

Island Odyssey Ventures B.V

Crypto Usage Risk Policy

1. Purpose & Scope

This policy sets out the risk management framework for the use of cryptocurrencies (virtual assets) in relation to gambling operations. It ensures compliance with Curaçao licensing requirements, global AML/CTF standards, and responsible gaming principles.

Scope:

- Applies to all customer interactions involving crypto deposits, withdrawals, and gameplay.
 - Covers AML/CTF, fraud prevention, consumer protection, and operational risk.
-

2. Risk Assessment Framework

2.1 Key Risk Areas

- **AML/CTF Risk:** Potential for crypto to facilitate money laundering, terrorist financing, or sanctions evasion.
- **Volatility Risk:** Exposure to sudden value fluctuations affecting customer balances and settlements.
- **Operational Risk:** Risk of technology failures, wallet mismanagement, or cybersecurity breaches.
- **Reputational Risk:** Association with illicit crypto activity damaging the brand and license standing.
- **Regulatory Risk:** Non-compliance with Curaçao, FATF, or future EU rules on crypto and gambling.

2.2 Risk Appetite

- **Zero tolerance** for money laundering, sanctions breaches, terrorist financing.
 - **Moderate risk** accepted for crypto volatility (managed via conversion and limits).
 - **Low tolerance** for operational disruption or technology failures.
-

3. Control Measures

3.1 Customer Due Diligence (CDD/KYC)

- Mandatory identity verification before first crypto deposit or withdrawal.
- Enhanced Due Diligence (EDD) for:
 - High-value transactions.
 - Customers from high-risk jurisdictions (per FATF lists, EU blacklists).

Island Odyssey Ventures B.V

- Politically Exposed Persons (PEPs).
- Source of funds/source of wealth checks where warranted.

3.2 Transaction Monitoring

- Use of blockchain analytics providers (e.g., Chainalysis, Elliptic) to screen deposits/withdrawals.
- Flagging & escalation of:
 - Use of mixers/tumblers.
 - Links to darknet markets, sanctioned wallets, or known illicit activity.
 - Structuring patterns to avoid reporting thresholds.

3.3 Crypto Handling & Conversion

- Only approved cryptocurrencies (e.g., BTC, ETH, USDT) permitted.
- Customer balances recorded in fiat-equivalent (e.g., USD/EUR) to mitigate volatility.
- Automatic or regular conversion of crypto deposits into stablecoin or fiat.
- Cold storage for treasury funds, hot wallets limited to operational needs.

3.4 Limits & Controls

- Deposit/withdrawal limits in line with risk profile.
- Additional checks for large transactions (> EUR 2,000, or local reporting thresholds).
- Prohibition of third-party wallet usage (customer must control the wallet).

3.5 Record Keeping & Reporting

- Retain full transaction logs, KYC/AML documentation, and wallet addresses for at least 5 years.
- File Suspicious Transaction Reports (STRs) with Curaçao FIU when red flags are detected.
- Regular internal audit of crypto processes.

4. Governance & Responsibility

- **MLRO (Money Laundering Reporting Officer):** Oversees crypto-related AML/CTF risk.
- **CRO (Chief Risk Officer):** Ensures operational, reputational, and financial risk controls.
- **Board Oversight:** Regular review of crypto risk reports and policy updates.

5. Training & Awareness

- Staff trained on crypto-specific AML/CTF risks, red flags, and reporting obligations.

Island Odyssey Ventures B.V

- Ongoing refreshers aligned with FATF guidance and Curaçao regulatory updates.
-

6. Review & Updates

- Policy reviewed **annually** or upon material regulatory/market changes.

.