

GLOBIS N.V.

Crypto Usage Policy

- CONFIDENTIAL -

Version Control:

<u>Document Version</u>	<u>Approving Official</u>	<u>Document Purpose</u>	<u>Release Date</u>	<u>Signature for Approval</u>
1.0	Kurason Trust Curaçao N.V., which in turn is represented by its Managing Director Jonathan Marshall Ruwel Heymans – Director	Initial Release	___20.06.2026__	DocuSigned by:  BFFB033639204B9...

Table of Contents

1. INTRODUCTION4

2. SCOPE AND PURPOSE.....4

3. DEFINITIONS5

4. RISK MENAGEMENT MEASURES.....7

5. GOVERNANCE.....15

6. STAFF TRAINING AND AWARENESS16

7. REPORTING AND ESCALATION14

8. REGULATION COMPLIANCE AND SANCTIONS SCREENING.....18

9. RECORD KEEPING.....19

1. INTRODUCTION

This Cryptocurrency Usage Policy (the “Policy”) establishes the internal governance, risk management and control framework adopted by Globis N.V. (the “Company”) for the responsible and transparent use of virtual assets. The purpose of this Policy is to ensure that all cryptocurrency-related activities are carried out in a secure, controlled and compliant manner, in line with applicable Anti-Money Laundering and Countering the Financing of Terrorism (“AML/CFT”) obligations.

The Website is operated by Globis N.V., a company incorporated under the laws of Curaçao, with registration number 155962 and registered office at Schottegatweg Oost 10 Unit 1-9, Bon Bini Business Center. The Company is committed to maintaining a safe, transparent and legally compliant environment for the processing and use of cryptocurrency transactions.

This Policy forms a crypto-specific supplement to the Company’s Anti-Money Laundering and Countering the Financing of Terrorism Policy (the “AML/CFT Policy”) and shall be read and interpreted together with it.

All AML/CFT requirements relevant to cryptocurrency operations, including customer identification and verification, KYC, CDD and EDD measures, sanctions screening, transaction monitoring, verification of source of funds and source of wealth, reporting of unusual transactions, and assessment of jurisdictional risks, are governed by the AML/CFT Policy and apply in full to all cryptocurrency-related transactions.

2. SCOPE AND PURPOSE

This Policy applies to all Company activities, procedures and internal processes that involve, or may involve, the use, receipt, processing, monitoring or oversight of cryptocurrency transactions. It covers the operational, compliance and risk management aspects of virtual asset governance and is intended to ensure that appropriate internal controls are applied consistently across all relevant activities.

The Policy applies to all employees, contractors, partners, service providers and other third parties acting on behalf of the Company who are involved in, or have responsibility for, the supervision, review, monitoring, compliance assessment or risk management of cryptocurrency-related transactions.

All activities falling within the scope of this Policy must be conducted in accordance with applicable Anti-Money Laundering and Countering the Financing of Terrorism (“AML/CFT”) standards, as well as the Company’s internal requirements relating to data protection, fraud prevention, transaction monitoring and regulatory compliance.

3. DEFINITIONS

For the purposes of this Policy, the terms set out below shall have the meanings assigned to them, unless the context requires otherwise:

“Business Risk Assessment” or **“BRA”** means a structured internal process used by the Company to identify, assess, understand and manage the risks to which it may be exposed in relation to money laundering, terrorist financing and the financing of proliferation of weapons of mass destruction.

“CDD” means customer due diligence procedures carried out to identify and verify customers, assess their risk profile and ensure that the Company complies with its AML/CFT obligations on an ongoing basis.

“Compliance Officer” means a senior management official with independent authority who is responsible for overseeing the Company’s AML/CFT framework, ensuring compliance with applicable regulatory requirements and reviewing, escalating or reporting identified risks, unusual activities or suspicious circumstances.

“Customer” means any natural person who uses, accesses or interacts with the Company’s services, including participation in real-money gaming, deposits, withdrawals or any other transaction conducted through the Website.

“Customer Risk Assessment” or **“CRA”** means the Company’s internal methodology for assigning risk ratings to customers based on predefined risk factors, including customer identification and verification results, jurisdictional exposure, transaction activity and behavioural patterns, in order to determine the appropriate level of due diligence to be applied.

