



Perfect Storm B.V.

Crypto Policy

Crypto Asset Policy – 500Casino.com (Aligned with AML Policy)

1. Purpose and Scope

This Crypto Asset Policy (“Policy”) governs the acceptance, custody, use and payout of crypto assets by Perfect Storm B.V. (“the Company”). It is fully aligned with the Company’s AML Policy v2.1 and forms an integral annex thereto. Where crypto-assets are used, the AML Policy shall prevail, supplemented by the additional controls defined herein.

2. Legal and Regulatory Framework

This Policy is adopted from a Curaçao legal and regulatory perspective and aligns with:

- Curaçao Gaming Authority (CGA) Crypto Policy Guidelines
- National Ordinance for Games of Chance (LOK)
- National Ordinance Reporting Unusual Transactions (NORUT)
- National Ordinance Identification when Rendering Services (NOIS)
- National Ordinance Penalization of Money Laundering (NOPML)
- FATF Recommendations (including Travel Rule – Recommendation 16)
- EU AML Directives (2015/849, 2018/843, 2018/1673) as referenced in the AML Policy
- Wolfsberg Group Guidance on Digital Assets

3. Policy Hierarchy and Cross-References

This Policy must be read together with:

- AML Policy v2.1 (Perfect Storm B.V.)
- Responsible Gambling Policy

Definitions, CDD/EDD thresholds, SAR procedures, record retention periods and staff responsibilities are incorporated by reference from the AML Policy unless explicitly overridden herein.

4. Governance and Accountability

Ultimate accountability rests with the Board of Directors.

Day-to-day oversight is delegated to the Compliance Officer (MLRO) in line with AML Policy sections 1.2 and 7.3.

All crypto-related changes (assets, wallets, VASPs, thresholds) require:

- Documented risk assessment
- Compliance Officer approval
- Board or senior management sign-off where material

5. Risk-Based Approach to Crypto Assets

Cryptocurrency is classified as a high-risk payment method under AML Policy section 3.2.4.

Accordingly:

- All crypto customers are subject to enhanced transaction monitoring
- Crypto activity materially increases a customer's ML/FT risk score
- Enhanced Due Diligence (EDD) applies where on-chain or behavioral indicators arise

6. Permitted and Prohibited Crypto Assets

Permitted assets are subject to asset-specific risk assessments.

The following are strictly prohibited:

- Privacy coins (e.g., Monero, Zcash, Dash)
- Meme coins (e.g., DOGE, SHIB, PEPE)
- Wrapped tokens of unknown or unverifiable origin
- Funds linked to mixers, tumblers, darknet markets, sanctioned wallets or entities

These prohibitions align with CGA guidance and AML Policy sections 3.2.4 and 5.2.

7. Stablecoins

Preference is given to fiat-backed, regulated stablecoins.

Algorithmic or unregulated stablecoins require:

- Enhanced Due Diligence
- Senior management approval
- Ongoing risk monitoring

8. Customer Due Diligence in a Crypto Context

CDD and EDD requirements follow AML Policy sections 4 and 3.4.

Additional crypto-specific measures include:

- Wallet ownership verification (signed message, Satoshi test, or VASP confirmation)
- Source of Funds and Source of Wealth verification explicitly addressing crypto origin
- On-chain tracing to identify exposure to high-risk typologies (mixers, scams, hacks)

9. Transaction Management Rules

- Deposits and withdrawals must occur to and from the same wallet/payment source
- Withdrawals must be made in the same crypto-asset as deposited
- Peer-to-peer transfers between players are prohibited

These rules reinforce AML Policy sections 5.3–5.5.

10. Wallet Custody and Segregation

Only entity-owned wallets are permitted.

Wallet architecture must segregate:

- Operational wallets
- Treasury wallets
- Player-flow wallets

Personal, employee, or UBO-linked wallets are strictly prohibited.

11. VASP and Exchange Standards

All crypto transactions must be routed via regulated or registered VASPs.

VASPs must demonstrate:

- Robust AML/CFT controls
- FATF Travel Rule compliance
- Transaction monitoring and sanctions screening

The Company shall not provide exchange services itself.

12. Monitoring, Red Flags and Reporting

Crypto activity is monitored under AML Policy sections 3.6 and 6.

Crypto-specific red flags include:

- High-velocity micro-deposits
- Self-transfer or chip-dumping patterns
- Mixer adjacency
- Sudden changes in wallet behavior

Suspicious activity must be escalated internally and reported to the FIU Curaçao without delay.

13. Responsible Gambling in a Crypto Context

Responsible Gambling controls apply irrespective of tender.

Monitoring shall consider:

- Masked affordability risks
- High-frequency betting enabled by crypto

Controls align with AML Policy behavioral monitoring principles.

14. Incident, Fraud and Cyber Response

Crypto-specific incidents include:

- Compromised private keys
- Smart contract failures
- Blockchain forks
- Exchange outages

All incidents must be documented and escalated per internal incident response procedures.

15. Record-Keeping and Audit Trail

In line with AML Policy section 7.2, the Company retains:

- KYC and EDD records
- Transaction logs and blockchain references
- Travel Rule data
- On-chain risk reports

Records must support independent audit reconstruction.

16. Training and Awareness

Staff training obligations follow AML Policy sections 1.6 and 7.4.

Crypto-specific modules include:

- On-chain risk indicators
- Wallet verification methods
- Travel Rule obligations

17. Review, Approval and Version Control

This Policy is reviewed at least annually or upon regulatory change.

Approved by the Board and signed by the Compliance Officer.

Version control follows AML Policy section 7.7.