

ZOOMBA B.V.

Crypto Usage Policy

Version	Status	Date	Comments	Signature of the Approver
1.0	Approved	25-August 2025	- Policy created and approved	

Approver	Kurason Trust Curacao N.V. / Managing Director
Date Approved	25-August-2025
Date last reviewed	25-August-2025
Review Frequency	Annual
Next review date	January-2026
Security classification	Private and Confidential

Table of Contents

1. INTRODUCTION.....4

2. SCOPE AND PURPOSE4

3. RISK MANAGEMENT MEASURES.....4

4. GOVERNANCE6

5. STAFF TRAINING AND AWARENESS7

6. REPORTING AND ESCALATION.....8

8. RECORD KEEPING8

9. POLICY BREACHES AND DISCIPLINARY ACTIONS9

1. INTRODUCTION

This Cryptocurrency Usage Policy outlines the framework ZOOMBA B.V. employs in managing cryptocurrency-related transactions within its online gambling services. It ensures compliance with regulatory requirements, risk mitigation strategies, and the protection of users and the company from fraud, money laundering, and illicit financial activities.

2. SCOPE AND PURPOSE

This policy applies to all cryptocurrency transactions facilitated by ZOOMBA B.V. and extends to all personnel responsible for handling, monitoring, and processing such transactions. It ensures that all cryptocurrency operations adhere to Anti-Money Laundering (AML) and Counter-Terrorist Financing (CFT) regulations, data protection laws, and fraud prevention best practices.

3. RISK MANAGEMENT MEASURES

3.1 Verification Process

ZOOMBA B.V. applies a rigorous Know Your Customer (KYC) and Customer Due Diligence (CDD) process to verify the identities of users engaging in cryptocurrency transactions. The verification measures include but are not limited to:

- Collection of proof of identity (e.g., government-issued ID, passport, or driver's license).
- Collection of proof of residence (e.g., utility bill, bank statement, or rental agreement).
- Verification of cryptocurrency wallet ownership when applicable.

Enhanced Due Diligence (EDD) is applied to users categorized as high-risk, including but not limited to:

- Politically Exposed Persons (PEPs) and their close associates.
- Users exhibiting irregular or unusual transaction patterns.
- Users from jurisdictions classified as high-risk or non-cooperative by international regulatory bodies.

Verification measures are periodically reviewed to ensure compliance with evolving regulatory requirements and industry best practices. The verification process shall be conducted in accordance with the company's **AML/CFT Policy**.

3.2 Transaction Monitoring

ZOOMBA B.V. utilizes advanced transaction monitoring systems to track cryptocurrency transactions in real-time, allowing for prompt detection of suspicious or unusual activity. Key elements of this monitoring process include:

- Screening transactions against predefined risk parameters (e.g., transaction limits, transaction frequency, and abnormal patterns).
- Identifying cryptocurrency red flags, including:
 - Rapid and high-value deposits and withdrawals.
 - Frequent transfers between multiple accounts.
 - Use of privacy-centric cryptocurrencies that may indicate attempts to obscure transaction details.

Automated alerts are generated for potentially suspicious activities, which are then reviewed by the compliance officer. If necessary, the compliance officer will escalate concerns to the Financial Intelligence Unit Curaçao (FIU) for further investigation and reporting.

All transaction monitoring and escalation procedures shall be conducted in strict accordance with the company's AML/CFT Policy and applicable legal frameworks.

3.3 Anti-Money Laundering (AML) Compliance

ZOOMBA B.V. aligns its AML program with local and international regulatory requirements. The company enforces strict AML controls, including:

- Mandatory identity verification for all users.
- Source of funds verification to ensure transactions originate from legitimate sources.
- Enhanced due diligence (EDD) for transactions exceeding predefined limits or deemed high-risk.
- Ongoing employee training on AML protocols, focusing on cryptocurrency-specific risks.

Suspicious Activity Reports (SARs) are filed promptly for any transactions suspected of involving money laundering. The AML process undergoes periodic audits to assess the effectiveness of controls and identify areas for improvement.

3.4 Data Security and Privacy

ZOOMBA B.V. ensures that all cryptocurrency transaction data is stored securely through:

- Encryption of sensitive data to prevent unauthorized access.
- Secure access controls to restrict data usage to authorized personnel only.
- Regular security assessments to detect and mitigate vulnerabilities.

The company fully complies with GDPR and other applicable data protection laws, ensuring that personal data collected during customer verification and transaction monitoring is lawfully processed and stored.

Regular audits of data security measures are conducted to identify and mitigate any risks. Responsible personnel ensure that all data security controls align with ZOOMBA B.V.'s Privacy Policy and regulatory obligations.

3.5 Anti-Fraud Measures

ZOOMBA B.V. implements fraud detection systems to identify and prevent fraudulent activities associated with cryptocurrency transactions. These measures include:

- IP tracking to detect suspicious geolocation activity.
- Device monitoring to identify multiple accounts linked to the same device.
- Behavior analytics to detect unusual user activity patterns.

