

CRYPTO RISK POLICY

Last updated: August 10, 2026

This Crypto Risk Policy (the “**Policy**”) sets out the controls applied by JetTon Games B.V. (“**JetTon**”, “**We**”, “**the Licensee**”), operator of the JetTon iGaming Platform available at <https://jetton.online> (the “Platform” or “Website”), when accepting, holding, processing and paying out crypto-assets in connection with its remote gambling operation.

<https://jetton.online> is owned and operated by JetTon Games B.V., a company incorporated under registration number 168122, with its registered office at Abraham Mendez Chumaceiro Boulevard 03, Curaçao.

<https://jetton.online> is licensed and regulated by the Curaçao Gaming Authority (“**CGA**”) under license number OGL/2024/2287/1195, under the laws and regulations of Curaçao, including the Landsverordening op de Kansspelen (“**LOK**”).

This Policy has been prepared in accordance with the CGA *Crypto policy guideline for online gaming operators* (June 2025) (the “CGA Guideline”), and is intended for submission to the CGA Portal as JetTon's crypto policy pursuant to the Transition Period set out in the CGA Guideline. This Policy does not replace, limit, or substitute JetTon's obligations under the LOK, the CGA's AML/CFT regulations, or any other applicable law or licence condition. Nothing in this Policy shall be interpreted as legal advice; JetTon has obtained independent legal and compliance advice in the preparation of this Policy and will continue to do so as its crypto operations evolve.

1. KEY DEFINITIONS

For the purposes of this Policy, the following terms shall have the meanings set out below, consistent with the CGA Guideline and the Financial Action Task Force (“FATF”) Recommendations:

- “Virtual Asset Service Provider” or “VASP”: a legal or natural person that conducts one or more of the following activities on behalf of another person: exchange between virtual assets and fiat currencies; exchange between virtual assets; transfer of virtual assets; or safekeeping/administration of virtual assets or instruments enabling control over them (in line with FATF Recommendation 15).
- “Compliant VASP”: a VASP demonstrating appropriate AML/CFT compliance, Travel Rule capability, sanctions screening, operational resilience and transparency, assessed by JetTon on a risk-based basis and not by jurisdiction label alone.
- “Unhosted Wallet”: a wallet not managed by a VASP and controlled directly by a user through private keys.
- “Wallet Ownership Verification”: the process of confirming that a customer controls a specific wallet address, through methods such as test transactions, signed messages, or equivalent mechanisms.
- “Blockchain Analytics Tools”: systems capable of tracing, analysing and risk-scoring virtual asset transactions, including identification of exposure to high-risk or prohibited sources.
- “FATF Travel Rule”: the requirement under FATF Recommendation 16 that originator and beneficiary information accompany virtual asset transfers between VASPs and be made available to competent authorities upon request.
- “Compliance Officer”: the individual appointed by JetTon with day-to-day responsibility for AML/CFT and crypto-asset risk compliance, as further described in Section 3.

2. PURPOSE AND SCOPE

- 2.1 This Policy applies to all crypto-asset workflows connected with the Platform, including deposits, wagering, withdrawals and treasury management.
- 2.2 This Policy applies to JetTon Games B.V. and to all group entities that support the licensed operation, including any affiliated payment-processing, treasury, or technology entities engaged by JetTon in connection with crypto-asset activity.
- 2.3 This Policy operates alongside, and does not replace or limit, JetTon's other regulatory obligations, including its AML/CFT policy submitted to the CGA Portal, its Responsible Gaming Policy, its Terms and Conditions, and any applicable VASP registration or licensing requirements in Curaçao or elsewhere. JetTon remains independently responsible for full compliance with all applicable registration, licensing, reporting and other regulatory requirements relevant to its crypto-asset activities.
- 2.4 This Policy applies with immediate effect to the prohibitions on sanctioned wallets, mixers or tumblers, expressly prohibited crypto-assets, and personal or UBO-linked wallets described in Sections 4, 7.6 and 12.1 of this Policy, and on the phased implementation basis set out in JetTon's crypto compliance roadmap submitted to the CGA Portal for all other requirements.

