

Cryptocurrency Risk Policy

Superstars Entertainment B.V.

1. Introduction and Purpose

This policy outlines the procedures for managing risks associated with the use of cryptocurrencies for deposits, wagers, and withdrawals on the gaming platform. The primary objective is to ensure compliance with Curaçao's laws and regulations, including the National Ordinance for Games of Chance (LOK), Anti-Money Laundering and Countering the Financing of Terrorism (AML/CFT) guidelines, and Financial Action Task Force (FATF) recommendations.

2. Regulatory Context in Curaçao

2.1. The **Curaçao Gaming Authority (CGA)** is the new central authority that regulates the online gaming sector in Curaçao.

2.2. The LOK, which came into effect in December 2024, requires greater rigor and transparency.

2.3. Cryptocurrencies are considered "virtual assets" and are subject to the same AML/CFT obligations as fiat currency transactions.

2.4. The company must be registered as a "Virtual Asset Service Provider" (VASP) with the Central Bank of Curaçao and Sint Maarten (CBCS) and comply with the requirements of the **National Ordinance on Identification when rendering services (LID)** and the **National Ordinance on the reporting of unusual transactions (LMOT)**.

3. Foundational Principles

3.1. Risk-Based Approach: The company will apply a strict risk assessment to all cryptocurrency transactions. Clients and transactions will be classified into different risk levels (low, medium, high).

3.2. Customer Due Diligence (CDD): All players who use cryptocurrencies must undergo a rigorous KYC (Know Your Customer) process, regardless of the transaction amount.

3.3. Transaction Tracing: The company will use blockchain monitoring tools to trace and analyze the origins and destinations of cryptocurrencies.

3.4. Continuous Monitoring: All cryptocurrency transactions will be monitored in real-time to identify suspicious behavioral patterns or "anomalous" transactions.

4. Risk Procedures and Internal Controls

4.1. Customer Due Diligence (CDD) and KYC

4.1.1. Identity Verification: All players must provide a valid form of identification (passport or national ID) and proof of residence.

4.1.2. Enhanced Due Diligence (EDD): EDD will be applied to players who fall into high-risk scenarios, such as:

- High-volume transactions.
- Transactions to and from "mixers," "tumblers," or other anonymity-enhancing wallets.
- Players from high-risk jurisdictions.
- Individuals listed on sanctions lists or PEPs (Politically Exposed Persons).

4.1.3. Prohibition of Anonymous Accounts: The platform will not allow anonymous or pseudonymous accounts. All accounts must be linked to a verified identity.

4.2. Transaction Monitoring

4.2.1. Deposit and Withdrawal Limits: The company will set deposit and withdrawal limits for cryptocurrencies, which may be adjusted based on the client's risk assessment.

4.2.2. Blockchain Analysis Tools: The company will use specialized software to:

- Analyze the source and destination of cryptocurrencies.
- Identify funds originating from illicit activities.
- Generate risk reports for each transaction.

4.2.3. Suspicious Transaction Alerts: The monitoring system will generate alerts for:

- Deposits and withdrawals to or from wallets associated with criminal activities.
- Multiple small transactions that total a large value (smurfing).
- Withdrawals to a wallet different from the one used for the deposit.

4.3. Reporting and Communication

4.3.1. Unusual Transaction Reports (UORs): The company will immediately report any transaction that fits the indicators of unusual activity to the **Financial Intelligence Unit (FIU) of Curaçao**, as per local legislation.

4.3.2. Compliance Reporting: The compliance team will be responsible for preparing regular reports for management and the CGA, detailing the volume of cryptocurrency transactions, the number of UORs, and the risk mitigation measures applied.

4.4. Training and Awareness

4.4.1. Employee Training: All employees involved in financial transactions, customer support, and compliance will receive regular training on AML/CFT best practices, with a specific focus on the risks and procedures of cryptocurrency transactions.

4.4.2. Policy Updates: This policy will be reviewed and updated annually, or more frequently if there are changes in the laws, regulations, or recommendations from the CGA and FATF.

5. Mitigation Measures

5.1. Source of Funds (SoF) Verification: For high-risk transactions, the company may ask the client to provide proof of the origin of their funds (e.g., wallet statements, mining records, exchange receipts).

5.2. Account Freeze: The company reserves the right to temporarily freeze a player's account if there is a suspicion of illegal activity or a lack of cooperation in verification.

5.3. Transaction Refusal: The company may refuse any cryptocurrency transaction that does not comply with this policy or is considered a high risk for money laundering or terrorist financing.

6. Responsibilities

6.1. The **Money Laundering Reporting Officer (MLRO)** is the primary person responsible for implementing and overseeing this policy.

6.2. The **Compliance** team is responsible for the daily execution of procedures and the monitoring of transactions.

6.3. **Senior Management** is responsible for ensuring that sufficient resources are allocated for compliance and for approving any exceptions to the policy.

Superstars Entertainment B.V. is committed to maintaining integrity and safeguarding both the business and its customers from financial crime. The use of cryptocurrencies provides operational efficiency; however, strict adherence to this policy is required to ensure ongoing compliance with Curaçao's regulatory requirements.

