

Crypto Usage Risk Policy

1. Purpose

This policy defines the framework for managing risks related to the use, storage, transfer, and handling of crypto assets by Innova Hub b.v..

The objective is to ensure secure, compliant, and controlled use of crypto assets.

2. Scope

This policy applies to all employees, systems, wallets, exchanges, and crypto-related activities performed by the Company.

3. Governance and Responsibilities

Management is responsible for approving crypto activities and risk appetite.

Compliance is responsible for regulatory compliance, AML controls, and transaction monitoring.

Finance is responsible for reconciliation and accounting treatment.

IT/Security is responsible for wallet security and access controls.

4. Approved Crypto Assets and Providers

Only approved crypto assets, blockchain networks, wallets, and service providers may be used.

Approval considers:

- Security and reliability;
- Regulatory status;
- Liquidity;
- Compliance capabilities.

Privacy-focused or high-risk crypto assets are prohibited.

5. Wallet and Asset Security

The Company shall maintain appropriate controls including:

- Secure wallet management;
- Multi-factor authentication;
- Restricted access;
- Multi-signature approval for material holdings;
- Secure backup and recovery procedures.

Private keys must never be shared or stored insecurely.

6. Transaction Controls

Crypto transactions must be subject to:

- Authorized approval processes;
- Wallet address verification;
- Transaction monitoring;
- Regular reconciliation.

Transactions above defined limits require additional approval.

7. Third-Party Provider Risk

Before using exchanges, custodians, or other crypto service providers, the Company shall assess:

- Regulatory status;
- Security measures;
- AML controls;
- Reputation and financial stability.

8. Cybersecurity and Fraud Prevention

The Company shall implement measures to prevent:

- Unauthorized access;
- Fraudulent transactions;
- Phishing attacks;
- Loss of crypto assets.

Employees with crypto access must receive appropriate security training.

9. Prohibited Activities

The following are prohibited:

- Use of personal wallets for company transactions;
- Sharing private keys;
- Transactions with sanctioned entities;
- Use of unapproved crypto assets or providers;
- Circumvention of compliance controls.

101. Incident Management and Review

Crypto-related incidents must be reported, investigated, and remediated.

This policy shall be reviewed at least annually or following significant regulatory or operational changes.

Approved by

Innova Hub b.v.

Gouloud Hammoud, Director