

Crypto Usage Risk Policy

TAKTONUM GROUP N.V.

Version: June 01, 2025

1. Company Policy

This Crypto Usage Risk Policy outlines the risk management framework applied by TAKTONUM GROUP N.V. (WEI\$\$) in relation to the use of cryptocurrency for payments within its online gaming platform, operating under its Online Gaming License issued in Curaçao. This Policy outlines the WEI\$\$'s approach to identifying, assessing, mitigating, and monitoring the risks associated with the use of cryptocurrencies in the context of its operations.

The purpose of this document is to ensure compliance with regulatory expectations, particularly regarding AML/CFT/CFP controls, Know Your Customer (KYC) obligations, risk mitigation, and operational integrity. This policy applies to all business activities related to the acceptance of cryptocurrency payments, the involvement of third-party crypto processors, and risk management processes across all jurisdictions in which WEI\$\$ operates.

1. Definitions

For the purposes of this Policy, the following terms shall have the meanings set forth below:

- "Cryptocurrency" (or "Crypto") means a digital representation of value that can be digitally traded, transferred or stored electronically using distributed ledger technology or similar technology, and can be used for payment;
- "Blockchain" means a distributed, decentralized public ledger that records all cryptocurrency transactions.
- "Wallet" means a software program or physical device that stores public and private keys and can be used to send and receive cryptocurrencies.
- "Fiat Currency" means an official currency of a country that is issued by a central bank or other monetary authority.
- "AML" means Anti-Money Laundering.
- "KYC" means Know Your Customer.
- "CFT" means combating of the Financing of Terrorism.
- "CFP" means combating of the Proliferation of weapons of mass destruction.
- "Confirmation": The process by which a cryptocurrency transaction is verified and added to the blockchain.

2. Key Principles

- No Direct Custody: WEI\$\$ does not own or operate any cryptocurrency wallets. All crypto-related transactions are conducted through regulated and contracted third-party crypto processors.

- No Exchange Services: WEI\$\$ does not directly conduct crypto-to-fiat or fiat-to-crypto exchange operations; however, such services may be performed by its authorized processing partners in accordance with applicable legislation.

- No Exposure to Crypto Volatility: Users pay through crypto, but WEI\$\$ receives fiat settlement as per processor agreement terms.
- Traceability and Transparency: All crypto transactions are logged and monitored via the processor's platform, which provides traceability and risk scoring.

3. Roles and Responsibilities

- 1) Compliance Officer oversees adherence to AML/CTF/CFT controls and periodic review of AML/CTF/CFT Policy.
- 2) Payment Manager maintains communication with crypto processing partners. Payment Manager is responsible for periodic crypto transaction risk assessments and alignment with AML/CTF/CFT frameworks.
- 3) Finance Department ensures accurate accounting and reconciliation of funds received via crypto processors.
- 4) IT & Security ensures data integrity, monitoring of API integrations with processors, and transactional alerts.

4. Crypto Processing Partners

WEI\$\$ maintains contractual relationships with crypto processing partners. These partners are responsible for:

- Providing all wallet addresses used for transaction processing.
- Conducting AML/KYC verification of users in accordance with applicable regulatory requirements under their licensing regime.
- Performing risk classification and assessment of each transaction to detect potentially suspicious or high-risk activity.
- Generating and maintaining transaction risk scores and related compliance reports.
- Ensuring the security, traceability, and auditability of all crypto transactions.
- Maintaining an access log to all wallets to ensure accountability and control over wallet-related operations.
- Implementing real-time monitoring and anomaly detection systems to identify irregular activity.
- Ensuring secure custody and management of private keys and applying secure access mechanisms where applicable.

WEI\$\$ selects partners based on:

- Licensing and regulatory standing.

- Reputation and industry standing.
- Technical capability, including real-time risk scoring.
- Transparent and auditable processes.

5. Risk Identification and Mitigation

To ensure the secure, transparent, and compliant use of cryptocurrency, WEI\$\$ applies a structured approach to risk identification and mitigation. The main categories of risk associated with crypto-related operations include volatility, AML/CTF/CFT exposure, operational issues, and reputational impact.

- **Volatility Risk.**
The value of cryptocurrencies may fluctuate during transactions, potentially affecting the settlement amount. To mitigate this risk, all cryptocurrency transactions are processed in real time by WEI\$\$'s crypto processing partners.
- **AML/CTF/CFT Risk.**
Cryptocurrencies may be misused for money laundering or terrorist financing purposes. To prevent this, all AML and KYC procedures are fully outsourced to verified crypto payment providers that operate under strong compliance frameworks and regulatory oversight.
- **Operational Risk.**
Errors may occur in transaction routing or wallet handling. WEI\$\$ mitigates this risk by not maintaining any crypto wallets directly. All routing and settlement activities are performed by experienced crypto partners who ensure proper transaction management and reconciliation.
- **Reputational Risk.**
There is a potential reputational risk of association with unregulated or opaque crypto activity. WEI\$\$ minimizes this by working exclusively with transparent and compliant crypto processors that maintain high standards of governance and reporting.
- **Regulatory and Legal Risk.**
The regulatory landscape for cryptocurrencies is rapidly evolving and varies significantly across jurisdictions. There is a risk that new laws, regulations, or interpretations could impact the legality of cryptocurrency usage, taxation, or the ability to convert crypto to fiat currency. WEI\$\$ operates under a license issued by the Curaçao Gaming Authority. However, User is responsible for ensuring that His use of cryptocurrencies on WEI\$\$'s Platform complies with all applicable laws and regulations in User's own jurisdiction of residence or citizenship.

6. Record Keeping and Transparency

To ensure transparency, accountability, and ongoing regulatory compliance, WEI\$\$ maintains comprehensive records of all cryptocurrency-related activities conducted through its authorized partners. This approach supports auditability, strengthens internal controls, and enables timely detection of any irregularities or compliance risks.

WEI\$\$:

- Retains complete audit trails of all crypto transactions, as reported by its processing partners.
- Maintains records of risk scores and partner compliance reports, ensuring that all counterparties operate within approved risk thresholds.
- Includes crypto-related compliance reviews as part of its internal audit schedule to verify adherence to AML/CTF/CFT, data protection, and operational control requirements.
- Ensures that all data is stored and processed in full compliance with applicable data protection laws.

7. Monitoring and Review

To ensure that this Policy remains effective, compliant, and aligned with evolving regulatory and operational requirements, WEI\$\$ maintains a structured review and amendment process.

This Policy shall be:

Reviewed at least annually, or earlier if there are material changes to cryptocurrency regulations, compliance obligations, or processing partners.

Amended as necessary to reflect updates in applicable legislation, technological developments, or modifications to WEI\$\$'s business or operating model.

All revisions must be documented, and communicated to relevant stakeholders to ensure continued adherence.

Signature of Managing Director:

Eduards Kalnins



Date: June 01, 2025