VAIOT AML and CFT Policy

"VAIOT LIMITED" (hereinafter referred as the **"ISSUER" "VAIOT"**, the **"Company"**) is a private limited liability company incorporated under the laws of Malta on 6 December, 2018 for indefinite period of time, having its registered office at Cornerstone Business Centre, Suite 1, Level 2, 16th September Square, Mosta MST 1180, Malta and registered with the Malta Business Registry (MBR) under the number C89746. In order to ensure that our operations are compliant with the necessary AML and CFT rules, VAIOT is implementing AML and CFT policies and procedures as detailed in this document. In doing so, VAIOT must apply the obligations emanating from the Prevention of Money Laundering Act (Chapter 373 of the Laws of Malta), the Prevention of Money Laundering and Funding of Terrorism Regulations (S.L. 373.01 of the Laws of Malta), the Criminal Code (Chapter 9 of the Laws of Malta), and the National Interest (Enabling Powers) Act (Chapter 365 of the Laws of Malta). Furthermore, the company is obliged to follow the measures stipulated in the Implementing Procedures (part 1) and the Implementing Procedures for the Virtual Financial Assets Sector (part 2) (hereinafter collectively referred to as the 'Implementing Procedures'). As part of its AML and CFT obligations, VAIOT carries out a Know Your Client (KYC) and due diligence procedures with all applicable entities ("Applicable Entity"), including IVFAO Participants, and Cooperating Parties to meet its requirements.

VAIOT pays special attention and takes responsibility to ensure that our business is in line with the applicable Acts, Regulations and FIAU Recommendations for the Virtual Financial Asset Sector, taking into account the size of the organization and its resources.

Definitions

Participant - a person or an entity participating in the Initial VFA Offering and Private Offering of VFA Tokens and has successfully completed all necessary steps to become a Tokenholder.

Cooperating Party ("Customer", "Client", "Partner", "Employee") - a legal or natural person seeking to form or has formed a Business Relationship, or a legal or natural person seeking to carry out an Occasional or recurring Transaction with a subject person.

Business relationship – in accordance with the EU AML Directive, means a business, professional or commercial relationship which relates to the professional activities of the institutions and persons covered by the EU AML Directive, and which is expected, at the time when the contact is established, to have an element of duration. VAIOT, in line with EU AML Directive, considers an interaction with a third party as a business relationship if:

- The interaction between parties reoccurs over time and it is not limited to a single transaction,
- Due to the business or contractual arrangements the relationship between the parties has an element of duration (e.g. services being provided by or for the third party in an ongoing manner; assets are being delivered by or for the third party in an ongoing manner such as token release schedule etc.).

Examples of business relationship: client-service provider where services are provided in an ongoing manner; investor-company where the investment is made over time or assets are delivered to the investor over time; business partner-company where the partnership lasts over time etc.

Occasional transaction - any transaction other than a transaction carried out in the exercise of an established business relationship that does not have an element of duration. In the case of an occasional transaction, the CDD measures are limited to the identification and verification of the customer and its beneficial owners where applicable.

1. Scope of Policy

1.1. This AML and CFT Policy applies to all participants, and cooperating parties during the Initial VFA Offering (IVFAO) and private offering of VAI Tokens.

1.2. This AML and CFT Policy applies to regular, operational business activities (Business as Usual – BaU).

1.3. Each Applicable Entity must carefully read and comply with this KYC and AML Policy. It is understood and presumed per se that by the fact of the VAIOT's Website use and VAI Tokens purchase, the respective Applicable Entity fully read, understood and accepted this Policy. If any Applicable Entity does not agree with this Policy in general or any part of it, such Applicable Entity must not access and use the VAIOT's Website and/or purchase VAI Tokens, tokens developed by VAIOT.

1.4. The Company reserves the right to modify or amend this Policy at its sole discretion. Any revisions to this Policy will be posted VAIOT's Website. If we make changes, we will notify you by revising the date at the top of this Policy. We strongly recommend You to periodically visit the VAIOT's Website to review any changes that may be made to this Policy to stay updated on our AML and CFT procedures. Your continued usage of the VAIOT's Website and/or services shall mean Your acceptance of those amendments.

1.5. This Policy is administered by compliance officer or compliance department within VAIOT or the company entrusted with this mission by VAIOT. Information can be accessed via aml@vaiot.ai .

2. Money Laundering and Terrorist Financing

2.1. Money Laundering is the process in which criminals try to disguise the identity, original ownership and destination of money that they have obtained through criminal conduct.
Terrorist financing provides funds for terrorist activity. The use of products and services by money launderers and terrorists exposes the Company to criminal, regulatory and reputational risk.

2.2. VAIOT is strongly committed to preventing the use of its operations for money laundering or any activity which facilitates money laundering, or the funding of terrorist or criminal activities.

2.3. On a global level, in order to prevent and combat money laundering and terrorism financing, there has been an introduction of the number of laws concerning the customer identification and verification procedures including but not limited to the EU Directive 2018/843 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing (the "5th AML Directive"), which brings the virtual currencies under the scope of the Anti-Money Laundering Directive.

