

V 1.0

WINLINK B.V.

CRYPTO ASSET POLICY

Document / Revision History

Document Reference: WINLINK B.V. CRYPTO ASSET POLICY Revision Number: 1.0 Total Pages: 16 Original issue date: 06.07.2026 Revision date: Effective Date:	CRYPTO ASSET POLICY
Written by: Compliance Officer Kristian Spasov  Date: _____ Kristian Spasov (Jul 15, 2026 19:11:53 GMT+3) Approved by: Gouloud Mercedes Hammoud obo Global Related Services B.V. Managing Director WINLINK B.V.  Date: _____	

Revision #	Version Date	Description of Changes
1.0		Initial Draft

Contents

1. INTRODUCTION, SCOPE AND REGULATORY FRAMEWORK

- 1.1 Purpose and Scope
- 1.2 Scope of Crypto Asset Activities
- 1.3 Regulatory Framework and AML/CFT Integration
- 1.4 Definitions
- 1.5 Implementation Timeline

2. GOVERNANCE AND RESPONSIBILITIES

- 2.1 Governance Framework and Board Oversight
- 2.2 Senior Management
- 2.3 First Line of Defence: Operations and Finance
- 2.4 Second Line of Defence: Compliance, MLRO and Information Security
- 2.5 Third Line of Defence: Internal Audit
- 2.6 Staff Competence and Training

3. ENTERPRISE CRYPTO RISK MANAGEMENT FRAMEWORK

- 3.1 Risk-Based Approach
- 3.2 Enterprise Crypto Risk Assessment
- 3.3 Risk Assessment Methodology
- 3.4 Risk Review and Reassessment

4. CRYPTO ASSET GOVERNANCE FRAMEWORK

- 4.1 Approved Crypto Asset Register
- 4.2 Prohibited Assets and Sources
- 4.3 Highly Speculative Tokens
- 4.4 Stablecoin Requirements

5. CUSTOMER AND WALLET DUE DILIGENCE

- 5.1 AML/CFT Integration
- 5.2 Wallet Ownership Verification
- 5.3 Unhosted (Self-Hosted) Wallets
- 5.4 Pooled and Omnibus Wallets

6. BLOCKCHAIN ANALYTICS AND TRANSACTION MONITORING

- 6.1 Blockchain Analytics Capability
- 6.2 Wallet Screening and Ongoing Transaction Monitoring

7. DEPOSIT AND WITHDRAWAL CONTROLS

- 7.1 Pre-Screening Principle
- 7.2 Transaction Management and the Closed-Loop Principle
- 7.3 Permitted Alternative Approaches

8. VIRTUAL ASSET SERVICE PROVIDERS (VASPs) AND THE TRAVEL RULE

- 8.1 Non-Transferability of Risk
- 8.2 VASP Due Diligence
- 8.3 Compliance with the FATF Travel Rule (Recommendation 16)
- 8.4 Ongoing Monitoring of VASP Relationships

9. WALLET GOVERNANCE AND ASSET CUSTODY

9.1 Ownership and Prohibited Arrangements

9.2 Wallet Segregation

9.3 Hot, Warm and Cold Wallet Architecture

10. INCIDENT MANAGEMENT, REGULATORY REPORTING AND RECORDKEEPING

10.1 Incident Management Framework

10.2 Regulatory Incident Reporting

10.3 Audit-Ready Recordkeeping

11. INTERNAL DOCUMENTATION

1. INTRODUCTION, SCOPE AND REGULATORY FRAMEWORK

1.1 Purpose and Scope

This Crypto Asset Policy establishes the governance principles, responsibilities, risk management framework and internal control requirements applicable to the Company's use of crypto assets in its business activities. The Policy defines the Company's governance framework for crypto asset activities and is intended to ensure compliance with applicable laws and regulations, the requirements of the Curaçao Gaming Authority (CGA), international AML/CFT standards and the Company's corporate governance framework.

This Policy applies to all activities involving crypto assets, including the acceptance of deposits, processing of withdrawals, management of corporate wallets, engagement with Virtual Asset Service Providers (VASPs), and any other activities involving crypto assets within the scope of the Company's business operations.

The requirements of this Policy apply to the Board of Directors, Senior Management, employees and, where applicable, third parties performing activities on behalf of the Company within the scope of their responsibilities or contractual obligations.

This Policy shall be read together with the Company's other internal policies and standards governing risk management, internal control, information security, AML/CFT and operational activities.

