ANTI-MONEY LAUNDERING AND COMBATING THE FINANCING OF TERRORISM POLICY

Effective Date: March 5, 2023

1. General Framework

We have no tolerance for money laundering, the financing of terrorism or any other form of illicit activity, and are committed to implementing appropriate policies, procedures and controls to prevent those activities. Our policies are shaped by industry best practices, a risk-based approach and the effective anti-money laundering standards applied worldwide. These policies apply, without exception, to all employees of Headframe Technologies - FZCO (the "**Company**" or "**we**" or "**us**"), its board members, officers and directors, as well as to its subsidiaries.

The purpose of this policy is to provide to the Company's customers, service providers, suppliers, consultants, agents, vendors, contractors and other partners, employees, law enforcement and other concerned stakeholders a high-level and summarized overview of the Company's main AML/CTF policies and procedures. By no means is this content to be considered as the whole set of all policies, procedures and controls that are implemented and in place by the Company for prevention of money laundering, financing of terrorism and other forms of illicit activity.

This document and all underlying policies, processes and procedures are prepared in line with provisions, requirements and recommendations of FATF Guidance for a Risk-Based Approach to Virtual Assets, Virtual Assets Service Providers and UAE Virtual Assets Regulatory Authority and the Law No. (4) of 2022 Regulating Virtual Assets in the Emirate of Dubai and other applicable laws and regulations.

Under certain circumstances (i.e. the use of certain Headframe, its affiliates' and partners' products and services) the Company is required to identify and verify its customers' identities appropriately, conduct ongoing monitoring of their activity (including transaction monitoring), maintain records of customers' activity and related documents.

The Company understands Money Laundering as:

(a) the conversion or transfer of property, knowing that such property is derived from criminal activity or from an act of participation in such activity, for the purpose of concealing or disguising the illicit origin of the property or of assisting any person who is involved in the commission of such an activity to evade the legal consequences of that person's action;

(b) he concealment or disguise of the true nature, source, location, disposition, movement, rights with respect to, or ownership of, property, knowing that such property is derived from criminal activity or from an act of participation in such an activity;

(c) the acquisition, possession or use of property, knowing, at the time of receipt, that such property was derived from criminal activity or from an act of participation in such an activity; and

(d) participation in, association to commit, attempts to commit and aiding, abetting, facilitating and counselling the commission of any of the actions referred to in points above.

The Company understands Terrorist financing as provision of funds for terrorist activity, meaning as the provision or collection of funds, by any means, directly or indirectly, with the intention that they be used or in the knowledge that they are to be used, in full or in part, in order to carry out any of the offences within the meaning of applicable laws and regulations. This activity is done by intentionally killing, seriously harming or endangering a person, causing substantial property damage that is likely to seriously harm people or by seriously interfering with or disrupting essential services, facilities or systems.

2. Risk-Based Approach

The Company takes a risk-based approach (the "**RBA**") towards assessing and containing the money laundering and terrorist financing risks arising from any transactions it has with customers and uses all available data when reviewing customers activity.

The Company performs a risk-based due diligence and collects necessary information and documentation on each prospective customer in order to assess the risk profile. Before entering into a customer relationship, necessary checks are conducted in line with the RBA so as to ensure that the identity of the customer does not match with an entity with a known criminal background or with banned entities, such as terrorist organizations. Enhanced due diligence is required for clients who are deemed to be of high risk, especially those for whom the business activity (sources of funds) are not clear, or for transactions of higher value and frequency, which can be determined by the Company at its sole and absolute discretion.

The Company's employees exercise care, due diligence and good judgement in determining the overall profile and business nature of its customers. The Company conducts its business in accordance with the highest ethical standards and may decide not to enter into a customer relationship that can adversely affect the Company's business or reputation.

For the purpose of identification, assessment and analysis of risks related to its activities, the Company has established a risk assessment, taking account of the following factors:

(a) customer risk;

(b) geographical risk;

(c) product risk;

(d) delivery channel risk.

After the risk is assessed and attributed to a particular customer, depending on the assigned degree of risk, it will be revised periodically upon knowledge of the customer and its activities.

3. Customer Due Diligence

We require all business clients to undergo due diligence or Know Your Customer (KYC) checks before using certain services (i.e. virtual assets disposal, etc.). This includes, without limitation:

(a) a high-resolution, clearly readable, non-expired, detailed and verifiable copy of the Company incorporation document. This must include details on the ownership of the Company, its address, tax number, website, purpose and activities;

(b) a description of the sector and business activities and corresponding website, which must be registered under the same entity name as the certificate of incorporation provided; and

(c) details of the bank account of the customer.

