

Latest Update: July 9, 2026.

1. SUBJECT OF THE AML & KYC POLICY

1) Axenor Holdings OÜ Private limited liability company registered and governed by law of Estonia Republic, at the following address: Harju maakond, Tallinn, Kristiine linnaosa, Rahumäe tee 6b-67, Estonia, entered into the Estonian Companies Register under number 17426720 (hereinafter referred to as “Company”, “we”), is committed to the highest standards of Anti-Money Laundering (AML) and Counter-Terrorist Financing compliance in accordance with European Union and Republic of Estonia legislation.

2) This AML/KYC Policy (“Policy”) is implemented to ensure:

- a. compliance with laws related to anti-money laundering and terrorist financing in jurisdiction where we operate,
- b. the prevention of the use of our services for money laundering, financing of terrorism, or other criminal purposes.

3) The Company requires its directors, officers, and employees to:

- a. comply with this Policy at all times,
- b. undergo regular training on AML/KYC compliance,
- c. report suspicious activities immediately through internal procedures.

4) We reserve the right to amend or update this Policy at any time.

5) Users are responsible for checking the notifications regularly to stay informed of changes.

6) We do not enter into business relationships with criminals or terrorists.

7) We do not process transactions resulting from criminal activity.

8) We do not support transactions that facilitate or fund terrorism or organized crime.

9) In any case not addressed by this Policy, applicable AML regulations in the relevant jurisdiction shall apply.

10) By registering and using the Platform, the User (“you”, “Customer”) confirms acceptance of this Policy.

2. GENERAL PROVISIONS AND DEFINITIONS

1) The purpose of this Policy is to:

- a. prevent money laundering and terrorist financing,
- b. verify and monitor the identities of Users,
- c. ensure secure and compliant transactions via our Platform.

2) The following terms are defined for the purposes of this Policy:

- a. *Account*: a registered profile created by the User to access the Platform.
- b. *Platform*: a digital infrastructure provided by the Company for service access.

- c. *Customer*: a person who has registered an Account to use the Platform.
- d. *Virtual Currency*: digital value accepted as payment, tradable or transferable.
- e. *Business Relationship*: legal relationship formed through acceptance of our Terms of Use.
- f. *Compliance Officer*: a designated person responsible for oversight of AML/KYC matters.
- g. *Money Laundering*: actions to conceal the criminal origin of funds.
- h. *Terrorist Financing*: provision of funds or support for terrorist acts.
- i. *Beneficial Owner*: the natural person who ultimately owns or controls a legal entity.
- j. *PEP (Politically Exposed Person)*: a natural persons who are or have been entrusted with prominent public functions and family members or persons known to be close associates of such persons.
- k. *Natural persons who are or have been entrusted with prominent public functions*: all natural persons, including:
 - (a) heads of State, heads of government, ministers and deputy or assistant ministers;
 - (b) members of parliament “or of similar legislative bodies”;
 - (c) members of supreme courts, of constitutional courts or of other high-level judicial bodies, the decisions of which are not subject to further appeal, except in exceptional circumstances;
 - (d) members of courts of auditors or of the boards “or directorates” of central banks;
 - (e) ambassadors, chargés d’affaires and high-ranking officers in the armed forces;
 - (f) members of the administrative, management or supervisory bodies of State-owned enterprises;
 - (g) important officials “and members of the governing bodies” of political parties;
 - (h) directors, deputy directors and members of the board or equivalent function of an international organisation
 - (i) the natural persons exercising the functions included in the list published by the European Commission based on Article 20a(3) of Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purpose of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC, hereinafter referred to as “Directive (EU) 2015/849.

- l. *“Persons known to be close associates” mean*: all natural persons, including:
 - (a) any natural person who is known to have joint beneficial ownership of legal entities or legal arrangements, or any other close business relations, with a PEP;
 - (b) any natural person who has sole beneficial ownership of a legal entity or legal arrangement which is known to have been set up for the benefit de facto of the PEP.
- m. *The Estonian AML Law*: Passed 26.10.2017 Money Laundering and Terrorist Financing Prevention Act.

