

RISK POLICY FOR THE USE OF VIRTUAL ASSETS

Zeno Club B.V.

Registration No. 154987

Chuchubiweg 17, E-Commerce Park 51, Curaçao

Email: info@zeno-club.com

Effective Date: July 1, 2026

Version: 3.0

1. Purpose

This Risk Policy for the Use of Virtual Assets (the “**Policy**”) establishes the principles and controls applied by Zeno Club B.V. (the “**Company**”) in connection with the acceptance, transfer, conversion, storage or other use of cryptocurrencies and other virtual assets.

The purpose of this Policy is to identify and mitigate the legal, regulatory, money laundering, terrorist financing, proliferation financing, sanctions, fraud, cybersecurity, liquidity, volatility and reputational risks associated with virtual assets.

The Company applies a conservative and risk-based approach to virtual assets. Virtual assets may only be used where the relevant transaction has a legitimate commercial purpose, is sufficiently transparent and does not expose the Company to an unacceptable level of risk.

2. Scope

This Policy applies to the Company’s directors, officers, employees, contractors and service providers involved in approving, processing, monitoring, recording or reconciling virtual asset transactions.

The Policy applies to all virtual asset transactions made by or for the benefit of the Company, including payments received from customers, payments made to counterparties, conversions between virtual assets and fiat currency, and transfers involving Company-controlled wallets.

This Policy does not authorise the Company to provide virtual asset services to third parties. In particular, the Company shall not conduct virtual asset exchange, transfer, custody, brokerage, portfolio management or similar activities as a business for or on behalf of customers unless the required licence, exemption, dispensation or other regulatory approval has been obtained.

3. Regulatory Framework

The Company shall conduct its activities in accordance with the applicable laws and regulations of Curaçao, including the National Ordinance on the Supervision of Virtual Asset Service Providers, the National Ordinance on Identification of Clients when Rendering Services, the National Ordinance on the Reporting of Unusual Transactions, applicable legislation concerning money laundering, terrorist financing and proliferation financing, and the sanctions legislation in force in Curaçao.

The Company shall also take into account binding regulations, decisions, instructions and guidance issued by the Centrale Bank van Curaçao en Sint Maarten (“**CBCS**”), FIU Curaçao and other competent authorities, to the extent applicable to the Company’s business model.

Curaçao’s National Ordinance on the Supervision of Virtual Asset Service Providers forms part of the current regulatory framework maintained by the CBCS. The CBCS also maintains the applicable AML/CFT framework, including the identification and unusual transaction reporting legislation, and publishes the sanctions measures applicable in Curaçao.

The Company shall periodically assess whether its activities fall within the definition of regulated virtual asset services. No new crypto-related product, payment flow or service may be launched without prior legal and compliance review.

4. Risk Assessment

Before approving the use of a virtual asset, blockchain network, wallet or crypto service provider, the Company shall assess the associated risks. The assessment shall consider the nature and purpose of the proposed use, the transaction flow, the jurisdictions involved, the type of customer or counterparty, the traceability of transactions, the volatility and liquidity of the relevant asset, the cybersecurity arrangements and the regulatory status of any external provider.

Particular attention shall be given to assets or technologies that provide enhanced anonymity, transactions involving high-risk jurisdictions, unusually complex transaction chains, the use of multiple intermediary wallets and transactions that are inconsistent with the customer's known profile or expected activity.

The assessment and approval shall be documented. The Company may establish transaction limits, restrict the use of particular assets or networks, require additional approvals or prohibit a proposed use where the risk cannot be adequately mitigated.

The Company shall periodically review its exposure to virtual asset risks, taking into account changes in legislation, typologies, sanctions, blockchain analytics, fraud trends and the Company's business activities.

5. Approved Virtual Assets and Providers

The Company may only use virtual assets, wallets, exchanges, payment processors and other crypto-related providers that have been approved by the responsible management and compliance personnel.

An external provider shall be subject to reasonable due diligence before onboarding. This review shall cover its corporate identity, jurisdiction, regulatory or registration status, reputation, ownership and management, AML/CFT and sanctions controls, security arrangements, custody model, transaction-monitoring capabilities and ability to provide transaction records.

Preference shall be given to providers that are subject to effective regulatory supervision, conduct customer due diligence, perform sanctions and blockchain screening, maintain adequate cybersecurity controls and provide sufficient information for accounting, audit and compliance purposes.

The Company shall not rely solely on the controls performed by an external provider. The use of a third-party provider does not remove the Company's responsibility for managing the risks arising from its own activities.

Approval of a new crypto service provider shall require documented due diligence and approval by Compliance together with senior management.

6. Customer and Counterparty Controls

Before permitting a customer or counterparty to use virtual assets, the Company shall obtain sufficient information to understand the identity of the person or entity, the nature of the relationship, the purpose of the transaction and the expected level of activity.

Where required by the applicable risk level, the Company shall identify and verify the customer or counterparty and its ultimate beneficial owner, perform sanctions and politically exposed person screening, establish the source of funds and, in higher-risk cases, the source of wealth, and obtain information confirming ownership or lawful control of the originating or destination wallet.

The level of due diligence shall be proportionate to the identified risk. Enhanced due diligence and management approval shall be required where the transaction involves a high-risk jurisdiction, a politically exposed person, an unusually high amount, a newly created or previously unknown wallet, a complex ownership structure or another material risk factor.

The Company shall not proceed with a transaction where the required information cannot be obtained or where the information provided appears false, incomplete, inconsistent or misleading.