Additionally, for any customers which are deemed to be of high risk, the identity verification may include:

(a) a high-resolution, clearly readable, non-expired copy of the business beneficial owners' government-issued ID or passport, national identity card and/or a driver's license;

(b) a high-resolution, clearly readable, non-expired proof of address document not older than 3 months. The document must carry the customer's business name and address (recent utility bill or bank statement); and

(c) a video conference with the account holder/business contact person and/or company director(s), if deemed necessary.

Further documentation may be required for businesses with high-risk profile.

Care must be taken that all documents provided are true copies of the original. Providing false, forged, modified or documents meant to deceive will be considered fraud and treated as such.

The Company may use recognized and specialized electronic providers for the technical acquisition of the customer's identity data. The Company may also decide to use the following non-documentary methods of verifying identity:

(a) independently verifying the customer's identity through the comparison of information provided by the customer with information obtained from a consumer reporting agency, public database or other source;

(b) checking references with partnering financial institutions;

(c) analysing whether there is logical consistency between the identifying information provided, such as the customer's name, street address, postal code, and date of birth;

(d) utilizing complex device identification (such as "digital fingerprints" or IP geolocation checks); and

(e) obtaining a notarized or certified true copy of an owner, manager, shareholder or UBO's government-issued ID for valid identification.

When there shall be any suspicion of illicit activity including money laundering or terrorism financing activities, or where there shall be any doubt about the adequacy or veracity of previously obtained customer's identification data, further due diligence measures shall be undertaken, including verifying the identity of the customer once again and obtaining information regarding the purpose and intended nature of the relationship with the Company.

4. Compliance Officer

A Compliance Officer performs all AML/CTF functions at the Company. A Compliance Officer reports directly to the management board and has the competence, means and access to relevant information across all the structural units of the Company.

Only a person who has the education, professional suitability, the abilities, personal qualities, experience and impeccable reputation required for performance of the duties listed below may be appointed as a Compliance Officer.

The duties of a Compliance Officer include, among others:

(a) organisation of the collection and analysis of information referring to unusual transactions or transactions or circumstances suspected of money laundering or terrorist financing, which have become evident in the activities of the Company;

(b) periodic submission of written statements on compliance with the requirements the management board of the Company;

(c) performance of other duties and obligations related to AML/CTF compliance by the Company;

(d) Updating internal policy document, business and customer risk assessment regularly.

5. Rules of Procedure & Internal Controls

The Company has developed and implemented rules of procedure that allow for effective mitigation and management of risks relating to money laundering and terrorist financing, which are identified in the risk assessment performed in accordance with the Company's risk-based approach. Each employee of the Company must strictly adhere to rules of procedure set forth herein.

The rules of procedure consist of the following:

(a) a procedure for the application of due diligence measures to the customer, including a procedure for the application of simplified and enhanced due diligence measures;

(b) a model for identification and management of risks relating to a customer and its activities and the determination of the customer's risk profile;

(c) the methodology and instructions where the Company has a suspicion of money laundering and terrorist financing or an unusual transaction or circumstance is involved;

(d) the procedure for data retention and making data available;

(e) instructions for effectively identifying whether a customer or any associated person (in case of customer being a legal person) is a politically exposed person or a politically exposed person subject to international sanctions.

The Company applies at least the following due diligence measures:

(a) requests identification of the Company based on documentation submitted by the customer;

(b) requests identification of the Company's sector of activity, place of incorporation and public profile (where applicable);

(c) verifies the Company-related information and documentation submitted by the customer;

(d) requests identification of the beneficial owner(s) at the proper tier level, for the purpose of verifying their identity, taking measures to the extent that allows the Company to make certain that it knows who the beneficial owner is, and understands the ownership and control structure of the customer;

(e) performing additional due diligence for the customer and its transactions, as necessary per established risk assessment policies and procedures;

(f) maintains ongoing monitoring of the business relationship and transactions.

6. Simplified Due Diligence

The Company may apply simplified due diligence (the "**SDD**") measures where a risk assessment prepared on the basis of these rules of procedure identifies that, in the case of the jurisdiction, economic sector of activity or amounts transacted the risk of money laundering or terrorist financing is lower than usual.

Before the application of the SDD measures to a customer, an employee of the Company establishes that the business relationship, transaction or act is of a lower risk and the Company attributes to the transaction, act or customer a lower degree of risk.