3. USER CONFIDENTIALITY

- 1) Reporting suspected money laundering does not breach customer confidentiality.
- 2) Confidentiality obligations are subject to mandatory legal disclosures and regulatory reporting.

- 3) The Company has implemented procedures to:
 - a. verify the identity of all new Users,
 - b. allow employees to flag and report suspicious activity,
 - c. securely maintain records of identity and transaction history.

4. COMPLIANCE

- 1) Compliance with this Policy is a legal and contractual requirement.
- 2) Violation may constitute a criminal offense and subject individuals to penalties.
- 3) Failure to comply may result in:
 - a. immediate suspension or termination of services,
 - b. notification to relevant authorities,
 - c. legal action or regulatory sanctions.

5. KYC PROCESS

- 1) Verification might be performed via dedicated tools integrating ID document verification and facial recognition.
- 2) Required documents include valid ID, passport, proof of address, and - if applicable - proof of source of funds.
- 3) Users rejected during KYC may appeal through the Compliance Officer at the above contact.
- 4) The first stage of verification is for the user to attach the relevant document in the appropriate place on the platform.
- 5) The second stage of verification is, if applicable, verification of the user's identity and status by the designated Compliance Officer - in relation to their binding obligations under the relevant laws on personal data protection, digital assets, or anti-money laundering.
- 6) KYC/AML data are retained for 5 years following the termination of the business relationship, as required by AML legislation.
- 7) Users may submit appeals or complaints regarding KYC rejection decisions by email to the Compliance Officer (see contact section).
- 8) In the event of suspected money laundering or other criminal activity or gross violation of a binding provision of the Agreement, the account may be temporarily suspended.
- 9) Temporary suspension of the account may last up to 6 months, with the possibility of further extension if there are legitimate legal reasons for doing so.
10. A person who is aware that they may be considered a PEP is required to notify the Compliance Officer, whose contact details are provided at the end of this document, within 7 days of becoming aware of this fact.

6. BUSINESS RELATIONSHIPS

- 1) The Company initiates a business relationship upon collecting:
 - a. full name,
 - b. unique identification number,
 - c. date of birth or registration,
 - d. nationality,
 - e. residential or registered address.
- 2) For legal entities, the Company must identify:
 - a. the beneficial owner(s),
 - b. controlling individuals,
 - c. any politically exposed persons involved.

7. DUE DILIGENCE MEASURES

- 1) Prior to any transaction, the Company requires verifiable identity documents, such as:
 - a. national ID,
 - b. passport,
 - c. driver's license,
 - d. business registration certificate (for entities).
- 2) In the absence of satisfactory identification:
 - a. no account or business relationship shall be initiated,
 - b. transactions will be blocked or frozen.
- 3) If a transaction or User is deemed suspicious:
 - a. the Company will file a suspicious activity report with competent authorities,
 - b. additional due diligence will be performed immediately.
- 4) Only the verified owner of submitted documents may use the Platform.
 - a. Third-party document submission is prohibited.
 - b. Any mismatch or inconsistency will result in immediate rejection of the account.

8. MODIFICATIONS AND UPDATES

- 1) Company reserves the right to:
 - a. update or modify these Policy,
 - b. alter or discontinue any feature of the Platform,
 - c. temporarily or permanently suspend access to the Platform.
- 2) Such changes will take effect immediately upon publication or notification to Users.
- 3) Continued use of the Platform constitutes acceptance of any changes.
- 4) The purpose of this regulation is to ensure that the company complies with AML requirements.

5) In all other respects not covered by this regulation, including the terms and definitions used, the Estonian AML Law and other laws in force in the Republic of Estonia shall apply.

Compliance Officer Contact email: contact@crypto-holdings.io

Data Protection Officer (DPO) contact email: contact@crypto-holdings.io