

CRYPTO RISK POLICY

MuchGaming B.V.

operating as Crypto.Games

Document Title	Crypto Risk Policy
Version	1.0
Effective Date	17 June 2026
Review Frequency	Annual (or upon material regulatory change)
Document Owner	Compliance Officer
Approved by	Board of Directors
Classification	Confidential – Internal Use Only
Regulatory Basis	CGA Crypto Policy Guideline (Dec 2025); LOK; LID; LMOT; FATF Recommendations

1. Purpose and Scope

1.1 Purpose

This Crypto Risk Policy (the “Policy”) establishes the framework under which MuchGaming B.V. (the “Company”) accepts, manages, and controls virtual assets and cryptocurrency transactions across all phases of the customer journey, including deposits, wagering, withdrawals, and treasury management.

The Policy is mandatory for all employees, contractors, and group entities that support licensed operations. It supplements, but does not replace, obligations arising under other applicable statutes, including Virtual Asset Service Provider (VASP) registration requirements and FATF Recommendations.

1.2 Scope

This Policy applies to:

- All crypto-asset workflows: deposits, wagering, withdrawals, and treasury management;
- All group entities and third parties (VASPs, payment processors, affiliates) supporting the licensed operation;
- All employees and contractors who handle, approve, or oversee virtual asset transactions;
- All jurisdictions from which the Company accepts players, to the extent those jurisdictions permit online gambling.

Regulatory basis:

- National Ordinance on Games of Chance (LOK), effective December 2024
- CGA Crypto Policy Guideline, December 2025
- National Ordinance on Identification when Rendering Services (LID)
- National Ordinance on Reporting of Unusual Transactions (LMOT)
- CGA AML/CFT Policy, effective 9 January 2025
- FATF Recommendations (virtual assets & VASPs)

2. Governance and Accountability

2.1 Board Responsibility

Ultimate accountability for this Policy rests with the Board of Directors. The Board approves this Policy, its amendments, and any material changes to the permitted virtual asset list or VASP relationships. The Board receives quarterly reports on crypto-risk metrics and annual Policy reviews.

2.2 Compliance Officer (MLRO)

The Compliance Officer (serving also as Money Laundering Reporting Officer, MLRO) is responsible for:

- Day-to-day oversight of this Policy and its implementation;
- Signing off on this Policy and all material amendments before Board approval;
- Approving on-chain risk screening procedures and escalation thresholds;
- Reviewing and authorising the addition or removal of any crypto asset or VASP;
- Filing Suspicious Transaction Reports (STRs) with FIU Curaçao via the goAML platform;
- Overseeing staff training on crypto-specific AML/CFT risks.

2.3 Payments Team

The Payments Team is responsible for:

- Executing crypto deposit and withdrawal processes in accordance with this Policy;
- Conducting wallet ownership and origin checks at onboarding and periodically thereafter;
- Maintaining the operational, treasury, and player-flow wallet architecture;
- Monitoring transaction volumes and escalating anomalies to the Compliance Officer.

2.4 Change Management

Any change to the scope of this Policy — including adding or removing a crypto asset or VASP, changing wallet architecture, or modifying risk thresholds — requires:

- A documented risk assessment prepared by the Compliance Officer;
- Formal sign-off by the Compliance Officer and Board (or delegated sub-committee);
- Updated training delivered to affected staff within 30 days of the change.

3. Permitted and Prohibited Crypto Assets

3.1 General Principle

The CGA treats cryptocurrencies as inherently higher-risk payment instruments. The Company therefore applies asset-specific risk assessments before accepting any virtual asset and maintains an approved asset list. Assets not on the approved list are prohibited by default.

3.2 Asset Classification

Asset / Activity	Risk Rating	Required Controls
Bitcoin (BTC)	HIGH	Standard KYC + on-chain screening

Asset / Activity	Risk Rating	Required Controls
Ethereum (ETH)	HIGH	Standard KYC + on-chain screening
Litecoin (LTC)	HIGH	Standard KYC + on-chain screening
Fiat-backed stablecoins (e.g. USDT, USDC)	HIGH	Standard KYC + on-chain screening
Unregulated / algorithmic stablecoins	HIGH	PROHIBITED — not accepted
Privacy coins (XMR, ZEC, DASH)	HIGH	PROHIBITED — not accepted
Meme coins (limited to DOGE, SHIB, PEPE)	HIGH	Permitted if market cap $\geq$ USD 300M at time of review (see §3.6); otherwise PROHIBITED
Wrapped tokens of unknown origin	HIGH	PROHIBITED — not accepted
Mixer / tumbler-linked funds	HIGH	PROHIBITED — rejected on-chain