2.4. In Malta, the Financial Intelligence Analysis Unit (FIAU) is responsible for monitoring of the implementation of the AML and CFT regulations and for monitoring compliance with the relevant legislative provisions. The FIAU was established by the Prevention of Money Laundering Act (PMLA).

2.5. In order to ensure that our operations are compliant with the AML and CFT rules and procedures, we are implementing the AML and CFT policies and procedures detailed below. In doing so, we rely on Cap 373 of the Laws of Malta – Prevention of Money Laundering Act and subsidiary legislation thereof: Prevention of Money Laundering and Funding of Terrorism Regulations S.L. 373.01, Civil Code (Second Schedule) (Register of Beneficial Owners - Associations) Regulations, S.L. 16.15, Prevention of Money Laundering and Funding of Terrorism Regulations, S.L. 373.02, L.N. 117 of 2018 - National Coordinating Committee on Combating Money Laundering and Funding of Terrorism Regulations, 2018 and related legislation thereof Criminal Code, Chapter 9. VAIOT relies on Implementing Procedures issued by the Financial Intelligence Analysis Unit in Terms of the Provisions of the Prevention of Money Laundering and Funding of Terrorism Regulations, Part I, issued on May 20, 2011 and last amended on January 27, 2017 (hereinafter referred as "Implementing Procedures").

3. AML Risk Assessment

3.1. As part of the Policy in order to combat money laundering and illegal financing activities, the Company performed a Business Risk Assessment (BRA) and Customer Risk Assessment (CRA) as part of its Risk Management process.

3.2. Within Business Risk Assessment the Company follows principles that include but are not limited to the following:

- Raise awareness on ML issues;
- Appoint a designated compliance officer of compliance department, who in case of reasonable doubt should report any suspicious transactions to the appropriate Financial Authority;
- Freeze any funds deemed suspicious and investigate the source of finance;
- Introduce a Know-Your-Customer Policy (KYC);
- Exercise reasonable measures to obtain information about the true identity of the persons on whose behalf a transaction is made;

- Record keeping procedures – maintain, for a specific time period, all necessary records on transactions, both domestic and international;
- Pay special attention to all complex, unusually large transaction;
- Adopt reasonable measures (economic, administrative, self-regulatory and other measures) which can be taken to create an effective shield against ML).

3.3. As part of the customer risk assessment, the following examples, followed by other red flags that can be identified, will act as Money Laundering and Terrorist Funding warning signs based on guidance provided by Financial Action Task Force (FATF) – international body set up to combat money laundering, Financial Intelligence Analysis Unit (FIAU) and other local legislation :

- Evasiveness or reluctance to provide information;
- Incomplete or inconsistent information; negative public information available about the client or company;
- When money is coming from the list of 'high-risk and non-co-operative jurisdictions' according to FATF;
- Customer tells that the funds are coming from one source but then at the last minute the source changes;
- Unusual money transfer or transactions, at times intended not to come under the threshold when KYC applies;
- Complex group structures without obvious explanation that may be designed to disguise the true source and ownership of money.

3.4. As a part of the risk assessment procedure employed by VAIOT, the Company should follow, among other AM: legislation and guidance documents, Implementing Procedures and Prevention of Money Laundering Act (Cap 373 of the Laws of Malta) and subsidiary legislation thereof Prevention of Money Laundering and Funding of Terrorism Regulations (S.L. 373.01 of the Laws of Malta) and take into account risk factors including those relating to customers, countries or geographical areas, products, services, transactions and delivery channels and shall furthermore take into consideration any national or supranational risk assessments relating to risks of money laundering and the funding of terrorism.

4. Due Diligence

4.1. Customer Due Diligence

4.1.1. Company due to its operations under the Virtual Financial Assets Act (VFAA) has to carry out Customer Due Diligence (CDD). Company adopts this Policy and its internal procedures and reserves the right to undertake CDD in order to identify the Customer and verify the identity of the Customer. Customer due diligence measures shall also be applied, at appropriate times, to existing customers on a risk-sensitive basis, including at times when the Company becomes aware that the relevant circumstances surrounding the occasional transaction or a business relationship have changed.

4.1.2. Customer due diligence measures shall be repeated whenever, in relation to a business relationship or an occasional transaction, doubts arise about the veracity or adequacy of the previously obtained customer identification information.

4.1.3. Please note that that the following countries are considered as restricted areas, the residents of such countries shall not be allowed to participate in the Company's IVFAO (public sale stage) and consequently, CDD Procedure will not be conducted: USA, Germany, Puerto Rico, US Virgin Islands, Canada, China, Singapore, Afghanistan, Central African Republic, Cuba, Democratic Republic of the Congo, Eritrea, Iran, Iraq, Libya, North and South Korea, Somalia, South Sudan, Sudan, Yemen, Zambia.

