

Yougmedia B.V.
Dr. H. Fergusonweg 1, Curacao

Crypto Usage Risk Policy

Version 2025

1. Purpose and Overview

This policy establishes a structured framework for the initial use of cryptocurrencies in the Company's licensed gaming operations. Recognizing the regulatory responsibilities associated with virtual assets, this document reflects our commitment to managing crypto-related risks responsibly and transparently from the outset.

Cryptocurrency functionality is being introduced in a **limited and controlled manner**, supported by strict compliance procedures, customer identity checks, and the use of regulated third-party crypto service providers. The scope of this policy and related procedures will expand as operations evolve.

2. Regulatory Compliance

The Company adheres to all legal obligations applicable under the Curacao gaming and financial compliance regime, including:

- **National Ordinance on the Reporting of Unusual Transactions (NORUT)**
- **National Ordinance on Identification when Rendering Services (NOIS)**
- Guidance from the **Central Bank of Curacao and Sint Maarten**
- FATF standards relating to **Virtual Assets (VA)** and **Virtual Asset Service Providers (VASP)**

The Company is prepared to cooperate with the **FIU Curacao** for reporting any unusual or suspicious crypto-related activity and considers AML/CFT compliance a core operational principle.

3. Current Scope of Crypto Usage

At this stage, the use of cryptocurrencies is limited to:

- Player deposits and withdrawals using approved crypto assets
- Use of external, regulated crypto payment processors
- Immediate or scheduled conversion of crypto to fiat (where applicable)

The Company does not engage in speculative crypto trading or long-term holding of cryptocurrencies on its balance sheet.

4. Accepted Cryptocurrencies

To minimize risk, only the below cryptocurrencies are accepted:

- USDT TRC-20
- USDT ERC-20
- Bitcoin
- Ethereum
- Litecoin
- Tron
- USDC Solana
- USDT Solana
- USDC ERC-20
- Solana
- Dogecoin
- Ripple
- BUSD
- Bitcoin Cash
- Cardano
- BNB BSC

No privacy-focused coins (e.g., Monero, Zcash, Dash) are allowed due to high anonymity risks.

All supported cryptocurrencies are subject to ongoing review. Any addition of new assets requires a compliance-led risk assessment.

5. KYC and Customer Verification

Cryptocurrency transactions are permitted once the customer has successfully completed KYC verification, which includes few or all of the below listed documentation/ information and might not be limited to (as the case may be)

- Government-issued ID/ passport
- Proof of address
- Sanctions and jurisdictional screening

The platform might restrict crypto access until the full identity of the user has been confirmed in line with applicable compliance standards.

6. Transaction Limits

To manage exposure, the following thresholds apply to cryptocurrency activity:

Tier	Verification Required	Monthly Limit (EUR)
1	ID/passport	Up to €1,000
2	ID/passport+ Proof of Address	€1,000 – €10,000
3	Enhanced Due Diligence	€10,000+

Higher-volume users must provide **Source of Funds (SoF)** and may be subject to ongoing monitoring or temporary restrictions.

7. Wallet Screening and AML Checks

The Company uses external tools (e.g., via its crypto payment provider) to ensure wallet addresses are screened before transactions are processed. Wallets are checked for:

- Connection to known illicit sources (e.g., darknet, scams)
- Use of mixing services
- Association with sanctioned entities or blocked addresses

Suspicious transactions are escalated to the Compliance Officer and, where necessary, reported to the **FIU Curacao**.

8. Custody and Fund Management

Crypto assets received are not stored long-term by the Company. All transactions shall be processed through **regulated third-party crypto payment service providers (PSPs)** that offer:

- Conversion to fiat (if required)
- Address screening and transaction history checks
- Secure custody for operational balances

Cold storage is not maintained internally at this stage; instead, reliance is placed on the PSP's licensed infrastructure.

9. Monitoring and Oversight

The Compliance Officer performs routine reviews of all crypto-related transactions using:

- Reports provided by the PSP or payment processor
- Internal customer behaviour analysis
- Manual review of flagged transactions

Any unusual activity (e.g., rapid deposits/withdrawals, behavioural anomalies) is investigated and documented. Compliance reports are prepared when feasible and to the extent applicable for internal review.

10. Staff Training

All relevant personnel are trained on the key risks associated with cryptocurrencies and the controls in place. Training includes:

- Basics of crypto transaction monitoring
- AML/CFT red flags
- Internal escalation procedures

Annual refresher sessions will be implemented, and training records shall be kept for auditing purposes.

11. Policy Review

This policy will be formally reviewed:

- Every 12 months, or
- Upon any material change in crypto usage, regulation, or payment partner operations

The Company commits to adapting this policy as the crypto program matures and additional tools or features are integrated.

12. Declarations

We confirm that this policy is enforced across all relevant departments and reflects our current operational scope and compliance strategy. It is designed to meet Curacao's legal requirements for AML/CFT risk management in relation to virtual assets.

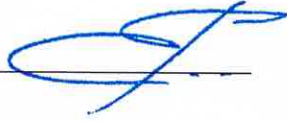
We will update this policy and notify relevant authorities in case of major procedural changes or risk findings.

Authorized Representative:

Name: Vivian Ersilia o.b.o.

Title: Managing Director of (SMES) Solutions for Management and Employment Support N.V.

Signature: _____

A handwritten signature in blue ink, consisting of a large, stylized 'S' followed by a horizontal line and a small flourish.

Date: 05.08.2025