Anti-Money Laundering & Counter-Financing of Terrorism Policy

Shuttle One Pte Ltd

July 2020

Version 2.0

Document information

Subject	Anti-Money Laundering & Counter-Financing of Terrorism Policy
Purpose	This document outline the general standards of anti-money laundering and counter-financing of terrorism (AML/CFT) measures, to comply with country specific laws and regulations to combat AML/CFT.
Country	Singapore
Applicability	All employees and staff
Responsibility	Lim Hongzhuang
Approval	
Review	Every 12 months or earlier as required
Classification	Internal

Version Control

Effective Date	Version	Author	Approver	Job Title	Description
November 2019	1.0	Lim Hong Zhuang	-	-	First Version
May 2020	2.0	Lim Hong Zhuang			Second Version

Table of Contents

1 Introduction

Shuttle One Pte. Ltd. (the "Company") is a private limited company incorporated on 19 February 2019 with Company Registration No. 201905436Z and having its registered office at 80 Playfair Road #02-11 Singapore 367998.

ShuttleOne operates a platform that leverages blockchain technology to facilitate the provision of remittance services to small and medium sized enterprises ("SMEs" or "users"), by connecting them with money service providers ("MSOs") to provide real-time settlement of cross-border money transfer services. ShuttleOne facilitates the provision of micro-loans on the MakerDao loan issuance platform via the stablecoin DAI. ShuttleOne also currently supports Global eTrade Services1 ("GeTS"), a subsidiary of Crimsonlogic Pte Ltd, with Artificial Intelligence -powered credit scoring technology services to assist GeTS with credit assessments.

ShuttleOne's does not service retail users. Currently, ShuttleOne only services SMEs in Indonesia, Thailand, and Malaysia and China but the service may be extended to Singapore users in future in 2021.

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. Money laundering is generally defined as engaging in acts designed to conceal or disguise the true origins of criminally derived proceeds so that the proceeds appear to have derived from legitimate origins or constitute legitimate assets. Generally, money laundering occurs in three stages. Cash first enters the financial system at the "placement" stage, where the cash generated from criminal activities is converted into monetary instruments, such as money orders or traveler's checks, or deposited into accounts at financial institutions. At the "layering" stage, the funds are transferred or moved into other accounts or other financial institutions to further separate the money from its criminal origin. At the "integration" stage, the funds are reintroduced into the economy and used to purchase legitimate assets or to fund other criminal activities or legitimate businesses.

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. In addition to charitable donations, legitimate sources include foreign government sponsors, business ownership and personal employment. Although the motivation differs between traditional money launderers and terrorist

[1] GeTS is a subsidiary of CrimsonLogic. Its mission is to power global trade connectivity by making trade more accessible, predictable, and easier to fulfil. The company has linkages to 61 Customs nodes across the world, with more than 175,000 connected parties and conducting 24.1 million transactions annually.

GeTS has a suite of logistics, compliance, and financial products under its wing. Products and services include CALISTA, TradeWeb, OTB, and many more. CALISTA™ is a global supply chain platform that brings together the key regulatory and financial activities of logistics in a digital ecosystem. For certain trade routes, GeTS has visibility and control of the entire supply chain. GeTS achieves this with its service coverage and strategic port partnerships.

financiers, the actual methods used to fund terrorist operations can be the same as or similar to methods used by other criminals to launder funds. Funding for terrorist attacks does not always require large sums of money and the associated transactions may not be complex.

The Company is aware that criminals and terrorists may attempt to use its services to channel funds from illegal activities and conduct illicit activities. The policies set forth herein (the "Policies") are intended to be a guidance for all employees of the Company to comply with its obligations to operate in Singapore, by taking all reasonable steps and exercising all due diligence to avoid the commission of an offence of money laundering or financing of terrorism.

The Policies outline the general standards of anti-money laundering and counter-financing of terrorism (AML/CFT) measures, which should be adhered by all employees, to prevent the use of its systems and/or services for money laundering or financing of terrorism and to mitigate any legal, regulatory, reputational and financial risks in general. The Company shall also use its best endeavours to ensure that its employees are not involved in money laundering and the financing of terrorism.

The Company is determined and committed to prevent any activities, during the normal course of business, that may be related to money laundering or the financing of terrorism, by establishing sufficient and appropriate policies on internal controls, risk assessment, risk management and compliance.

