15.6 A report should be filed with Suspicious Transaction Reporting Office, CAD as soon as practicable. If a decision is made not to file a suspicious transaction report by the compliance officer or senior management of the Company, the reasons for the non-filing should be documented and made available to CAD when required.

3.15.7 Where the Company forms knowledge or suspicion of money laundering or terrorism financing or proliferation, and reasonably believes that performing any of the measures as required by this paragraph 3.15 will tip-off a customer, a natural person appointed to act on behalf of the customer, a connected party of the customer or a beneficial owner of the customer, the Company may stop performing those measures. The Company will document the basis for its assessment and file an STR without delay.

Not to prejudice investigation

3.15.8 If the Company knows or has reasonable grounds to suspect that a suspicious transaction report has been made; it will not, under section 48 of the CDSA and section 10B of the TSOFA, disclose to any other person information or any other matter which is likely to prejudice any investigation which might be conducted following the disclosure.

Indicators to file a suspicious transaction report

3.15.9 The Company will refer to Annex A for indicators that the Company shall take note of in deciding whether to file a STR report.

Appointment of an AML/CTF compliance officer

3.15.10 The Company has appointed an officer at the management level to hold the position of the AML/CTF compliance officer. The AML/CTF compliance officer will ensure the Company's compliance with its IPPCs and is responsible for keeping informed of and responding to any feedback regarding the AML/CTF compliance and notify the business owner, board of directors and relevant employees of the Company.

Procedures for responding to feedback from authority

3.15.11 The Company is currently **NOT** subject to any specific legislation relating to any specific AML/CFT legislation. However in the event that the Company receives any feedback from the authority in relation to its AML/CTF IPPCs, the AML/CTF compliance officer will be the point of liaison between the Company and the authority and address any queries requested from the Company.

ANNEX A

INDICATORS OF SUSPICIOUS TRANSACTIONS

The following list is not exhaustive and is used as a general guide only. The Company will file a suspicious transaction report if there are indicators that a transaction is suspicious. There may, however, be valid or legitimate explanations for the transactions. In such a case, a suspicious transaction report need not be filed but the Company will document the reasons why a report was not filed. As a supplier of products or services, the Company is not in the same position as banks or service providers regulated by specific AML/CFT legislation to have access to the fund movements in a customer's bank account(s) or their financial statements, and will therefore be unable to detect any movements in such bank account(s).

Indicators relating to incorporation of shell companies
▪ Companies with no apparent business and low paid up capital.
▪ Addresses of the Company or PO Box addresses are used by companies as their registered/mailing addresses.
▪ Companies incorporated by foreign directors with no links or activities in Singapore
▪ Multi-jurisdictional or complex structures of corporate entities are established

Indicators relating to other crimes
▪ Customers give suspicious information for CDD purposes.
▪ Customers unwilling/unable to provide information for CDD purposes.
▪ Customers use suspicious looking identity documents for CDD purposes.
▪ Customers uncontactable for CDD purposes.
▪ Customers featured in adverse news.
▪ Transactions involving politically exposed persons.

INDICATORS OF TERRORISM FINANCING

Adverse News Related to Terrorism Financing
▪ Clients featured in adverse news or sanction lists related to terrorism and/or terrorism financing.
▪ Counterparties of client featured in adverse news or sanction lists related to terrorism and/or terrorism financing.
▪ Clients who are designated entities in the following sanctions lists: a) United Nations (Sanctions – Iran) Regulations 2014, UN 1737 b) United Nations (Sanctions – DPRK) Regulations 2010, UN 1718
▪ Counterparties of client who are designated entities in the following sanction lists: a) United Nations (Sanctions – Iran) Regulations 2014, UN 1737 b) United Nations (Sanctions – DPRK) Regulations 2010, UN 1718

ANNEX B

CUSTOMER ACCEPTANCE CHECKLIST

Conducting CDD is important for the Company as a thorough understanding of the Company's customers and their behaviour using appropriate due diligence measures will allow the Company to discover unusual or possibly suspicious activities undertaken by their customers.

This checklist is to assist the Company in conducting CDD on its customers before determining if they should establish a business relationship with its customers. The information collected should be verified against an independent or reliable source. As noted in paragraph 3.5.7, the Company may, instead of using the checklists in this Annex B, rely on the procedures used by its external service provider.

