

CONFIDENTIAL

CRYPTO ASSET POLICY

REVISION HISTORY

Version Number	Date	Summary of changes	Author
1.0	01/11/2025	New policy drafted	Alper Soylemez

Approved by: Gouloud Hammoud, Director	
---	--

PURPOSE

This Crypto Asset Policy defines how the Company manages, monitors, and controls all crypto-related activities used for customer deposits and withdrawals, in full alignment with:

- Curaçao AML/CFT National Ordinance
- Curaçao Sanctions Regulations
- Curaçao Gaming Authority (CGA) AML & Responsible Gaming Guidelines
- FATF Recommendations (especially 15 & the VA/VASP Interpretive Note)
- Internal AML, Fraud, KYC, and Risk policies

The Company does **not** hold, control, or operate any type of Virtual Asset (VA) wallet. All crypto transactions are processed exclusively through **regulated third-party Virtual Asset Service Providers (VASPs)**, ensuring that at no time does the Company have custody of customer crypto assets.

SCOPE

This policy applies to:

- All customers interacting with crypto deposit and withdrawal channels
- All employees in AML, Payments, Finance, Compliance, Risk, Fraud, or VIP teams
- All systems integrating with VASP solutions

- All crypto-related reporting, monitoring, and reconciliation processes

The Company interacts only with **fiat results of crypto transactions**, not with the crypto assets themselves.

OPERATING MODEL – ZERO CUSTODY

The Company operates a **full-outsourced, zero-custody model**:

1. The customer sends crypto directly to the **regulated VASP**, not to the Company.
2. The VASP performs **all blockchain monitoring, screening, sanctions checks, and Travel Rule compliance**.
3. The VASP converts crypto to fiat.
4. The VASP transfers **fiat only** to the Company.
5. The Company credits the customer account based on VASP-confirmed settlement value.

For withdrawals:

1. Customer requests a withdrawal in crypto.
2. The Company performs internal AML/EDD checks.
3. The Company instructs the VASP to pay the customer.
4. The VASP sends crypto directly to the customer's wallet.
5. The Company never touches the crypto.

This model ensures the Company is **not classified as a VASP** and does not fall under FATF "custodial wallet provider" definitions.

ACCEPTED CRYPTOCURRENCIES

The Company only accepts cryptocurrencies supported by the regulated VASP.

Common supported assets include:

- **USDT (TRC-20 / ERC-20)**
- **USDC**
- **BTC**
- **ETH**
- **LTC**

The Company does not receive, hold, or store any of these assets. All are handled solely by the VASP.

REGULATED VASP REQUIREMENT

To comply with CGA and FATF guidelines, the Company **only partners with VASPs that are licensed or registered** in a jurisdiction that:

- Implements FATF standards
- Has AML/CFT supervisory oversight
- Supports the Travel Rule
- Provides blockchain monitoring and sanctions screening
- Maintains robust custody and treasury controls
- Is not FATF-blacklisted or subject to international sanctions

Examples of acceptable VASP jurisdictions include Lithuania, Estonia, Canada, Switzerland, and EU MiCA jurisdictions once fully implemented.

Unregulated VASPs are strictly prohibited.

The Company reviews VASP due diligence annually.

CUSTOMER CRYPTO ONBOARDING & KYC

Customer Identification Requirements

The Company applies a **risk-based customer identification approach** for users engaging with Virtual Asset payment methods. Customer identity verification is performed **at appropriate stages of the customer lifecycle**, taking into account:

- transactional behaviour,
- deposit and withdrawal patterns,
- product and market risk,
- jurisdictional exposure,
- blockchain analytics indicators, and
- regulatory expectations under Curaçao AML/CFT laws.

Identity verification is required prior to the approval of withdrawals and the Company may require earlier verification where risk factors or AML/CFT indicators justify it. Crypto-related customer activity may be restricted,

suspended, or subject to enhanced verification at any time based on the Company's ongoing monitoring, internal assessments, or alerts received from the regulated VASP.

Risk Assessment for Virtual Asset Activity

The Company conducts continuous, risk-based monitoring of customers who use Virtual Asset payment methods. Additional verification measures may be applied **where customer behaviour, transactional patterns, blockchain-monitoring results, or jurisdictional considerations indicate elevated AML/CFT risk.**

Risk indicators may include, but are not limited to:

- unusual or inconsistent transaction behaviour,
- large-value or rapid-frequency Virtual Asset activity,
- wallet address characteristics identified by the VASP's analytics tools,
- inconsistencies in customer-provided information, or
- exposure to high-risk jurisdictions or typologies.

Where such risk factors are identified, the Company may request further information, apply Enhanced Due Diligence, impose temporary restrictions, or suspend activity until appropriate checks have been completed.

The timing and extent of verification measures are determined by the Company **in line with its internal risk assessments and regulatory obligations.**

RELIANCE ON THIRD-PARTY VASPs FOR CDD

The Company may rely on regulated VASPs to perform certain components of Customer Due Diligence (CDD) in accordance with Chapter III.9 of the CGA AML Regulations. Where such reliance is placed, the following requirements apply:

Equivalent or Higher CDD Standards

The Company ensures all partner VASPs are subject to AML/CFT regulations **equivalent to or stronger than** Curaçao requirements, including customer identification, sanctions screening, recordkeeping, and ongoing monitoring.

Access to CDD Information

The Company maintains written agreements stating that VASPs will provide upon request:

- All identification data
- Full CDD/KYC records
- Blockchain risk screening outputs
- Travel Rule information

Testing the Arrangement

The Company conducts **periodic testing** to confirm the VASP can and does provide CDD records as agreed. Testing may include sample requests, response-time checks, and documentation audits.

Responsibility Retained by the Company

Reliance on third parties does not transfer responsibility. The Company retains full obligation for AML/CFT compliance for all customers using VA payment methods.

Recordkeeping

All reliance arrangements, testing activities, and audit results are documented and retained for 7 years.

DEPOSITS – CONTROLS & PROCESS

Deposit Flow

1. Customer selects crypto deposit.
2. Platform redirects to the VASP.
3. Customer sends crypto directly to the VASP.
4. The VASP performs AML/CFT checks, blockchain screening, and Travel Rule compliance.
5. The VASP converts crypto to fiat and sends settlement confirmation.
6. The Company credits customer account in fiat equivalent.

Customer deposits via Virtual Assets are subject to ongoing monitoring and may trigger verification requirements in accordance with the Company's risk-based approach.

Blockchain Screening (Performed by VASP)

The VASP must screen:

- Sanctioned addresses
- Mixer/tumbler use
- Dark-web market exposure
- Scams, stolen funds, ransomware
- High-risk exchanges
- Structuring behaviour

Any flagged transaction requires **manual AML approval** before crediting.

Deposit Limits

Crypto deposits are subject to the same RG/AML limits as fiat:

- Daily/weekly/monthly limits
- Affordability checks
- High-risk reviews

WITHDRAWALS – CONTROLS & PROCESS

Withdrawal Flow

1. Customer requests crypto withdrawal.
2. Company conducts AML/EDD checks.
3. Company instructs VASP to process payment.
4. VASP sends crypto directly to customer wallet.
5. VASP provides settlement confirmation.

Wallet Screening

The VASP must screen customer withdrawal wallets for:

- Sanctions exposure
- Dark-web indicators
- Mixer association
- High-risk jurisdictions
- Illicit fund typologies

No Third-Party Withdrawals

Withdrawals may only be sent to wallets owned by the customer.

RECONCILIATION & FINANCIAL CONTROLS

Even though the Company does not handle crypto, it must reconcile:

- Daily VASP settlement reports
- Fiat settlement transfers
- Transaction-level summaries (TXIDs provided by VASP)
- Payment provider fees
- Customer account ledger entries

Reconciliations are documented and retained for **7 years**.

PROHIBITED ACTIVITIES

The following activities are expressly prohibited to ensure compliance with AML/CFT obligations and to maintain the integrity of the platform's Virtual Asset operations:

- Use of **third-party or non-beneficial-owner wallets** for deposits or withdrawals.
- Attempting to withdraw funds **without completing mandatory identity verification**.
- Use of **unregulated, high-risk, or FATF-blacklisted VASPs** for customer transactions.
- Use of VASPs, exchanges, or wallet providers that are sanctioned or restricted by **the United States (OFAC), the United Kingdom (HMT), Curaçao authorities**, or any other competent sanctions authority.
- Use of **privacy-enhancing coins or technologies** (e.g., mixers, tumblers, privacy coins) unless expressly permitted by the Company's risk assessment.
- Attempts to circumvent AML/CFT controls, including structuring, rapid value movement, or masking transactional behaviour.
- Use of Virtual Assets to obscure the source of funds or evade identity verification measures.
- Attempts to transfer value **between customer accounts or wallets** in a manner inconsistent with platform rules.

- Any activity that may cause the Company to be classified as a Virtual Asset Service Provider (VASP), including holding, operating, or controlling customer Virtual Asset wallets or engaging in crypto-to-crypto exchange activity.
- Any behaviour flagged by the regulated VASP's blockchain-monitoring systems as indicative of illicit activity, sanctions exposure, or elevated AML/CFT risk.

The Company may suspend, restrict, or review any customer activity where Virtual Asset behaviour indicates potential financial crime risk, regardless of verification stage or transaction size.

TRAVEL RULE COMPLIANCE

The Company ensures Travel Rule compliance via the VASP.

The VASP must:

- Collect originator/beneficiary information
- Transmit Travel Rule data where required
- Retain full Travel Rule logs
- Provide data to the Company when needed for AML investigations

The Company reviews Travel Rule compliance as part of VASP onboarding and annual due diligence.

REPORTING OBLIGATIONS

The Company files reports to **FIU Curaçao** including:

- UTRs
- STRs
- Sanctions reports
- Voluntary intelligence reports

VASP alerts and blockchain risk indicators inform STR/UTR decisions.

RECORD KEEPING

The Company retains for **7 years**:

- VASP onboarding due diligence
- VASP licensing/registration evidence
- Daily settlement and conversion reports
- Blockchain risk reports provided by the VASP
- Customer KYC and EDD files
- Internal AML investigations and decisions
- Reconciliation logs
- Travel Rule compliance reports

ROLES & RESPONSIBILITIES

MLRO

- Oversight of crypto-related AML/CFT risk
- Assessment of VASP performance and compliance
- Investigation of alerts and high-risk users
- Reporting to FIU Curaçao
- Annual policy review

Payments Team

- Reconciliation of VASP settlement reports
- Investigation of delays and unusual flows
- Monitoring VASP-related issue logs

AML/Fraud Team

- Review of VASP blockchain alerts
- EDD on high-risk crypto users
- Analysis of withdrawal patterns

Executive Management

- Approval of VASP partners
- Ensure adequate AML resources
- Review of crypto risk exposure

POLICY REVIEW

This policy is reviewed annually or sooner if:

- CGA requirements change
- VASP partners change
- New crypto risks or vulnerabilities emerge

All versions are logged in the central policy repository.