2 Scope of the Policy

The scope of these Policies is to prevent the carrying out of activities that may be related to money laundering or the financing of terrorism, by establishing policies and procedures on internal control, risk assessment, risk management and compliance.

Users of these Policies should also refer and read in conjunction, the laws, regulations, notices, and guidelines which may be issued from time to time by the Government of Singapore, the Monetary Authority of Singapore ("MAS"), the Financial Action Task Force ("FATF") and/or any relevant authority or supranational agency, to combat money laundering and terrorism financing.

Unless the context otherwise requires, the words and expressions used in these Policies shall have the same meaning as set out in the relevant Acts and Regulations.

These Policies shall be updated regularly in accordance to prevailing laws, regulations and licensing conditions imposed by the Monetary Authority of Singapore, and any revisions or changes, that will be applicable to the Company's operating business model.

The relevant Singapore laws, regulations, and standards regarding anti-money laundering and as applicable to remittance licensees and stored value facility holders below have been considered in the preparation of this policy:

- Payment Services Act 2019 (No. 2 of 2019)
- Notice PSN01 – Prevention of Money Laundering and Countering the Financing of Terrorism – Specified Payment Services and the associated Guidelines to Notice PSN01
- Notice PSN02 – Prevention of Money Laundering and Countering the Financing of Terrorism – Holders of Payment Service Licence (Digital Payment Token Service) and the associated Guidelines to Notice PSN02
- Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act (Cap. 65A)
- Organised Crime Act 2015 (No. 26 of 2015)
- Prevention of Corruption Act (Cap. 241)
- Terrorism (Suppression of Financing) Act (Cap. 325) ("TSOFA")
- Standards set by FATF

The Company will observe requirements under the Personal Data Protection Act 2012 in the collection and use of customer data (as set out in the Company's personal data privacy policy).

3 Money Laundering Reporting Officer

A Money Laundering Reporting Officer (MLRO) will be appointed to be the business owner of the Company's AML/CFT Risk Assessment, Controls, Policies and Procedures. The role of the MLRO carries significant responsibility and should be undertaken by an appropriately experienced and qualified individual.

The Company's MLRO is an assigned officer from Ingenia Consultants, with support from Ingenia Consultants.

The MLRO will report directly to Lim Hong Zhuang and Yvonne Lim (the directors of the Company) and will have responsibilities including, but not limited to, the following:

(a) Ensuring that the AML/CFT policies and procedures are accurate and up to date with current requirements;
(b) Establishing and maintain adequate arrangements on employee's awareness and training on AML/CFT;
(c) Ensuring proper conduct of customer due diligence (CDD) measures and ongoing monitoring;
(d) Receiving and evaluate reports from employees on activities and transactions on suspicion for money laundering and financing of terrorism;
(e) Submitting reports to the Suspicious Transactions Reporting Office (STRO);
(f) Maintaining the register of all STRs submitted;
(g) Monitoring relevant employee and agent screening;
(h) Liaising with Law Enforcement Authorities;

(i) Managing Production Order requests; and
(j) Conducting enterprise-wide AML/CFT risk assessment and formulate appropriate internal controls for risk management.

Duties of the MLRO may be delegated to other suitably qualified individuals within the Company, however, the MLRO will take ultimate managerial responsibility and oversight to ensure that the duties imposed on the MLRO are complied with.

If the position of the MLRO falls vacant, the Company must appoint another individual as its MLRO.

Although the MLRO is obligated to take reasonable steps to ensure all elements of these policies and procedures are implemented, adhered to and updated, complying with the Company's AML policies and procedures is an obligation of all employees.

4 Risk Assessment

4.1 Risk Assessment Overview

The Company assess the risk of money laundering and terrorist financing of specific customers by using a formalised risk assessment matrix. The risk assessment measures the risk of a customer, considering various risk factors, and thereafter categorising a customer as Low, Medium or High risk. A customer's risk rating will initially determine a customer's periodic review timeframe. In addition to a customer's risk rating, trigger events are used in order to identify changes in a customer's risk profile.

As a consequence, the Company has implemented a Risk assessment procedure alongside the matrix in order to determine when and how risk assessments are performed. The Company uses the following risk factors in assessing the risk of a SME:

- Transactional activity;
- Purpose of transactions
- Customer risk due to any link with Politically Exposed Persons ("PEPs")
- Geographic risk accounting for the enhanced risk that jurisdictions identified by sources including but not limited to FATF, Transparency International, Basel etc., that have identified countries with deficiencies;
- Any adverse news identified.