4.1.4. As part of the exercise of this right, Customers will be required to provide the information in the transaction and KYC processes.

4.1.5. The Personal Information requested as part of the KYC procedure will be collected, processed, used and stored in accordance with the General Data Protection Regulation (GDPR), rules and principles of which have been reflected in the Privacy Policy and implemented on the legal, technical and organizational level.

4.1.6. If any doubt arises, we reserve the right to check the information provided, as part of the KYC and AML Policy and procedures, using nondocumentary methods including but not limited to contacting the customer directly.

4.1.7. Compliance officer or compliance department retains the right to freeze any funds already transferred should the suspicion as to the sources of those funds arise after they have been deposited. Such situation can occur if the Compliance Officer or Compliance department is in possession of any new information in regards to the transaction that might raise any concerns or suspicion in regards to the legitimacy of the source funds.

4.2. Simplified Customer Due Diligence

4.2.1. Simplified Due Diligence (SDD) will be applied in situations presenting a low risk of ML/FT.

4.2.2. Simplified due diligence will be performed by VAIOT or by the Company entrusted by VAIOT, whereas it will only be required to maintain a minimal amount of information about the applicant for business or the beneficial owner. Although, SDD might include conducting number of electronic checks, including running on Politically Exposed Persons (PEPs) and Sanctions lists.

4.2.3. Simplified Customer Due diligence shall not constitute an exemption from all customer due diligence measures. The Company retains the right to carry measures commensurate with the low risk identified.

4.3. Enhanced Customer Due Diligence

4.3.1. Enhanced level of CDD must be applied in the followingsituations: presenting a high risk of ML/FT, when the applicant for business has not been physically present for identification purposes, where applicants are Politically Exposed Persons (PEPs), individuals having otherwise prominent public positions , their immediate family members or persons known to be close associates of such persons.

4.4. Cooperation with third parties for CDD purposes

4.4.1. VAIOT may, on a risk-based approach, rely on a third party to carry out the required KYC/CDD ("the Third Party/ies"), where this introducer/third party consents to being relied upon and itthe introducer meets the criterion set out in the FIAU Implementing Procedures I, and EU AML legislation. Where such reliance is permitted, the ultimate responsibility for KYC/CDD measures remains with VAIOT.

4.4.2. The Implementing Procedures mention scenarios in which subject persons can rely on CDD carried out by other entities:

- Subject person A enters intoenters relationshipa relationship with the customer of another subject person (B) by accepting instructions given throughnthrough subject person B on behalf of the customer;
- Subject person A and subject person B both act for the sameesame customer in respect of an occasional transaction;
- Subject person A and subject person B form part of the same group of companies but carry out different relevant activities

4.4.3. VAIOT must implement monitoring measures for each KYC/CDD outsourcing arrangement with any service provider.

5. Ongoing Monitoring

5.1. A continuous monitoring process should be implemented in order that any unusual or irregular transactions may be identified at a preliminary stage.

6. Suspicious Activity Report

6.1. Suspicious Activity Report must occur whenever there is a suspected case of money laundering or terrorist financing.

6.2. As a regulated company we have an obligation to report a suspicious transaction with the Financial Analysis Unit.

7. Reference to the Agreements and the Law

7.1. Besides the present Policy, VAIOT shall ensure full compliance with any AML specific provision provided by any agreement including but not limited to the "VAIOT's Internal AML/CFT Procedures", "Privacy Policy", "Purchase Agreement for VAI Tokens", "VAIOT Whitepaper" as published on the VAIOT's Website or otherwise communicated to the Applicable Entity.

7.2. VAIOT shall ensure full compliance with the Fourth Anti-Money Laundering Directive (**Directive 2015/849**) being fully transposed into Maltese law by virtue of Legal Notice 372 of 2017, through ensuring compliance with **Cap 373** of the Laws of Malta – Prevention of Money Laundering Act and subsidiary legislation thereof: Prevention of Money Laundering and Funding of Terrorism Regulations **S.L. 373.01**, Civil Code (Second Schedule) (Register of Beneficial Owners - Associations) Regulations, **S.L. 16.15**, Prevention of Money Laundering and Funding of Terrorism Regulations, **S.L. 373.01**, L.N. 117 of 2018 - National Coordinating Committee on Combating Money Laundering and Funding of Terrorism Regulations, 2018 and related legislation thereof Criminal Code, Chapter 9, Implementing Procedures issued by the Financial Intelligence Analysis Unit in Terms of the Provisions of the Prevention of Money Laundering and Funding of Terrorism Regulations, Part I, issued on May 20, 2011 and last amended on January 27, 2017.

7.3. The new **EU Directive 2018/843** on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing (the **"5th AML Directive"**) has entered into force on 9 July 2018. As a member state Malta is required to implement the "5th AML Directive" into national law by 10 January 2020. Such transposition might result in the modification or amendment of this Policy as envisioned in the subsection 1.3.

8. Contact Details

If you have any further questions regarding this AML Policy, please contact Us at aml@vaiot.ai.