3.3 Prohibited Assets and Sources

The following are absolutely prohibited and must be rejected or blocked:

Prohibited Asset / Source	Reason for Prohibition
Privacy coins (Monero, Zcash, Dash)	Anonymisation features prevent on-chain tracing
Wrapped tokens of unknown origin	Cannot verify underlying asset legitimacy
Meme coins below USD 300M market cap	Insufficient market depth; elevated pump-and-dump and fraud risk; inadequate on-chain liquidity
Tornado Cash, Blender.io or similar mixers/tumblers	Sanctioned mixer; obfuscates transaction trail
Sanctioned wallet addresses	OFAC / EU / UN sanctions compliance
Anonymous or unhosted wallets with no verifiable owner	Cannot satisfy CDD obligations under LID

3.4 Stablecoin Policy

Fiat-backed stablecoins issued by regulated entities are the preferred alternative to unbacked cryptocurrencies. Unregulated or algorithmic stablecoins require heightened review and Board approval before being added to the permitted list. The Company shall conduct issuer due diligence annually and after any material market event affecting a stablecoin.

3.5 Meme Coin Policy

Notwithstanding the general prohibition on meme coins, the Company permits acceptance of selected high-market-capitalisation meme coins, specifically DOGE (Dogecoin), SHIB (Shiba Inu), and PEPE, subject to the conditions set out in this section. This exception is justified by the demonstrated on-chain liquidity, widespread exchange availability, and mainstream adoption of these assets, which reduce — though do not eliminate — the fraud and volatility risks otherwise associated with the meme coin category.

Market Capitalisation Threshold:

A meme coin is eligible for acceptance only if its market capitalisation equals or exceeds USD 300,000,000 (three hundred million US dollars) at the time of the most recent quarterly review. The Compliance Officer, in consultation with the Payments Team, assesses market capitalisation at least quarterly using data from at least two independent sources (e.g. CoinGecko, CoinMarketCap). If a coin falls below the threshold at any review, deposits in that coin are suspended immediately and existing balances must be withdrawn or converted within 30 days of the suspension notice.

Permitted Coins (as of effective date):

Coin	Ticker	Condition	Review Frequency
Dogecoin	DOGE	Market cap ≥ USD 300M	Quarterly
Shiba Inu	SHIB	Market cap ≥ USD 300M	Quarterly
PEPE	PEPE	Market cap ≥ USD 300M	Quarterly

Any meme coin not listed above remains prohibited by default. Addition of a new meme coin requires a documented risk assessment and Compliance Officer and Board approval, regardless of market capitalisation.

Enhanced Controls for Permitted Meme Coins:

Given the elevated volatility and speculative nature of meme coins, the following additional controls apply:

- Deposit and withdrawal limits: lower per-transaction and monthly limits than apply to major cryptocurrencies (BTC, ETH), set and reviewed quarterly by the Compliance Officer;
- On-chain screening: mandatory for every deposit, with risk scoring equivalent to that applied to other high-risk assets;
- Same-wallet and same-asset rule: applies without exception (see Section 4.1);
- Slippage disclosure: due to the price volatility of meme coins, players are shown real-time exchange rates and slippage warnings at the point of deposit and withdrawal;
- Suspension trigger: if the 7-day average price of a permitted meme coin drops by 50% or more, deposits are suspended pending an emergency review by the Compliance Officer;
- KYC/CDD: standard CDD applies; players depositing above the equivalent of NAF 2,000 in meme coins within 30 days are subject to source-of-funds verification.

Review and Removal:

The Compliance Officer reviews the meme coin permitted list quarterly. A coin is removed from the permitted list if: (a) its market capitalisation falls below USD 300M; (b) it becomes subject to regulatory prohibition in a key jurisdiction; (c) it exhibits characteristics of market manipulation or wash trading; or (d) the Compliance Officer or Board otherwise determines that its risk profile is unacceptable. Removal takes effect immediately upon the Compliance Officer's decision, with a 30-day wind-down period for existing player balances.

3.6 Deposit and Withdrawal Limits

The Company sets deposit and withdrawal limits for each permitted asset. Limits are reviewed quarterly by the Compliance Officer and calibrated to player risk profile and CDD status. Players who have completed Enhanced Due Diligence (EDD) may access higher limits subject to Compliance Officer approval.

Cooling-off periods apply between deposits and withdrawals to deter structuring. All fees and slippage rules are disclosed to players prior to transaction execution.