1.2 Scope of Crypto Asset Activities

The Company uses crypto assets solely within the scope of its authorised business activities and in accordance with applicable legislation and regulatory requirements.

Where activities involving virtual assets are performed by another legal entity within the corporate group, each entity shall remain responsible for complying with the legal and regulatory requirements applicable to the activities it performs.

Nothing in this Policy shall be interpreted as extending the Company's activities beyond those permitted under the applicable legal and regulatory framework.

1.3 Regulatory Framework and AML/CFT Integration

The use of crypto assets does not exempt the Company from its AML/CFT obligations.

This Policy complements the Company's AML/CFT & CPF Manual and forms an integral part of the Company's overall AML/CFT control framework. Where requirements differ, the provision establishing the higher level of control shall prevail.

This Policy has been developed with reference to:

- the National Ordinance for Games of Chance (LOK);
- the Curaçao Gaming Authority Crypto Policy Guideline;
- the FATF Recommendations, including Recommendation 15 and Recommendation 16 (Travel Rule).

The Company shall monitor changes in applicable legislation, regulatory requirements, international standards and official regulatory guidance and shall ensure that this Policy and related governance arrangements are reviewed and updated where appropriate.

1.4 Definitions

For the purposes of this Policy, terms shall have the meanings assigned to them under applicable legislation, the guidance issued by the Curaçao Gaming Authority, the FATF Recommendations and the Company's internal regulatory framework, unless otherwise expressly stated.

For the purposes of this Policy, the following definitions apply:

Approved Crypto Asset Register means the Company's internal register of crypto assets approved for use within its business activities following completion of the applicable risk assessment and internal approval process.

Blockchain Analytics means the processes, methodologies and technological solutions used to analyse blockchain transactions, assess wallet risk, determine the origin of funds, identify links to high-risk entities and support financial crime investigations.

Cold Wallet means a cryptocurrency wallet that is not permanently connected to the Internet and is used for the long-term secure storage of crypto assets.

Crypto Asset means a digital representation of value capable of being transferred or stored electronically that falls within the definition of a Virtual Asset under applicable FATF standards and the requirements of the Curaçao Gaming Authority.

Customer Due Diligence (CDD) means the customer identification, verification and risk assessment measures performed in accordance with the Company's AML/CFT Framework.

Enhanced Due Diligence (EDD) means enhanced customer due diligence measures applied where higher ML/TF risk has been identified in accordance with the Company's AML/CFT Framework.

Hot Wallet means a cryptocurrency wallet connected to the Internet and used for processing day-to-day crypto asset deposits and withdrawals.

Mixer (Tumbler) means a service, protocol or other mechanism designed to obscure the origin, destination or transaction trail of crypto assets by combining transactions from multiple users.

User Funds means fiat currency and/or crypto assets belonging to users and held by the Company in connection with its business activities.

Politically Exposed Person (PEP) means an individual identified as a politically exposed person in accordance with applicable legislation and the Company's AML/CFT Framework.

Prohibited Source means any crypto asset, wallet address, service, transaction or other source of funds prohibited under applicable legislation, sanctions regimes, CGA requirements or the Company's internal policies.

Risk Appetite means the level and type of risk that the Board of Directors and Senior Management are willing to accept in relation to crypto asset activities, taking into account applicable regulatory requirements and the Company's internal control framework.

Risk-Based Approach (RBA) means an approach under which the nature and extent of controls, monitoring and due diligence measures are proportionate to the level of risk presented by a customer, transaction, crypto asset, wallet, VASP or other relevant activity.

Sanctioned Wallet means a cryptocurrency wallet address or other virtual asset identifier included in applicable sanctions lists or otherwise designated by a competent authority as subject to sanctions.

Self-Hosted (Unhosted) Wallet means a cryptocurrency wallet controlled directly by its user without the involvement of a regulated Virtual Asset Service Provider (VASP).

Source of Funds (SoF) means the origin of the funds used for a particular transaction or series of related transactions.

Source of Wealth (SoW) means the origin of a customer's overall wealth.

Transaction Monitoring means the ongoing risk-based process of reviewing crypto asset transactions to identify unusual, suspicious or prohibited activity requiring additional review or control measures.

Travel Rule means the requirements established under FATF Recommendation 16 relating to the collection, transmission and retention of originator and beneficiary information for applicable virtual asset transfers.

