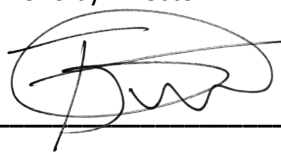


APPENDIX No. 3
VIRTUAL ASSETS RISK POLICY
to the AML/CFT and Sanctions Compliance Policy

Date of effectiveness: 07.04.2026

Approved on: 07.04.2026 by Director

Prepared

A handwritten signature in black ink, appearing to be 'Iryna Vlasova', is written over a horizontal line.

**and
accepted by:**

**Vlasova Iryna
AML Officer/MRLO**

1. Purpose and Scope

1.1 Purpose

This Annex addresses the specific money-laundering, terrorist-financing and proliferation-financing (ML/TF/PF) risks arising from the acceptance and processing of virtual assets (cryptocurrency) as a payment and wagering method on the COLDBET platform. Its objective is to fulfill the responsibilities of operators with a business model that has partial risks, such as cryptocurrencies, to address these high-risk components.

1.2 Relationship to the AML/CFT Policy

This Annex supplements, and must be read in conjunction with, the AML/CFT and Sanctions Compliance Policy of GAME2NET B.V. (the “AML/CFT Policy”). It does not replace the AML/CFT Policy. The definitions, risk-classification framework, sanctions procedures, due-diligence procedures, reporting procedures, record-keeping obligations and officer roles of the AML/CFT Policy apply in full to virtual-asset activity except where this Annex prescribes a stricter or crypto-specific measure.

In the event of conflict on a crypto-specific matter, this Annex governs; in all other respects the AML/CFT Policy governs. Where the LOK, License Conditions, , the Regulations for the Combating of Money Laundering, the National Ordinance PB 2024 No. 41, and the NORUT/LMOT PB 2017 No. 99 impose a requirement stricter than either document, the regulations shall prevail.

1.3 Licence-condition constraints on virtual currencies

The following binding licence conditions apply to all virtual-currency activity and are reproduced here for operational clarity:

- Virtual currencies accepted as stakes or bets must be tradable on internationally licensed virtual-currency exchanges.
- The Organisation shall not exchange currencies in the player account or otherwise, nor exchange virtual currencies for fiat currencies, and shall not offer investment alternatives to players (this does not prevent the issuance/purchase of in-game tokens).
- Prize money is paid out in the same currency, virtual or fiat, that was used to play the game.

1.4 Scope

This Annex applies to all employees, departments and third-party service providers involved in the acceptance, screening, monitoring, processing or reconciliation of virtual-asset deposits and withdrawals on the COLDBET platform.

1.5. Governance, Accountability, and Resource Delegation

1.5.1 The Board of Directors of GAME2NET B.V. retains ultimate constitutional accountability for all crypto-asset strategies, policies, and systemic risk exposures.

1.5.2 Day-to-day operational execution of this policy, including active on-chain risk screening, is delegated jointly to the AML Officer and the internal Payments Team.

1.5.3 Any structural modification to this framework, including adding or removing an accepted cryptocurrency asset, onboarding or offboarding a Virtual Asset Service Provider (VASP), or adjusting automated on-chain risk-scoring thresholds, requires a documented risk assessment and formal sign-off from both the AML Officer and the Board

1.5.4. The Organisation must structurally separate its corporate cryptographic holdings into three independent, clear wallet categories that cannot be mixed:

- Operational Wallets: dedicated strictly to day-to-day corporate transactional flows and third-party vendor settlements.
- Treasury Wallets: reserved exclusively for strategic financial reserves, capital management, and company assets.
- Player-Flow Wallets: utilized strictly for hosting customer-facing deposits and staging outbound player withdrawal allocations

1.5.5 Only wallets owned and controlled by the Organisation itself, or by a dedicated payment subsidiary within the GAME2NET B.V. group, are permitted for the wallet categories described above. The use of personal wallets, or wallets linked to any director, ultimate beneficial owner (UBO), employee or other related person, is strictly prohibited for the receipt, holding or disbursement of player or corporate crypto-assets.