7. Transaction Monitoring

Virtual asset transactions shall be monitored both before and, where appropriate, after execution. Monitoring shall be designed to identify unusual transaction patterns, sanctions exposure, links to illicit activity and material deviations from the expected customer or counterparty profile.

Where technically and commercially available, the Company shall use blockchain analytics or equivalent screening tools to assess wallet addresses, transaction history and exposure to identified illicit or high-risk sources.

A transaction shall be escalated for additional review where it has no clear economic purpose, involves an unusual amount or frequency, is divided into several smaller transfers, passes through numerous unrelated wallets, involves a wallet linked to unlawful activity, or is otherwise inconsistent with the information available to the Company.

The Company may suspend, delay or reject a transaction while compliance checks are being completed, subject to applicable law and contractual obligations. Employees shall not inform a customer or counterparty that a transaction is being reviewed for possible regulatory reporting where such disclosure could constitute prohibited tipping-off.

8. Prohibited Transactions

The Company shall not knowingly accept, initiate or facilitate a virtual asset transaction involving:

- a sanctioned person, entity, wallet address, country, territory or prohibited activity;
- funds suspected to originate from fraud, theft, hacking, ransomware, terrorist financing, trafficking, sanctions evasion or other criminal conduct;
- mixers, tumblers or other services primarily designed to conceal the origin, ownership or destination of virtual assets;
- an unapproved anonymity-enhancing asset, wallet, service or protocol that prevents adequate monitoring;
- false identities, nominee arrangements or third-party wallets used without a reasonable explanation;
- an unlicensed or unapproved provider where regulatory authorisation is required; or
- any attempt to avoid customer identification, transaction monitoring, reporting obligations or internal approval limits.

The Company may additionally prohibit any asset, blockchain, jurisdiction, wallet or service provider that presents risks exceeding the Company's risk appetite.

9. Financial and Operational Risk

The Company recognises that virtual assets may be subject to significant price volatility, limited liquidity, technological failure, market manipulation, loss of access credentials, irreversible transfers, network congestion, forks and changes in applicable law.

Virtual asset balances shall therefore be kept at a level reasonably necessary for operational purposes. Unless otherwise approved by management, the Company shall not hold virtual assets for speculative investment purposes and may convert received virtual assets into fiat currency within a commercially reasonable period.

Transactions shall be checked before execution, including verification of the asset, network, wallet address, amount and applicable fees. Material transfers shall be subject to dual approval or another appropriate segregation-of-duties control.

Private keys, seed phrases, access credentials and authentication devices shall be protected against unauthorised access, disclosure, loss and misuse. Access shall be limited to authorised persons and reviewed periodically. The Company shall maintain appropriate backup, recovery and incident-response arrangements.

10. Sanctions and Unusual Transaction Reporting

Customers, counterparties, beneficial owners and relevant wallet addresses shall be screened against sanctions measures applicable in Curaçao before a virtual asset transaction is completed and periodically during an ongoing relationship.

Where a possible sanctions match is identified, the transaction shall not proceed until the match has been reviewed and resolved. Where required by applicable law, assets shall be frozen or otherwise restricted and the relevant competent authority shall be notified.

A transaction that meets the applicable indicators of an unusual transaction or otherwise gives rise to a reporting obligation shall be promptly referred to the responsible compliance officer. Any required report shall be submitted to FIU Curaçao within the applicable period and in the prescribed manner.

The CBCS identifies the National Ordinance on the Reporting of Unusual Transactions and the National Ordinance on Identification of Clients when Rendering Services as key components of Curaçao's AML/CFT framework. The official CBCS framework also includes the current sanctions legislation and the Omnibus Sanctions Decree Curaçao.

11. Record Keeping

The Company shall maintain adequate records of virtual asset transactions and related compliance checks for the period required by applicable law.

Records shall include, where available, the identity of the customer or counterparty, beneficial ownership information, wallet addresses, transaction hashes, transaction dates and amounts, the virtual asset and network used, the fiat equivalent, screening results, source-of-funds information, internal approvals and any investigation or reporting records.

Records shall be accurate, protected against unauthorised alteration or deletion and available to competent authorities where legally required.

12. Roles and Responsibilities

The Company's management is responsible for approving the Company's approach to virtual assets, determining its risk appetite and ensuring that adequate resources and controls are maintained.

The responsible compliance personnel shall oversee customer and counterparty due diligence, sanctions screening, transaction monitoring, internal escalation, regulatory reporting and periodic review of this Policy.

Employees and contractors involved in virtual asset transactions shall follow the approved procedures, complete required training and promptly report any suspected breach, unusual transaction, security incident or control weakness.

13. Breaches and Incidents

Any actual or suspected breach of this Policy shall be reported immediately to the responsible manager or compliance officer.

The Company shall investigate the incident, assess whether transactions or systems should be suspended, preserve relevant evidence, take corrective measures and determine whether notification to the CBCS, FIU Curaçao, law enforcement authorities, affected parties or another competent authority is required.

A breach of this Policy by an employee or contractor may result in suspension of access, disciplinary action, termination of the relevant relationship and, where appropriate, referral to the competent authorities.

14. Training and Review

Relevant employees shall receive periodic training on virtual asset risks, customer and wallet due diligence, sanctions controls, unusual transaction indicators, cybersecurity and internal escalation procedures.

This Policy shall be reviewed at least annually and whenever there is a material change in the Company's business model, virtual asset exposure, applicable legislation, regulatory guidance, technology or risk profile.

Any material amendment to this Policy shall be approved by the Managing Director or the Board of Directors.

Approved by authorized signatory

/Denis Kuznecov