There could be other risk elements discovered during the on-boarding or periodic review process that may affect the overall ML/TF risk associated with the customer, or the acceptability of the customer.

4.2 Business Risk Assessment

The Company shall conduct, at a minimum, once every 12 months, a Business Risk Assessment to:

- Identify ML/FT Vulnerabilities; and
- Identify ML/FT Risks.

Based on the results of the Risk Assessment, the following shall be revised to minimise the risk of funds originating from ML/FT activities that may channelled through the Company's business:

- Measures;
- Policies;
- Controls; and
- Procedures.

The risk assessment will also be updated when there is any material change to the Business Services and/or customer profile. In addition, the Company will consider the results of the Singapore National Money Laundering and Terrorist Financing Risk Assessment ("NRA") Report, when assessing the ML/TF risk factors in relation to the customers, geographical exposure, products, services, transactions and delivery channels, and whether the Company is susceptible to prevailing crime types identified in the NRA Report.

4.3 Customer Risk

All customers are Risk Assessed before the start of their relationship with the Company, based on the following factors:

- Products, services and likely transactions to be undertaken;
- Politically Exposed Person (PEP)/ Sanctions nexus status;
- Delivery channels; and
- Geographical location.

The Company does not accept any customer who falls within the categories below:

- PEPs (as defined above);
- Public sector bodies, government, state-owned companies and supranationals, sovereign wealth funds;
- Clubs, societies and charities;
- Sole proprietors; or
- Partnerships and unincorporated bodies.

4.4 Note on PEPs

A PEP is defined as "an individual who is or has, at any time in the preceding year, been entrusted with prominent public functions and an immediate family member (including a parent, step-parent, child, step-child, adopted child, spouse, sibling, step-sibling and adopted sibling), or a known close associate (including a natural person who is closely connected to a politically exposed person, either socially or professionally), of such a person. "

Individuals who have, or have had, a high political profile, or hold, or have held, public office, can pose a higher money laundering risk to the Company, as their position may make them vulnerable to corruption. This risk also extends to members of their immediate families and to know close associates. PEP status itself does not, of course, incriminate individuals or entities. It does, however, put the client or the beneficial owner into a higher risk category.

Establishing whether individuals are categorised as PEPs is not always straightforward and can present difficulties. The Company carries out Internet searches or consults relevant reports and databases on corruption risk published by specialised national, international, non-governmental and commercial organisations.

4.5 Country risk

Circumstances where a customer presents or may present a higher risk for money laundering or terrorism financing include but are not limited to the following:

- where a customer is from or in a country or jurisdiction in relation to which the FATF has called for countermeasures; and
- where a customer is from or in a country or jurisdiction known to have inadequate AML/CFT measures, as determined by the licensee for itself or notified to the Company by the MAS or other foreign regulatory authorities.

5 Ongoing monitoring

After account opening, a customer's account activity remains under monitoring, to identify any potential ML/TF activities. The results of screening and assessment by the Company is documented.

The Company has established a risk-based transaction monitoring program designed to detect, evaluate, and report unusual or suspicious customer transaction activity.

The Company has developed a proprietary system that facilitates the review and analysis of all transaction data to identify patterns of behaviour that constitute outlier activity. These patterns are configured into automated queries that run against all transaction data on a daily basis to "flag" any customers engaged in such activity.

6 Customer Due Diligence

The Company will perform due diligence on its customers when:

- Prior to the establishment of an account relationship with the customer;
- Prior to the undertaking of any transaction for any customer;
- Prior to the deposit of any funds for customer;
- Where there is a suspicion of money laundering or terrorism financing; or
- Where the licensee has doubts about the veracity or adequacy of any information previously obtained.

No account will be opened for any entity on an anonymous basis or any entity using a fictitious name. Accounts will only be opened for SMEs (i.e. private companies limited by shares).

6.1 Identification of customer

Account opening Customer Due Diligence (CDD) measures, using the Visage Protocol, includes:

- Obtaining information to identify the SME customer, which will include at a minimum the following information:
    - Full name of entity;
    - Incorporation number or business registration number;
    - The customer's registered or business address;
    - Date of establishment, incorporation or registration;
    - Jurisdiction of incorporation;
    - If listed, information regarding listed status;
    - No. of employees; and
    - Contact information of company.