1.5.6 The Organisation applies the following minimum technical security controls to all corporate wallets and crypto-asset infrastructure:

- Multi-Factor Authentication (MFA) and/or Hardware Security Modules (HSM) for all access to wallets and signing keys;
- Withdrawal-address whitelisting to restrict outbound transfers to pre-approved addresses only;
- Multi-signature authorisation protocols for all Treasury Wallet operations, requiring sign-off by more than one authorised person.

2. Definitions

The following terms supplement the Definitions section of the AML/CFT Policy. Terms already defined in the AML/CFT Policy shall retain their meaning:

- **Virtual Asset** means a digital representation of value that can be digitally traded or transferred and used for payment or investment purposes, including cryptocurrencies; for the purposes of this Annex, the term covers all crypto-assets accepted on the COLDBET platform.
- **Virtual Asset Service Provider (VASP)** means a natural or legal person conducting, as a business, the exchange, transfer, safekeeping or administration of virtual assets, or the provision of financial services relating to the offer or sale of a virtual asset (e.g. a crypto exchange or hosted-wallet provider).
- **Blockchain** means the distributed-ledger technology underlying virtual assets, recording transactions across a network of participants.
- **Wallet** means a software or hardware instrument used to hold and transfer virtual assets. A hosted (custodial) wallet is controlled by a VASP that holds the private keys on the customer's behalf; an unhosted / self-custodied wallet is controlled directly by the customer, who holds the private keys.
- **Blockchain Analytics** means the use of specialised tooling to trace, attribute and risk-score virtual-asset addresses and transactions across the blockchain.

- **Mixing / Tumbling Services** means services that obscure the origin or destination of virtual assets by pooling and redistributing funds across multiple addresses.
- **Privacy Coin** means a virtual asset designed to conceal transaction details (sender, recipient, amount), such that standard blockchain analytics cannot reliably trace it.

3. Inherent Risk Assessment of Virtual Assets

Virtual assets are treated by the Organisation as an inherently high-risk payment channel. The elevated risk derives from the pseudo-anonymity of addresses, decentralisation, the speed of cross-border transfers, the availability of mixing/tumbling services, and the existence of privacy-enhancing coins.

Accordingly, any customer whose primary or significant deposit or withdrawal method is cryptocurrency is automatically assigned a High Risk profile at onboarding, subject to re-classification only after full EDD clearance.

Before any new virtual-asset type, wallet arrangement or crypto delivery mechanism is launched, a documented risk assessment must be carried out to determine whether the innovation creates a weakness capable of misuse for ML/TF, and mitigating measures applied where risks are identified.

The following risk factors must be assessed for each crypto transaction:

- a. Type of cryptocurrency (transparent ledger versus privacy coin);
- b. Wallet type (hosted VASP wallet versus unhosted / self-custodied wallet);
- c. Blockchain-analytics risk score;
- d. Geographic origin of the sending wallet / VASP jurisdiction;
- e. Transaction pattern (frequency, amounts, layering indicators).

4. Prohibited Instruments and Absolute Restrictions

4.1. The Organisation will not accept deposits from, nor process withdrawals to, any of the following assets, tools, or delivery networks:

4.1.1 Privacy Coins: total prohibition on privacy-enhancing assets designed to conceal transaction details, including but not limited to Monero (XMR), Zcash (ZEC), and Dash.

4.1.2 Meme Coins: total prohibition on speculative meme coins, including but not limited to DOGE, SHIB, and PEPE.

4.1.3 Wrapped Tokens: total prohibition on wrapped tokens or synthetic assets of unknown, obfuscated, or un-verifiable origin, specifically including wrapped Bitcoin (wBTC) variants failing tracking transparency.

4.1.4 Explicitly Sanctioned Mixers and Tumblers: total blockage of any transaction routing that interacts with or passes through sanctioned mixing/tumbling protocols, including but not limited to Tornado Cash, Blender.io, and Sinbad.io, as well as any address listed on international sanctions trackers.

4.1.5 Unhosted Wallets Without Clearance: rejection of transactions involving unhosted/self-custodied wallets unless the player passes comprehensive Enhanced Due Diligence (EDD) and the specific wallet address maintains low-risk blockchain analytics scoring.

4.1.6 Unregulated Peer-to-Peer Flows: rejection of direct peer-to-peer (P2P) transfers that circumvent a regulated or registered VASP intermediary.