“EDD” means enhanced due diligence, being additional verification, review and monitoring measures applied to customers, transactions, business relationships or circumstances identified as presenting a higher level of risk. EDD may include, where appropriate, senior management approval, verification of source of funds and/or source of wealth, and increased monitoring of customer activity.

“Internal Suspicion Report” or **“ISR”** means a confidential internal report prepared by an employee and submitted to the Compliance Officer where any activity, transaction or behaviour gives rise to a suspicion of money laundering, terrorist financing or any other financial crime. The ISR is used by the Compliance Officer to determine whether an Unusual Transaction Report should be filed with the Financial Intelligence Unit. The ISR template and escalation process are set out in Annex D of the Company’s AML/CFT Policy.

“KYC” means the process of identifying and verifying the identity of a customer before, during or in connection with the establishment of a business relationship, in accordance with applicable AML/CFT requirements.

“Politically Exposed Person” or **“PEP”** means a person who is, or has been, entrusted with a prominent public function, whether in a foreign country, domestically or by an international organisation, as well as the direct family members and close associates of such person. This may include, without limitation, heads of state or government, senior politicians, senior government officials, judicial or military officials, senior executives of state-owned enterprises, senior political party officials, and members of senior management of international organisations, including directors, deputy directors, board members or persons holding equivalent functions.

“Source of Funds” or “SoF” means the origin of the specific funds used in a particular transaction. The purpose of SoF verification is to confirm that the relevant funds derive from legitimate and identifiable sources. Supporting evidence may include, where appropriate, financial statements, bank or wallet transaction records, payslips, sale agreements, tax documents or other relevant documentation.

“Source of Wealth” or “SoW” means the origin of a person’s overall accumulated wealth, including, for example, income from employment, business activities, investments, inheritance, sale of assets or ownership interests.

“Virtual Asset” or “VA” means a digital representation of value that can be digitally transferred, stored or exchanged and used for payment, investment or other legitimate purposes, as defined under the FATF Recommendations.

“Unusual Transaction” means any transaction, activity or pattern of behaviour that is inconsistent with the customer’s expected profile, known source of funds or wealth, usual transaction activity or normal behavioural patterns, or which otherwise gives rise to concern from an AML/CFT, fraud prevention or compliance perspective.

3. RISK MANAGEMENT MEASURES

3.1 Verification Process

The Company applies a comprehensive Know Your Customer (“KYC”) and Customer Due Diligence (“CDD”) framework to all customers whose activity involves, or may involve, cryptocurrency transactions. The verification process is designed to establish the customer’s identity, assess the legitimacy of the customer’s activity, and determine the appropriate risk classification in accordance with applicable Curaçao AML/CFT requirements and the Company’s internal policies.

Enhanced Due Diligence (“EDD”) is applied where a customer, transaction or activity presents an increased level of risk, including where there is exposure to higher-risk jurisdictions, activity inconsistent with the customer’s known profile, or other indicators requiring additional scrutiny. Depending on the outcome of the risk assessment, the Company may request further information or supporting documentation, apply additional verification measures, and obtain senior management approval where required.

The verification framework is reviewed periodically to ensure that it remains aligned with the FATF Recommendations, applicable Curaçao AML/CFT standards, evolving regulatory requirements and relevant industry practices.

3.2 Transaction Monitoring

The Company maintains targeted monitoring controls for cryptocurrency transactions in accordance with the indicators, procedures and escalation mechanisms set out in its Anti-Money Laundering and Countering the Financing of Terrorism Policy (“**AML/CFT Policy**”).

Cryptocurrency activity is classified as a high-risk delivery channel under the Company’s Business Risk Assessment (“**BRA**”) and Annex B of the AML/CFT Policy, being the Trigger-Based Risk Scoring Table. As a result, enhanced transaction monitoring is applied to all cryptocurrency-related activity.