Virtual Asset Service Provider (VASP) means any natural or legal person conducting activities falling within the FATF definition of a Virtual Asset Service Provider and applicable legislation.

Wallet Ownership Verification means the measures applied to obtain reasonable assurance that a cryptocurrency wallet is controlled by the relevant customer or another duly authorised person.

Wallet Screening means the screening of cryptocurrency wallet addresses using blockchain analytics, sanctions screening and other risk assessment mechanisms before or during transaction processing.

Warm Wallet means a cryptocurrency wallet used for intermediate storage of crypto assets and liquidity management, providing a higher level of security than a Hot Wallet while maintaining operational

accessibility.

Unless otherwise expressly provided in this Policy, capitalised terms shall have the meanings assigned under applicable legislation, the guidance of the Curaçao Gaming Authority, the FATF Recommendations and the Company's internal regulatory framework.

1.5 Implementation Timeline

The implementation milestones set out below reflect the Company's transition plan for implementing the Curaçao Gaming Authority's crypto asset requirements and serve as internal reference points for the phased implementation of the Company's crypto asset governance framework.

Upon completion of the implementation period, this section shall be reviewed and amended or removed, as appropriate, to reflect the prevailing regulatory framework.

To support compliance with the CGA requirements, the Company has adopted the following implementation roadmap:

- **Immediate:** Prohibition of dealings with sanctioned wallets, mixers, prohibited crypto assets and other prohibited sources of funds.
- **September 2026:** Approval of this Policy, submission to the CGA Portal and commencement of internal capability development.
- **December 2026:** Completion of documented risk assessments, implementation of VASP due diligence processes, transaction monitoring arrangements and staff training.
- **June 2027:** Full implementation of wallet segregation, blockchain analytics capabilities, withdrawal controls (including wallet whitelisting) and reconciliation controls.

2. GOVERNANCE AND RESPONSIBILITIES

2.1 Governance Framework and Board Oversight

The Company shall maintain an effective governance framework for its crypto asset activities based on the principles of accountability, independent oversight, clear allocation of responsibilities and a risk-based approach.

Governance of crypto asset activities shall operate in accordance with the Three Lines of Defence model, ensuring an appropriate segregation of management, control and independent assurance functions.

The Board of Directors shall provide overall oversight of the Company's crypto risk management framework and retain ultimate responsibility for its effectiveness.

The responsibilities of the Board of Directors include:

- approving this Policy and reviewing its effectiveness at least annually;
- determining the Company's Risk Appetite for crypto asset activities;
- overseeing compliance with the applicable requirements of the Curaçao Gaming Authority relating to crypto assets.

The Board of Directors shall retain overall accountability for the governance framework irrespective of any delegation of operational responsibilities to management committees or designated officers.

2.2 Senior Management

Senior Management shall be responsible for implementing this Policy, establishing appropriate control measures and ensuring that adequate financial, technical and human resources are available to support its effective implementation.

Senior Management may establish internal governance bodies, including a Risk Committee or other authorised management committees, to support decision-making in relation to:

- approval of new crypto assets and maintenance of the Approved Crypto Asset Register based on documented risk assessments;
- approval of new relationships with Virtual Asset Service Providers (VASPs) and payment service providers.

Senior Management shall ensure that the requirements of this Policy are effectively embedded within the Company's operational processes, coordinate activities across relevant functions, monitor the adequacy of internal controls and ensure the timely remediation of identified deficiencies.

Where appropriate, having regard to the nature, scale and complexity of the Company's activities, specific crypto risk matters may be considered by a designated management committee or other authorised governance body.

2.3 First Line of Defence: Operations and Finance

The first line of defence shall own and manage the operational risks arising from the Company's crypto asset activities and shall be responsible for the day-to-day operation of the relevant controls.

Operations / Payments shall be responsible for processing crypto asset deposits and withdrawals, performing wallet verification procedures, conducting day-to-day transaction monitoring and escalating higher-risk transactions where appropriate.

Finance shall be responsible for performing periodic reconciliations of crypto assets, ensuring appropriate segregation of user funds from the Company's own assets and managing liquidity across operational and custodial wallets.

The first line of defence shall be responsible for the ongoing operation of the relevant controls, timely identification of control deficiencies and escalation of material issues in accordance with the Company's governance arrangements.

2.4 Second Line of Defence: Compliance, MLRO and Information Security

The second line of defence shall provide independent oversight of the Company's crypto asset control framework and support the effective management of regulatory, AML/CFT and information security risks.

