

Crypto Risk Policy

1. Introduction

This Crypto Risk Policy (hereinafter - the "Policy") has been developed by Topxgo N.V. (hereinafter - the "Company"), registered in Curaçao under number 165952, in strict compliance with the requirements of the Curaçao Gaming Control Board (CGA), including the National Ordinance on Games of Chance (LOK, P.B. 2024 no. 157), National Ordinance on Offshore Games of Hazard (NOOGH, P.B. 1993 no. 63), Provisional Online Gaming Licence (Chapter 4 LOK, OGL/2024/496/0781 issued on 23 May 2025), AML/CFT/CPF-Regulations, National Ordinance on Identification when Rendering Services (LID, PB 2017 no. 92), National Ordinance on Reporting of Unusual Transactions (LMOT, PB 2017 no. 99), and other applicable legal and regulatory acts, recommendations, and studies.

The purpose of the Policy is to minimize risks associated with virtual assets (cryptocurrencies) in online gambling on the platform (hereinafter - the "Site"), prevent money laundering, terrorism financing (AML/CFT), and other crimes, and protect both players and the Company. The Policy is mandatory for all employees, contractors, partners, and is integrated with the Company's existing policies, including those posted on the Site.

2. Definitions

Terms beginning with a capital letter and used in this Policy have the following meanings, unless otherwise derived from the context:

- **Virtual Assets (Cryptocurrencies):** Digital representations of value intended for payments and not classified as fiat currencies (in accordance with FATF and LID definitions, including stablecoins such as USDT).
- **Licensed International Exchanges:** Regulated platforms (e.g., Binance, Coinbase, Kraken) with confirmed AML/CFT compliance (Article 9(6) LOK).
- **KYC/AML/CFT:** Client identification procedures, anti-money laundering, and terrorism financing (per LMOT and AML/CFT-Regulations).
- **STR (Suspicious Transaction Report):** Report on suspicious transactions submitted via the goAML system (LB 2019 no. 19/0283).
- **Mixing-Lists:** Lists of addresses linked to mixing services for obfuscation (per FATF risk indicators).
- **Sanctions Lists:** Lists approved by OFAC, EU, UN, and CGA (updated weekly).
- **Travel Rule:** FATF requirement for transmitting sender/recipient data for transactions exceeding \$1000.
- **VASPs:** Virtual Asset Service Providers, including the Company as an operator (Recommendation 15 FATF).
- **Source of Funds (SoF):** Sources of funds for cryptocurrency deposits subject to mandatory verification (CGA refusal grounds, strengthened in 2025).

3. Identification and Assessment of Risks

The Company is obliged to identify and assess risks in strict accordance with CGA, FATF, and ICGR Research guidelines. Key risk categories include:

- **Regulatory Risks:** Non-compliance with Articles 9(6-8) LOK, LID, or LMOT, potentially leading to license revocation (probability: medium; impact: high).
- **AML/CFT Risks:** Money laundering through cryptocurrency, terrorism financing, or sanctions violations (per Section 4.2 AML/CFT-Regulations; high probability in decentralized finance (DeFi) and stablecoins).
- **Operational Risks:** Exchange rate volatility, blockchain failures, or cyberattacks (including storage risks for non-custodial wallets and ransomware attacks).
- **Reputational Risks:** Association with illegal activities (per Chainalysis reports, where the share of illegal cryptocurrency transactions was approximately 0.14% in 2024, with a declining trend in 2025).
- **Financial Risks:** Losses from unauthorized transactions or volatility (including DeFi protocol exploits).
- **Technological Risks:** Integration with high-risk VASPs or vulnerabilities related to offshore operations.
- **Risks to Players:** Volatility, transaction irreversibility, and potential financial losses (per ICGR Research publications).

Risk assessment uses a matrix (probability multiplied by impact, supplemented by metrics such as volatility above 10%, classified as high risk; KPI: less than 5% high-risk transactions). High-risk scenarios require immediate mitigation measures. Stress testing and external certification are conducted as needed, based on assessed risk levels, with special attention to stablecoins and DeFi per FATF guidelines.

4. Measures to Manage Risks

The measures outlined in this section are based on strict adherence to CGA and FATF standards, establishing a zero-tolerance policy for violations and adapting measures according to risk levels.

4.1. Permissible Assets

Acceptance of only cryptocurrencies from licensed international exchanges (e.g., Binance, Coinbase) or Company-controlled wallets is permitted. Privacy coins (e.g., Monero) are prohibited unless approved by CGA (Article 9(8) LOK). Monitoring is conducted automatically with audit logs to ensure compliance.