In accordance with the AML/CFT Policy, the Company monitors and, where appropriate, investigates cryptocurrency-related activity involving the following risk typologies:

- use of unregulated, anonymous or insufficiently transparent payment service providers, including providers facilitating cryptocurrency or voucher-based payments;
- receipt of cryptocurrency followed shortly by a withdrawal, conversion or transfer request, which may indicate layering or rapid movement of funds;
- use of privacy-focused cryptocurrencies or other instruments intended to obscure transaction details;
- interaction with unlicensed, unverified or high-risk cryptocurrency exchanges, mixers, tumblers or other anonymising services;
- transactions involving Virtual Assets transferred through, or associated with, entities, wallets or Virtual Asset Service Providers (“**VASPs**”) connected to high-risk jurisdictions, as identified under the Company’s jurisdictional risk assessment and relevant FATF listings.

The use of mixers, tumblers or other anonymising services is treated as a high-risk indicator and may trigger Enhanced Due Diligence and/or the filing of an Unusual Transaction Report (“**UTR**”), in accordance with Annex B of the AML/CFT Policy.

Where cryptocurrency-related activity gives rise to potential money laundering, terrorist financing, fraud or other financial crime concerns, the matter is escalated to the Compliance Officer for further review. Where required, the Company reports the relevant activity to the Financial Intelligence Unit Curaçao in accordance with Section 6.8 of the AML/CFT Policy.

All cryptocurrency-related alerts, investigations, decisions and outcomes are documented and retained in the Company’s transaction monitoring records as part of its ongoing compliance framework.

3.3 Anti-Money Laundering Compliance

The Company’s Anti-Money Laundering and Countering the Financing of Terrorism (“**AML/CFT**”) framework applies in full to all cryptocurrency-related activities. Virtual asset operations are therefore integrated into the Company’s wider AML/CFT Program, and all relevant principles, procedures and controls under the AML/CFT Policy apply equally to cryptocurrency transactions.

The Compliance Officer is responsible for ensuring that cryptocurrency-related risks are properly identified, assessed, monitored and mitigated in accordance with the Company’s Business Risk Assessment (“**BRA**”) and

Customer Risk Assessment (“CRA”). Where cryptocurrency activity is assessed as presenting a higher level of risk, the Company applies Enhanced Due Diligence (“EDD”), obtains management approval where required, and maintains ongoing monitoring of the relevant customer, transaction or activity.

As part of AML/CFT oversight, the Compliance Officer is responsible for:

- reviewing alerts generated by cryptocurrency transaction monitoring systems and blockchain analysis tools;
- ensuring that internal escalation and reporting procedures are followed in accordance with the National Ordinance on the Reporting of Unusual Transactions (“NORUT”);
- confirming that personnel involved in cryptocurrency-related processes receive appropriate AML/CFT training;
- maintaining records of reviews, investigations, internal escalations and reports submitted to the Financial Intelligence Unit Curaçao.

The Company’s AML/CFT controls relating to cryptocurrency transactions are reviewed at least annually as part of the independent audit process. Any findings, deficiencies or recommendations identified during such review are reported to senior management to support continuous improvement and ensure alignment with applicable Curaçao regulatory requirements, FATF standards and internal compliance expectations.

3.4 Data Security and Privacy

The Company protects information relating to cryptocurrency activities through appropriate technical and organisational safeguards. Customer information, verification records, transaction monitoring data and blockchain analysis records are stored securely and may be accessed only by authorised personnel for legitimate compliance, risk management and regulatory purposes.

The Company’s information security controls include encryption, access restrictions, user permission controls and periodic system reviews designed to preserve the confidentiality, integrity and availability of relevant data and to protect it against unauthorised access, alteration, disclosure or misuse.

Personal data collected or processed in connection with AML/CFT procedures is handled in accordance with applicable Curaçao data protection requirements and, where applicable, the General Data Protection Regulation (“GDPR”).

All records relating to cryptocurrency compliance are retained for a minimum period of five years in secure, access-controlled systems. Upon expiry of the applicable retention period, such records are deleted, anonymised or otherwise handled in accordance with applicable legal and regulatory requirements.

3.5 Anti-Fraud Measures

The Company applies targeted anti-fraud controls to address risks associated with the use of cryptocurrency, as set out in the AML/CFT Policy. Cryptocurrency-related fraud risk is treated as a high-risk exposure category and is subject to enhanced detection, review and escalation procedures.

