AML/KYC Policy

1. Introduction

(1) **Finteria Limited** (hereinafter the **"Company", "we", "our",** or **"us"**) is registered in the Republic of Marshall Islands (hereinafter the **"RMI"**) under registration number 121257 on August 7, 2023.

(2) The Company's business address is Trust Company Complex, Ajeltake Road, Ajeltake Island, Majuro, Marshall Islands.

(3) In accordance with the Law, the Company has set out policies and procedures for preventing money-laundering activities that aim to adhere to the principles of knowing your customer, monitoring the Client's activity, and keeping appropriate records.

(4) Please read this Anti-Money Laundering Policy carefully before signing the Agreement or engaging in any other way with the Company. You are required to read and understand it before using any of the Services. If you are in any doubt about any of the contents of this document, you should obtain independent professional advice.

(5) Our services are not being offered to any resident of or any person located or domiciled in the restricted jurisdictions as defined herein, as well as any region or any country or territory that is subject to country-wide or territory-wide sanctions, as well as to any person or entity subject to sanctions.

(6) In accordance with all regulatory requirements, such as identifying and knowing our clients:

(i) the Company does not allow the opening of anonymous or numbered accounts;

(ii) the Company does not open accounts for those who have criminal records, are under investigation, or are serving prison sentences;

(iii) the Company shall identify, monitor, and report any and all suspicious transactions;

(iv) the Company shall preserve all transaction records for a minimum of 5 years after the termination of contractual relationships with clients;

(v) the Company shall provide continuous training to its staff in order to enable recognition and reporting of any suspicious transactions to authorities as provided by applicable laws and regulations;

(vi) the Company shall have the right to request and verify proof of identification from its clients before opening an account and payment processing;

(vii) the Company shall refuse access to the trading platform and fund transfers at any point in time to the Client if the Client is suspected and/or identified in any way to be connected to criminal activities or money laundering.

(7) All Clients are required to comply with the Company's AML policy. By confirming the account registration, the Client unconditionally agrees to comply with all requirements of the Company's AML policy.

(8) As a responsible and liable member of the financial community, the Company puts all possible efforts in place to protect our Clients and maintain our impeccable reputation when it comes to AML/CTF and international financial sanctions measures.

2. Risk Considerations

(1) The broad objective is that we should understand at the outset of the relationship who our associates are, where they operate, what they do, and their expected level of activity with us. There are additional risk considerations relating to the position of the jurisdictions involved, their regulation and standing as regards the inherent money laundering (ML) and terrorist financing (TF) risk, and the effectiveness of their anti-money laundering and combating the financing of terrorism (AML/CFT) enforcement regime.

(2) Money laundering (ML) is the process of concealing or attempting to conceal the true origin and ownership of the proceeds of criminal activities in an effort to legitimate such funds.

It is accomplished in three stages:

- Placement – the physical disposal of cash proceeds derived from criminal activity. Among other things, placement may entail converting proceeds into financial instruments or bank deposits in a manner that will not raise suspicions.
- Layering – separating the illicit proceeds from their source by creating complex layers of financial transactions designed to disguise the audit trail and provide anonymity; and
- Integration – the provision of apparent legitimacy to wealth derived from crime. If the layering process succeeds, integration schemes place the laundered proceeds back into the economy in such a way that they re-enter the financial system appearing as normal business funds.

(3) Terrorist Financing (TF). Terrorist financing means the provision or collection of funds by any means, directly or indirectly, with the intention that they are used or in the knowledge that they are to be used, in full or in part, in order to carry out any offenses related to terrorism.

(4) There are factors suggesting the possibility of a higher risk of ML/TF activities, such as geographic location, associates, and type of service provided. During ML/TF risk assessment,

the above-mentioned factors are considered a priority to identify risk variables. When weighting factors, we should ensure that weighting is not unduly influenced by just one factor, economic or profit considerations do not influence the risk rating, and situations identified by national legislation or risk assessments as always presenting a high money laundering risk cannot be overruled by us.

(5) Meanwhile, there are some circumstances where the risk of money laundering or terrorist financing may be lower. In such circumstances, provided there has been an adequate analysis of the risk, we may apply simplified CDD measures: country of incorporation with a low risk of ML/TF, such as associates with a long-term and active business relationship with us. However, assessment of a jurisdiction as a low risk only allows for some easement of the level of due diligence carried out – it is not a complete exemption from the application of CDD measures in respect of associates identification.

(6) The most essential procedures the Company implements in order to achieve these are the following:

(i) identification and due diligence procedures of clients;

(ii) record-keeping procedures in relation to clients' identity and their transactions;

(iii) internal reporting procedures to a competent person (the MLRO) appointed to receive and consider information that gives rise to knowledge or suspicion that a client is engaged in money laundering activities;

(iv) appropriate procedures of internal control and risk management, with the purpose of preventing money-laundering activities;

(v) detailed examination of every transaction that, due to its nature, is considered vulnerable to money laundering, especially of complicated or unusually large transactions and transactions that take place without an obvious financial or legal purpose;

(vi) measures for making employees aware of the above procedures to prevent money laundering and of the legislation relating to money laundering; and

(vii) provision of regular training to employees to help them in the recognition and handling of transactions suspected to be associated with money laundering.

(7) We will conduct our KYC/CDD and activities monitoring based on a risk-based approach:

(i) for some Clients, determined by us to present a low risk of ML/TF, simplified KYC/CDD and monitoring may be applied;

(ii) in the case of high-risk profiles, enhanced KYC/ CDD measures (including, but not limited to, additional verification details or proof of sources of funds) and enhanced monitoring will be applied.

(8) Where the risks of ML/TF are higher, we must conduct enhanced due diligence measures consistent with the risks identified. In particular, we should increase the degree and nature of determining the business relationship. Examples of EDD measures that must be applied for highrisk business relationships include:

(i) obtaining and, where appropriate, verifying additional information on the potential Client and updating more regularly the identification of the potential Client and any beneficial owner;

(ii) obtaining additional information on the intended nature of the business relationship;

(iii) obtaining information on the source of funds of the potential Client;

(iv) obtaining information on the reasons for intended or performed transactions;

(v) obtaining the approval of senior management to commence or continue the business relationship.

(9) Clients that are deemed to present a high risk are, but not limited to:

(i) clients whose identification process is incomplete;

(ii) clients that have discrepancies in provided ID Information and documents;

(iii) clients qualified as PEPs (Politically Exposed Persons) or persons known to be close associates of PEPs;

(iv) clients who have been prosecuted for financial crimes;

(v) Clients on a terrorist wanted and/or other sanction lists: the United Nations (UN) Security Council consolidated sanctions list, the EU's consolidated list of persons, groups, and entities, the US Department of the Treasury, Office of Foreign Assets Control (OFAC) sanctions lists, the US Department of the Treasury, Financial Crimes Enforcement Network (FinCEN) list, the UK HM Treasury (HMT), Office of Financial Sanctions Implementation, "consolidated list of targets").

(10) When dealing with the potential ML risks of those Clients that are determined to be at higher risk as the result of our risk assessment process, we may apply one or more of the following measures and controls:

(i) increased awareness by us of higher-risk situations within business lines across the Company;

(ii) enhanced levels of KYC or CDD;

(iii) escalation for approval of the establishment of a business relationship;

(iv) enhanced monitoring of transactions; and

(v) enhanced levels of ongoing controls and reviews of relationships.

(11) Application of Risk Criteria. The same measures and controls may often address more than one of the risk criteria identified, and it is not necessarily expected that we will apply specific controls targeting each and every risk criterion set forth in this KYC/AML Policy.

(12) Receiving funds payable through accounts and shell banks or any financial institutions from Restricted Jurisdictions is forbidden. We shall report all transactions that involve suspicious banks and territories. Clients are prohibited from using our Services for the assets received from any illegal or otherwise restricted services and products under applicable law.

(13) Restricted Jurisdictions. We do not provide Services to any person who is a citizen or resident (tax or otherwise) of any jurisdiction that is:

- a Restricted Jurisdiction;
- any country or territory that is subject to country-wide or territory-wide sanctions.

(14) Therefore, we deny entering into an Agreement and providing Services to any natural person or legal entity when the KYC and CDD procedures identify a potential or existing Client as a citizen or a resident of the jurisdictions listed herein.

