KNOW YOUR CUSTOMER (KYC) & ANTI-MONEY LAUNDERING (AML) POLICY AND PROCEDURES

It is the policy of Soco Foundation Company Limited (the "**Company**") to prohibit and actively prevent money laundering and any activity that facilitates money laundering or the funding of terrorist or criminal activities by complying with all applicable requirements of the Cayman Islands and its implementing regulations.

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 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.

Our AML policies, procedures and internal controls are designed to ensure compliance with all applicable regulations and rules and will 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 regulations and changes in our business.
The Company operates so that it is in compliant with ‘anti -money laundering’ (“AML”) and ‘know your customer’ (“KYC”) rules and regulations in the jurisdictions it operates in or sells products or services to and has developed this KYC and AML Policy to protect itself from involvement in money laundering or suspicious activity as follows:

- 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

I. POLICIES AND PROCEDURES

All policies will be approved by the Company’s Board. A 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 or as required by the Cayman Islands.

II. 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 thirty 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.

III. INTERNAL CONTROLS

Internal controls are in place at the Company 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 Participant Identification Program, the Flagged Activity Reporting system, and the required reports on the Program's effectiveness to the Board.

IV. 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.

V. 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; (iii) not permit any payment above **500 U.S.** Dollars value to be made with incomplete account-opening information; and (iv) not permit any token holders to redeem/use their tokens on the platform with incomplete account-opening information.

VI. PROOF OF IDENTIFICATION

Individuals (For corporate entities, the Company collects all the points mentioned below for a director of the entity)

1 Name

2 Date and place of birth
3 Residence address and mailing address if different (PO Boxes are not acceptable unless accompanied by a valid mailing address)
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)

Corporate Entities

1 Name of business and corporate representatives
2 Copies of current photo identifications of corporate representatives using the account
3 Mailing address of the client’s principal place of business (we reserve the right to request the customer’s local address if the local address is not the same as the business’ principal place of business)
4 Customer identification procedures shall be adhered to determine the beneficial owners of trust or corporate accounts. These procedures include establishing whether a customer is an agent of another; deriving information concerning the ownership or structure of a company that is a legal entity not publicly traded in the US or other countries; and for trustees, getting data about the trust structure, determining the provider of funds, and discerning who has control over the funds and power to remove the trustee.

VII. 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.

VIII. AML SCREENING

The Company shall screen each prospective purchaser in its token sale for matches in the following categories:

- Global Sanctions List: Screening prospective purchasers against OFAC sanctions.
- PEPs: Screening prospective purchasers for identification as a "politically exposed person". A PEP is a term describing someone who has been entrusted with a prominent public function. A PEP generally presents a higher risk for potential involvement in bribery and corruption by virtue of their position and the influence that they may hold.
- Adverse Media: Screening prospective purchasers against adverse media involves looking for any negative mentions of them in traditional news media and publicly available information more broadly.

Any prospective participant that has a match on any of the above categories shall be flagged and blocked pending review by the Company and its counsel of the red flag. The prospective purchaser will receive an email letting them know that it is being reviewed and a follow-up email letting the prospective purchaser of the disposition of the review as set out below.

IX. DISPOSITIONS OF AML FLAGS

- Global Sanctions List: If the flag is a match on the Global Sanctions List, the Company shall outright deny the purchaser and let them know of the disposition of the review.
- PEPs: If the flag is a match on PEPs the Company's counsel shall review the AML report and may request proof of identification or additional verification from the prospective purchaser within seventy-two (72) hours of the flag. After receiving any additional verification information the Company shall provide the prospective purchaser with notice of disposition within seventy-two (72) working hours of receipt of such additional information.
- Adverse Media: If the flag is a match on Adverse Media, the Company's counsel shall review the adverse media and make a determination on whether to allow the prospective purchaser within seventy-two (72) working hours of the flag.

X. FLAGGED 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.

XI. AML COMPLIANCE PERSON – DESIGNATION AND DUTIES

The Company has identified and designated a compliance person to be its Anti-Money Laundering Program Compliance Person (AML Compliance Person), with full responsibility for the firm's AML program. The duties of the AML Compliance Person will include monitoring the firm's compliance with AML obligations, overseeing communication and training for employees. The AML Compliance Person will also ensure that the firm keeps and maintains all of the required AML records and will ensure that suspicious activity reports are filed with the relevant authority with appropriate jurisdiction. The AML Compliance Person is vested with full responsibility and authority to enforce the firm's AML program.

XII.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.

XIII. 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 corrective actions will continue until all are resolved.