Flagged transactions undergo manual review, and suspicious accounts are frozen pending investigation. If fraud is confirmed, ZOOMBA B.V. reserves the right to terminate accounts and take appropriate legal action.

All anti-fraud actions are documented in compliance with regulatory reporting requirements. Responsible personnel continuously evaluate and enhance fraud prevention measures in response to evolving cryptocurrency risks.

4. GOVERNANCE

4.1 Independent Audit

An independent audit of ZOOMBA B.V.'s cryptocurrency policies and AML/CTF framework is conducted annually to evaluate effectiveness, compliance, and risk management practices related to cryptocurrency usage.

The audit covers all relevant aspects, including:

- Customer verification;
- Transaction monitoring;

- AML compliance;
- Data security;
- Fraud prevention;

Findings from the audit are used to refine and enhance policies, ensuring all identified risks or gaps are addressed promptly. Audit results and necessary improvements are documented and reported to senior management for further action.

4.2 Review and Updating of the Policy

This policy is reviewed annually by the compliance officer and is updated to reflect:

- Changes in regulatory requirements;
- Technological advancements;
- Company-specific needs;

Policy updates are communicated to all employees, who must acknowledge and comply with any new guidelines or procedures introduced.

5. STAFF TRAINING AND AWARENESS

5.1 Mandatory Training

All relevant staff receive mandatory training on cryptocurrency transaction risks, controls, and procedures. Training sessions cover:

- Identification of red flags;
- Proper transaction monitoring protocols;
- Data security requirements;
- AML procedures tailored to cryptocurrency usage;

5.2 Ongoing Awareness and Assessment

ZOOMBA B.V. ensures employees understand their responsibilities under this policy, including when and how to escalate suspicious activity to the compliance officer.

Refresher training sessions are conducted annually or as needed, based on:

- Policy updates;

- Regulatory changes;
- Emerging threats;

The training program includes assessments to measure staff comprehension and readiness. Employees failing to demonstrate adequate understanding may be subject to:

- Additional training sessions;
- Corrective actions or disciplinary measures;

6. REPORTING AND ESCALATION

All staff must report any suspicions regarding cryptocurrency transactions immediately to the compliance officer. Reporting mechanisms include direct reporting channels and escalation procedures in line with ZOOMBA B.V.'s AML/CTF Policy.

The compliance officer is responsible for investigating and, where necessary, filing SARs with the FIU. All reports are documented, securely stored, and handled to maintain confidentiality and prevent tipping off.

Annual reports in accordance with LOK (Landsverordening op de Kansspelen) regulation are prepared and submitted, ensuring transparency and regulatory compliance.

7. REGULATORY COMPLIANCE AND SANCTIONS SCREENING

ZOOMBA B.V. is committed to ensuring compliance with international sanctions and local regulatory requirements by screening all cryptocurrency transactions and counterparties against relevant sanctions lists. This process is designed to prevent engagement with individuals or entities that are prohibited under applicable laws.

Sanctions screening is conducted in real-time using automated systems that cross-reference transactions against updated international and local sanctions lists. In cases where transactions or counterparties are flagged, they are immediately halted and placed under review by the compliance officer.

If a confirmed match is found with a sanctions list, ZOOMBA B.V. will take the necessary actions, including freezing the transaction and notifying relevant authorities, in compliance with Curaçao's regulatory framework. The company adheres to the legal requirements outlined by the Curaçao Financial Intelligence Unit (FIU) and the Central Bank of Curaçao and Sint Maarten.

8. RECORD KEEPING

ZOOMBA B.V. is fully compliant with Curaçao's the National Ordinance on identification when rendering services (LID) and the National Ordinance on the reporting of unusual transactions (LMOT), ensuring

the maintenance of accurate, complete, and up-to-date records for all cryptocurrency transactions, verification documents, monitoring activities, SARs for a minimum of five years. This is in accordance with both Curaçao's national regulations and international best practices.

Transaction records, verification documents, and other relevant materials are securely stored using encryption and robust access control systems, ensuring data integrity, confidentiality, and accessibility for regulatory audits.

The company's records are regularly reviewed to ensure completeness and accuracy, with the compliance officer overseeing compliance with record-keeping obligations. ZOOMBA B.V. adheres to strict data retention schedules aligned with legal requirements, and is committed to ensuring that all records are readily available for inspection by regulatory authorities annually.

9. POLICY BREACHES AND DISCIPLINARY ACTIONS

Failure to comply with this Crypto Usage Policy, including breaches of verification processes, monitoring protocols, AML regulations, data security standards, or fraud prevention measures, may result in disciplinary action, up to and including termination of employment.

Any violations identified through internal audits, transaction monitoring, or external regulatory reviews are immediately escalated to the Compliance Department. The department evaluates the breach and enforces corrective actions, ensuring that all violations are documented and that appropriate remedial measures are taken.

The compliance officer is responsible for overseeing all compliance violations and ensuring that corrective actions are implemented swiftly. Repeated violations or significant breaches may result in further legal actions or sanctions, depending on the nature and severity of the violation. ZOOMBA B.V. will cooperate fully with relevant authorities and take all necessary steps to ensure continued compliance with applicable laws.