4. Transaction Management

4.1 Same-Wallet and Same-Asset Rule

In accordance with the CGA Crypto Policy Guideline, the following rules apply to all transactions:

- Withdrawals must be sent to the same wallet address used for the player's most recent deposit;
- Withdrawals must be paid in the same cryptocurrency as the deposit;

- Player-to-player transfers are strictly prohibited;
- The Company does not offer cryptocurrency exchange services; links to third-party exchanges on separate websites may be provided, but the Company does not facilitate exchange directly.

4.2 Threshold Monitoring

Transactions are monitored against the following thresholds:

Threshold	Trigger	Action Required
NAf 1,000 (or equiv.)	Single deposit or withdrawal	Verify wallet ownership
NAf 4,000–5,000 (or equiv.)	Cumulative within 30 days	Full CDD / identity verification
NAf 10,000+ (or equiv.)	Any single transaction	Enhanced Due Diligence (EDD)
Any amount	High-risk wallet exposure detected	Immediate block & STR filing

Exact thresholds are reviewed annually by the Compliance Officer and updated in line with FIU Curaçao and CGA guidance. The above figures reflect current regulatory guidance as of June 2026 and are subject to change.

4.3 Structuring Prevention

The transaction monitoring system is configured to detect patterns indicative of structuring (smurfing), including but not limited to:

- Multiple deposits just below reporting thresholds within a short timeframe;
- Rapid alternation between cryptocurrencies to obscure transaction trails;
- Use of multiple accounts or wallets by the same beneficial owner.

Detected structuring patterns are escalated immediately to the Compliance Officer.

5. Wallet Architecture, Custody and VASP Standards

5.1 Wallet Ownership and Segregation

Only entity-owned wallets are permitted. Personal wallets or wallets linked to the Ultimate Beneficial Owner (UBO) are prohibited for business purposes. The Company maintains the following segregated wallet architecture, as required by the CGA:

Wallet Type	Purpose	Security Controls
Operational Wallets	Day-to-day transactions; routine player payments	MFA; withdrawal whitelist; daily reconciliation
Treasury Wallets	Strategic reserves; long-term holdings	Multi-signature; HSM; cold storage; restricted access
Player-Flow Wallets	Customer deposits and withdrawals	MFA; on-chain screening on receipt; segregated per asset

5.2 Access Security

All wallet systems must implement the following minimum security controls:

- Multi-Factor Authentication (MFA) for all wallet access;
- Hardware Security Modules (HSMs) for private key storage on treasury wallets;
- Withdrawal whitelist: withdrawals only to pre-approved, verified addresses;
- Multi-signature (multi-sig) protocols for treasury wallet transactions (minimum 2-of-3);
- Audit logs of all access events and transaction approvals, retained for a minimum of 7 years.

5.3 VASP Standards and Due Diligence

All crypto transactions must be routed through regulated Virtual Asset Service Providers (VASPs). Before engaging any VASP, and annually thereafter, the Company conducts VASP due diligence to confirm that the VASP:

- Holds a valid registration or licence with a recognised regulatory authority;
- Implements robust AML/CFT controls, including transaction monitoring;
- Complies with the FATF Travel Rule (Recommendation 16), providing originator and beneficiary information with every transfer;
- Does not operate in FATF high-risk or black-listed jurisdictions;
- Maintains adequate cyber-security and business continuity measures.

VASP due diligence records are maintained by the Compliance Officer and made available to the CGA upon request.

6. AML/KYC in the Crypto Context

6.1 Risk-Based Approach

The Company applies a Risk-Based Approach (RBA) to all crypto transactions as required by the CGA AML/CFT Policy. Cryptocurrency payments are treated as inherently higher-risk, requiring proportionately more rigorous controls than fiat payment methods. Risk is assessed at two levels:

- Business Risk Assessment (BRA): annual assessment of the Company's overall exposure to crypto-related ML/TF risk;
- Customer Risk Assessment (CRA): classification of each player as low, medium, or high risk, reviewed at each significant transaction and at least annually.

6.2 Customer Due Diligence (CDD)

Standard CDD is applied to all players prior to allowing significant deposits or wagers. CDD includes:

- Identity verification: government-issued photo ID and proof of address;
- Beneficial ownership verification for accounts showing complex ownership structures;
- Sanctions screening against OFAC, EU Consolidated, UN, and other applicable lists;
- PEP (Politically Exposed Person) screening;
- Wallet ownership verification (see Section 6.4).

Identity must be verified before the regulatory CDD threshold is reached (NAf 4,000–5,000 cumulative or as updated by CGA/FIU guidance).