5. Limits, Fees, and Stablecoin Governance

5.1 The Organisation implements asset-specific deposit and withdrawal limits, mandatory cooling-off periods, and transaction hold durations that scale proportionately with the risk scores generated by blockchain analytics.

5.2 High-volume deposit patterns trigger automated transactional hold periods pending review by the payments team.

5.3. The Organisation must explicitly disclose all network gas fees, internal transaction processing fees, and asset conversion slippage rules to the player prior to transaction execution. No hidden conversion costs may be applied.

5.4. The Organisation explicitly prefers to process transactions in fiat-backed, highly regulated stablecoins. Any consideration of unregulated or algorithmic stablecoins is subject to a separate, heightened, independent risk assessment by the AML Officer prior to system integration.

5.5. The Organisation must process all player withdrawal requests exclusively to the identical, specific on-chain wallet address from which the initial deposit was received. Cross-wallet withdrawals, account-to-account internal transfers, and payouts to unverified third-party wallets are strictly prohibited. Withdrawals must be processed in the same cryptocurrency as the corresponding deposit, consistent with the licence condition that prize money is paid out in the same currency used to play. Players may not transfer funds or balances to one another on the platform.

6. Customer Due Diligence for Crypto Users

6.1 Standard CDD

All crypto users must complete full standard CDD (identity verification, address verification, PEP screening and sanctions screening) before any crypto deposit is accepted or any crypto withdrawal is processed.

The NAF. 4,000 CDD threshold applies regardless of whether funds are denominated in fiat or cryptocurrency, and is calculated using the market rate at the time of the transaction. The threshold is also reached where a series of linked transactions cumulatively meets or exceeds NAF. 4,000.

6.2 Enhanced Due Diligence (EDD)

All crypto users are automatically classified as High Risk and must undergo EDD before their first withdrawal transaction is approved. EDD comprises at least:

- a. Source of Funds declaration (origin of the crypto holdings);
- b. Source of Wealth documentation;
- c. Wallet-ownership confirmation (wallet ownership and origin verification checks must extract verifiable evidence of physical control. This must utilize signed message protocols, cryptographic micro-transactions (Satoshi test), or verified FATF Travel Rule data payloads transmitted securely by a counterparty VASP);
- d. A blockchain-analytics report on all submitted wallet addresses;

6.3 Ongoing EDD for Existing Crypto Users

- CDD records for crypto users are reviewed not less frequently than every 6 months, consistent with the high-risk review cadence.
- Every deposit and withdrawal transaction is subject to blockchain-analytics screening.
- Any wallet address not previously verified triggers a fresh wallet-ownership confirmation and analytics check before funds are accepted or released.

7. Blockchain Analytics

The Organisation shall utilise blockchain analytics tools for automated screening of all wallet addresses and transactions.

Screening is performed:

- at onboarding, for all submitted wallet addresses;
- on every subsequent deposit and withdrawal; and
- on any new wallet address added to an existing account.

A blockchain-analytics report is retained on the customer's file for each transaction and forms part of the CDD/EDD record.

8. Sanctions Screening for Virtual Assets

All wallet addresses and VASP counterparties are screened against the sanctions programmes of the authorities recognised by the AML/CFT Policy (including the UN Security Council, the European Union, the United States (OFAC), the United Kingdom (HM Treasury/OFSI) and Australia (DFAT/AUSTRAC)) before any transaction is processed.

Blockchain-analytics results are treated as supplementary to, and not a substitute for, the formal sanctions screening performed under the AML/CFT Policy.

In the event of a sanctions match on a wallet address or VASP:

- the transaction is blocked immediately;
- the relevant account is frozen pending AML Officer review; and
- the case is escalated under the AML/CFT Policy's freezing procedure.

9. Transaction Monitoring for Crypto Payments

In addition to the general monitoring triggers of the AML/CFT Policy, the following crypto-specific triggers are monitored.