Compliance Officer / MLRO shall oversee the implementation of AML/CFT controls applicable to crypto asset activities, the use of blockchain analytics capabilities, compliance with the FATF Travel Rule and the investigation of suspicious activity. The Compliance function shall operate with an appropriate degree of independence from operational functions.

Information Security shall be responsible for the governance of wallet security architecture, protection of cryptographic keys, access management and coordination of the Company's response to cybersecurity incidents affecting crypto asset activities.

2.5 Third Line of Defence: Internal Audit

The Internal Audit function, or an appropriately independent external assurance provider where applicable, shall provide independent and objective assurance regarding the design and effectiveness of the Company's crypto asset governance and control framework.

Internal Audit shall periodically assess the effectiveness of the controls implemented by the first and second lines of defence and report its findings directly to the Board of Directors or the appropriate governing body.

2.6 Staff Competence and Training

The Company shall ensure that employees involved in crypto asset activities receive appropriate training commensurate with their roles and responsibilities.

Training programmes shall be risk-based, periodically reviewed and designed to maintain an appropriate level of competence in relation to applicable regulatory requirements, AML/CFT obligations, crypto asset risks and internal control procedures.

As appropriate to their responsibilities, training shall include the identification of financial crime red flags, wallet verification procedures, incident escalation requirements, blockchain analytics awareness and the secure handling of crypto asset infrastructure.

3. ENTERPRISE CRYPTO RISK MANAGEMENT FRAMEWORK

3.1 Risk-Based Approach

The Company shall apply a Risk-Based Approach (RBA) to all crypto asset activities throughout the customer relationship and transaction lifecycle.

The nature and extent of due diligence, monitoring and control measures shall be proportionate to the level of risk associated with the customer, transaction, crypto asset, wallet, Virtual Asset Service Provider (VASP) or any other relevant risk factor.

3.2 Enterprise Crypto Risk Assessment

The Company shall perform an enterprise-wide assessment of the risks arising from its crypto asset activities as an integral component of its Business Risk Assessment.

The assessment shall identify, evaluate, document and, where appropriate, establish mitigation measures for risks including:

- money laundering, terrorist financing and proliferation financing risks;
- sanctions risks associated with wallets, counterparties or jurisdictions subject to applicable sanctions;
- operational and technology risks, including blockchain infrastructure failures, smart contract vulnerabilities and cryptographic key management risks;
- fraud risks arising from the misuse of the Company's platform for scams, social engineering or other financial crime.

3.3 Risk Assessment Methodology

The Company shall maintain a documented and consistently applied methodology for assessing risks associated with crypto asset activities.

The methodology shall support the consistent, evidence-based and proportionate assessment of risks relating to customers, crypto asset wallets, crypto assets, transactions, Virtual Asset Service Providers (VASPs) and other relevant risk factors.

The methodology shall establish the principles for assigning risk ratings (Low, Medium, High and Unacceptable), determining when Enhanced Due Diligence (EDD) is required and conducting periodic reassessments where changes in circumstances or new risk factors are identified.

Detailed assessment criteria, risk indicators, scoring methodologies and supporting guidance shall be established within the Company's internal documentation.

3.4 Risk Review and Reassessment

The Company's Enterprise Crypto Risk Assessment shall be reviewed at least annually and additionally where required in response to internal reviews, audit findings, significant incidents or material changes to the Company's risk profile.

A reassessment shall also be performed where appropriate following, including but not limited to:

- the introduction of new crypto asset products, blockchain networks or relationships with new VASPs or payment service providers;
- significant changes in applicable CGA requirements, FATF standards or relevant legislation;
- the identification of emerging financial crime typologies or material information security incidents.

4. CRYPTO ASSET GOVERNANCE FRAMEWORK

4.1 Approved Crypto Asset Register

The Company shall accept, process and hold only those crypto assets that have undergone a documented risk assessment and have been formally approved for use within the Company's business activities.

The decision to approve a new crypto asset or remove a previously approved asset shall be based on a documented risk assessment, taking into account, among other factors, applicable regulatory requirements, the characteristics of the relevant crypto asset, operational risks, financial crime risks and the Company's ability to maintain an appropriate level of control.

The Company shall maintain an up-to-date Approved Crypto Asset Register and ensure its periodic review in light of changes to the Company's risk profile, regulatory requirements and other material circumstances.