- Obtaining the following documents from customers:
    - Certificate of incorporation or Company's ACRA;
    - Where relevant, certificate of incumbency, certificate of good standing, share register;
    - Passport or equivalent ID for all directors;
    - Corporate ownership structure (eg. organisation chart);
    - Latest annual audited financial statements;
    - Board Resolution authorising the customer's account with the Company;

- Information about the jurisdictions where the customer operates or has offices or business

- Verifying the identity of the customer using reliable, independent source data, documents or information

6.2 Connected parties

- Identifying and verifying the connected parties[2] of the customer, by obtaining at least the following information of each connected party:
  - Full name, including any aliases;
  - Role in company;
  - Contact information; and
  - Unique identification number (such as an identity card number, birth certificate number, or passport number of the connected party).

6.3 Natural persons appointed to act

- Identifying and verifying the identity of natural persons appointed to act on the customer's behalf by obtaining at least the following information:
  - Full name, including any aliases;
  - Unique identification number (such as an identity card number, birth certificate number or passport number);
  - Residential address;
  - Date of birth;
  - Nationality;
  - Appropriate documentary evidence authorising the appointment of such natural person by the customer to act on his or its behalf (eg. board resolution or similar authorisation documents); and
  - The specimen signature of each natural person appointed[3].

[2] Connected party, in relation to an SME, means:
(a) in relation to a legal person (other than a partnership), means any director or any natural person having executive authority in the legal person;
(b) in relation to a legal person that is 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

[3] Where there is a long list of natural persons appointed to act on behalf of the customer (e.g. a list comprising more than 10 authorised signatories), the payment service provider should verify at a minimum those natural persons who deal directly with the payment service provider.

6.4 Beneficial owners

Th Company enquires if there exists any beneficial owner owning more than 25% in relation to the customer[4], and collects the relevant information below from each beneficial owner for identification and verification:

- Full name
- ID Number
- % of shares / voting rights
- Birth country
- Country and city of residence
- Job title
- Date of birth
- Copy of government-issued ID
- Proof of address

The Company will collect the following information for all legal entities that are identified as 25% or greater beneficial owners:

- Full legal name
- Date of formation
- Jurisdiction of formation

6.5 Information as to the customer's business

- Obtaining from the customer information as to the nature of the customer's business and its ownership and control structure, including the following questions:
    - Whether any subsidiaries / parent company /partner or customer have any current business activity in high risk countries[5];
    - Description of the nature of specific business activities, and assessment of % of each activity against annual turnover;
    - Check whether the customer or its affiliated companies, family members, suppliers, providers, distributors are carrying out high risk activities[6];
- Obtain information as to the source of funds, and purpose and intended nature of business relations and transactions;

[4] To the extent that there is doubt as to whether the natural persons who ultimately own the legal person are the beneficial owners or where no natural persons ultimately own the legal person, identify the natural persons (if any) who ultimately control the legal person or have ultimate effective control of the legal person. Where no natural persons are identified, identify the natural persons having executive authority in the legal person, or in equivalent or similar positions.

[5] Afghanistan, Belarus, Myanmar, Burundi, Central African Republic, Cuba, Eritrea, Iran, Libya, North Korea, Russia, Somalia, Sudan, Syria, Ukraine (Crimea Sevastopol Region), Venezuela, Yemen, Zimbabwe.

[6] The list of activities considered include pawn brokers, dealers in commodities, arms/defence, dating services, marijuana and recreational drugs, counterfeit and pirated goods, etc.

- Checks and confirmation from customers as to whether they have key company policies and procedures to address business risks:
    - Whether the customer has a data protection and information security policy in place;
    - Whether the customer has a data protection officer;
    - Whether the customer has a AML/CTF programme;
    - Whether the customer has undergone an internal audit or independent third party review to test the effectiveness of the data protection / information security function;
    - Whether the customer has an approved Anti-Bribery and Corruption ("**ABC**") policy in place; and
    - Whether the customer have undergone an internal audit or an independent third party review that assessed compliance with ABC policies, and information about such audit / reviews.

