Rules of procedure and internal audit rules prepared pursuant to the Money Laundering and Terrorist Financing Prevention Act

Description

EVE is a full-service mobile based crypto exchange and high-security wallet. EVE provides the possibility for users to trade over 400 cryptocurrencies across 18 different blockchains. We also provide a payments services solution for businesses that would like to accept crypto payments online or in person.

Business benefits compared to other projects

EVE offers users the highest security possible, our system is built using Fireblocks the same technology which Banks and Institution al traders use to manage billions of dollars in crypto assets. This service removes the possibility of any single point of failure, making the application highly resilient to hacking or other digital attacks.

Our trading engine sources liquidity from over 20 different exchanges and liquidity providers, meaning when users trade they will get best price execution and limited slippage when compared to trading on traditional exchanges.

Crypto currencies involved

We currently support the following crypto currencies:

1INCH AAVE ADA ALCX ALGO AMP ANKR ANT API3 ATOM AUDIO AVAX AXS BAL BAND BAT BCH BNB BNT BOND BTC BZRX CAKE CELO CFG CHR CHZ CLV COMP CONV CQT CREAM CRO CRV CSPR CTSI CTX CUBE CVP DOGE DOT EGLD ENJ EOS ETH EXRD FIL FET FLOW FTM FTT GRT HBAR HOPR HT ICP ICX IOST IOTX KAVA KEEP KIN KNC KSM LINK LON LPT LRC LTC LUNA MANA MATIC MINA MINDS MIR MKR MTA NEAR NEO NEXO NKN NU OCEAN OGN OMG ONE OPIUM OXT OXY PERP QTUM RARI REEF REN RENBTC RENDOGE REQ RFIL RLC RLY RNDR RSR RUNE RVN SAND SBTC SETH SHIB SKL SNX SOL SRM STMX STORJ STX SUSHI THETA TRB TRX TWT UMA UNI VET VTHO WBTC WCELO WCUSD WFIL WOOFY XDC XEM XLM XTZ XVS YFI YFII YLD YOP ZEE ZEN ZIL ZRX CEL SUKU UMB XRP.

The full list of available cryptocurrencies may not be reflected in this policy but are available on our website.

Pairs may be available with the following stable coins:
DAI USDT USDC PAX TUSD BUSD HUSD CUSD GUSD UST

Pairs may be available with the following fiat currencies:
USD EUR GBP

Procedural Rules and Internal Control Regulations
The company has no tolerance for money laundering, the financing of terrorism or any other form of illicit activity, and is committed to implementing policies, procedures and controls shaped by the best industry practices and the most effective anti-money laundering standards.

These rules apply to, without exception, all employees of the Company, its Board members, officers, contractors, and consultants.

The purpose of this document is to provide the Company's partners, clients, vendors, contractors,

employees, regulators, law enforcement and other concerned stakeholders with a high-level overview of the Company's AML/CTF compliance regime elements and procedures. This document shall not be read as an entire set of all policies, procedures and controls in place implemented 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 and Virtual Assets Service Providers.

The Company understands ***money laundering*** as:

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;

The 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;

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;

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 (a), (b) and (c).

The company understand terrorist funding 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 Articles 1 to 4 of Council Framework Decision 2002/475/JHA. Terrorist activity has as its main objective to intimidate a population or compel a government to do something. This 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.

Client identification

The following information will be requested to identify clients:

ID/passport

Passport/ID of applicant showing all information clearly.
Image of the applicant holding Passport/ID.
The uploaded document must be readable, of good quality and with all relevant data provided in English alphabet character.

Source of wealth

In the event the initial deposit will be in cryptocurrency the wallet address will be evaluated by chainanaysis or similar software.
The applicant must provide a history of the source of wealth. Source of wealth means the details of the bank account that the investment funds come from.

Proof of address:

Bank Statement or Utility bill

Control of documents provided by clients:

All data on our clients will be stored in our office in digital format.
All client data will be carefully checked by our KYC/AML processor. If the applicant will raise suspicion of our specialists, the company will be unable to open an account.
All documents submitted by those who wish to purchase tokens (passport copy, bank statement, cryptocurrency wallet balance, proof of residence) will be checked and stored for 5 years. These documents will be verified for authenticity.
Such data will be stored for 5 years.