3. GOVERNANCE AND ACCOUNTABILITY

- 3.1 This Policy is signed off by JetTon's Compliance Officer and approved by JetTon's board of directors (the "Board"). The effective date of this Policy is set out on the cover page.
- 3.2 This Policy shall be reviewed at least once every twelve (12) months, and on an ad-hoc basis where triggered by: (a) a material change in JetTon's crypto-asset product offering (including the addition or removal of a supported asset or a VASP); (b) a material regulatory development, including further guidance issued by the CGA; (c) a significant crypto-related incident reportable under Section 14; or (d) a material adverse finding from an internal or external audit or risk assessment.
- 3.3 Ultimate accountability for this Policy and for JetTon's crypto-asset risk exposure rests with the Board. Day-to-day implementation and monitoring is delegated to the Compliance Officer, supported by JetTon's payments and risk teams, including on-chain risk screening functions.
- 3.4 Any addition or removal of an accepted crypto-asset, VASP, or wallet/payment provider, or any change to a risk threshold set out in this Policy, requires (a) a documented risk assessment, and (b) formal sign-off by the Compliance Officer prior to implementation, with Board notification for material changes.

In furtherance of the above, JetTon will:

- maintain and operate blockchain analytics and transaction-monitoring tools capable of identifying prohibited assets and transaction patterns (JetTon is not required to act as a blockchain analyst, but must not operate blindly with regard to crypto transactions connected to its licensed operation; the underlying risk assessment function may be outsourced, but visibility and accountability may not be outsourced);
- reject, freeze, or return funds where prohibited activity is detected, in accordance with its internal escalation procedures;
- report relevant incidents in accordance with Section 14 (Incident Reporting) and Article 5.10 of the LOK;
- maintain documented procedures for identifying and handling prohibited assets; and
- ensure that relevant personnel receive training in digital-asset risk identification and assessment, appropriate to their role.

4. NOT A FINANCIAL INSTITUTION

- 4.1 Consistent with JetTon's other CGA-facing policies (including its AML policy), JetTon does not, and will not, operate as an exchange, payment services provider, or VASP.
- 4.2 JetTon accepts crypto-asset payments solely as a means of payment for gambling services offered on the Platform. JetTon makes it explicitly clear to players, including in its Terms and Conditions and cashier interface, that JetTon is not responsible for the services of any third-party exchange or VASP used by a player to acquire, convert, or dispose of crypto-assets.
- 4.3 Accordingly, JetTon will not: (a) convert crypto-assets to other crypto-assets or to fiat currency on behalf of players; (b) offer trading, swapping, or exchange services of any kind;

or (c) offer custody, transfer, or wallet services to players outside the scope of gambling-related transactions on the Platform.

5. AML/KYC IN A CRYPTO CONTEXT

- 5.1 The use of crypto-assets is not, and shall not be treated as, a carve-out from JetTon's AML/CFT or Responsible Gaming obligations. JetTon's AML/CFT policy submitted to the CGA Portal applies equally to fiat and crypto-asset transactions.
- 5.2 Where crypto-asset transactions are accepted, JetTon's AML/CFT policy explicitly details the controls applicable to such transactions, cross-referenced with this Policy.
- 5.3 JetTon applies risk-based Know-Your-Customer (“KYC”) and Enhanced Due Diligence (“EDD”) measures to crypto-asset transactions, including: (a) verification of customer identity and, where applicable, beneficial ownership; (b) application of EDD where high-risk indicators are present (including elevated transaction volumes/velocity, use of privacy-enhancing assets, or exposure to high-risk jurisdictions or counterparties); (c) wallet ownership verification, such as evidence of wallet control through a signed message or return transaction; and (d) on-chain tracing to detect exposure to darknet markets, mixers, sanctioned entities, or fraud-linked wallets.
- 5.4 JetTon recognises and will comply with the FATF Travel Rule as further described in Section 8.
- 5.5 JetTon establishes and maintains thresholds for crypto-asset activity that trigger enhanced monitoring or escalation, escalates suspicious activity in accordance with its AML/CFT policy and reports to the Curaçao Financial Intelligence Unit (“FIU”) as required, and maintains a typology library of crypto-related risk indicators (including, without limitation, chip-dumping and mixer-adjacent activity) to support staff in identifying suspicious patterns.