4.2 Prohibited Assets and Sources

The Company shall not engage in transactions involving crypto assets, sources of funds or other high-risk assets where their use is inconsistent with applicable legislation, sanctions regimes, the Company's Risk Appetite or this Policy.

The following shall be prohibited:

- Crypto assets directly or indirectly associated with wallet addresses included in applicable sanctions lists.
- Funds originating from sanctioned anonymisation services, mixers or tumblers.
- Privacy-enhancing cryptocurrencies where their functionality prevents effective blockchain analytics or transaction transparency.
- Wrapped tokens and bridged assets where the transaction history or provenance of the underlying asset cannot be reasonably verified.
- Any source of funds identified by blockchain analytics providers as presenting an unacceptable level of risk, including darknet marketplaces, ransomware-related wallets or other prohibited sources.

4.3 Highly Speculative Tokens

The Company shall exercise enhanced caution when considering the use of highly speculative crypto assets characterised by significant price volatility, limited liquidity, insufficient project maturity or the absence of a sustainable economic model.

The decision to permit the use of such crypto assets shall be supported by a documented risk assessment taking into consideration, where relevant:

- liquidity and market resilience;
- historical volatility;
- project maturity and ecosystem sustainability;
- governance transparency;
- the ability to perform effective blockchain analytics;
- potential exposure to financial crime risks.

Where the Company is unable to obtain sufficient assurance regarding the associated risks or implement appropriate control measures, it may decline to approve the relevant crypto asset.

4.4 Stablecoin Requirements

The Company shall give preference to stablecoins demonstrating an appropriate level of transparency, stability, liquidity and effective risk management characteristics.

When assessing the suitability of a stablecoin, the Company shall consider, among other factors, the reserve structure, issuer reliability, transparency of issuance and redemption mechanisms, regulatory status, market liquidity, resilience of the stabilisation mechanism and the ability to apply effective blockchain analytics and other control measures.

Algorithmic, crypto-backed or other higher-risk stablecoins may only be used following a documented risk assessment and where the Company is satisfied that the associated risks can be appropriately managed.

The Company may restrict or discontinue the use of any stablecoin where there is a material deterioration in its risk profile, loss of transparency, de-pegging from its reference asset, changes to its regulatory status or any other circumstance that may affect its safety or compliance with this Policy.

5. CUSTOMER AND WALLET DUE DILIGENCE

5.1 AML/CFT Integration

When conducting crypto asset activities, the Company shall apply the requirements of its AML/CFT Framework in full, including Customer Due Diligence (CDD), Enhanced Due Diligence (EDD), identification of Politically Exposed Persons (PEPs), Source of Funds (SoF), Source of Wealth (SoW), sanctions screening and ongoing monitoring of business relationships.

The use of crypto assets shall not alter the Company's AML/CFT obligations. However, additional risk-based control measures shall be applied, where appropriate, taking into account the characteristics of virtual assets, wallet types, transaction profiles and the results of blockchain analytics.

The criteria for applying Enhanced Due Diligence shall be established in the Company's internal documentation.

5.2 Wallet Ownership Verification

The Company shall apply reasonable and proportionate measures to obtain sufficient assurance that a cryptocurrency wallet used by a customer is under that customer's control or is otherwise used on a lawful basis.

The scope and method of verification shall be determined having regard to the customer's risk profile, the nature of the transaction, the wallet type and other relevant risk factors. The Company may apply different verification methods, provided they provide an appropriate level of assurance and remain consistent with the Risk-Based Approach.

5.3 Unhosted (Self-Hosted) Wallets

The Company may accept deposits from and process withdrawals to Unhosted (Self-Hosted) Wallets, provided that appropriate risk-based control measures are applied.

For such transactions, the Company shall utilise blockchain analytics to assess the origin of funds, transaction characteristics, potential links to prohibited or high-risk sources and the need for additional control measures.

Where appropriate, the Company may apply Enhanced Due Diligence (EDD), request additional information or decline to process a transaction in accordance with its AML/CFT Framework and this Policy.

5.4 Pooled and Omnibus Wallets

The use of pooled wallets or omnibus accounts operated by third-party Virtual Asset Service Providers (VASPs) shall be permitted only where the Company is able to obtain sufficient information to attribute each transaction to the relevant customer.

Structures that prevent effective customer identification, source of funds monitoring or independent audit shall not be accepted.

The Company may refuse to process transactions involving such arrangements where they do not enable compliance with AML/CFT requirements, effective monitoring or the availability of information necessary for internal control and audit purposes.

6. BLOCKCHAIN ANALYTICS AND TRANSACTION MONITORING

6.1 Blockchain Analytics Capability

The Company shall maintain blockchain analytics capabilities appropriate to the nature, scale and risk profile of its crypto asset activities.

For this purpose, the Company may utilise specialised blockchain analytics solutions, internally developed analytical capabilities or a combination thereof to support the analysis of the origin and destination of funds, assessment of cryptocurrency wallet risk, identification of links to prohibited or high-risk sources and the investigation of suspicious activity.

The blockchain analytics capabilities employed by the Company shall be appropriate to the nature, scale and complexity of its crypto asset activities and shall support the effective management of financial crime risks.

6.2 Wallet Screening and Ongoing Transaction Monitoring

The Company shall apply risk-based monitoring to crypto asset transactions throughout the customer relationship lifecycle.

Control measures shall include the screening of cryptocurrency wallet addresses and transactions prior to execution, as well as ongoing monitoring where appropriate, taking into account the nature of the transaction, the assessed level of risk and the requirements of the Company's AML/CFT Framework.

Where circumstances indicate an elevated level of risk or potential suspicious activity, the Company shall apply additional control measures, including, where appropriate, Enhanced Due Diligence (EDD), escalation, further investigation or other actions in accordance with this Policy and the Company's internal regulatory framework.

7. DEPOSIT AND WITHDRAWAL CONTROLS

7.1 Pre-Screening Principle

The Company shall apply a Risk-Based Approach to all inbound and outbound crypto asset transactions. Prior to accepting a deposit or executing a withdrawal, the Company shall apply proportionate control measures designed to identify sanctions risks, prohibited sources of funds, indicators of financial crime and any other circumstances that may affect the security of the transaction or compliance with AML/CFT requirements.

The scope and nature of such controls shall be determined having regard to the level of risk, the nature of the transaction, the crypto asset involved, the results of blockchain analytics and any other relevant risk factors.

7.2 Transaction Management and the Closed-Loop Principle

The Company shall apply the Closed-Loop Principle as its primary approach to the management of crypto asset transactions.

Under this principle, the Company seeks to ensure that crypto assets are transferred between wallets controlled by the same customer, thereby reducing the risk of unjustified changes to the receiving wallet and preventing the use of the Company's platform as a transit mechanism for the movement of virtual assets. The Closed-Loop Principle is intended to mitigate the risks of money laundering, fraud, the use of nominee wallets and other arrangements that may obscure the identity of the beneficial owner of crypto assets. Unless otherwise provided for under this Policy or justified by the outcome of a risk-based assessment, crypto asset withdrawals shall be made to a cryptocurrency wallet previously used by the customer for deposits and, where reasonably practicable, in the same crypto asset.

Any exception to the Closed-Loop Principle shall be permitted only where additional control measures provide sufficient assurance as to the legitimacy of the transaction, compliance with AML/CFT requirements and the transparency of the movement of crypto assets.

7.3 Permitted Alternative Approaches

The Company recognises that, in certain circumstances, the strict application of the Closed-Loop Principle may not be possible or appropriate for legitimate operational reasons.

In such cases, an alternative approach may be applied provided that the Company is able to maintain an appropriate level of transaction transparency, establish the legitimate origin of the funds, obtain reasonable assurance that the cryptocurrency wallet is controlled by the customer and comply with all applicable AML/CFT requirements.

Such circumstances may include, but are not limited to:

- replacement of a previously used cryptocurrency wallet by the customer;
- inability to use the wallet from which the original deposit was made;
- the need to process a withdrawal in another supported crypto asset for legitimate operational reasons;
- other justified circumstances that are consistent with this Policy.

In such circumstances, the Company shall apply additional risk-based control measures, which may include wallet ownership verification, blockchain analytics, obtaining additional customer information, Enhanced Due Diligence (EDD) or other measures provided for under the Company's AML/CFT Framework.

The decision to apply an alternative approach shall be based on a documented risk assessment.

8. VIRTUAL ASSET SERVICE PROVIDERS (VASPs) AND THE TRAVEL RULE

8.1 Non-Transferability of Risk

The Company may engage third-party Virtual Asset Service Providers (VASPs), including cryptocurrency exchanges, custodians and payment service providers, based on a Risk-Based Approach.

