

OPTIM DEVELOPMENT B.V.

Crypto risk policy

Effective Date:

20.05.2025

Next Review Date:

10.01.2026



**Anastasiia
Latypova, MLRO**

1. PURPOSE AND SCOPE

This Policy outlines Optim Development B.V.'s approach to identifying, managing, and mitigating risks associated with the use, storage, and acceptance of cryptocurrency within our operations. It applies to all departments, systems, and personnel handling crypto-related functions.

2. RISK IDENTIFICATION

Volatility Risk: Crypto assets are inherently volatile. The Company limits exposure by converting balances to fiat when appropriate and does not rely on crypto as a primary treasury asset.

Fraud Risk: All crypto transactions are subject to transaction verification, origin tracing, and enhanced KYC to detect potential misuse.

Cybersecurity Risk: Wallets are protected via encryption, 2FA, and limited access controls. Regular vulnerability assessments are conducted.

Regulatory Risk: The Company monitors regulatory developments across all jurisdictions where we operate. All crypto-related activities comply with applicable AML, tax, and reporting laws.

Liquidity Risk: We ensure that crypto assets are kept at levels sufficient for operational needs and reserve user withdrawal funds in readily accessible wallets.

3. TRANSACTION MONITORING

All cryptocurrency transactions are monitored for anomalies.

The Company applies:

- Real-time tracking and logging of incoming/outgoing crypto flows;
- Red flag detection (e.g., high-volume transfers, rapid wallet cycling);
- Enhanced due diligence for transactions exceeding thresholds or linked to higher-risk jurisdictions.

4. WALLET MANAGEMENT AND CUSTODY

Operational funds are stored in hot wallets with limited balances;

Majority of crypto holdings are secured in cold wallets with multi-sig access;

Wallet credentials are stored securely with access restricted to authorized personnel only; Third-party custody or insurance may be used to protect client funds.

5. USER EDUCATION

We provide players and partners with basic education on crypto risks, including:

- Recognizing phishing and fraud attempts;
- Securing personal wallets and credentials;
- Understanding volatility and transaction finality.

6. INTERNAL CONTROLS AND AUDITS

All crypto-related functions are subject to internal control procedures and periodic audits; Segregation of duties is enforced across asset custody, transaction execution, and reconciliation; All crypto movements are logged and reviewed by compliance and finance staff.

7. POLICY REVIEW

This Policy shall be reviewed at least annually, or more frequently in response to:

- Significant changes in crypto market conditions;
- Introduction of new crypto services;
- Updates in applicable regulation.