6. BLOCKCHAIN ANALYTICS CAPABILITY

- 6.1 As of the date of this Policy, JetTon has not yet selected or engaged a specific blockchain analytics provider or internal tooling solution. JetTon commits to deploying, as a priority and in line with the implementation timeline submitted to the CGA Portal in accordance with the CGA Guideline, blockchain analytics tools sufficient to achieve the functionality described in this Section, whether through a third-party solution, internal systems, or a combination of both. The CGA does not mandate use of any specific provider, and JetTon will select its provider(s) on a risk-based basis (illustrative examples of providers active in this market include Chainalysis, Elliptic, and TRM Labs, without preference or commitment to any of them).
- 6.2 Once selected, JetTon's blockchain analytics capability will address, at minimum, the following functions:
 - tracing the origin and destination of funds;
 - identifying exposure to high-risk or prohibited sources (e.g., mixers, sanctioned addresses, fraud-linked wallets);
 - assessing and risk-scoring wallets and transactions;
 - investigating and evidencing suspicious activity for reporting purposes;

- deposit screening: screening wallet addresses at the point of deposit and risk-scoring/flagging exposure to darknet markets, scams or mixers;
- ongoing transaction monitoring: detecting new risk exposure and suspicious patterns over time;
- source-of-funds verification: tracing fund origins and documenting findings for KYC/EDD and audit purposes; and
- withdrawal screening: screening destination wallets prior to outbound transfers.

7. DIGITAL ASSETS AND TRANSACTION SOURCES

JetTon treats all crypto-assets as high risk and applies an asset-specific risk assessment to each asset it accepts. JetTon's preference is to transact in fiat-backed, regulated stablecoins. Where JetTon accepts other crypto-assets, the controls below apply, commensurate with the risk of the relevant asset type.

7.1 Supported assets and preference for fiat-backed regulated stablecoins

As displayed in the Platform's cashier as of the date of this Policy, JetTon supports deposits and withdrawals in USDT, TON, ETH, BTC, and a broader range of additional crypto-assets (over twenty (20) in total). Consistent with the CGA Guideline, JetTon's stated preference is to transact in fiat-backed, regulated stablecoins (such as USDT) wherever practicable. Every crypto-asset displayed in the Platform's cashier is subject to the asset-specific risk assessment described in this Section 7, and JetTon will remove or restrict any supported asset that is found, on review, not to meet the standards set out in this Policy. Unregulated or algorithmic stablecoins are subject to heightened review before onboarding and are not accepted without a documented risk assessment and Compliance Officer sign-off.

7.2 Privacy-enhancing cryptocurrencies

JetTon does not accept deposits denominated in, or facilitate withdrawals to, assets that obscure transaction data and prevent effective monitoring, blockchain analysis, or source-of-funds verification, including without limitation: Monero; Zcash (including shielded transactions); Dash (where privacy features are utilised); and Litecoin transacted via MWEB where privacy features are enabled. This list is illustrative and will be kept under review as new privacy-enhancing assets and features emerge.

7.3 Pooled / omnibus wallet structures

Where a VASP used by JetTon operates pooled or omnibus wallet structures, JetTon will only rely on such structures where it can obtain sufficient data from the VASP to attribute transactions to individual customers, assess source of funds, and perform monitoring and reporting. JetTon will not use structures that specifically prevent effective attribution or auditability.

7.4 Meme or highly speculative tokens

JetTon does not, by default, accept so-called “meme coins” or other highly speculative digital assets for deposits or withdrawals. Should JetTon consider supporting such an asset, it will categorise and assess the asset against objective, documented criteria, including: (a) liquidity and volatility profile; (b) governance and ecosystem maturity; and (c) financial-crime risk factors arising from the asset's

design features (including any anonymity-enhancing functionality), prior to any onboarding decision and Compliance Officer sign-off.

7.5 Wrapped tokens and bridged assets of unverified origin

JetTon does not accept deposits or facilitate transactions involving wrapped tokens or bridged assets where the provenance of the underlying asset cannot be clearly established, including wrapped versions of established crypto-assets (e.g., wrapped Bitcoin) where custody, backing, or transactional history of the underlying asset cannot be independently verified.

