

BitBook

AML/KYC policy

Know Your Customer (KYC) and Anti-Money Laundering (AML) Policy and Procedures

It is the policy of BitBook (the “Company”) to prohibit and prevent money laundering and any activity that facilitates money laundering or the funding of terrorist or criminal activities by complying with all applicable legal requirements of Gibraltar.

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. Terrorist financing may not involve proceeds of criminal conduct but is rather an attempt to conceal either the origin of the funds or their intended use.

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, rules and laws 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 in compliance 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 the given KYC and AML Policy to protect itself from involvement in money laundering or suspicious activity as follows:

- The Company is performing an enterprise-wide risk assessment to determine the risk profile of the Company.
- The Company has established KYC and AML policies and procedures that have been reviewed and approved by the Company’s Board of Directors (the “Board”).
- The Company is implementing internal controls throughout its operations designed to reduce risks of money laundering, including designating a person responsible for AML compliance. The Company performs know your customer (“KYC”) procedures on all token sale purchasers.

POLICIES AND PROCEDURES

1. Purchaser Identification (Know Your Customer)

The Company collects identifying information on each purchaser in its token sale. The Company shall collect the following information about each purchaser:

1.1. Individuals

Full Name

Wallet Address

Telephone

Email address

Residential Address

Copy (front and back) of ID Data collected from ID:

Date of birth, Nationality,

ID scan

Personal photograph (with ID in Hand) A Description of Source of Funds

PEP checks with filters like Worldcheck

1.2. Companies

Summary of information requested/gathered

Company Name

Wallet Address

Company Address

Description of Business Activities

Government-issued business registration number or tax identification number

Copy of a recent trade register extract or similar document

Authorised Representative, compare Individual of KYC process

Even after KYC approval the Company can do additional checks and ask for further documents.

2. Contributor Eligibility

-The Company shall not accept purchasers (individuals or entities) who are not at least eighteen (18) years of age or purchasers from the following jurisdictions (the "Prohibited Purchasers"):

-United States - Individuals or entities from or residing in the United States, including American Samoa, Guam, Northern Mariana Islands, Puerto Rico, U.S. Virgin Islands, or any entity organized or incorporated under the laws of the United States. U.S. citizens living abroad may also be deemed "U.S. Persons" under certain rules.

The Company explicitly prohibits the Prohibited Purchasers in its Token Sale Terms and Conditions (the "T&C"). Any purchasers that purchase tokens in violation of the T&C shall be deemed invalid and such purchasers shall have their purchase amount returned to them at their expense.



3. 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 could 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 purchaser 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 of that it is under review and a follow-up email letting the prospective purchaser of the disposition of the review.

4. Dispositions of AML Flags

- Global Sanctions List - If the flag is a match on the Global Sanctions List, the Company shall 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 council shall review the AML report and may request proof of identification or additional verification from the prospective purchaser.
- After receiving any additional verification information, the Company shall provide the prospective purchaser with notice of disposition.
- 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.

5. Appointment of an AML Compliance Person - Designation and Duties

The Company is in the process of designating 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. The AML Compliance Person is vested with full responsibility and authority to enforce the firm's AML program.