6.3 Enhanced Due Diligence (EDD)

EDD is mandatory for players classified as high-risk. High-risk indicators in the crypto context include:

- Large or unusual transaction volumes relative to the player's stated profile;
- Transactions involving jurisdictions on the FATF high-risk list;
- Wallet addresses with prior exposure to darknet markets, mixers, or sanctioned entities;
- Inconsistent or unverifiable source of funds;
- PEP status or association with a PEP;
- Use of unregulated or algorithmic stablecoins.

EDD measures include:

- Source-of-funds documentation and verification;
- Source-of-wealth documentation where cumulative transactions exceed material thresholds;
- Senior Management approval before the relationship continues;
- Enhanced ongoing monitoring with lower alert thresholds.

6.4 Wallet Ownership and Origin Checks

Before processing any crypto deposit, the Company must verify that the player controls the originating wallet. Verification methods include:

- Signed message: the player provides a cryptographic signature from the wallet address;
- Return micro-transaction: a small amount is sent to the player's declared address and the player confirms receipt.

All deposits are subject to on-chain screening to detect exposure to:

- Darknet markets;
- Mixers and tumblers (including Tornado Cash, Blender.io);
- Sanctioned entities (OFAC SDN list and equivalents);
- Fraud-linked or theft-linked wallets;
- Addresses associated with known ransomware or cybercrime operations.

Transactions with a risk score above the Company's defined threshold are automatically blocked pending manual review. Transactions confirmed as high-risk are rejected and, if there are grounds for suspicion, reported to FIU Curaçao.

6.5 FATF Travel Rule Compliance

In accordance with FATF Recommendation 16, the Company ensures that originator and beneficiary information accompanies all crypto transfers. Specifically:

- When sending crypto, the Company transmits originator name, wallet address, and (where technically feasible) account number and physical address;
- When receiving crypto via a VASP, the Company verifies that Travel Rule data is provided and reconciles it with CDD records;
- Where Travel Rule data is absent or incomplete, the transaction is held pending receipt of the required information.

7. Transaction Monitoring and Reporting

7.1 Monitoring System

The Company operates an automated transaction monitoring system configured to detect crypto-specific risk typologies, including:

- Rapid deposits followed by immediate withdrawals ('in-and-out' patterns);
- Chip-dumping and collusion in multiplayer games;
- Mixer adjacency: transactions from wallets that recently interacted with known mixers;
- Structuring and layering across multiple accounts or sessions;
- Rapid cryptocurrency conversion to obscure fund origin;

-
- Unusual betting patterns inconsistent with recreational gambling.

Alert thresholds and typology libraries are maintained and updated at least quarterly by the Compliance Officer in collaboration with the Payments Team.

7.2 Alert Handling

All automated alerts are reviewed by a trained compliance analyst within 24 hours. The analyst classifies the alert as:

- False positive – document reasoning and close;
- Requires further review – escalate to Compliance Officer;
- Suspicious – prepare STR for filing with FIU Curaçao.

The Compliance Officer reviews all escalated alerts and makes the final STR decision. STRs are filed via the goAML platform within the timeframe required by the LMOT.

7.3 Tipping-Off Prohibition

Staff must not disclose to a player, or to any third party not authorised to receive such information, that an STR has been filed or that a suspicious activity investigation is underway. Breach of this prohibition may result in disciplinary action and criminal liability.

8. Responsible Gambling in a Crypto Context

Crypto's characteristics — high transaction velocity, micro-deposit capability, pseudonymity, and 24/7 availability — can mask problem gambling behaviour. The Company therefore applies enhanced responsible gambling controls to crypto players, equivalent to those applied to fiat players, and supplemented where appropriate.

8.1 Markers of Harm

The monitoring system identifies crypto-specific markers of harm, including:

- Frequency of micro-deposits that aggregate to material amounts;
- Rapid consecutive deposits following losses (chasing behaviour);
- Prolonged play sessions without breaks;
- Disproportionate spend relative to declared income or account history.

Identified markers trigger a responsible gambling intervention workflow, including player contact, spending review, and, where appropriate, temporary account restriction.

8.2 Affordability and Source-of-Funds

Affordability checks are conducted when a player's cumulative deposits exceed defined thresholds. For crypto players, affordability verification may include:

- Bank statements or payslips;
- Evidence of investment or asset liquidation;
- Tax returns or audited accounts for high-value players.

8.3 Player Protection Tools

All player protection tools apply regardless of payment method:

- Deposit limits (daily, weekly, monthly) in both fiat equivalent and crypto amount;
- Session time limits and reminders;
- Self-exclusion (temporary and permanent) from all gambling services;
- Cooling-off periods;
- Bonus and promotional restrictions for players showing markers of harm.