The engagement of third-party service providers shall not relieve the Company of its responsibility for complying with AML/CFT requirements, applicable regulatory obligations, user protection requirements, transaction monitoring or any other obligations arising under applicable legislation or this Policy.

The Company shall retain overall responsibility for the appropriate selection, assessment, ongoing monitoring and oversight of all VASPs to the extent relevant to the services they provide.

8.2 VASP Due Diligence

Prior to establishing a business relationship with a Virtual Asset Service Provider (VASP), the Company shall conduct a risk-based due diligence assessment proportionate to the nature of the proposed relationship.

The assessment shall be designed to confirm that the proposed relationship does not expose the Company to an unacceptable level of regulatory, operational or AML/CFT risk and is consistent with the requirements of this Policy.

The results of the due diligence assessment, information relating to approved VASPs, decisions taken, any applicable restrictions and the results of ongoing monitoring shall be documented and maintained in an up-to-date manner.

The Company shall periodically review the outcome of the assessment and perform a reassessment where circumstances arise that may materially affect the associated level of risk or the continuation of the business relationship.

8.3 Compliance with the FATF Travel Rule (Recommendation 16)

The Company recognises and implements the requirements of FATF Recommendation 16 (the Travel Rule) to the extent applicable to its business activities and the relevant regulatory requirements.

Where crypto asset transfers are conducted between regulated entities, including Virtual Asset Service Providers (VASPs), the Company shall collect, verify and transmit the required originator and beneficiary information in accordance with applicable legal and regulatory requirements.

The Company shall ensure that such information accompanies the relevant transfer where required and is retained and made available to competent authorities in accordance with applicable legislation.

8.4 Ongoing Monitoring of VASP Relationships

The Company shall perform ongoing monitoring of its relationships with Virtual Asset Service Providers to identify changes that may affect the level of risk, regulatory compliance or the continued suitability of the business relationship.

Where material changes are identified, including changes to regulatory status, the application of sanctions, deficiencies in the VASP's AML/CFT framework or any other circumstances affecting the associated level of risk, the Company shall perform a reassessment and, where appropriate, restrict, suspend or terminate the business relationship.

9. WALLET GOVERNANCE AND ASSET CUSTODY

9.1 Ownership and Prohibited Arrangements

All cryptocurrency wallets used in connection with the Company's business activities shall be under the control of the Company or another legal entity within the Company's corporate group formally authorised to perform the relevant functions.

The Company shall ensure that the purpose of each corporate wallet can be identified, that responsibility for its management is assigned where appropriate, and that its use is appropriately documented.

The use of personal wallets belonging to employees, Ultimate Beneficial Owners (UBOs), or any other unauthorised arrangements for holding or managing the Company's crypto assets shall not be permitted.

9.2 Wallet Segregation

The Company shall ensure the segregation of cryptocurrency wallets according to their intended purpose, including wallets used for user funds, operational activities and treasury functions.

User Funds shall be maintained separately from the Company's own assets to ensure transparency, accountability and to prevent the commingling of customer funds with the Company's proprietary assets. The wallet segregation framework shall support the clear identification of wallet purpose, transparency of fund movements and the effective operation of internal controls.

9.3 Hot, Warm and Cold Wallet Architecture

The Company shall maintain a layered crypto asset custody architecture comprising Hot, Warm and Cold Wallets. The custody architecture shall be documented, appropriate to the nature and risk profile of the Company's activities, and designed to support effective internal control.

Within this custody architecture:

- **Hot Wallets** shall primarily be used for processing day-to-day customer deposits and withdrawals. The amount of crypto assets maintained in Hot Wallets shall be limited to operational requirements.
- **Warm Wallets** shall be used for operational liquidity management and the transfer of assets between different custody layers, supported by additional control measures.
- **Cold Wallets** shall be used for the long-term storage of reserves, treasury assets and other crypto assets that do not require continuous operational access.

The allocation of crypto assets across different wallet types shall take into account security requirements, business continuity, liquidity needs and the effectiveness of internal controls.

The custody architecture shall be reviewed periodically to reflect changes in the Company's activities, transaction volumes and risk profile.

10. INCIDENT MANAGEMENT, REGULATORY REPORTING AND RECORDKEEPING

10.1 Incident Management Framework

The Company shall maintain a documented incident management framework designed to ensure the timely identification, assessment, escalation, investigation, response to and resolution of incidents that may adversely affect the security of crypto assets, compliance with AML/CFT requirements, business continuity or the Company's reputation.

