

Crypto Risk Management Policy

Version	Status	Date	Comments	Signature of the Approver
1.0	Approved	August 1, 2025	Policy created in order to align the activity of the Company with the regulatory requirements	

Policy owner:	Favorit United N.V.
Created by:	Yevhenii Pyroh / MLRO
Approved by:	Vedran Frelj / Managing Director
Date Approved:	August 1, 2025
Date last reviewed:	August 1, 2025
Review Frequency:	Annual
Security classification:	Private and Confidential

1. INTRODUCTION

The Company is dedicated to maintaining a secure, transparent, and compliant approach to cryptocurrency transactions within its online gaming operations. This Policy outlines the Company's methodology for managing cryptocurrency-related risks, including compliance with regulations, oversight of third-party collaborations, mitigation of operational threats, technological safeguards, market volatility management, and robust AML and fraud prevention controls.

2. SCOPE AND PURPOSE

This Policy applies to all cryptocurrency transactions processed by the Company, covering employees, third-party service providers, and partners engaged in the handling, monitoring, and processing of such transactions. Its objective is to establish a structured risk management framework to identify, assess, and mitigate potential threats arising from cryptocurrency

3. RISK MANAGEMENT MEASURES

3.1 Customer Verification and Due Diligence

The Company employs a rigorous customer verification system to authenticate users engaging in cryptocurrency transactions.

Key verification protocols include:

- Collection of essential identity documents (proof of identity and residence);

- Enhanced verification for high-risk users, such as politically exposed persons (PEPs) or users exhibiting unusual transaction patterns;
 - Regular review and updates to verification procedures to align with evolving regulatory requirements.
- These measures are applied consistently and integrated with the Company's AML/CFT compliance framework.

3.2 Transaction Monitoring and Anomaly Detection

The Company utilizes automated real-time transaction monitoring tools to detect potential irregularities, such as:

- Rapid, high-value transactions or withdrawals;
- Frequent movement of funds between multiple accounts;
- Engagement with high-risk or unregulated cryptocurrency exchanges;
- Use of privacy-focused cryptocurrencies (e.g., Monero, Zcash).

Suspicious activities are immediately flagged and escalated to the Money Laundering Reporting Officer (MLRO) for further investigation and potential reporting to the Financial Intelligence Unit Curaçao (FIU).

3.3 Anti-Money Laundering (AML) Compliance

The Company maintains an AML framework aligned with international and local standards, which includes:

- Real-time customer identity verification, including biometric validation where applicable;
- Verification of the source of funds for transactions exceeding predefined limits;
- Screening all transactions against international sanctions lists (OFAC, UN, EU, etc.).

Suspicious Activity Reports (SARs) are filed promptly for any transactions suspected of money laundering.

3.4 Cybersecurity and Data Protection

The Company ensures strong data security protocols to protect cryptocurrency-related transactions. Security measures include:

- End-to-end encryption of sensitive transaction data;
- Implementation of multi-factor authentication (MFA) for platform access;
- Frequent cybersecurity audits to detect and address vulnerabilities.

3.5 Fraud Prevention Mechanisms

To minimize fraudulent activities, the Company employs AI-driven fraud detection systems, including:

- IP address monitoring and geolocation tracking;
- Behavioral analytics to detect anomalies in user activity;
- Immediate freezing of accounts flagged for fraudulent behavior, pending investigation.

The Company reserves the right to terminate accounts in cases where fraudulent activity is confirmed, with documentation maintained for compliance records.

3.6 Risk Identification and Assessment

The Company implements a comprehensive risk assessment framework to identify and evaluate the various risks associated with cryptocurrency transactions. Key risk categories include:

- **Regulatory and Compliance Risks** – risks arising from non-compliance with local and international cryptocurrency regulations.

- **Operational Risks** – risks related to transaction processing failures, security vulnerabilities, and human error.
- **Market Risks** – risks associated with cryptocurrency price volatility affecting liquidity and financial stability.
- **Cybersecurity Risks** – risks related to hacking attempts, phishing, and unauthorized access.
- **AML and Fraud Risks** – risks associated with money laundering, financial crime, and fraud involving cryptocurrency transactions.

Each risk category is regularly reviewed and monitored to ensure effective risk mitigation strategies are in place.