PART 1 – INFORMATION ABOUT CUSTOMERS, AGENTS, BENEFICIAL OWNERS AND POLITICALLY EXPOSED PERSONS

Section A1 – Information of Customer/ Agent

(The section below will be duplicated if there is more than one customer, agent, or connected parties.)

Individual Customer's / Agent's Information	
Capacity in which the individual is acting	□ Self □ Agent □ Connected Party
Full Name (including any aliases)*	
Residential Address*	
Unique Identification Number/ Passport/FIN Number*	Expiry date of Identification Document (if applicable)
Date of Birth*	
Gender	□ M □ F
Nationality/Nationalities (where applicable)*	
Contact Number(s) with Country Code*	+
Email Address(es)	
Intended nature and purpose of business relationship	*(To be completed only if the business relationship goes beyond the purchase of the Company's product)*

Section A2 – Information on Business Entity

(The section below will be duplicated to provide more information on the entity that the customer/agent is representing or entity to be registered.)

Entity's information
Name of entity or Name of proposed entity*
Unique Entity Number (UEN) issued by the Registrar*
Address or intended address of the registered office*

Address of principal place of business (if different from above)	
Place or Proposed Place of registration*	
Date or Proposed Date of registration*	
Contact Number(s) with Country Code*	+
Email Address(es)	
Intended nature and purpose of business relationship	*(To be completed only if the business relationship goes beyond the purchase of the Company's product)*
Name(s) of all connected parties (directors/partners)*	*(Please use section A1 to obtain information for each connected parties identified)*

Section B – Information on Customer's Beneficial Owner(s)

The purpose of obtaining beneficial owners' information is to:

a) identify the natural persons (whether acting alone or together) who ultimately own all the assets or undertakings of the customer;

b) if there is doubt as to whether the natural persons who ultimately own all the assets or undertakings of the customer are the beneficial owners or where no natural persons ultimately own all the assets or undertakings of the customer, to then identify the natural persons (if any) who ultimately control the customer or have ultimate effective or significant control over the customer; and

c) where no natural persons are identified above, to identify the natural persons having executive authority in the customer, or in equivalent or similar positions.

*(*The section below will be duplicated if there is more than one Beneficial Owner.)*

Beneficial Owner Details	
Full name of beneficial owner (including any aliases)	
Residential Address	
Nationality	
Unique Identification Number/Passport or FIN Number	Expiry date of Identification Document (if applicable)
Date of birth	
Contact Number(s) with Country Code	+
Email Address(es)	
Provide information of nature of beneficial ownership or person having executive authority (e.g. more than 25% of ownership of the customer)	
Information on ownership and control structure of, or over the customer	*For customers that are legal persons, the Company shall understand and provide the control structure when identifying who is the beneficial owner.*

Section C1 – Information relating to Politically Exposed Person(s).

Politically Exposed Persons		
Is the customer, agent, beneficial owner or any party connected to the customer, a Politically Exposed Person (PEP)? A PEP includes the following: (a) a person who is or has been entrusted with any prominent public function in Singapore, a country or territory outside Singapore, or by an international organisation at present; (b) a person who has been entrusted with any prominent public function in Singapore, a country or territory outside Singapore, or by an international organisation who has stepped down from his prominent public function; or (c) an immediate family member or a close associate of a politically exposed person or a politically exposed person who has stepped down.	Yes (Please complete Section C2 for each Identified PEP)	No

Section C2 – Information about Politically Exposed Persons, their Immediate Family Members and Close Associates
*(*The section below will be duplicated if there is more than one PEP.)*

Information on Political Exposed Person (PEP)	
Name of PEP	
Country which PEP holds prominent public function	
Describe nature of prominent public function that the person is or has been entrusted with (for e.g. as a domestic politically exposed person, a foreign politically exposed person, or a politically exposed person of an international organisation)	
Period of time in which the person is/ was a politically exposed person	
Nature of PEP relationship with the customer (for e.g. self, family member, close associate, Ultimate Beneficial Owner etc)	
Information on the person's source of wealth	
Information on the person's source of funds in the proposed business relationship	

RISK ASSESSMENT FORM

The Company may assess the risk of the customer using this form. The following checklists are examples of factors that the Company will consider when performing a risk assessment. The checklists are not exhaustive and shall be enhanced on a case by case basis.