The application of the SDD measures is permitted to the extent that the Company ensures sufficient monitoring of transactions, acts and business relationships, so that it would be possible to identify unusual transactions and allow for notifying of suspicious transactions in accordance with these rules of procedure.

7. Enhanced Due Diligence

The Company applies enhanced due diligence (the "**EDD**") measures in order to adequately manage and mitigate a higher-than-usual risk of money laundering and terrorist financing.

EDD measures are applied always when:

(a) prior to client onboarding:

  (i) upon analysis of submitted customer information and documents, there are reasonable doubts as to the truthfulness of the submitted data, authenticity of the documents or the true purpose of its business activities;

  (ii) the customer is engaged in a sector or activity classified as high-risk;

  (iii) the customer is incorporated in a jurisdiction classified as high-risk (e.g. in jurisdictions that have not established effective AML/CTF systems that are in accordance with the recommendations of the Financial Action Task Force);

(b) after client onboarding:

  (i) when the client processed transactional volume exceed the assigned risk threshold for the customer;

  (ii) if unusual or suspicious patterns of activity are detected;

  (iii) if a transaction request is not consistent with a customer's stated business activity.

The Company also applies EDD measures whereas the assessment of risk is assessed as higher, in accordance to its internal policies and procedures.

8. Sector and Jurisdiction Restrictions

We do not serve customers from certain jurisdictions that are deemed too high-risk and/or unwelcoming from a legal, regulatory or sanctions perspective.

While it's beyond our scope to set policies for the customer's own business dealings, we reserve the right to not serve customers who have business activities, clients or otherwise participate in transactions originating from certain jurisdictions.

It goes without saying that we can't provide services to any customer that isn't legally established or is offering illegal goods or services in their operating jurisdiction(s). Besides this base consideration we also cannot serve customers who operate in certain restricted sectors.

We update and review those lists periodically, taking into account a range of international policies and recommendations.

Attempts to circumvent this policy, by providing false, forged or modified documents meant to deceive or mislead will be considered fraud and will result in banning the customer from using our services.

9. Politically Exposed Persons

Politically Exposed Persons (the "**PEP**") (as well as their families and persons known to be close associates, as described below) are required to be subject to EDD. This is because international standards issued by the Financial Action Task Force recognize that a PEP may be in a position to abuse their public office for private gain and a PEP may use the financial system to launder the proceeds of his abuse of office.

PEP means a natural person who is or who has been entrusted with prominent public functions including:

(a) head of State;

(b) head of government;

(c) minister and deputy or assistant minister;

(d) a member of parliament or of a similar legislative body;

(e) a member of a governing body of a political party;

(f) a member of a supreme court;

(g) a member of a court of auditors or of the board of a central bank;

(h) an ambassador, a chargé d'affaires and a high-ranking officer in armed forces;

(i) a member of an administrative, management or supervisory body of a State-owned enterprise;

(j) a director, deputy director and member of the board or equivalent function of an international organisation.

PEP does not include middle-ranking or junior officials.

Family member of a PEP means the spouse, or a person considered to be equivalent to a spouse, of a PEP or local PEP; a child and their spouse, or a person considered to be equivalent to a spouse, of a PEP or local PEP; a parent of a PEP or local PEP.

A person known to be a close associate of a PEP means a natural person who is known to be the beneficial owner or to have joint beneficial ownership of a legal person or a legal arrangement, or any other close business relations, with a PEP or a local PEP; and a natural person who has sole beneficial ownership of a legal entity or legal arrangement which is known to have been set up for the de facto benefit of a PEP or local PEP.

While the Company does not accept natural persons as customers, the PEP definition and classification still applies to the beneficial owners of the business and may constitute an additional factor of risk.

10. Sanctions

Dealing with persons who are subject to international sanctions poses a great risk to the Company, its directors, officers and owners. The Company may employ automated screening software to identify and block known virtual asset addresses associated with sanctions and numerous illegal and high-risk activity. All verified matches are automatically blocked and the matter is escalated to a Compliance Officer for further analysis and appropriate actions.

11. Suspicious Activity

An internal investigation into suspicious activity will try to establish the true motivation behind the activity in question. This may result in confirmation of the suspicious activity or removal of reasonable doubt. If suspicious activity is confirmed, the issue will be escalated accordingly.

Where the Company identifies an activity or facts whose characteristics refer to the use of criminal proceeds or terrorist financing or other criminal offences or an attempt thereof or with regard to which the Company suspects or knows that it constitutes money laundering or terrorist financing or the commission of another criminal offence, a Compliance Officer must act accordingly.