7.6 Expressly prohibited

JetTon does not accept, and will reject, freeze or return (as appropriate and in accordance with its AML/CFT procedures), crypto-assets that: (a) originate from, pass through, or are associated with sanctioned cryptocurrency mixers or tumblers; or (b) are linked to wallet addresses appearing on any applicable sanctions list or flagged by JetTon's blockchain analytics provider(s) as high-risk. JetTon acknowledges the CGA's reserved right to designate further digital assets, token types, or transaction mechanisms as prohibited, and will incorporate any such designation into this Policy without delay.

8. FATF TRAVEL RULE COMPLIANCE

- 8.1 JetTon recognises the requirements of the FATF, including Recommendation 16 (the “Travel Rule”).
- 8.2 Where crypto-assets are transferred between regulated entities in connection with JetTon's operations, including exchanges, custodial wallet providers, and VASPs, JetTon ensures that the required originator and beneficiary information accompanies the transaction and is retained so as to be made available to competent authorities upon request.
- 8.3 JetTon's VASP due diligence (Section 9) includes assessment of each VASP's Travel Rule capability as a condition of onboarding and continued use.

9. USE OF THIRD-PARTY VASPS AND PAYMENT PROVIDERS

- 9.1 As of the date of this Policy, JetTon has not yet finalised or contractually committed to specific VASP or payment-provider partners for its crypto-asset operations. JetTon adopts a risk-based approach to the selection of third-party VASPs and payment providers, taking into account jurisdictional availability, operational requirements and market constraints. JetTon does not restrict itself to any specific provider or jurisdiction, and equally does not treat jurisdiction label alone as a proxy for VASP quality.
- 9.2 Before onboarding any VASP or payment provider, JetTon assesses and documents whether the provider is regulated, registered, or otherwise subject to reputable oversight in its home jurisdiction, and whether it demonstrates: (a) robust AML/CFT controls; (b) FATF Travel Rule capability; (c) sanctions screening; (d) transaction-monitoring capability; (e) operational resilience; and (f) transparency.
- 9.3 The use of a third-party VASP or payment provider does not transfer, reduce, or dilute JetTon's own obligations in respect of AML/CFT, transaction monitoring, player protection, or incident reporting. JetTon remains fully accountable for compliance regardless of any outsourcing arrangement.

9.4 JetTon documents its due diligence and risk assessment for each VASP relationship and will have regard to any further guidance published by the CGA on acceptable standards or jurisdictions.

10. UNHOSTED (SELF-HOSTED / NON-CUSTODIAL) WALLETS

JetTon may accept crypto-assets from unhosted wallets or DeFi protocols, subject to the following risk-based controls:

- wallet ownership or control must be verified in accordance with Section 5;
- blockchain analytics must be applied to assess transaction risk before funds are credited to a player account;
- Enhanced Due Diligence is applied where elevated risk is identified; and
- such transactions must not impair JetTon's AML/CFT, monitoring, or reporting obligations. Where these conditions cannot be met, JetTon will decline, freeze, or return the relevant funds.

11. TRANSACTION MANAGEMENT

- 11.1 As a default rule, withdrawals are processed to the same wallet address, and in the same crypto-asset, as the corresponding deposit.
- 11.2 Where this default is not operationally practicable (for example, due to volatility exposure or operational inefficiency at scale), JetTon may permit the following alternative approaches, provided equivalent controls are demonstrated and documented: (a) withdrawal to a different wallet address, where that wallet has been whitelisted, pre-screened, and verified as belonging to the same customer, and the customer has passed applicable KYC/AML checks and whitelisting controls; or (b) withdrawal in a different crypto-asset or stablecoin, where the full transaction flow remains transparent and auditable, any conversion is conducted via a Compliant VASP, and records of the conversion are maintained.
- 11.3 Player-to-player transfers of funds on the Platform are prohibited.
- 11.4 JetTon applies deposit and withdrawal limits, cooling-off periods where appropriate, and discloses applicable fees and slippage rules to players in its cashier interface and Terms and Conditions.