Customer risk

Customer due diligence measures are applied based on risk sensitive basis, the nature of the business relationship or transaction and the risks arising therefrom shall be taken into account upon selection and application of the measures. Risk-based customer due diligence calls for the prior weighing of the specific business relationships or transaction risks and, as a result thereof, qualification of the business relationship in order to decide on the nature of the measure to be taken (for instance, normal, enhanced or simplified due diligence measures could be applied).

If the risk level of a customer or a person participating in a transaction is low, the Company may apply simplified due diligence measures, but may not skip customer due diligence entirely. If the risk level arising from a customer or a person participating in a transaction is high, enhanced due diligence measures will be applied.

To ensure the prevention of money laundering and terrorist financing, the Company does not process transactions or establish relationships with anonymous or unidentified persons. The company shall reject relationships If a person fails to provide sufficient information to identify the person or about the purpose of the transactions or if the operations of the person involve a higher risk of money laundering or terrorist financing.

Legislation requires the Company to terminate a continuing contract without the advance notification if the person fails to submit sufficient information for application of customer due diligence measures.

General Obligatory Identification Rules

The Code of Conduct for the application of customer due diligence requires the identification and verification with persons with whom the Company has no previous business relationships.

Economic or professional activities via agents and outsourcing

The Company has the right, taking account the special requirements and restrictions provided by law, to use the services of a third party under a contract the subject of which is the continuing performance of activities and continued taking of steps required for the provision of (a) service(s) by the Company to its customers and that would normally be performed and taken by the Company itself.

The Company shall choose the third party in order to ensure the ability of the person to fulfil the requirements provided for in the Money Laundering and Terrorist Financing Prevention Act and to ensure the reliability and the required qualifications of such a person.

Upon outsourcing an activity the Company shall ensure that the third party has the knowledge and skills required, above all, for the identification of situations of a suspicious and unusual nature

The outsourcing contractor shall specify the rights and duties of the Company upon reviewing compliance by the third party with the requirements provided by law. The outsourcing of economic activities to a third party shall not impede state supervision over the Company and the latter shall, under contract, grant competent authorities access to the third party for supervisory purposes to whom the Company has outsourced its duties, tasks or functions.

The Company shall immediately notify the Financial Supervision Authority of entry into a contract serving as the basis for outsourcing its activity (activities)

Risk-based approach

The Company shall recognize, assess and understand money laundering and terrorist financing risks in its own activities and in the activities of its customers and take measures to mitigate the risks. The applicable measures shall correspond to the identified risk level.

In the event of the risk-based approach, the Company shall assess the probability of the realization of risks and what the consequences of their realization are. Upon assessment of probability, the chance of an increase in the threat and the possibility of occurrence of the respective circumstances shall be taken into account, e.g. the possible threats that may influence the activities of the customer and the service provider shall be taken into account.

The Company shall take all customer due diligence measures. The scope of taking the measures depends on the characteristics of the given business relationship or the risk level of the person or customer.

Upon identifying and substantiating the risk levels of a customer or a person participating in a transaction, the Company shall consider, among other things, the following risk categories:

Customer risk whose factors arise from the person or customer participating in a transaction; among other things, the following shall be considered:

Circumstances (including suspicious transactions identified in the course of a prior business relationship) resulting from the experience of communicating with the person, its business partners, owners, representatives and any other such persons.

Whether the person renders the service to anonymous customers.

Risk level assessment (overview)

National identity

Representatives of **Eve Exchange** rejects clients from high-risk countries: (http://www.fatf-gafi.org/countries/#high-risk)

Specific risks related to virtual currency trade and means of risk mitigation

The AML/CFT risks specific to virtual currency trade are:

The anonymity provided by the trade in virtual currencies on the internet.

The limited identification and verification of participants.

The lack of clarity regarding the responsibility for AML/CFT compliance, supervision and enforcement for these transactions that are segmented across several countries.