6.6 Ongoing monitoring

- Conducting on-going monitoring of the business relationship, to ensure transactions are consistent with what the business knows about the customer, and the risk assessment, and where appropriate, the source of funds;
- Paying special attention to all complex, unusually large or unusual patterns of transactions, undertaken throughout the course of account relationships, that have no apparent or visible economic or lawful purpose; and
- Retaining records of CDD information and analysis performed, updating them regularly, particularly for higher risk categories of customers.

6.7 Other notes regarding CDD

The Company will not provide services:

- to entities where the ultimate beneficial owners or controlling interests in the business are not understood or known;
- to individuals or entities that are doing business with any nation, entity or individual designated on sanctions or terrorisms lists, or any nations on a restricted list maintained by the Company;
- to entities that require, but are unable to demonstrate, the required licensing to carry on business in their industry;

- when the source of funds of a customer is not well understood or reasonable given the knowledge of the customer;
- to shell entities;
- in instances where due diligence information is incomplete or being withheld;
- to persons who have been black-listed by the Company in the past in relation to fraud or abusive behavior, or where a suspicious transaction report has been filed;
- arms dealers; and
- entities engaged in non-U.S. federally approved cannabis-related activities.

The Company does not carry out any simplified due diligence measures.

The Company does not engage in further business with customers who are not able to complete the CDD / EDD satisfactorily and will consider whether the circumstances are suspicious so as to warrant the filing of an STR. Such a decision will be determined by the MLRO, and a copy of the relevant STR will be extended to the MAS.

For the purposes of the above, completion of the measures means the situation where the Company has obtained, screened and verified all necessary CDD information, and where the Company has received satisfactory responses to all inquiries in relation to such necessary CDD information.

Where the Company forms a suspicion of money laundering or terrorism financing, and reasonably believes that performing any measures will tip-off a customer, the Company may stop performing the measures. The Company shall document the basis for its assessment and file an STR.

6.8 Foreign Currency Exchange Transactions

For Singapore entities, the Company does not permit any cash payouts exceeding S$20,000, and does not make any foreign exchange remittance transactions on behalf of customers.

For other entities, any cash withdrawals are carried out by partners in line with the relevant laws and jurisdictions of the other countries. As the Company only handles DPT and does not handle cash transfers, it does not process FX transfers, and hence does not fall in the scope of foreign exchange transaction reporting.

7 Enhanced Due Diligence

If a customer is flagged as a higher risk customer, senior management approval must be obtained in order to onboard the customer.

In conducting enhanced due diligence, the MLRO may:

- Require the customer to provide additional supporting documentation, including documentation evidencing net worth, income and/or source of funds;
- Conduct additional web searches;
- Put additional limits and controls on the account.

8 Screening

The Company conducts screening of customers, Connected Persons and beneficial owners against the following key sanctions lists/ sources:

- Lists of sanctioned individuals and entities, as covered by the TSOFA and MAS Regulations issued under section 27A of the MAS Act;
- Global sanctions, including lists of prohibited persons, entities and wallets issued by the Office of Foreign Assets Controls[7];
- Countries highlighted as having strategic deficiencies in the AML/CFT regimes, such as the Democratic People's Republic of Korea and Iran which have been highlighted by the Financial Action Task Force ("**FATF**") to be high risk jurisdictions, as well as the FATF Grey List;
- Lists issued by law enforcement and regulatory bodies worldwide; and
- Potential adverse media sources.

The Company may also undertake additional screenings depending on risk factors and the jurisdiction where the customer is located.

Where customer is identified as a sanctions nexus, the Company will freeze without delay and without prior notice, existing funds and accounts maintained by the customer with the Company and report customer's account activity to relevant authorities.

Where there are any changes or updates to the lists above, the Company screens the customer to determine if there are any money laundering or terrorism financing risks in relation to the customer.

9 Suspicious Transaction Reporting

An internal Suspicious Transaction Report ("STR") is to be filed directly to the MLRO whenever there is a suspicion that a customer is engaged in ML/FT activities.

[7] One of the key lists usually included in screening is the Specially Designated Nationals and Blocked Persons List. In the case of DPTs, the Office of Foreign Assets Control includes digital currency addresses on its Specially Designated list of blocked persons, companies and entities.