9. Incident, Fraud and Cyber Response

The Company maintains written response procedures for the following crypto-specific incidents:

Incident Type	Immediate Response
Compromised private keys	Immediately rotate keys; freeze affected wallets; notify CGA within 24 hours; conduct forensic review
Suspicious deposit rings	Freeze accounts; file STR with FIU; conduct on-chain tracing; preserve evidence
Smart contract failure	Halt affected asset deposits; notify VASP; engage technical forensics; assess player impact
Blockchain hard fork	Suspend trading of affected asset; assess split-chain risk; Board decision on handling forked coins
VASP exchange outage	Activate backup VASP; notify affected players; document business continuity measures
Ransomware or cyber attack	Isolate affected systems; notify CGA and relevant authorities; engage incident response team; preserve logs

All incidents are logged in the Company's incident register. Post-incident reviews are conducted within 14 days and findings are reported to the Board.

10. Record-Keeping and Audit

10.1 Retention Requirements

In accordance with the LID, LMOT, and the CGA Crypto Policy Guideline, the following records are retained for a minimum of 7 years from the date of transaction or relationship termination (whichever is later):

- FATF Travel Rule payloads for all crypto transfers;
- On-chain risk screening reports (including raw risk scores and reasoning);
- KYC/CDD documentation: identity documents, wallet ownership evidence, source-of-funds records;
- All transaction logs, including deposit/withdrawal timestamps, amounts, addresses, and asset types;
- STR filings and supporting documentation;
- VASP due diligence records;
- Incident logs and post-incident review reports;
- Training records.

10.2 Reconciliation

Daily reconciliation is performed between:

- On-chain transaction records (blockchain explorer data);
- VASP/exchange statements;
- Internal ledgers and player account balances.

Discrepancies above a defined materiality threshold are escalated to the Compliance Officer for investigation within 24 hours. All reconciliation records are retained as part of the audit trail.

10.3 Independent Audit

The Company's crypto compliance framework is subject to independent internal or external audit at least once every 12 months. The audit scope includes:

- Adequacy of wallet architecture and access controls;
- Effectiveness of on-chain screening and alert handling;
- Completeness and accuracy of CDD/EDD records;
- VASP due diligence documentation;
- Compliance with the same-wallet and same-asset withdrawal rules;
- Travel Rule implementation.

Audit findings and management responses are reported to the Board and made available to the CGA upon request.

11. Staff Training

All staff who handle or oversee crypto transactions, or who have AML/CFT responsibilities, must complete training on this Policy. Training requirements:

Audience	Frequency	Topics
All staff	On boarding + annual refresh	Crypto fundamentals; prohibited assets; escalation duties; tipping-off prohibition
Payments Team	On boarding + semi-annual	Wallet operations; on-chain screening tools; same-wallet / same-asset rules; VASP standards
Compliance Team	On boarding + quarterly	Risk typologies; STR filing via goAML; EDD procedures; Travel Rule; audit requirements
Board	Annual	Regulatory updates; crypto risk metrics; Policy review

Training records (dates, attendees, content, assessment results) are maintained by the Compliance Officer and retained for 7 years. Third-party processors and affiliates are contractually required to ensure their own staff receive equivalent training.

12. Policy Review and Updates

This Policy is reviewed at least annually by the Compliance Officer and approved by the Board. An out-of-cycle review is triggered by any of the following:

- Material change to CGA, FATF, or FIU guidance;
- Addition or removal of a permitted crypto asset or VASP;
- Significant incident or regulatory finding;
- Introduction of new products or technologies involving virtual assets.

All versions of this Policy are retained in the document management system. The current effective version is displayed on the Company's intranet and is distributed to all relevant staff upon each update.

13. Sanctions and Consequences of Non-Compliance

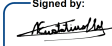
Failure to comply with this Policy may result in:

- Disciplinary action, up to and including dismissal, for employees;
- Termination of agreements with third-party processors, VASPs, or affiliates;
- Regulatory sanctions imposed by the CGA, including administrative fines, suspension of the licence, or revocation of the licence;
- Criminal liability under the LMOT and other applicable laws for knowing facilitation of money laundering or terrorist financing.

The Company reports material non-compliance incidents to the CGA proactively and cooperates fully with any investigation.

Approval

This Policy has been reviewed and approved by the undersigned on behalf of MuchGaming.

Compliance Officer (MLRO)	Board Representative
Signature: _____ Name: _____ Date: _____	Signature: Signed by:  8737E2B30CF043F... Signed by:  E5C1A4A3P74E4ED... Name: Analissa Heiland & Lorenza Godett Date: 6/26/2026

Initial

IC