The lack of a central oversight body.

The Company and its employees shall apply the following means to mitigate the above specific risks:

Transactions of virtual currency trade and exchange shall be made using the customer's bank account The Company shall not engage in any transactions where a party to the transaction remains anonymous or the party cannot be sufficiently identified according to the present rules

Upon each transaction whereby the value of the transaction exceeds 15,000 euros or an equal sum in another currency the Company shall require from customers evidence of the source of the virtual currency used by the customer in the transaction.

Transaction control

If the transaction value exceeds 15,000 EUR or the party to a transaction is a person from a high-risk country or suspected of criminal activity, money laundering or terrorism financing, the company will request additional information about the origin of funds.

After receiving information, data will be checked by our specialists and risk assessment will be performed for a particular transaction.

Simplified control

If transaction value does not exceed this amount and the client is not a person from a high-risk country, client data will be recorded by our specialists in a simplified form. All documentation will be stored for at least 5 years.

Risk level assessment (overview)

The risk level will be assessed by the combinations of the following parameters:

1 Risk classification

To ensure the best control of risks emanating from clients, **Eve Exchange classifies** clients into three risk categories: low, medium and high. Each category has certain control restrictions/specifics described further in this document.

Low risk
Low risk is assigned to clients having a risk status of 0 through 4.

Medium risk

Medium risk is assigned to clients having a risk status of 5 through 8.

High risk

High risk is assigned to clients having a risk status of 9 through 12. High risk clients are subject to having their client agreements terminated.

The risk statuses are assigned according to the risk scale which ranges from 0 to 12, where 0 means the lowest risk and 12 means the highest risk. The risk score is determined upon analysis of data collected from clients. The risk status is assigned according to the final score on the risk scale. Risks are assessed on the basis of several criteria which are outlined below:

- Country of registration.
- Type of registration, i.e. physical person or legal entity.
- Screening results (e.g. sanctions, adverse media, PEP).
- Planned investments.
- Duration of relationship with the client.

For the purpose of this policy, the assessment and monitoring of the above criteria are performed in three steps:

Step 1 – Pre-application client classification.
Step 2 – Client application handling.
Step 3 – Post-application client management.

Each step of the assessment of client applications will be further reviewed in detail.

Pre-application client classification

The first pillar of the **Eve Exchange risk**-based approach is client initial risk group segregation based on the country of registration. European Union nationals and clients originating from these countries fall under the category of “low risk” and have the preliminary zero score on the risk scale. However, this is not the final risk status of the client as it is constructed of various factors outlined further within this policy.

Further, **Eve Exchange takes** necessary steps to eliminate and avoid certain degree of risks associated with the origin of its clients already before accepting applications for services. In this endeavor, **Eve Exchange decision** whether to establish any relationships with the client or not, and simultaneously in attempt to act in good faith on the international regulatory arena, is guided by the official FATF blacklist which is constantly followed by **Eve Exchange for** changes and updates. FATF calls on its members and other jurisdictions to apply counter-measures to protect the international financial system from the on-going and substantial money laundering and terrorism financing (ML/TF) risks emanating from a list of countries.

Finally, **Eve Exchange** separates clients into two more categories according to the country of their residence:

1) Latin America and African country residents would fall under the “medium risk” category and have a score of 4 applied on the risk scale.

2) Asia Pacific and rest of the world residents fall under the “low risk” category and have a score of 3 applied on the risk scale.

Risk scale

Blacklisted countries – 12

Improving Global AML/CFT Compliance countries – 6

Latin America and Africa – 4

Asia Pacific and rest of the world – 3

Europe - 0

It should be noted **Eve Exchange checks** the FATF country lists on an ongoing basis as well as other reputable authorities for up to date information on suggested restrictions applicable to high risk countries. Should there be any change in policies and/or recommendations, **Eve Exchange shall** as soon as practicable review its client database to identify should the risk assessment be done repeatedly considering the latest information. This policy shall also be updated immediately, once such information becomes available.