This is done by completing a STR form and emailing it directly to the MLRO on mlro@shuttleone.com**.**

An employee who has raised a STR should not share any information with his/her co-workers, for risk of tipping off. All information and any subsequent updates should only be shared and forwarded to the MLRO. keep records of all transactions referred to STRO, together with all internal findings and analysis done in relation to them

The MLRO shall:

- Maintain a register of all STRs that have been received, together with all internal findings and analysis done in relation to them;
- Assess whether the reported activity constitutes a potential ML/TF activity;
- Decide whether there is scope to escalate to STRO via STR filing.
    - If yes, to file a STR using SONAR and to extend a copy to the MAS for information
    - If not, rationale of no filing should be recorded with sufficient and appropriate evidence maintained. If not existed, the customer's account relationship will also be subject to commensurate risk mitigation measures, including enhanced ongoing monitoring, and approval must be obtained from Lim Hongzhuang to retain the customer;
- Keep records of all transactions referred to STRO, together with all internal findings and analysis done in relation to them; and
- Ensure that the reporting to STRO is performed timely and within 15 working days, from date of internal STR form receipt, unless circumstances are exceptional or extraordinary.

9.1 Red Flags

Red flags that signal possible money laundering or terrorist financing include, but are not limited to, the following:

Insufficient or Suspicious Information

- Provides unusual or suspicious identification documents that cannot be verified.
- Reluctant to provide complete information about nature and purpose of business, anticipated account activity, or business location.
- Refuses to identify a legitimate source for funds or information is false, misleading or substantially incorrect.
- Background is questionable or differs from expectations based on business activities.
- Customer has no discernable reason for using the Company's service.

Efforts to Avoid Reporting and Recordkeeping

- Reluctant to provide information needed to file reports or fails to proceed with the transaction.
- Tries to persuade an employee not to file required reports or not to maintain required records.
- Requests that a transaction be processed in such a manner so as to avoid the Company's normal documentation requirements.
- Unusual concern regarding the Company's compliance with government reporting requirements.

Activity Inconsistent with Business

- Transaction patterns show a sudden change inconsistent with normal activities.
- Maintains multiple accounts, or maintains accounts in the names of family members or corporate entities with no apparent business or other purpose.
- Appears to be acting as an agent for an undisclosed principal, but is reluctant to provide information.
- Engages in transactions that lack business sense, apparent investment strategy, or are inconsistent with the Customer's stated business/strategy

Other Suspicious Customer Activity

- Unexplained high level of account activity.
- Law enforcement requests.
- Buying and selling with no purpose or in unusual circumstances.
- No concern regarding price volatility.
- Source of funds information appears false, misleading, or substantially incorrect.
- Difficulty describing the nature of Customer's business or lacks general knowledge of Customer's industry.
- Customer (or a person publicly associated with the Customer) has a questionable background or is the subject of news reports indicating possible criminal, civil or regulatory violations.
- Engages in multiple transfers of funds or wire transfers to and from countries that are considered bank secrecy or "tax havens" that have no apparent business purpose or are to or from countries listed as non-cooperative by FATF and FinCEN, or are otherwise considered by the Company to be high-risk.

- Account has inflows of funds or other assets well beyond the known income or resources of the Customer.
- Exhibits an unusual level of concern for secrecy, particularly with regard to the Customer's identity, type of business or source of assets.
- Customer is from, or has a bank account in a country identified as a haven for bank secrecy, money laundering or narcotics production.

10 Employee Training

Within 7 working days from the start of employment, all employees will be provided ML/FT trainings delivered by an external service provider via classroom trainings and/or e-learning, to ensure that they are aware of measures, policies, controls and procedures that are in forced. This training includes:

- General awareness of Money Laundering / Terrorism Financing;
- Specific guidance of the related measures, controls, policies and procedures in place within the Company; and
- A graded assessment to ensure that the employee has grasped the key points of the training.

The training attendance/ completion status will be recorded and monitored by the MLRO. Refresher training will be provided at a minimum once every 12 months.

11 Employee Screening

The Company will ensure high standards when hiring employees and appointing officers. Prospective employees will be screened before the beginning of their employment to ensure that they are fit and proper, to occupy positions in which they will participate in the provision of services to the customer or managing the Company's operations.

The criteria for considering whether a relevant person is fit and proper include but are not limited to the following:

- Honesty, integrity and reputation;
- Competence and capability; and
- Financial soundness.

The use of third-party screening providers may be engaged to ensure the execution of this screening. Screening results will be reviewed by the Company's Human Resource Department. Any exceptions will be consulted with the Compliance Manager for further appropriate actions to be taken.