All material incidents shall be recorded, documented, analysed and reviewed to determine their root causes, assess their impact and identify measures to prevent recurrence.

10.2 Regulatory Incident Reporting

The Company shall ensure the timely identification, assessment and, where required, notification of material incidents to the Curaçao Gaming Authority in accordance with applicable legislation and regulatory requirements.

Material incidents may include, but are not limited to:

- security incidents, including the compromise of cryptographic keys, unauthorised access to wallets or unauthorised transactions;
- significant failures affecting the Company's crypto asset infrastructure or third-party service providers that impact the security or availability of services;
- identified fraud schemes or other financial crime involving crypto assets;
- material discrepancies identified through internal controls or reconciliation processes;
- confirmed exposure to prohibited sources of funds or any other event that may materially affect compliance with AML/CFT obligations.

10.3 Audit-Ready Recordkeeping

The Company shall maintain records sufficient to demonstrate compliance with this Policy, its AML/CFT Framework, applicable legislation and the regulatory requirements of the Curaçao Gaming Authority. Records shall include, where applicable, risk assessment documentation, Virtual Asset Service Provider (VASP) due diligence, evidence of control measures applied, blockchain analytics results, investigation records, documented management decisions, crypto asset transaction records and any other information required for internal control, audit or regulatory purposes.

Record retention periods and recordkeeping arrangements shall be governed by applicable legislation and the Company's internal regulatory framework.

11. INTERNAL DOCUMENTATION

The requirements of this Policy shall be supported by the Company's internal regulatory framework, consisting of interconnected internal documents governing specific aspects of crypto asset governance to the extent necessary for the effective implementation of this Policy, applicable legislation and the regulatory requirements of the Curaçao Gaming Authority.

Depending on the subject matter, such documentation may include:

- Regulatory policies, methodologies and guidance governing risk management, AML/CFT compliance, the assessment of crypto assets, Virtual Asset Service Providers (VASPs) and other relevant risk areas.
- Operational standards, procedures and work instructions governing crypto asset transaction processing, the use of blockchain analytics, transaction monitoring, Travel Rule compliance, incident management and other operational processes.
- Information security standards and technical documentation governing crypto asset custody architecture, cryptographic key management, access control, cyber resilience and other technical security measures.

- Internal registers, inventories and other records supporting the documentation of management decisions, including information relating to approved crypto assets, approved Virtual Asset Service Providers (VASPs) and other matters subject to internal governance and monitoring.

Such documentation shall be maintained, reviewed as necessary and made available to employees in accordance with their responsibilities and authorised level of access.

2026 0714 Crypto Policy Winlink

Final Audit Report

2026-07-15

Created:	2026-07-15
By:	Sovianca van Eps (Sovianca@gfcgroup.co)
Status:	Signed
Transaction ID:	CBJCHBCAABAAjbJ2Wn_kYRf3Ba1keDngJIHF-qyiqEW4

"2026 0714 Crypto Policy Winlink" History

-  Document created by Sovianca van Eps (Sovianca@gfcgroup.co)
2026-07-15 - 4:00:40 PM GMT
-  Document emailed to gouloud@gfcgroup.co for signature
2026-07-15 - 4:00:44 PM GMT
-  Document emailed to kristian.s@mserverone.com for signature
2026-07-15 - 4:00:45 PM GMT
-  Email viewed by kristian.s@mserverone.com
2026-07-15 - 4:01:04 PM GMT
-  Email viewed by gouloud@gfcgroup.co
2026-07-15 - 4:02:17 PM GMT
-  Signer gouloud@gfcgroup.co entered name at signing as Gouloud Hammoud
2026-07-15 - 4:03:03 PM GMT
-  Document e-signed by Gouloud Hammoud (gouloud@gfcgroup.co)
Signature Date: 2026-07-15 - 4:03:05 PM GMT - Time Source: server - Signature Appearance Selected: IMAGE
-  Signer kristian.s@mserverone.com entered name at signing as Kristian Spasov
2026-07-15 - 4:11:51 PM GMT
-  Document e-signed by Kristian Spasov (kristian.s@mserverone.com)
Signature Date: 2026-07-15 - 4:11:53 PM GMT - Time Source: server - Signature captured from device with phone number XXXXXXXX0845
- Signature Appearance Selected: MOBILE_DRAW
-  Agreement completed.
2026-07-15 - 4:11:53 PM GMT