Having the country risk established, client applications are analyzed for further risk factors in step 2 which addresses the handling of client applications once submitted.

Client application handling

The second step encompasses consideration of several risk categories which are further outlined in detail.

Eve Exchange shall not provide a client with access to his/her account (including payments), until it is satisfied that the client’s account has been successfully verified on the basis of the provided information and documents irrespective the possible risk emanating from the client. Moreover, the client shall not have the possibility to make any fund transfer instructions, since **Eve Exchange banking** details are available only via client area to clients who have completed the entire account verification process.

Physical person vs Legal entity

It is crucial that the type of client is established during the application process, since it will further affect the Know Your Client procedures applied. Therefore, using the registration form, **Eve Exchange** will establish whether the prospective client is a physical person or a legal entity. Physical persons (by default are classified as low risk clients and have zero score on the risk scale). However, a different approach is applied to legal entities, which is further reviewed in detail.

Moreover, **Eve Exchange** shall establish whether the client is the sole beneficial owner of the account, or there are several beneficial owners. This is performed using the registration form, where the client shall specify such parties. Should there be several beneficial owners, all such parties (either legal or physical) shall be identified based on relevant documentation according to the procedures outlined within this and supplementary policies. The account shall not be opened until all such beneficial owners are properly identified and verified.

Legal entities

Legal entities pose a higher risk due to unlimited variations of legal structures diminishing their transparency and making the establishment of the initial fund source very complex. **Eve Exchange** to protect itself from attempts of money-laundering or terrorism financing, hence, being guided by The Wolfsberg Group principles, distinguishes following legal entity types and assigns risk scores accordingly:

• Cash (and cash equivalent) intensive businesses including: money services businesses (remittance houses, exchange houses, casas de cambio, bureaux de change, money transfer agents and bank note traders), casinos, betting and other gambling related activities, or businesses that while not normally cash intensive, generate substantial amounts of cash for certain transactions.
• Unregulated charities and other unregulated “not for profit” organizations (especially those operating on a “cross-border” basis).
• Dealers in high value or precious goods (e.g. jewel, gem and precious metals dealers, art and antique dealers and auction houses, estate agents and real estate brokers).
• Accounts for "gatekeepers" such as accountants, lawyers, or other professionals for their clients, where the identity of the underlying client is not disclosed to the financial institution. Accounts for clients introduced by such gatekeepers may also be higher risk where the financial institution places unreasonable reliance on the gatekeeper for KYC and AML matters.
• Armament manufacturers, dealers and intermediaries.
• Other legal entities.

To establish the type of business, **Eve Exchange** collects respective corporate documents identified in the KYC policy. Risk scores are assigned as follows:

Unregulated charities – 5
Armament manufacturers – 4

Cash intensive businesses – 4

“Gatekeepers” – 3

Dealers in high value and precious goods – 2

Other legal entitles – 0-3

Web-based screening

Eve Exchange maintains accounts with WorldCompliance, which allows conducting manual searches when desired. The company uses these accounts as part of standard due diligence. The web-system can be accessed via https://members.worldcompliance.com/SignIn.aspx

The search engine allows multiple search options such as “Single Search”, “Multiple Search” and “Keyword Search”.

Every search result is carefully analyzed and search results are exported as PDF reports. Such PDF reports are saved and attached to the client profile, should relations with the prospective client be established.

Newly registered client screening

Eve Exchange uses an automated mechanism that is designed to screen client applications according to the WorldCompliance databases upon their registration submissions. At the first step of verification, **Eve Exchange** clients are asked to submit detailed personal information where first name, last name, date of birth and passport number (optional) are collected and sent to the WorldCompliance desktop solution to have the data screened against the available databases. The screening results are saved on the platform as “pending” and are to be reviewed by the Compliance Officer.

The Compliance Officer shall review screening results with the “pending” status on a daily basis and decide whether there is a match with the registered client or these have been false-positive results. Following that, a search result report is attached to the client profile and the respective status is applied.