Customer's Risk Factors

Question	Yes	No
1) Is this an existing customer?	☐	☐
2) Is the customer a public company listed on a stock exchange and subject to disclosure requirements?	☐	☐

If "No" has been selected for the 2 questions above, the Company shall adopt a risk-sensitive approach and consider whether to perform enhanced CDD measures before establishing a business relationship with the customer.

Question	Yes	No
1) Is the customer a legal person or an entity that that can hold assets in its own name?	☐	☐
2) Does the customer use nominee director(s) or shareholder(s)?	☐	☐
3) Does the ownership structure of the customer appear unusual or excessively complex given the nature of its business?	☐	☐
6) Does the proposed directors/partners/shareholders have prior criminal convictions involving fraud or dishonesty?	☐	☐
7) Is any of the customer, beneficial owner or its agent a politically exposed person?	☐	☐
8) Are the customer's company accounts updated?	☐	☐
9) Does the customer's shareholders and/or directors frequently change, and the changes are unaccounted for?	☐	☐
10) Is there any problem obtaining evidence of identification from the customer for both the customer and beneficiary owner(s); and/or is the documentation found to be unsatisfactory?	☐	☐
11) Is the customer a charitable or non-profit organisation that is not registered in Singapore (charities.gov.sg/charity/index.do)?	☐	☐

If "Yes" has been selected for a majority of the 11 questions above, the Company shall adopt a risk-sensitive approach and consider whether to perform enhanced CDD measures before establishing a business relationship with the customer.

The Company may also ask the following questions of the customer:

1) Which country is the customer's business mostly based in?
2) What is the type of business activity for the customer's business?

B2 Country/Territory Risk Factors

Consider the following factors (if applicable): Customer's nationality, Place of formation/incorporation, Residential address, Permanent address, Place of operation, Place where business is established; etc.

Question	Yes	No
1) Is the customer connected to or transacting with a country or a territory that is identified as not having adequate anti-money laundering or counter financing terrorism measures?	☐	☐
2) Is the customer connected to or transacting with a country or a territory that is identified to having significant levels of corruption or other criminal activity?	☐	☐
3) Is the customer connected to or transacting with a country or a territory that is sanctioned by a regulatory body, such as the United Nations (UN)?	☐	☐
4) Is the customer connected to or transacting with a country or a territory that is identified to be funding or supporting terrorist activities or that have designated terrorist organisations operating within their territories?	☐	☐

If "Yes" has been selected for the questions above, the Company shall adopt a risk-sensitive approach and consider whether to perform enhanced CDD measures before establishing a business relationship with the customer.

B3 Services/ Transactions Risk Factors

Question	Yes	No	NA
1) Has the customer given any instruction to perform a transaction (which may include cash) anonymously?	☐	☐	☐
2) Has the customer transferred any funds without the provision of underlying services or transactions?	☐	☐	☐
3) Are there unusual patterns of transactions that have no apparent economic purpose or cash payments that are large in amount, in which disbursement would have been normally made by other modes of payment (such as cheque, bank drafts etc.)?	☐	☐	☐
4) Are there unaccounted payments received from unknown or un-associated third parties for services and/or transactions provided by the customer?	☐	☐	☐
5) Is there instruction from the customer to incorporate shell companies with nominee shareholder(s) and/or director(s)?	☐	☐	☐

6) Does the customer purchase companies or business entities that have no obvious commercial purpose?	☐	☐	☐
7) Are there business relationships that were established, or transactions performed without any physical meeting?	☐	☐	☐
8) Is there any divergence in the type, volume or frequency of services and/or transactions expected in the course of the business relationship with the customer?	☐	☐	☐

If “Yes” has been selected for a majority of the 8 questions above, the Company adopt a risk-sensitive approach and consider whether to perform enhanced CDD measures before establishing a business relationship with the customer.

The Company notes that separation of duties is a good practice with regard to having separate persons conducting risk assessments of customers and approving the acceptance of the customers.

Customer Risk Rating
Low ☐ Medium ☐ High ☐
Remarks:
Recommendation For Acceptance of Customer
Recommended ☐ Not Recommended ☐
Name of Recommending Officer:
Date:
Signature:

Approval for Acceptance of Customer
Approved ☐ Not Approved ☐
Name of Approving Officer:
Date:
Signature: