Know Your Customer (KYC) &

Anti-Money Laundering (AML) Policy

The Company protects itself from involvement in money laundering or suspicious activity by the following:

- Performing an enterprise-wide risk assessment to determine the risk profile of the Company
- Establishing AML policies and procedures
- Implementing internal controls throughout its operations that are designed to mitigate risks of money laundering
- Performing know your customer ("KYC") procedures on all users
- Designating a Compliance Officer with full responsibility for the AML Program
- Conducting an annual AML audit
- Providing AML training to all employees

POLICIES AND PROCEDURES

The Policy will be approved by the Company's Board. The Policy once approved will be provided to all employees. Each employee will acknowledge the Policy in writing. All policies and procedures will be reviewed and updated or revised as needed, but no less often than annually.

INTERNAL CONTROLS

The Company has developed and implemented internal controls for the purpose of ensuring that all of its operations comply with all AML legal requirements and that all required reports are made on a timely basis. Some of those internal controls are listed within this document and include, but are not limited to, the Customer Identification Program, the Suspicious Activity Reporting system, and the required reports on the Program's effectiveness to the Board.

TRAINING

All of the officers and employees of the Company are required to receive AML training at least annually. New employees will receive appropriate AML training within 30 days of their hire date. Training for all employees will include not only the legal elements of AML laws and regulations but will also cover job specific applications of these laws. Ongoing training will be provided and updated regularly to reflect current developments and changes to laws and regulations.

CUSTOMER IDENTIFICATION

It is the Company's policy to ensure that it has reasonably identified each customer who uses the Company's platform. Users may be identified using a variety of methods.

ACCOUNT OPENING PROCEDURES.

Additionally, the Company will, as part of its account-opening process: (i) cross-check the names of users against compliance databases such as the OFAC Specially Designated Nationals list and other governmental watch lists; (ii) require users to provide proof of identification; and (iii) not permit any payment above 1,000 Singapore dollar to be made with incomplete account-opening information.

PROOF OF IDENTIFICATION:

Individual

1. Name
2. Date and place of birth
3. Residence address and mailing address if different (PO Box alone will not be acceptable)

4. Official issued identification number (e.g., passport number, social security number, employee identification number or individual taxpayer identification number)
5. Copy of valid photo identification of the principal(s) involved with the account (e.g., driver's license, passport, alien identification card)

VERIFICATION

Documents used in opening an account relationship must be verified prior to establishing the account. Verification of identity will require multi-factor authentication, layered security and other controls to ensure a meaningful user identity confirmation process based on account size or other factors.

The following are examples of verification methods the Company may use:

- Obtaining proof of address, such as a copy of a utility bill or bank statement from the account holder.
- Comparing the identifying information with information available from a trusted third party source, such as a credit report from a consumer-reporting agency
- Analyzing whether there is logical consistency between the identifying information provided, such as the customer's name, street address, ZIP code, telephone number, date of birth, and social security number (logical verification).
- Utilizing knowledge-based challenge questions.
- Utilizing complex device identification (such as "digital fingerprints" or geo-location checks).
- Obtaining a notarized copy of an individual's birth certificate for valid identification.
- When the type of account increases the risk that the Company will not be able to verify the true identity of the customer through documents is confirmed the account will be closed.

SUSPICIOUS TRANSACTION AND ACTIVITY REPORTS

The Company will diligently monitor transactions for suspicious activity. Transactions that are unusual will be carefully reviewed to determine if it appears that they make no apparent sense or appear to be for an unlawful purpose. Internal controls will be implemented so that an ongoing monitoring system is in place to detect such activity as it occurs. When such suspicious activity is detected, the Company will determine whether a filing with any law enforcement authority is necessary.

Suspicious activity can include more than just suspected money laundering attempts. Activity may be suspicious, and the Company may wish to make a filing with a law enforcement authority, even if no money is lost as a result of the transaction.

The Company will initially make the decision of whether a transaction is potentially suspicious. Once the Company has finished the review of the transaction details, he or she will consult with the Company's senior management to make the decision as to whether the transaction meets the definition of suspicious transaction or activity and whether any filings with law enforcement authorities should be filed.

The Company will maintain a copy of the filing as well as all backup documentation. The fact that a filing has been made is confidential. No one, other than those involved in the investigation and reporting should be told of its existence. In no event should the parties involved in the suspicious activity be told of the filing. The Company may inform the Company's Board of the filing and the underlying transaction.

REPORTING REQUIREMENTS

Reasonable procedures for maintaining records of the information used to verify a person's name; address and other identifying information are required under this Policy. The following are required steps in the record keeping process:

- The Company is required to maintain a record of identifying information provided by the customer.
- Where the Company relies upon a document to verify identity, the Company must maintain a copy of the document that the Company relied on that clearly evidences the type of document and any identifying information it may contain.

- The Company must also record the methods and result of any additional measures undertaken to verify the identity of the customer.
- The Company must record the resolution of any discrepancy in the identifying information obtained.
- All transaction and identification records will be maintained for a minimum period of five years.

AML AUDIT

The Company is responsible for directing the annual AML audit of the Company's operations. The independent audit will be conducted by an independent third party with working knowledge of BSA requirements, or by Company personnel with working knowledge of BSA requirements. The Company will develop corrective action plans for all issues that are raised in the audit and will provide the audit report and all corrective action plans to the Company's senior management for review. Reports of the corrective action will continue until all are resolved.