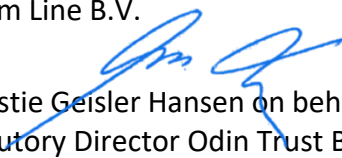


Boom Line B.V.

Crypto Policy

Policy Owner	Boom Line B.V.
Approver	 Christie Geisler Hansen on behalf of Statutory Director Odin Trust B.V.
Date approved	31 May 2025
Date last reviewed	31 May 2025
Review frequency	Annual
Next review date	May 2026
Responsible for document management	Kyryl Shvets, MLRO
Security classification	Private and Confidential

Crypto Policy

1. Introduction

The Policy outlines security measures, user verification, transaction controls, risk management procedures, and compliance obligations pursuant to applicable laws, including anti-money laundering (AML), counter-financing of terrorism (CFT), and responsible gambling principles.

2. Purpose and Objectives

The purpose of this Policy is to:

- Ensure legal and regulatory compliance in relation to the use of cryptocurrencies.
- Prevent the misuse of the platform for money laundering, terrorism financing, and other illegal activities.
- Safeguard users' assets and ensure secure handling of digital currencies.
- Promote transparency, integrity, and accountability in all crypto-related activities.
- Mitigate operational, market, and cybersecurity risks associated with crypto assets.

3. Scope

This Policy applies to:

- All departments and employees of the Company.
- Contractors, consultants, and third-party service providers handling crypto transactions.
- Users and customers engaging in gaming activities using cryptocurrencies.

4. Governance Structure

4.1. The Compliance Officer (CO) and/or Money Laundering Reporting Officer (MLRO) oversee implementation of this Policy.

4.2. A dedicated Crypto Risk Committee (CRC) may be established to evaluate crypto-specific risks and provide periodic reporting to senior management.

4.3. Roles and responsibilities shall be clearly assigned for:

- Wallet management
- Risk screening
- Regulatory reporting
- System integrity

5. Approved Cryptocurrencies

The Company supports the following cryptocurrencies:

- Bitcoin (BTC)
- Ethereum (ETH)
- Tether (USDT) on ERC-20
- Bitcoin Cash (BCH)
- Dogecoin (DOGE)
- Litecoin (LTC)
- Additional tokens may be added upon completion of a formal risk and compliance review.

A due diligence assessment will be conducted on each token including factors such as liquidity, volatility, use cases, anonymity features, and public reputation.

6. Wallet Infrastructure and Key Management

6.1. Wallets shall be structured as follows:

- Hot Wallets: Used for day-to-day transactions; protected by multi-signature access.
- Cold Wallets: Used for long-term storage; held offline with hardware encryption.

6.2. Key Management:

- Private keys shall be stored in encrypted form using HSMs (Hardware Security Modules).
- At least two senior managers shall be required to authorize any movement of crypto from cold storage.
- A Disaster Recovery Plan must include key recovery and business continuity mechanisms.

7. User Onboarding and KYC Requirements

7.1. All users must undergo identity verification (KYC) before:

- Making cumulative deposits exceeding EUR 2250 equivalent.
- Withdrawing any funds, regardless of amount.

7.2. Verification includes:

- Valid government-issued ID.
- Proof of address.
- Selfie with document (liveness check).
- Sanctions and PEP screening.

7.3. Enhanced Due Diligence (EDD) is mandatory for:

- Users from high-risk jurisdictions.
- Users with irregular or large-volume activity.

8. Crypto Deposits and Monitoring

8.1. All incoming wallet addresses will be screened via blockchain analytics providers (e.g., Chainalysis, TRM Labs).

8.2. Deposits from wallets associated with darknet marketplaces, mixers, sanctioned entities, or flagged by risk scoring tools will be blocked.

8.3. Risk triggers will include:

- Unusually high frequency or volume.
- Cross-border transfers from opaque exchanges.
- Use of privacy-enhancing tokens.

9. AML/CFT Transaction Controls

9.1. All transactions are continuously monitored using automated and manual review systems.

9.2. The following types of transactions will be flagged:

- Structuring or layering activity
- Use of anonymous wallets
- Rapid movement between deposit and withdrawal

9.3. The MLRO shall report any suspicious activity to the relevant Financial Intelligence Unit (FIU) in compliance with legal obligations.

10. Crypto Withdrawals

10.1. All withdrawals must be made to pre-approved wallets verified during the KYC process.

10.2. The Company will maintain a whitelist of allowed withdrawal addresses.

10.3. Manual review is triggered for:

- Withdrawals above EUR 1000 equivalent in crypto.

- Requests to change withdrawal wallet address.
- Repeated withdrawal attempts to flagged jurisdictions.

11. Transaction Limits and Thresholds

Limits shall be defined and periodically reviewed by the Compliance Officer:

- Daily deposit limit: EUR 2000 equivalent
- Monthly withdrawal limit: EUR 10000 equivalent
- Real-time alerts for cumulative deposits over EUR 2250
- Automated freezes for single transactions over EUR 2000

12. Accounting, Reconciliation, and Reporting

12.1. Crypto balances shall be reconciled daily with user ledger accounts.

12.2. Variance reports and audit trails must be maintained.

12.3. External audits of crypto systems shall occur at least annually.

13. Data Retention

13.1. All crypto transaction data, KYC records, and risk analysis reports shall be retained for no less than five (5) years.

13.2. Data shall be encrypted and stored in compliance with GDPR and other applicable data protection laws.

14. Cybersecurity and Systems Integrity

14.1. Penetration testing and security audits shall be conducted semi-annually.

14.2. Two-Factor Authentication (2FA) and role-based access controls (RBAC) are mandatory.

14.3. Crypto-related systems shall be segregated from general IT infrastructure and monitored 24/7.

15. Third-Party Service Providers

15.1. Exchanges, payment processors, and custodians must be vetted for:

- Licensing and jurisdictional credibility
- AML/CFT controls
- Security and insurance coverage

15.2. Third parties must sign service-level agreements (SLAs) and undergo regular compliance reviews.

16. Staff Training and Awareness

16.1. All employees involved in crypto operations shall receive:

- Annual AML/CFT crypto training
- Scenario-based red flag training
- Phishing and social engineering awareness programs

17. Policy Enforcement and Violations

17.1. Breach of this Policy shall result in internal disciplinary procedures and may be reported to authorities.

17.2. Repeated or serious violations may result in termination, contract cancellation, and criminal liability.

18. Policy Review and Maintenance

18.1. This Policy shall be reviewed annually and updated to reflect:

- Changes in legal frameworks
- Technological advancements
- Internal risk assessments and audits