4.2. Transaction Monitoring

Real-time monitoring of all cryptocurrency transactions using AI tools to detect anomalies (e.g., large volumes, high-risk jurisdictions). Transactions from mixing-lists or sanctions-listed addresses are blocked immediately. KPI: 100% screening of addresses.

4.3. Wallet and Exchange Integration

Integration is limited to licensed exchanges and Company wallets. Non-custodial wallet usage is allowed only with enhanced KYC/AML checks, subject to CGA approval.

4.4. KYC/AML Procedures for Cryptocurrency Addresses

Screening of addresses against sanctions lists and mixing-lists (OFAC, EU, UN, CGA) using mandatory tools (e.g., Chainalysis or Elliptic – per Section 4.2 AML/CFT-Regulations). Full KYC: identity, SoF, and address verification (per LID); enhanced due diligence for high-risk scenarios (e.g., transactions over \$3000 per FATF guidelines; mandatory SoF verification for all crypto deposits, prohibiting origins from FATF gray or black lists). Travel Rule: sender/recipient data transmission for transactions over \$1000 (per TFR from June 2025, emphasizing immediate compliance). Monitoring: AI-based screening for anomalies as needed. Suspicious activity triggers asset freezing, STR submission via goAML within 24 hours (per LMOT); compliance level in reporting exceeds 95%; integration with the Player Complaints Policy for related claims.

4.5. Monitoring and Audit

Monitoring using AI (for volatility and illegal flows; KPI: 100% address screening) as needed. Audits: internal as needed, external on a regular basis depending on risk levels (with ISO 27001 standards integration). Training: conducted as needed on AML/CFT and cryptocurrency risks (applicable to all employees).

4.6. Player Protection and Education

Player warnings: risk notifications (volatility, irreversibility, potential losses) displayed before crypto deposits per CGA Responsible Gaming Policy and ICGR research. Integration with responsible gambling: betting limits in cryptocurrency for vulnerable players (e.g., self-exclusion from crypto transactions, deposit limits) as needed. Behavior monitoring: AI used to detect problematic cryptocurrency usage as needed.

4.7. Incident Response

Protocol for cryptocurrency-specific incidents (e.g., wallet compromise, blockchain forks, ransomware): immediate isolation, CGA notification within 24 hours, and recovery from backups (with monthly reports per the May 2025 AML reboot) in case of significant events. Incident Response Team (IRT): operates 24/7, with annual simulations as needed (per PayRam guidelines).

5. Responsibility and Control

- **Compliance Officer:** Responsible for implementation, monitoring, and reporting to CGA.
- **Management:** Approves the Policy, allocates resources; bears personal liability for violations.
- **Employees:** Must strictly comply; violations lead to disciplinary actions (including termination and fines).

- **Players:** Informed via the platform; non-compliance results in account blocking.
- **Control:** Reports in case of significant incidents, integration with goAML; external reporting (e.g., mutual evaluations FATF) as needed.

6. Review and Update

The Policy is subject to regular review as needed, triggered by regulatory changes (e.g., FATF updates) or incidents.

Last version: 17 August 2025. Contact: compliance@top-x-go.com

Appendix A: Risk Matrix

Risk	Probability	Impact	Metric	Measures for Management
AML in DeFi	High	High	>5% illicit	Enhanced due diligence, AI-monitoring
Currency volatility	Medium	High	>10% fluctuations	Daily monitoring, bet limits
Wallet hacking	Low	Critical	>1 vulnerabilities/year	Encryption, external audit
Sanctioned jurisdictions	Medium	High	From blacklists	Automatic address screening
Risks for players	High	Medium	>20% complaints	Warnings, self-exclusion

Appendix B: Glossary of Extensions

- **DeFi (Decentralized Finance):** Blockchain-based decentralized financial services such as lending, staking, or exchanges without a central intermediary. Related investment products are prohibited to minimize risks.
- **Stablecoins:** Cryptocurrencies pegged to stable assets (e.g., USDT to USD), intended to reduce volatility. Allowed only with low anonymity risk and per FATF standards.
- **VASPs (Virtual Asset Service Providers):** Providers of virtual asset services, including exchange, storage, or transfer of cryptocurrencies (Recommendation 15 FATF). The Company is recognized as a VASP in transaction processing.
- **Travel Rule:** FATF rule on sender/recipient data transmission for transactions over \$1000, updated in June 2025 with an emphasis on immediate compliance.
- **Privacy Coins:** Cryptocurrencies with enhanced anonymity (e.g., Monero), prohibited without CGA approval due to high AML risks.
- **Custody Risks:** Risks associated with storing crypto-assets, including non-custodial wallets where the Company is not liable for losses.
- **goAML:** CGA system for submitting STRs, mandatory for suspicious transaction reports within 24 hours.