

Crypto User Risk Policy

Prepared by	Date	Version
Denitza Dimitrova	01.06.2025	1.0

TC ENTERTAINMENT N.V.

1. Purpose and Scope

This Risk Policy outlines the framework for identifying, assessing, managing, and mitigating risks associated with the use of cryptocurrencies by users engaging with our online gambling platform licensed under Curaçao law. It ensures compliance with:

- Curaçao National Ordinance on the Prevention and Combating of Money Laundering and Terrorist Financing (NOIS).
- GCB compliance guidelines and AML/CFT regulations.
- FATF recommendations.
- Internal controls and responsible gaming standards.

This policy applies to all crypto-using customers and all departments within the company handling customer interaction, payments, compliance, and risk management.

2. Risk Categories

The following risk categories are addressed:

2.1. Customer Risk

- Use of pseudonymous or anonymous cryptocurrencies.
- Lack of verifiable identity or source of funds.
- History of suspicious transactions or gaming behavior.

2.2. Transactional Risk

- Unusually large deposits or rapid deposit-withdrawal cycles.
- Cross-chain transactions and obfuscation techniques (e.g., mixers, tumblers).
- Use of privacy-focused wallets or exchanges with insufficient KYC/AML practices.

2.3. Geographic Risk

- Users accessing the platform from sanctioned jurisdictions or high-risk countries per FATF list.
- Use of VPNs or proxy IPs to obscure true geographic location.

2.4. Technological Risk

- Smart contract vulnerabilities or third-party custodianship of crypto assets.
 - Volatility in crypto markets affecting platform liquidity or user withdrawals.
-

3. Risk Assessment and Scoring Framework

A risk score is assigned to each user based on the following weighted criteria:

Risk Factor	Weight	Example Triggers
KYC Verification Completeness	30%	Incomplete ID or proof of address
Crypto Source Transparency	25%	Funds from high-risk exchanges, mixers
Transaction Pattern	20%	Rapid deposit/withdraw cycles, abnormal volumes
Geolocation and IP Analysis	15%	Use of VPNs, logins from sanctioned jurisdictions
Behavior/Gameplay Monitoring	10%	Bonus abuse, arbitrage betting

Users are classified as:

- **Low Risk (0–40)**
- **Medium Risk (41–70)**
- **High Risk (71–100)**

High-risk users are flagged for Enhanced Due Diligence (EDD) and subject to transaction monitoring or account suspension.

4. Know Your Customer (KYC) and Customer Due Diligence (CDD)

4.1. KYC Requirements for Crypto Users

All users must complete identity verification prior to making a crypto deposit or withdrawal, including:

- Government-issued ID.
- Proof of address (utility bill or bank statement).
- Optional: Live selfie and/or video verification for flagged accounts.

4.2. Source of Funds for Crypto Users

Where necessary, users may be asked to provide:

- Blockchain explorer links verifying wallet ownership.
 - Statements from exchange accounts showing crypto purchase.
 - Declaration of source of income (e.g., salary, trading profits).
-

5. Cryptocurrency Acceptance Policy

The platform will only accept cryptocurrencies that meet the following criteria:

- Listed on a reputable exchange with fiat on-ramps.
- Traceable via blockchain analytics tools (e.g., Chainalysis, TRM Labs).
- Not primarily used for anonymity (e.g., Monero, Zcash not accepted).

Supported assets include but are not limited to:

- Bitcoin (BTC)
 - Ethereum (ETH)
 - USDT (ERC-20, TRC-20)
 - USDC
-

6. Transaction Monitoring and Blockchain Analytics

All crypto transactions are screened through blockchain analysis tools to detect:

- Transactions from/to sanctioned wallets.
- Use of privacy-enhancing techniques.
- Patterns consistent with money laundering.

Suspicious Activity Reports (SARs) are filed with the Financial Intelligence Unit (FIU) Curaçao as required.

7. Enhanced Due Diligence (EDD)

EDD is triggered for:

- High-value transactions (over USD 10,000 or equivalent in crypto).
- Users scoring high on the risk scoring framework.
- Crypto funds originating from decentralized exchanges (DEXs), mixers, or unknown wallets.

EDD includes:

- Manual transaction review.
 - Source of wealth verification.
 - Live verification interview (where feasible).
-

8. Responsible Gambling and User Protection

For crypto users, the following risk mitigation and protection measures apply:

- Deposit and loss limits by default until user profile is fully verified.
 - Self-exclusion and cooling-off options available regardless of crypto activity.
 - Monitoring for compulsive behavior or excessive losses in volatile crypto environments.
-

9. Regulatory Compliance

The company ensures:

- Compliance with NOIS and Curaçao GCB directives.
 - Ongoing risk training for relevant staff.
 - Annual audit of crypto risk controls and AML systems.
 - Cooperation with regulatory authorities and law enforcement when needed.
-

10. Policy Review and Updates

This Crypto Risk Policy is reviewed **annually** or in response to:

- Significant regulatory changes.
- Updates to FATF guidance.
- Emerging risks in the cryptocurrency landscape.

Changes are approved by the Compliance Officer and documented in internal records.

11. Record Keeping

All user due diligence documents, blockchain analysis reports, transaction records, and risk assessments are retained for a **minimum of 5 years**, in accordance with Curaçao AML obligations.

12. Contact and Escalation

For questions, risk concerns, or reporting suspicious behavior:

Compliance Department

Email: compliance@tcentertainment.com