(15) Clients should assume that all information provided to the Company is available to the competent regulatory authorities in:

- the country of incorporation of the Company;
- the country of origin of any funds transmitted to the Company; and
- the destination country of any funds refunded by or withdrawn from the Company.

(16) Third-party or anonymous payments shall not be accepted. If the Company is not confident that the Client is the sender of the money, it reserves the right to reject the deposit and return it to the remitter with any transfer fees or other charges deducted. The Company further reserves the right to terminate your account held with us with immediate effect.

3. Client Identification and Verification (KYC and CDD)

(1) The objective of KYC and CDD is to identify Clients and verify their identity. We may ask you either at the time of registering as a Client or periodically for purposes of updating records and ongoing CDD and procedures to provide ID Information and certain documents.

Natural persons may be required to provide the following documents:

(i) a national passport or its notarized copy;

(ii) proof of residence (a certificate of residence, a utility bill, or a bank statement with details of residence) or its notarized translation issued within 3 months before the date they are provided to us;

(iii) lease agreement for the premises with an unexpired term;

(iv) valid ID card of a foreign resident or a valid driving license.

Legal entities may be required to provide the following documents:

(i) a certified excerpt of the registry of commerce (or equivalent) in English;

(ii) bylaws in English;

(iii) share certificates;

(iv) director's appointment resolution;

(v) a national passport of the Client's director or its notarized copy with an apostille;

(vi) a national passport of the Client's beneficial owner;

In case a director or an owner of the Client is a legal entity, and the Client is also a legal entity, all the documents set forth above must be provided.

Company directors:

Company directors, as well as other persons with significant control, are subject to enhanced due diligence verification procedures which include screening against PEP and sanctions lists. When another person deals with assets under a power of attorney, that person, as well as the company director, should also undergo screening against PEP and sanctions lists.

Beneficiary (beneficial owner)

The ML Regulations define beneficial owners as individuals either owning or controlling more than 25% of body corporates or partnerships or otherwise owning or controlling the partner. These individuals must be identified, and reasonable measures must be taken to verify their identities. It is obligatory to know the names of all individual beneficial owners owning or controlling more than 25% of the company's shares or voting rights (even where these interests are held indirectly) or who otherwise exercise control over the management of the company.

The obligation to verify the identity of a beneficial owner is for our company to take reasonable measures so that we are satisfied that we know who the beneficial owner is. It is up to us to make a decision on whether it is appropriate, in consideration of the money laundering or terrorist financing risk associated with the business relationship, to make use of records of beneficial owners in the public domain, ask our associates for relevant data, and require evidence of the beneficial owner's identity on the basis of documents information obtained from a reliable source which is independent of the associates, or obtain the information in some other way.

In low-risk situations, it may be reasonable to confirm the beneficial owner's identity based on information supplied by the associates. This could include information the associates provide (including trustees or other representatives whose identities have been verified) as to their identity and confirmation that they are known to the associates.

(2) All documents provided by a Client to the Company must:

(i) be issued by state authorities;

(ii) have a photo of the holder, full name, document number or a personal number of the holder, and date of birth (in its absence, we request an additional document, if there is any, with the specified date of birth); (iii) be valid and up to date.

(3) Where identity is verified electronically, we can apply an additional verification check to manage the risk of impersonation fraud. For example, one of these checks may require a copy of documents to be certified by an appropriate authority.

(4) Third-Party Authentication. As a part of the verification process, we reserve the right to request one or more appropriate third-party service providers to assist us in the authentication and/or verification of the valid documents and other incidental details provided by you.

(5) Independent Sources. We reserve the right to conduct the verification of identity by verifying some of the ID Information against documents or information obtained from a reliable source, which is independent of the Client.

(6) Authentication Through Visit. We reserve a right to pay visits to the places where you or the controlling person or beneficial owner of the assets carry on your/their business activity.

(7) Enhanced KYC/CDD. In addition to standard KYC/CDD procedures, we also reserve the right to apply additional KYC/CDD measures outlined in this KYC/AML Policy when:

- there is a suspicion of ML/TF, regardless of any derogation, exemption, or threshold;
- there are doubts about the veracity or adequacy of previously obtained ID Information and documents;
- new ID Information or documents have been provided by you.

