ANTI-MONEY LAUNDERING (AML) AND COUNTERING THE FINANCING OF TERRORISM (CFT) of BLOCKOVILLE OÜ

2026

ANTI-MONEY LAUNDERING (AML) AND COUNTERING THE FINANCING OF TERRORISM (CFT) of BLOCKOVILLE OÜ

TABLE OF CONTENTS

1. STATEMENT OF COMMITMENT

Blockoville OÜ ("Blockoville" or "the Company"), incorporated in Republic of Estonia, is committed to maintaining the highest standards of integrity, transparency, and regulatory compliance in all its operations. Blockoville recognizes its obligation to cooperatewith and support regulators and law enforcement agencies in their efforts to prevent, detect and control financial crime, and to comply with AML laws and regulation to close off the financial channels that money launderers and terrorist organizations use for illicit purposes. Every officer, director, employee and associated person of Blockoville is responsible for assisting in the Company's efforts to detect, deter and prevent money laundering and other activities intended to facilitate the funding of terrorist or criminal activities.

This Policy is adopted pursuant to the Prevention of Money Laundering Act, 2002 ("PMLA") and the applicable rules framed thereunder. The Board of Directors has approved this Policy and shall review it at least annually or earlier if required due to regulatory developments.

Blockoville is committed to the highest standards of compliance with the Prevention of Money Laundering Act, 2002 (PMLA) and the Prevention of Money Laundering (Maintenance of Records) Rules, 2005. As a reporting entity under the Ministry of Finance, Blockoville recognizes its responsibility to prevent its platform from being used for money laundering (ML) and terrorist financing (TF).

Blockoville OÜ has its headquartes at Marati tn 5, Põhja-Tallinna linnaosa, 11712 Tallinn, Harju maakond, Estonia and is supervised by Estonian Financial Supervision and Resolution Authority and Estonian Financial Intelligence Unit.

The Company recognises that entities engaged in financial technology services, including virtual digital asset services, payment facilitation, wallet services, and digital marketplaces, are inherently exposed to risks of money laundering, terrorist financing, fraud, and other financial crimes.

Accordingly, the Company adopts a zero-tolerance approach toward:

- Money laundering
- Terrorist financing
- Sanctions violations
- Fraud and misuse of financial systems
- Concealment of beneficial ownership

All employees, officers, consultants, and representatives of the Company are required to strictly adhere to this Policy.

2. INTRODUCTION

Money laundering involves the process of converting or transferring property derived from criminal activity in order to conceal its illicit origin. Terrorist financing involves the collection or provision of funds with the intention that they be used to carry out terrorist acts.

With the rise of digital finance and virtual digital assets, financial systems have become more accessible and technologically advanced. However, these innovations also introduce

vulnerabilities that may be exploited for criminal purposes, including layering of illicit proceeds through rapid digital transactions.

The Company acknowledges its responsibility as a reporting entity under Indian AML laws and undertakes to implement robust systems and controls to prevent misuse of its services.

3. OBJECTIVES OF THE POLICY

This Policy aims to:

- Establish a structured AML/CFT compliance framework.
- Define roles and responsibilities of management and employees.
- Ensure implementation of effective Customer Due Diligence (CDD).
- Introduce risk-based monitoring mechanisms.
- Provide procedures for identification and reporting of suspicious transactions.
- Ensure maintenance and preservation of records as required by law.
- Promote a culture of compliance across the organisation.

4. KEY DEFINITIONS

Money Laundering: As defined under Section 3 of PMLA, money laundering includes any direct or indirect attempt to indulge, assist, knowingly be a party to, or actually involved in any process connected with the proceeds of crime, including its concealment, possession, acquisition, use, or projecting it as untainted property.

Proceeds of Crime: Any property derived or obtained directly or indirectly by any person as a result of criminal activity relating to a scheduled offence.

Terrorist Financing: Provision, collection, or use of funds with the knowledge or intention that such funds be used to carry out terrorist acts under applicable Indian law.

Beneficial Owner: The natural person who ultimately owns or controls a client and/or the person on whose behalf a transaction is being conducted, as defined under PML Rules.

Politically Exposed Person (PEP): An individual who is or has been entrusted with prominent public functions in India or a foreign jurisdiction, including heads of state, senior politicians, judicial or military officials, senior executives of state-owned corporations, and important political party officials.

Virtual Digital Asset (VDA): As per Section 2(47A) of the Income Tax Act, 1961, any information, code, number, or token generated through cryptographic means or otherwise, providing a digital representation of value exchanged with or without consideration.

Beneficial Owner (BO): The natural person who ultimately owns or controls a client. In accordance with Rule 9 of the PML Rules:

- **For Companies:** A person acting alone or together through one or more juridical persons, has a controlling ownership interest (exceeding 10%) or exercises control through other means.

- **For Trusts/Unincorporated Bodies:** The identification of any individual entitled to more than 15% of the interest.

Officially Valid Document (OVD): Includes the Passport, Driving License, Proof of possession of Aadhaar number, Voter's Identity Card and PAN.

Suspicious Transaction: A transaction, including an attempted transaction, that gives rise to a reasonable ground of suspicion that it may involve proceeds of an offense or appears to be made in circumstances of unusual or unjustified complexity.

