

ROZAIRO N.V

Cryptocurrency Usage Policy

Compliance Department

Version Control

Version	Version Date	Approved By
1.0	16/04/2025	The Board

1. PURPOSE

This policy outlines the responsible and compliant use of cryptocurrency in the operations of Rozairo N.V ensuring alignment with the applicable laws of Curaçao, particularly the National Ordinance on Games of Chance (LOK), Anti-Money Laundering and Counter-Terrorism Financing (AML/CFT) regulations, and standards issued by the Curaçao Gaming Authority (CGA).

2. SCOPE

This policy applies to all departments, employees, contractors, and digital platforms operated by Rozairo N.V. that facilitate gaming or financial transactions using cryptocurrency.

3. RISK MANAGEMENT PRINCIPLES

- **Volatility Management:** All crypto funds are settled in stablecoins or fiat within 24 hours.
- **Wallet Security:** Cold storage is used for long-term holdings. Operational wallets employ multi-signature access and real-time monitoring.
- **Transaction Limits:** User deposits and withdrawals in cryptocurrency are subject to the same limits as fiat, including mandatory source of funds checks over €2,000.
- **Licensing:** Cryptocurrency-related services are limited to activities authorized under our CGA license. Additional services such as crypto exchanges or ICOs are not offered without separate CGA approval.

4. AML/CFT COMPLIANCE

In accordance with the LID and LMOT:

- Customer Due Diligence (CDD):
- All crypto users must undergo full KYC verification (ID, proof of address, source of funds).
- Transaction Monitoring:
- All crypto transactions are screened using blockchain analytics to detect suspicious behavior, including links to dark markets or sanctioned addresses.
- Unusual Transactions Reporting:

Any transaction flagged as suspicious or above threshold amounts is reported to the FIU Curaçao as per LMOT.

5. USER RESPONSIBILITIES

- All users transacting with cryptocurrency must:
- Complete KYC verification before making deposits or withdrawals.
- Acknowledge and accept the volatility and potential delays associated with blockchain-based transactions.
- Use wallets not linked to high-risk or sanctioned jurisdictions.

6. DATA PRIVACY & RECORDKEEPING

- All KYC/AML data related to cryptocurrency transactions are stored securely and retained for a minimum of 5 years.
- Wallet addresses used by users are logged and monitored for ongoing risk assessment.

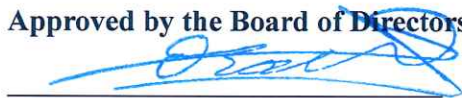
7. INTERNAL CONTROLS & TRAINING

- Regular audits are conducted to verify the integrity of crypto operations.
- All relevant staff are trained in handling crypto-related risks, regulatory expectations, and suspicious transaction identification.

8. POLICY REVIEW

This policy will be reviewed annually or as required by changes in law, technology, or business operations. Amendments must be approved by the Compliance Officer and the Board of Directors.

Approved by the Board of Directors:



Theoklis Andreou

Rozairo N.V.

Date: 16th of April 2025

Appendix A: KYC Checklist for Cryptocurrency Users

Checklist Item	Details / Document Type	Verified (✓)
1. Identity Verification (Passport / National ID)	See policy details	
2. Proof of Address (utility bill or bank statement)	See policy details	
3. Facial Verification / Liveness Check	See policy details	
4. Age Verification (must be 18+)	See policy details	
5. Source of Funds (e.g., payslip, tax return)	See policy details	
6. Crypto Wallet Ownership Verification	See policy details	
7. Blockchain Risk Screening	See policy details	
8. Sanctions & PEP Screening	See policy details	
9. Transaction Pattern Review	See policy details	
10. Approval / Rejection Decision by Compliance Officer	See policy details	

Compliance Officer Notes:

Reviewed By: _____ Date: _____

Appendix B: Crypto Risk Log Template

Date	User ID / Wallet	Crypto Type	Amount (USD)	Risk Flags	Blockchain Score	Action Taken	Reviewed By
2025-04-15	usr_4872 / 0xabc...	BTC	\$5,200	Large deposit	Medium (60/100)	KYC Triggered	A. Mensah

Risk Categories:

- Low (0–40): No immediate action.
- Medium (41–70): Trigger enhanced due diligence.
- High (71–100): Block and report transaction.