When such suspicious activity is detected, the Compliance Officer will determine whether a filing with appropriate authority is necessary. The Company and all its employees, officers and directors are prohibited to inform customer, its beneficial owner, representative or any third party of an intention to submit a report, any submission made, as well as about the commencement of any proceedings by relevant authorities.

12. Termination of Services

The Company reserves the right to deny or terminate servicing a customer or relevant account at any time in line with the terms stipulated in the User Service Agreement if suspicion arises that such customer (user) or account is involved with or connected with money laundering, criminal activity, terrorist financing or any other predicate offense to money laundering or terrorist financing.

13. Data Retention

The Company is obligated to retain all documents and information which was served for identification and verification purposes by the customer for certain period of time.

The Company implements necessary rules for the protection of personal data upon application of the requirements arising from its obligations hereunder.

The Company is allowed to process personal data gathered upon implementation of these rules only for the purpose of preventing money laundering and terrorist financing and the data must not be additionally processed in a manner that does not meet the purpose, for instance, for marketing purposes unless a proper consent has been provided by the customer.

14. Training

The Compliance Officer shall ensure that Company's employees are fully aware of their obligations under the AML/CTF regime, by introducing a complete employees' education and training program.

The timing and content of the training provided is determined according to the needs of the Company. The frequency of the training can vary depending on the amendments of legal and/or regulatory requirements, employees' duties as well as any other changes in the business model. The training program aims at educating the Company's employees on the latest developments in the prevention of money laundering and terrorist financing, including the practical methods and trends used for this purpose.

15. Cooperation and Information Requests

The Company is required to cooperate with authorities in preventing money laundering and terrorist financing, thereby replying to queries within a reasonable time. We comply with law enforcement bodies requests for information where it pertains to specific orders.

We will not and do not voluntarily disclose non-public information to a requesting party. The Company will only disclose non-public user information if it has received consent of the user and in response to a legitimate and an enforceable subpoena, court order or search warrant from a body that has jurisdiction to compel the Company to disclose that information. Please note that in case you represent the law enforcement agency, procedure under the Mutual Legal Assistance Treaty ("**MLAT**") shall apply to any cross-border requests.

General Guidelines for Requests:

A. When law enforcement agencies request non-public information (such as a client personal or financial information), we will not share this information unless an enforceable court order, subpoena or search warrant has been issued, received and validated as legitimate.

B. We will notify affected customers if we believe we are legally required to provide their personal or financial information to a law enforcement agency, unless we are prohibited by law from doing so.

C. When law enforcement agencies request information about a customer, we cannot and will not provide information about such customers who are not our customers or platform users. We consider this information to be in the possession, control and custody of the customer, who is the controller and processor of such information. If law enforcement agencies request this information, such requests for information should be directed to the relevant customers and not us.

D. Only information specifically requested and clearly outlined in an enforceable court order, subpoena or search warrant will be disclosed.

This policy does not constitute legal advice or a promise or guarantee that we will respond to any requests for information in a specific way, timeframe or at all. All legal requests for information are evaluated on a case-by-case basis. We reserve the right to change this policy or these guidelines in our sole discretion at any time.

When requesting the confirmation of the existence of data on our platform the law enforcement agency must be very specific about what information it is looking to obtain as we may not be able to respond to vague, ambiguous or blanket requests. Certain identifiers may be helpful in determining whether we currently retain the requested information.

Submitting a Request:

All legal requests must be submitted by email to compliance@headframe.dev, originating from an email address domain of a recognized government or enforcement authority.

To aid the expeditious review of information requests received, law enforcement officers must include at least the following information in their request:

(a) name of the law enforcement authority;

(b) proof that the officer is authorized to request the information (proof of authority) and current position within the law enforcement organization;

(c) proof of identification of the requesting officer within the law enforcement organization (e.g. photo or other official ID which includes badge number, internal ID number);

(d) email address from a government domain;

(e) contact information (email address, phone number) from the governmental organization;

(f) the name of the legal entity that the request is addressed to;

(g) details of the request, including:

  (i) the subpoena / court order identification number in the subject line;

  (ii) instructions on how we should authenticate the subpoena as valid (e.g. call-back procedure);

  (iii) any public address or transaction IDs in either plain, excel or comma-separated file formats (images or PDFs are not accepted);

  (iv) a reasonable deadline for the request;

  (v) an official and enforceable court order, subpoena or search warrant;

  (vi) the reason for the requested information (e.g. possible crimes in question);

  (vii) MLAT request for cross-border law enforcement (if applicable).

Please do note that failure to include all the mandatory information stated above may result in delayed response times and/or no response.