

# Crypto Usage Risk Policy

**Effective Date:** December 1, 2022

**Last Reviewed:** February 15, 2025

**Version:** 1.0

---

## 1. Introduction

This Crypto Usage Risk Policy is established to outline the risks associated with the use of cryptocurrency in MIBS N.V.'s operations, particularly in relation to payments, transactions, and customer activities. The purpose of this policy is to inform of potential risks and to set guidelines on how these risks are managed to ensure compliance, transparency, and financial security.

## 2. Scope

This policy applies to all employees, contractors, customers, and business partners of MIBS N.V. who engage in cryptocurrency transactions, or handle, store, or manage cryptocurrency on behalf of the company.

## 3. Definitions

- **Cryptocurrency:** A digital or virtual currency that uses cryptography for security and operates independently of a central authority, such as Bitcoin, Ethereum, etc.
- **Blockchain:** A decentralized digital ledger that records transactions across multiple computers.
- **Exchange:** Platforms that allow the trading of cryptocurrency for fiat or other digital currencies.

## 4. Risks Involved in Cryptocurrency Usage

### 4.1 Volatility Risk

Cryptocurrency values are highly volatile, with prices often fluctuating drastically over short periods.

- **Risk:** Significant financial losses can occur from the sudden decrease in the value of cryptocurrencies.
- **Mitigation:** MIBS N.V. will monitor market trends and implement strategies, such as frequent conversions of cryptocurrency to fiat currency, to reduce exposure to volatility.

## 4.2 Regulatory and Compliance Risk

Cryptocurrency regulations differ across jurisdictions and are often subject to change.

- **Risk:** Legal risks associated with the use of cryptocurrency, such as non-compliance with anti-money laundering (AML) and know-your-customer (KYC) regulations, can result in penalties.
- **Mitigation:** The company will adhere to all applicable Curacao regulations and monitor regulatory developments to ensure ongoing compliance.

## 4.3 Security Risk

Cryptocurrency transactions are irreversible, and wallets can be vulnerable to hacking and theft.

- **Risk:** Unauthorized access to cryptocurrency wallets or transactions may lead to the loss of funds.
- **Mitigation:** The company will employ robust security measures, including multi-signature wallets, cold storage, two-factor authentication (2FA), and regular security audits.

## 4.4 Fraud Risk

Cryptocurrencies can be used for fraudulent activities, including money laundering, financing illegal activities, or fraudulently obtaining services or goods.

- **Risk:** The use of cryptocurrencies can expose the company to fraudulent transactions and illegal activities.
- **Mitigation:** MIBS N.V. will perform due diligence on customers and implement transaction monitoring tools to identify suspicious activity.

## 4.5 Operational Risk

Cryptocurrency networks may suffer from congestion or technical failures, which could disrupt services.

- **Risk:** Network issues could delay or prevent the completion of cryptocurrency transactions.
- **Mitigation:** The company will utilize reliable cryptocurrency platforms and exchanges with a strong track record of operational performance and will have contingency plans for such events.

#### 4.6 Liquidity Risk

Limited market liquidity for certain cryptocurrencies may hinder the company's ability to buy or sell assets efficiently.

- **Risk:** Low liquidity could lead to unfavorable prices or inability to convert cryptocurrency to fiat currency.
- **Mitigation:** MIBS N.V. will maintain relationships with multiple exchanges to ensure liquidity and diversify its cryptocurrency portfolio.

#### 5. Internal Controls

To manage the risks associated with cryptocurrency, the following internal controls will be implemented:

- **Access Control:** Only authorized personnel will have access to cryptocurrency wallets and transaction systems.
- **Audit Trails:** All cryptocurrency transactions will be logged and regularly reviewed by internal audit teams.
- **Regular Training:** Employees will receive regular training on cryptocurrency risks, security protocols, and compliance requirements.

#### 6. Incident Reporting

In the event of a security breach, theft, or significant loss related to cryptocurrency transactions, employees must report the incident immediately. A full investigation will be conducted, and necessary actions will be taken to address the incident and prevent future occurrences.

For external parties (clients or players) a communication channel to report security incidents will be provided.

---

**Approved by:** Miodrag Miletikj

**Position:** Compliance Officer

**Date:** May 15, 2025