On-going screening

Eve Exchange understands that a one-time client screening is not sufficient to mitigate and control client risks, therefore **Eve Exchange** has also established an on-going screening routine. **Eve Exchange** screens its entire client database on a daily basis against the WorldCompliance databases. This allows identifying possible matches in a continuous manner and whenever WorldCompliance updates their supplied data, **Eve Exchange** will immediately establish if this data is relevant to any of its existing clients. Should such a match be established, **Eve Exchange** shall record this in the client profile and, depending on the history of relations with the client and the type of match identified, decide whether to continue relationship with the client or not.

Result analysis

While client screening is conducted according to three different procedures, the result analysis is performed using a single model. To understand the action model, **Eve Exchange** further provides a list of databases and information contained in the screening solution delivered by WorldCompliance:

1) **Global Sanction List**. WorldCompliance aggregates information from the most important sanction

lists around the world and groups them into one category called the Global Sanction List, which is comprised of individuals and companies with the highest risk score. The following lists are included: Her Majesty Treasury List, Bureau of Industry and Security, Department of State, EU Terrorism List, FBI Top Ten Most Wanted, Interpol Most Wanted, ICE List (U.S. Immigrations and Customs Enforcement), Office of Foreign Assets Control (OFAC) Sanctions, CBI List (The Central Bureau of Investigation), SDN & Blocked Entities, SECO List, Treasury PML List, UN Consolidated List, OCC Shell Bank List and World Bank Debarred Parties List.

2) **PEP List**. The Global PEP list includes profiles of Politically Exposed Persons, as well as those of their family members and close associates. Politically Exposed Persons (PEPs) are considered high risk in today's regulatory environment. Regulation requires enhanced due diligence when conducting business with Politically Exposed Persons. While there is no global definition of PEP, the Financial Action Task Force (FATF) has issued guidelines. Local legislation, like the USA Patriot Act or the European Union Directive, uses similar definitions of a Politically Exposed Person, typically consisting of the following five categories:

I. Current or former senior official in the executive, legislative, administrative, military, or judicial branch of a foreign government (elected or not).

II. A senior official of a major foreign political party.

III. A senior executive of a foreign government owned commercial enterprise, and/or being a corporation, business or other entity formed by or for the benefit of any such individual.

IV. An immediate family member of such individual; meaning spouse, parents, siblings, children, and spouse's parents or siblings.

V. Any individual publicly known (or actually known by the relevant financial institution) to be a close personal or professional associate.

3) **Adverse Media List**. The Global Adverse Media List is an extensive proprietary database of individuals and companies that have been linked to illicit activities by news sources. Listings are comprised of money launderers, fraudsters, arms dealers, drug dealers, and other criminals.

4) **Enforcement List**. The Global Enforcement List (GEL) is comprised of information received from regulatory and governmental authorities. It includes the content of warnings and actions against individuals and companies; listing drug dealers, money launderers, fraudsters, human traffickers, fugitives and other criminals.

Risk score:

Global Sanction List – 12

Adverse Media List – 12

Adverse Media List – 12

PEP List – 5

Each client, irrespective whether a newly registered or already with an active account, is continuously screened against the above lists. Client data is reviewed against the data contained within the available

screening lists for possible matches. **Eve Exchange** differentiates several preliminary match result statuses: positive (full match), false positive/negative (partial match), or negative (no match).

Positive - Each positive match result is reviewed manually by designated employees on a case by case basis using the desktop platform.

False positive – A full 100% or less match, however after thorough review it is clear that the match does not hold.

False negative – Same as false positive, with the exception that it is applicable only to partial (non 100%) matches, however, after thorough review it is clear that the match in fact can be established on the basis of one of the results obtained.

Negative – Negative matches are recorded in client profiles only once to reflect that the required screening has been conducted. No further actions are required in relation to the client.

Clients identified with a positive match based on any of the above lists, except the PEP List, will have a risk score of 12 applied and consequently have their applications rejected with relevant information registered and submitted in the Suspicious Activity Report (SAR)2 to the respective authority. Clients identified as PEPs will have a risk score of 5 applied and marked within the system (the designation of marking will be further explained in "post-application client management" section).