- a. Structuring: multiple transactions below the NAf. 4,000 threshold from the same or linked wallets within a short period;
- b. Layering indicators: rapid conversion of crypto to fiat followed by withdrawal, or vice versa;
- c. Use of multiple wallet addresses for a single account without explanation;
- d. Any transaction passing through a mixer, tumbler or privacy-enhancing service (automatic block and report);

- e. High-value single transactions above NAf. 5,000;
- f. Wallet addresses appearing on the OFAC SDN List or other sanctions lists (automatic block);
- g. Sudden change in payment method from fiat to crypto, or vice versa, without business rationale.

The Organisation maintains and regularly updates crypto-specific typology libraries to inform monitoring thresholds and player-verification triggers, including self-transfer chip-dumping, high-velocity deposit/withdrawal patterns, and mixer adjacency. Suspicious activity identified through crypto monitoring is escalated and reported to the FIU in accordance with the reporting procedures of the AML/CFT Policy.

10. VASP Due Diligence

Where the Organisation accepts deposits from, or sends withdrawals to, a third-party VASP (exchange or wallet provider), the Organisation conducts due diligence on the VASP, including:

- a. Confirmation that the VASP is licensed / registered in its jurisdiction of incorporation, and (where the counterparty operates an exchange) that it is an internationally licensed virtual-currency exchange;
- b. Confirmation that the VASP applies AML/CFT standards equivalent to Curacao requirements;
- c. Confirmation that the VASP is not domiciled in, or operating from, a prohibited jurisdiction.
- d. Confirmation that the VASP complies with the FATF Travel Rule, transmitting required originator and beneficiary information for qualifying transfers;
- e. Confirmation that the VASP maintains robust AML/CFT controls and effective transaction-monitoring and on-chain screening capabilities.

The Organisation does not itself offer exchange, conversion or other virtual-asset services to players; any reference to a crypto exchange is provided only as a link to a separate, independently operated website. Consistent with CGA expectations, the Organisation holds its wallets only on regulated and/or registered crypto exchanges or VASPs.

11. FATF Travel Rule Compliance

Where applicable, the Organisation ensures that the required originator and beneficiary information accompanies crypto-asset transfers sent to, or received from, VASPs, in line with FATF Travel Rule requirements. Travel Rule data payloads received from counterparty VASPs are retained as part of the transaction record and may be used as supporting evidence of wallet ownership and origin.

12. Responsible Gambling in a Crypto Context

Responsible-gambling controls apply equally irrespective of whether a player funds their account in fiat or virtual assets. The Organisation applies the same markers-of-harm monitoring, affordability assessment, time-outs, self-exclusion and bonus restrictions to crypto users as to fiat users, in accordance with the operator's responsible-gambling policy.

The Organisation specifically monitors behavioural signals of problem gambling that may be masked by high-velocity, on-chain micro-deposits, and ensures that such patterns trigger a responsible-gambling review.

13. Incident, Fraud and Cyber Response

The Organisation defines and maintains response procedures for crypto-specific incidents, including but not limited to:

- compromised private keys or wallet credentials;
- suspicious deposit rings or coordinated deposit/withdrawal activity;
- smart-contract failures or exploits;
- blockchain forks or network disruptions; and
- outages or insolvency of a counterparty exchange or VASP.

Each such incident is escalated to the AML Officer, documented, and where relevant reported to the CGA and the FIU in accordance with the AML/CFT Policy.

14. Record-keeping and Audit Trail

In addition to the record-keeping obligations of the AML/CFT Policy, the Organisation retains, for the statutory retention period, all crypto-specific records, including FATF Travel Rule payloads, blockchain-analytics and on-chain risk reports, KYC/CDD/EDD records, and full transaction logs.

The Organisation ensures reconciliation between blockchain explorers, exchange/VASP statements and its internal ledgers, and maintains an audit trail sufficient to enable independent reproduction and verification of any crypto transaction.

15. Review and Update

This Annex is reviewed:

- at least annually;
- upon any change in the accepted cryptocurrency types;
- upon any material change in CGA guidance on virtual assets; and
- upon any significant change in AML/CFT Policy.

Any revision must be approved by the Director and the AML Officer. This policy is signed off by the AML Officer (compliance officer), approved and ratified by the Board of Directors of GAME2NET B.V., and states its effective date on the cover.

Reviewed and approved by the Director:

Mr. Dmytro Rodionov

