



# **Risk Policy for Cryptocurrency Usage**

POL-AML-001-03

# Risk Policy for Cryptocurrency Usage

## 1. Introduction

- 1.1. Vavada B.V., 143168, Curacao (hereinafter referred to as “Company”) recognizes the unique risks associated with cryptocurrency usage in our operations. This Risk Policy outlines the measures implemented to manage, mitigate, and monitor risks related to accepting and processing cryptocurrency transactions in compliance with applicable laws, including anti-money laundering (AML) and counter-terrorism financing (CTF) regulations. It combines regulatory requirements, ensuring compliance with Curacao and international standards like FATF, while maintaining a secure and transparent operational environment.

## 2. Objectives

- 2.1. The objectives of this Risk Policy are:
  - 2.1.1. To ensure compliance with international and local regulations related to cryptocurrency usage.
  - 2.1.2. To minimize exposure to risks such as fraud, money laundering, and illicit financial activities.
  - 2.1.3. To maintain a secure and transparent environment for cryptocurrency transactions.
  - 2.1.4. To align cryptocurrency-related practices with the Company’s broader risk management framework.
  - 2.1.5. This Risk Policy for Cryptocurrency Usage operates in conjunction with the Company’s AML Policy, which provides a comprehensive framework for customer due diligence (CDD), enhanced due diligence (EDD), transaction monitoring, and suspicious activity reporting. In case of any discrepancies, the AML Policy prevails in ensuring full compliance with regulatory requirements.

## 3. Risk Identification and Assessment

The Company identifies and assesses the following key risks associated with cryptocurrency usage:

- 3.1. Fraud Risk
  - 3.1.1. Use of stolen or unauthorized cryptocurrency wallets.
  - 3.1.2. Fraudulent transactions initiated by malicious actors.
- 3.2. AML/CTF Risk

- 3.2.1. Transactions involving privacy coins (e.g., Monero, Zcash) are subject to enhanced scrutiny and may be restricted or prohibited, in compliance with current regulatory guidelines.
  - 3.2.2. Inability to trace anonymous transactions effectively.
  - 3.2.3. Transactions originating from high-risk jurisdictions.
  - 3.2.4. Use of cryptocurrency for laundering proceeds of crime or financing terrorism
- 3.3. Regulatory Risk
  - 3.3.1. Non-compliance with Curacao or FATF reporting requirements
  - 3.3.2. Potential sanctions or penalties from regulatory authorities.
- 3.4. Operational Risk
  - 3.4.1. Errors in processing or reconciling cryptocurrency transactions.
  - 3.4.2. Vulnerabilities in cryptocurrency wallets or exchange platforms.

## 4. Risk Mitigation Measures

To address the identified risks, the Company implements the following measures:

- 4.1. AML/CTF Compliance
  - 4.1.1. The Company applies risk-based Know Your Customer (KYC) and Enhanced Due Diligence (EDD) procedures for cryptocurrency users in accordance with its AML Policy and regulatory requirements. The level of scrutiny is adjusted based on the assessed risk of each transaction or customer.
  - 4.1.2. Blockchain analysis tools to monitor and trace cryptocurrency transactions.
  - 4.1.3. Reporting of suspicious activities to the relevant authorities within the timeframe required by the Curaçao AML/CFT framework. All flagged cryptocurrency transactions above the threshold of NAf 4,000 must be reviewed and, if deemed suspicious, reported in accordance with regulatory obligations.
  - 4.1.4. Flag and review transactions exceeding the regulatory threshold of NAf 4,000 (or its equivalent in other currencies), in accordance with *Section III of the January 10, 2025 AML/CFT Regulations issued by the Curacao GCB*
  - 4.1.5. Utilization of automated systems for real-time monitoring of transaction patterns to detect anomalies or high-risk activities, in line with current regulatory standards.
- 4.2. 4.2. Cryptocurrency Wallet Management
  - 4.2.1. Use of secure, multi-signature wallets to protect funds.
  - 4.2.2. Regular audits and penetration testing of wallet infrastructure.
- 4.3. 4.3. Regulatory Alignment
  - 4.3.1. Continuous monitoring of regulatory developments and updating internal policies accordingly.
  - 4.3.2. Collaboration with legal and compliance teams to ensure adherence to jurisdictional requirements.

## 5. Governance and Accountability

- 5.1. Risk Management Committee
  - 5.1.1. A dedicated committee oversees cryptocurrency risk management activities.
  - 5.1.2. Regular meetings to review risk reports and implement corrective actions.
- 5.2. Escalation Procedures
  - 5.2.1. Clear escalation channels for reporting cryptocurrency-related incidents.
  - 5.2.2. Incident response plans to address breaches or fraudulent activities promptly.
- 5.3. Accountability
  - 5.3.1. Designation of a Cryptocurrency Risk Officer responsible for policy implementation and compliance monitoring.

## 6. Monitoring and Reporting

- 6.1. The Company ensures continuous monitoring and periodic reporting of cryptocurrency-related risks:
  - 6.1.1. Regular risk assessments and audits of cryptocurrency transactions are conducted based on materiality and risk factors.
  - 6.1.2. Suspicious transactions are reviewed and, if necessary, reported to the relevant authorities in compliance with AML/CFT obligations.
  - 6.1.3. Internal reporting on cryptocurrency usage trends and associated risks.

## 7. Payment Agents

- 7.1. The Casino operates with the assistance of intermediaries and payment agents, including Magefin Ltd (HE456432, Cyprus), to facilitate cryptocurrency transactions.
- 7.2. All intermediaries must comply with the Company's AML/CFT policies and regulatory requirements, including reporting suspicious transactions and ensuring proper KYC procedures.

This Risk Policy will be reviewed annually or upon significant changes in regulatory requirements, market conditions, or operational practices. In particular, any amendments to the AML/CFT regulatory framework issued by the Curacao Gaming Control Board will be assessed to determine necessary updates.

This document was prepared by the AML Department of Vavada B.V. For any inquiries, please contact [support@vavada.net](mailto:support@vavada.net) or use the live chat available on our website.