(8) Information Update. For the purposes of the implementation of this KYC/AML Policy and ML/TF risk mitigation and to ensure that the information that we hold on to you is always accurate and up to date, you are required to provide us with updated ID Information and applicable documents in order to continue using our Services in any of the following cases:

- at any time, you obtain a new ID document instead of the previous one;
- at any time, you change your personal identity number (if applicable);
- at any time, you change your name or part of it;
- at any time, you change phone number, email address, or residential address;
- at any time, there is a new director and/or a beneficial owner of the Client (if the Client is a legal entity).

While using our Services, you will also be asked to update your ID information:

- once every 12 months if you are a Low and Medium Risk Profile Client;
- once every 6 months if you are a High-Risk Profile Client.

(9) We do our best to protect your ID Information and provide documents in accordance with the applicable laws and regulations.

4. Amendments to the policy

(1) We reserve the right to update this KYC/AML Policy at any time with immediate effect by adopting an updated version of the Policy. All such changes will take effect once they have been approved by the Company's authorized representative and updated on the Company's website. If you continue using the Services, you are deemed to accept any such changes. Where possible, the Company may give notice of KYC/AML Policy changes to you by email to your last known email address, such notice being effective immediately.

(2) It is important that you review this KYC/AML Policy on a regular basis to ensure that you are familiar with the terms in force and/or any changes made to them. If you do not agree to any amendments, you must discontinue using our Services and contact us to terminate the Agreement.

5. Definitions

Agreement means the asset management agreement that is being entered into between you and the Company.

AML/CTF means anti-money laundering and counter-terrorism financing.

CDD means customer due diligence.

Client or you, your means a natural person or a legal entity using the Services.

ID Information means the information we obtain about you in order to provide the Services to you, which may include:

(i) for a natural person: full legal name, date of birth, national passport or other valid ID numbers, date and place of issue and expiration date of such document, title, gender, residential address, telephone number, email address, marital status, job title or profession and other identification information as might be required by us;

(ii) for a legal entity: entity's name, registration address, the jurisdiction of incorporation, registration number, tax number, if applicable, telephone number, email address, information on directors and shareholders, including the information set forth in Clause 1 of this document.

If necessary, the required ID Information may be provided to you by us in a separate KYC document. We reserve the right to request any additional information as we may deem appropriate at the time.

KYC means know your customer.

KYC/AML Policy means this Know Your Customer and Anti-Money Laundering Policy.

Politically Exposed Person or PEP means a natural person who is or who has been entrusted with prominent public functions including, but not limited to:

- head of state;
- head of government;
- minister and deputy or assistant minister;
- member of parliament or a similar legislative body;
- member of a governing body of a political party;
- member of a supreme court;
- member of a court of auditors or the board of a central bank;
- ambassador or chargé d'affaires
- high-ranking officer in the armed forces;
- member of an administrative, management, or supervisory body of a state-owned enterprise;
- director, deputy director, and member of the board or equivalent function of an international organization, except middle-ranking or more junior officials.

Restricted Jurisdictions means the jurisdictions where the Company does not offer its Services or operate in any other way. The complete list of Restricted Jurisdictions is set forth in Schedule 1 of this KYC/AML Policy.

Risk Profile means a risk assessment of the Client Profile which allows determining the necessary corresponding mitigating due diligence measures to be taken, where a Client Profile is an individual profile of the Client assembled based on the information gathered via the registration and KYC process.

Services mean asset management services that are offered by us.

Shell bank means a bank that has no physical presence, namely meaningful mind and management located within a country, in the country in which it is incorporated and licensed, and which is unaffiliated with a regulated financial group that is subject to effective consolidated supervision.

Virtual Currency means a digital representation of value that is not issued or guaranteed by a central bank or a public authority, is not necessarily attached to a legally established currency, and does not possess a legal status of currency or

money but is accepted by natural or legal persons as a means of exchange and which can be transferred, stored, and traded electronically.

6. Schedule 1

- the Democratic People's Republic of Korea (DPRK)
- Eritrea
- the Islamic Emirate of Afghanistan
- the Islamic Republic of Iran
- Libya
- the Republic of Cuba
- the Republic of Iraq
- the Republic of the Union of Myanmar (formerly Burma)
- Sudan
- Syria
- United States
- Canada
- Japan