3.7 Risk Mitigation Strategies

To minimize risks associated with cryptocurrency transactions, the Company employs the following mitigation strategies:

- **Regulatory Compliance:** the Company ensures compliance with all applicable Curaçao, FATF, and EU cryptocurrency regulations by regularly reviewing updates in laws and regulatory requirements.
- **Transaction Monitoring:** all cryptocurrency transactions are subject to real-time risk scoring, anomaly detection, and escalation to compliance teams in case of suspicious activities.
- **Cybersecurity Measures:** the Company employs advanced encryption protocols, two-factor authentication (2FA), and cold storage solutions to protect customer assets and private keys.
- **Liquidity Management:** risk exposure is controlled by limiting cryptocurrency holdings and integrating fiat conversion mechanisms to mitigate market volatility risks.
- **AML Controls:** the Company performs enhanced due diligence (EDD), sanctions screening, and real-time blockchain analytics to prevent illicit financial activities.

- **Third-Party Risk Management:** the Company conducts regular due diligence on third-party partners such as cryptocurrency exchanges and payment processors to ensure they adhere to compliance and security standards.

3.8 Ongoing Risk Monitoring and Adaptation

The Company continuously monitors its risk landscape using machine learning algorithms, blockchain forensics tools, and compliance analytics. Regular risk assessments are conducted to adapt risk management strategies based on:

- **Emerging threats and vulnerabilities** in the cryptocurrency industry.
- **Regulatory changes** that impact cryptocurrency risk exposure.
- **Performance of implemented risk controls**, ensuring their continued effectiveness.
- **Audit findings and external compliance reviews.**

All risk management measures are dynamically updated to reflect new threats, industry best practices, and regulatory expectations.

4. GOVERNANCE AND POLICY REVIEW

4.1 Risk Governance Structure

The Company has established a risk governance structure that ensures accountability and oversight in managing cryptocurrency risks. Responsibilities are allocated as follows:

- **Board of Directors:** oversees overall risk management strategy and ensures compliance with regulatory standards.
- **Money Laundering Reporting Officer (MLRO):** responsible for AML compliance and escalation of suspicious activities to regulators.
- **IT Security and Compliance Team:** ensures the security of crypto transactions and protects customer data from cyber threats.

4.2 Independent Risk Audits and Compliance Reviews

An independent risk audit is conducted semi-annually to evaluate:

- Effectiveness of risk controls and mitigation strategies;
- Compliance with evolving regulatory standards;
- Identification of new or emerging risks in cryptocurrency transactions.

Findings from the audit are used to enhance risk mitigation frameworks and improve risk management practices.

4.3 Annual Policy Review and Amendments

This Policy is reviewed annually by the MLRO and external compliance advisors to ensure ongoing compliance with:

- Curaçao Financial Intelligence Unit (FIU) requirements;
- The latest FATF cryptocurrency guidelines;
- International regulatory developments.

Any amendments are communicated to all employees, and acknowledgment of compliance is mandatory.

5. STAFF TRAINING AND REPORTING

5.1 Employee Risk Awareness and Training

All staff involved in cryptocurrency-related transactions undergo mandatory risk awareness training, covering:

- Identifying and mitigating cryptocurrency-specific financial crime risks;
- Best practices for transaction monitoring and red flag detection;
- Incident response and risk escalation procedures.

Training sessions are conducted bi-annually or as needed based on changes in risk exposure.

5.2 Risk Incident Reporting and Escalation

All staff are required to report cryptocurrency-related risks and suspicious transactions to the MLRO immediately. The MLRO investigates incidents and files SARs with FIU Curaçao, ensuring:

- Secure storage of reports;
- Protection of whistleblowers;
- Prevention of "tipping-off".

Incident reports are analyzed to improve risk mitigation strategies and prevent recurrence.

6. RECORD-KEEPING AND RISK DATA MANAGEMENT

The Company maintains comprehensive records of cryptocurrency transactions, risk assessments, and monitoring activities in compliance with Curaçao AML regulations.

All data is stored securely with encryption protocols and access controls, ensuring:

- Protection from cyber threats;
- Confidentiality and integrity of transaction records;
- Availability for regulatory audits upon request.

7. POLICY BREACHES AND DISCIPLINARY ACTIONS

Non-compliance with this Policy may result in immediate disciplinary actions, fines, or termination. Employees failing to adhere to risk management protocols will be subject to sanctions, including:

- Mandatory compliance re-training;
- Financial penalties (if applicable under Company policy);
- Termination of employment for repeated or severe breaches.

Significant Policy violations may lead to regulatory reporting and potential legal consequences.