5. COMPANY'S RISK APPETITE

The Company adopts a conservative risk appetite with respect to financial crime exposure.

The Company shall not:

- Establish relationships with anonymous or fictitious persons.
- Provide services to sanctioned individuals or entities.
- Facilitate transactions for shell banks.
- Engage with customers who refuse to provide required KYC documentation.
- Continue relationships where risk cannot be reasonably mitigated.

The Company recognises that virtual digital asset activities may involve:

- Rapid cross-border transfers
- High transaction velocity
- Anonymity-enhancing technologies
- Layering risks

Therefore, enhanced monitoring controls are implemented for such services.

6. RISK-BASED APPROACH

The Company applies a Risk-Based Approach (RBA) to identify, assess, and mitigate risks.

Risk assessment considers:

- Customer profile
- Geographic exposure
- Product and service characteristics
- Transaction patterns
- Delivery channels

Customers are categorised into Low, Medium, or High risk. High-risk customers are subject to Enhanced Due Diligence (EDD). Risk profiles are documented and periodically reviewed.

7. CUSTOMER DUE DILIGENCE (CDD)

Threshold-Based CDD: In compliance with FIU-IND mandates for VDAs:

- Every VDA transaction requires basic identity verification.
- Transactions exceeding INR 50,000 (or equivalent) require full OVD-based verification.
- Connected transactions totaling INR 10,00,000 (Ten Lakhs) within a month trigger an automatic high-risk review.

CDD is conducted:

- At onboarding.
- Before establishing business relationships.
- When suspicion arises.
- Upon material change in customer information.
- When transaction behaviour deviates from expected patterns.

CDD includes:

- Identification of customer.
- Verification of identity.
- Identification of beneficial ownership.
- Understanding purpose and intended nature of business relationship.

Failure to complete CDD satisfactorily shall result in refusal to establish or continuation of business relationship.

8. IDENTIFICATION AND VERIFICATION OF INDIVIDUALS

The Company shall obtain:

- Full name
- Date of birth
- Permanent Account Number (PAN)
- Government-issued identification
- Address proof
- Contact details

Verification shall be conducted using reliable and independent sources. Digital verification tools may be used, including liveness detection and document authentication technologies. Where identity cannot be verified satisfactorily, the relationship shall not proceed.

9. IDENTIFICATION OF NON-INDIVIDUAL CUSTOMERS

For legal entities, the Company shall obtain:

- Certificate of Incorporation
- Memorandum and Articles
- PAN of entity
- Registered office address
- List of directors/partners
- Board resolution authorising account
- Beneficial ownership structure

The Company shall identify and verify natural persons exercising ultimate control.

Where ownership is layered, the Company shall trace ownership until ultimate natural persons are identified.

10. ENHANCED DUE DILIGENCE (EDD)

EDD shall be applied in cases involving:

- PEPs
- High-risk jurisdictions
- Complex ownership structures
- Unusually large or complex transactions
- Adverse media reports
- High-volume virtual asset trading

EDD measures may include:

- Source of funds verification
- Source of wealth confirmation
- Bank statements review
- Tax return verification
- Senior management approval
- Increased transaction monitoring

If EDD requirements are not satisfied, the relationship shall be declined or terminated.

11. SANCTIONS SCREENING

The Company shall screen customers and beneficial owners against:

- United Nations sanctions lists
- Domestic designated lists under UAPA
- Other relevant global sanctions databases as risk mitigation practice

Screening shall occur:

- At onboarding
- Periodically thereafter
- When updated lists are issued

If a confirmed match is identified:

- Account shall be frozen.
- Appropriate authorities shall be informed.
- Reporting obligations shall be fulfilled.
- No tipping-off shall occur.

12. ONGOING MONITORING AND REVIEW

Ongoing monitoring is a core component of AML compliance.

Monitoring includes:

- Reviewing transaction patterns
- Detecting structuring behaviour
- Identifying unusual wallet activity
- Monitoring sudden increases in transaction volume
- Reviewing dormant accounts becoming active

Customer information shall be periodically updated based on risk categorisation:

- Low Risk: Every 3 years
- Medium Risk: Every 2 years
- High Risk: Annually

13. REPORTING TO FIU-IND

Where the Company suspects money laundering or terrorist financing, it shall file a Suspicious Transaction Report (STR) with FIU-IND within the prescribed time frame. Employees must immediately escalate suspicious activity internally to the Principal Officer.
The Company strictly prohibits tipping-off. All STR-related records shall be securely maintained.

14. RECORD RETENTION

The Company shall retain:

- Identity verification records
- Transaction records
- Business correspondence
- Suspicious transaction documentation

Records shall be retained for a minimum of five (5) years after termination of relationship or completion of transaction, whichever is later.

Records must be retrievable promptly upon lawful request.

15. TRAINING AND AWARENESS

The Company shall conduct:

- Mandatory onboarding AML training
- Annual refresher training
- Specialised training for compliance personnel

Training shall include practical examples relevant to digital asset risks.

Attendance records shall be maintained.

16. POLICY ADMINISTRATION

This Policy shall be:

- Reviewed annually
- Updated upon regulatory changes
- Approved by the Board

Minor procedural updates may be issued by the Compliance Officer, subject to Board oversight.