

# Cryptocurrency Usage Risk Policy

## 1. Purpose and Scope

The purpose of this policy is to establish guidelines and procedures to identify, assess, and mitigate risks associated with the use of cryptocurrency within the organization. This policy applies to all departments, employees, and third-party partners involved in cryptocurrency transactions or management.

## 2. Policy Objectives

- To ensure compliance with regulatory and licensing requirements concerning cryptocurrency usage.
- To protect company assets and user funds from risks inherent to cryptocurrency transactions.
- To safeguard against money laundering, fraud, and other financial crimes associated with cryptocurrency.
- To manage the operational, financial, and reputational risks linked to the use of cryptocurrency.

## 3. Key Risk Categories and Controls

### 3.1 Compliance and Regulatory Risks

- **Compliance Framework:** The organization shall adhere to local and international regulations related to cryptocurrency usage, including Anti-Money Laundering (AML) and Counter-Terrorist Financing (CTF) laws.
- **Record-Keeping:** All cryptocurrency transactions will be documented and stored in compliance with legal standards, ensuring traceability and auditability.

### 3.2 AML/KYC Risk Management

- **AML Program:** The organization will implement an AML program with stringent procedures to prevent, detect, and report suspicious activities involving cryptocurrency.
- **Enhanced KYC Requirements:** Cryptocurrency transactions require enhanced Know Your Customer (KYC) measures, including verifying the identity of clients and the origin of funds.
- **Transaction Monitoring:** Real-time monitoring of cryptocurrency transactions will be implemented to flag suspicious activity, applying enhanced due diligence for high-risk transactions.

### 3.3 Cybersecurity and Asset Protection Risks

- **Cold and Hot Wallet Segregation:** The organization will segregate assets between cold (offline) and hot (online) wallets, minimizing online exposure. Operational funds in hot wallets will be limited to the amount necessary for liquidity purposes.

- **Access Control:** Multi-signature authentication and strict access controls will govern cryptocurrency wallet management, requiring multiple approvals for fund transfers.

### 3.4 Financial Risks: Volatility and Liquidity Management

- **Real-Time Value Monitoring:** The organization will monitor cryptocurrency values in real-time, converting assets to fiat currency when needed to manage exposure to market fluctuations.
- **Liquidity Reserves:** Adequate liquidity reserves in fiat currency will be maintained to cover sudden increases in cryptocurrency withdrawals, ensuring financial stability.

### 3.5 Fraud Prevention and Financial Crime Risks

- **Fraud Detection Measures:** Fraud detection tools and transaction monitoring systems will be employed to identify unusual transaction patterns or fraudulent activity.

## 4. Risk Mitigation and Controls

### 4.1 Risk Assessment Procedures

- **Periodic Risk Assessments:** Regular risk assessments will be conducted to identify, measure, and address cryptocurrency-related risks, with updates based on market changes or regulatory adjustments.
- **Risk Scoring:** Each identified risk will be scored for likelihood and potential impact, with corresponding mitigation measures prioritized according to risk level.

## 5. Policy Review and Updates

- This policy will be reviewed and updated annually or as needed to reflect changes in regulatory requirements, emerging risks, and industry best practices.
- Any significant policy changes will be communicated to relevant stakeholders and training sessions will be provided to ensure awareness and adherence.

## 6. Communication and Training

- **Employee Training:** Employees involved in cryptocurrency transactions will receive training on this policy, covering risk identification, AML/KYC procedures, and cybersecurity best practices.
- **Customer Education:** Educational resources will be provided to customers regarding cryptocurrency risks, usage guidelines, and security recommendations.

---

### Policy Approval and Effective Date

This Cryptocurrency Usage Risk Policy has been approved by is effective as of [effective date].

---