12. OPERATOR WALLETS AND WALLET ARCHITECTURE

- 12.1 All wallets used in connection with JetTon's licensed operation are owned or controlled exclusively by JetTon Games B.V. or an approved group/payment entity. Personal wallets, UBO-linked wallets, employee wallets, or other informal wallet arrangements are strictly prohibited for use in connection with the licensed operation.
- 12.2 JetTon's wallet architecture segregates player-flow wallets, operational wallets, and treasury wallets, in order to ensure accountability and prevent commingling of player funds and company funds. Player funds are held in segregated wallets, separate from JetTon's operational and corporate funds.

- 12.3 JetTon may use a combination of hot, warm and cold wallets, provided that the wallet architecture is documented, risk-assessed, and subject to the controls described below:
- Hot wallets: used for day-to-day player deposits and withdrawals; balances are limited to operationally necessary amounts;
 - Warm wallets: used for liquidity management, subject to enhanced access controls and transaction-approval procedures;
 - Cold wallets: used for treasury, reserves, or longer-term safeguarding of funds, with access, key management, reconciliation and auditability maintained at all times;
 - Security controls: multi-signature authorisation, withdrawal whitelisting, multi-factor authentication (MFA), hardware security modules (HSMs), or equivalent measures, applied proportionately to the value and risk profile of each wallet.

JetTon maintains records sufficient to evidence wallet ownership/control, transaction history, reconciliations, access rights, approvals, and any movement of funds between wallets, in a manner that supports independent audit reproduction.

13. RESPONSIBLE GAMING IN A CRYPTO CONTEXT

- 13.1 JetTon applies the same Responsible Gaming controls to crypto-asset transactions as it applies to fiat transactions, including deposit limits, loss limits, cooling-off periods, and self-exclusion tools, as set out in JetTon's Responsible Gaming Policy.
- 13.2 JetTon recognises that the speed and micro-denomination of crypto-asset transactions can mask indicators of problem gambling. Accordingly, JetTon applies behavioural monitoring to crypto-funded accounts to identify markers of harm (including rapid deposit/withdrawal cycling and chasing losses) with the same rigour applied to fiat-funded accounts, irrespective of payment method.

14. INCIDENT REPORTING

In line with the incident reporting requirements established under the LOK, JetTon ensures that all crypto-related incidents are identified, assessed, and reported in accordance with Article 5.10 of the LOK (Incident Reporting). Reportable incidents include, without limitation:

- security breaches, including compromised private keys, wallet access, or unauthorised transactions;
- system failures impacting crypto processing (e.g., exchange outages, blockchain congestion, or failed transactions);
- detection of fraud schemes involving crypto-assets (e.g., coordinated deposit/withdrawal patterns, chip-dumping, or collusion);
- material discrepancies in wallet balances or transaction records;
- any event that may impact the integrity, security, or traceability of crypto transactions;
- exposure to sanctioned wallets, mixers, or other prohibited sources;
- smart-contract failures; and
- blockchain forks or chain-level disruptions.

JetTon's Compliance Officer is responsible for assessing reportable incidents and ensuring timely notification to the CGA in accordance with Article 5.10 of the LOK.

15. RECORD-KEEPING AND AUDIT

JetTon retains, for the periods required under applicable law and, in any event, for no less than five (5) years:

- Travel Rule payloads;
- on-chain risk reports produced by its blockchain analytics tools;
- KYC/EDD documentation relating to crypto-funded accounts;
- transaction logs for all crypto-asset deposits, wagers, and withdrawals; and
- records evidencing wallet ownership/control, reconciliations, access rights, and approvals as described in Section 12.

JetTon ensures reconciliation between blockchain explorer data, VASP/exchange statements, and its internal ledgers, and maintains its records and systems in a manner that enables independent audit reproduction by the CGA or JetTon's external auditors.

16. APPROVAL AND SIGN-OFF

This Policy has been reviewed and approved in accordance with Section 3 of this Policy.

Policy owner	Compliance Officer, JetTon Games B.V.
Effective date	August 10, 2026
Review frequency	At least annually, and on an ad-hoc basis per Section 3.2
Version	1.0

Signed for and on behalf of JetTon Games B.V.:



Mr. Dmytro Artemenko

Compliance Officer, JetTon Games B.V.

Date: 10.08.2026