Once the legal form of the client is established as well as the screening results are obtained and analyzed, the declared financial standing of the client is further assessed.

Planned investments

It is crucial for **Eve Exchange** to establish the potential investments of the client as well as sources of such funds beforehand. During the registration, **Eve Exchange** clients are requested to provide the following information:

• Gross annual income (less than 100,000 EUR; 100,000 – 250,000 EUR; 250,000-500,000 EUR; 500,000-2,000,000 EUR; more than 2,000,000 EUR).

• Net worth (less than 100,000 EUR; 100,000-500,000 EUR; 500,000-1,500,000 EUR; more than 1,500,000 EUR).

• Planned investments (less than 50,000 EUR; 50,000-250,000 EUR; 250,000-1,000,000 EUR; more than 1,000,000 EUR).

• Origin of funds (salary, dividends, investment, real estate sale or other sources that should be specified).

The information provided should be consistent and is assessed by the Compliance Officer for conflicts (e.g. a client with gross annual income of less than 100,000 EUR and the same net worth should raise awareness if the planned investment is more than 1,000,000 EUR). The assessment is performed using the following logic:

Step 1 What is the planned investment?

Step 2 Is the planned investment more than the annual income?

i. If yes, is the net worth more than the planned investment?

1. If yes, a risk score of 4 is applied.
2. If no, a risk score of 7 is applied.

ii. If no, a risk score of 0 is applied.

Step 3 Assignment of the relevant risk score.

It should be noted note that this logic is not only applied to the initially collected information from the client within the application form, but also extends to the actual transactions. Should the transactions in question be inconsistent with the information provided within the application form, the Payments Department shall report such clients to the Compliance Officer for manual transaction approval. The Compliance Officer may request the Declaration of Source of Funds from the client, should he/she find it necessary to ensure that the funds originate from a legal source. If the client is unable to produce a valid DSF or it is rejected by the Compliance Officer, or if the remitter of funds does not have an active account with **Eve Exchange** such transfers shall be reversed; and if the DSF is not produced or rejected, the Suspicious Activity Report shall be produced.

Post-application client management

After client applications have been confirmed, the final risk score is calculated by summarizing the information acquired. Risk statuses are applied according to the final outcome, however, should the risk score exceed 12 points, the client shall be subject to rejection and the final decision will be made by the Compliance Officer after thoroughly and manually assessing all the information collected (additional information may be requested, or certain individual restrictions may be applied).

Eve Exchange also takes measures to monitor client activity on an on-going basis and according to the assigned final risk status. However, irrespective of the risk status, clients are monitored separately and can be identified within the system using filtering tools, if necessary.

Low risk clients

The following requirements are applied to clients assigned a “low risk” status through the application:

- All deposit/withdrawal requests in the amount of less than 15,000 EUR are processed automatically;
- The Declaration of Source of Funds is requested for any transaction exceeding 100,000 EUR;
- Funds can be transferred to any deposit account of the client within the same bank.

All documentation will be stored for at least 5 years.

Medium risk clients

More stringent requirements are applied to clients assigned a “medium risk” status through the application:

• All deposit/withdrawal requests in the amount of less than 15,000 EUR are processed automatically.
• The Declaration of Source of Funds is requested for any transaction exceeding 100,000 EUR;
• Funds can be transferred to any deposit account of the client within the same bank.

All documentation will be stored for at least 5 years.

High risk clients

The most stringent requirements are applied to clients assigned a “high risk” status through the application, and their operations are closely monitored:

• All deposit/withdrawal requests are handled manually and approved by the Compliance Officer prior to their execution.

• The Declaration of Source of Funds is requested for any transaction (or a set of transactions throughout the whole period) exceeding 15,000 EUR;

• Funds can only be transferred to the deposit account.

Data storage

Data on all transactions and all clients will be stored at our office. Data will be stored for at least 5 years.

Company development

Representatives of **Eve Exchange** are trying to keep up with the latest technologies and methods of payment (cryptocurrency, PayPal, WebMoney and other alternative payment methods) and will in every way impede fictitious transactions, money laundering and terrorism financing.