12 Responding to Regulatory & Law Enforcement Enquiries

The Company will at all times, where it is legally possible, cooperate with regulators and law enforcement agencies in a timely manner. All enquiries and requests received from the regulators and law enforcement agencies, should be directed to the MLRO or the Compliance Manager for proper follow up actions.

13 Audit & Quality Assurance

The Company endeavours to maintain high standards of design and operating effectiveness in its compliance policies, controls and procedures. As such, on a periodic basis, sample testing and assurance review will be performed by the internal Operations team to assess the effectiveness of measures taken to prevent ML/TF. This would include, among others:

- Determining the adequacy of the AML/CFT policies, procedures and controls, ML/TF risk assessment framework and application of risk-based approach;
- Reviewing the quality of work performed by an external party on any outsourced AML/CFT activities;
- Reviewing the content and frequency of AML/CFT training programmes, and the extent of employees' and officers' compliance with established AML/CFT policies and procedures; and
- Assessing whether instances of non-compliance are reported to senior management on a timely basis.

The frequency and extent of the sample testing and assurance review will commensurate with the ML/TF risks presented and the size and complexity of the Company's prevailing business. The Company has also engaged an external firm, RSM Chio Lim LLP, to perform the testing and reviews.

14 Record Retention

The Company maintains a record retention period of 5 years on the following:

- Records of CDD information relating to the business relations, transactions as well as account files, business correspondence and results of any analysis undertaken, following the termination of such business relations or completion of such transactions;
- Records of data, documents and information relating to a transaction, including any information needed to explain and reconstruct the transaction, following the completion of the transaction;
- Records of data, documents and information on all business relations with or transactions for a customer, pertaining to a matter which is under investigation or

which has been the subject of an STR, in accordance with any request or order from STRO or other relevant authorities in Singapore.

The Company will observe requirements under the Personal Data Protection Act 2012 in the collection and use of customer data.

15 References

Payment Services Act 2019 (No. 2 of 2019)

https://sso.agc.gov.sg/Acts-Supp/2-2019/Published/20190220?DocDate=20190220

Notice PSN01 – Prevention of Money Laundering and Countering the Financing of Terrorism – Specified Payment Services and the relevant Guidelines to PSN01

https://www.mas.gov.sg/-/media/MAS/Regulations-and-Financial-Stability/Regulatory-and-Supervisory-Framework/Anti_Money-Laundering_Countering-the-Financing-of-Terrorism/PSN01-Prevention-of-Money-Laundering-and-Countering-the-Financing-of-Terrorism--Specified-Payment-Se.pdf

Notice PSN02 – Prevention of Money Laundering and Countering the Financing of Terrorism – Holders of Payment Service Licence (Digital Payment Token Service) and the relevant Guidelines to PSN02

https://www.mas.gov.sg/-/media/MAS/Regulations-and-Financial-Stability/Regulatory-and-Supervisory-Framework/Anti_Money-Laundering_Countering-the-Financing-of-Terrorism/PSN02-Prevention-of-Money-Laundering-and-Countering-the-Financing-of-Terrorism--Digital-Payment-Toke.pdf

Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act (Cap. 65A)

https://sso.agc.gov.sg/Act/CDTOSCCBA1992

Organised Crime Act 2015 (No. 26 of 2015)

https://sso.agc.gov.sg/Act/OCA2015?ProvIds=P12-.

Prevention of Corruption Act (Cap. 241)

https://sso.agc.gov.sg/Act/PCA1960

Terrorism (Suppression of Financing) Act (Cap. 325)

https://sso.agc.gov.sg/Act/TSFA2002?ValidDate=20190624&ProvIds=P1II-

How to Submit an STR –
https://www.police.gov.sg/e-services/report/suspicious-transaction-report-online-lodging-system

FATF High Risk and other monitored Jurisdictions –
http://www.fatf-gafi.org/countries/#high-risk

Singapore National Money Laundering and Terrorist Financing Risk Assessment Report -
http://www.mas.gov.sg/Regulations-and-Financial-Stability/Anti-Money-Laundering-Countering-The-Financing-Of-Terrorism-And-Targeted-Financial-Sanctions/Anti-Money-Laundering-and-Countering-the-Financing-of-Terrorism/National-Risk-Assessment.aspx