Fraud indicators may include, without limitation, the use of unregulated, anonymous or insufficiently transparent payment providers, including cryptocurrency-based payment systems. The Company also monitors for potential misuse of virtual assets in connection with identity fraud, multiple account creation, account takeovers, circumvention of due diligence thresholds or other deceptive activity.

Fraud-related alerts are reviewed by the first line of defence and, where appropriate, escalated to the Compliance Officer for further assessment. Accounts or transactions suspected of fraudulent, deceptive or abusive activity may be suspended or restricted while an internal investigation is conducted.

Where fraudulent conduct is confirmed, the Company takes appropriate remedial and regulatory action, which may include filing a report with the Financial Intelligence Unit Curaçao or notifying other competent authorities where required.

The effectiveness of these controls is assessed on an ongoing basis as part of the Company's AML/CFT Program to ensure that they remain responsive to emerging typologies, evolving fraud risks and cryptocurrency-related threats.

3.6 Jurisdictional Restrictions

The Company applies a risk-based approach to jurisdictional exposure in relation to cryptocurrency transactions. In accordance with the Business Risk Assessment and the AML/CFT Policy, cryptocurrency activity connected to prohibited or high-risk jurisdictions may be restricted, rejected, blocked or subject to additional due diligence measures.

The Company does not permit cryptocurrency-related activity where counterparties, wallets, exchanges, Virtual Asset Service Providers or other relevant parties are located in, incorporated in, operating from or otherwise linked to:

- jurisdictions subject to sanctions imposed by the United Nations, the European Union or the Kingdom of the Netherlands;
- jurisdictions identified by the Financial Action Task Force ("FATF") as "High-Risk Jurisdictions Subject to a Call for Action" or "Jurisdictions Under Increased Monitoring";
- countries classified as prohibited or high-risk under Annex C of the AML/CFT Policy, including jurisdictions with systemic AML/CFT deficiencies, elevated corruption risk or other material financial crime concerns;
- any jurisdiction where local laws prohibit, restrict or materially limit the use, transfer or processing of virtual assets.

The Company reserves the right to refuse, suspend, block or terminate any cryptocurrency-related activity that exposes the Company to unacceptable jurisdictional, regulatory, sanctions, AML/CFT or reputational risk.

The jurisdictional risk classification is reviewed periodically and updated in line with applicable FATF publications, Curaçao regulatory expectations, Curaçao Gaming Authority guidance and Annex C of the AML/CFT Policy, which classifies jurisdictions as prohibited, high-risk, medium-risk or standard-risk.

3.7 Technology and System Integrity

The Company recognises that the use of cryptocurrencies and virtual assets involves specific technological, operational and information security risks. Accordingly, the Company maintains appropriate technical safeguards and system controls to support the integrity, security and resilience of the infrastructure used for cryptocurrency monitoring, compliance review and related operational processes.

The Company conducts regular internal reviews, technology risk assessments and, where appropriate, penetration testing to assess the effectiveness of relevant systems and to protect data and operational environments against unauthorised access, alteration, disruption or misuse.

The Company works with reputable technology, compliance and cybersecurity service providers whose systems and controls support the detection, prevention and monitoring of risks such as phishing, identity fraud, unauthorised access, system abuse and other technology-enabled financial crime threats.

The Company periodically evaluates the performance, security and reliability of its technology framework to ensure that it remains effective, proportionate to the risks associated with cryptocurrency operations and aligned with the Company's AML/CFT compliance obligations.

3.8 Permitted and Prohibited Crypto Assets

The Company applies the general principle that only virtual assets allowing sufficient transparency, traceability and effective application of AML/CFT controls may be accepted or processed. The Company does not process cryptocurrency transactions involving virtual assets, technologies or transaction methods that materially limit the Company's ability to identify, monitor or assess the origin, destination or risk profile of funds.

The Company may restrict or prohibit the use of virtual assets that are commonly associated with anonymity enhancement, privacy-preserving mechanisms, lack of verifiable transaction provenance, or other features that may impair compliance with applicable AML/CFT requirements. This includes assets or transaction methods that are widely recognised as presenting elevated financial crime risks or that prevent the Company from conducting adequate due diligence and transaction monitoring.

Where the Company identifies that a cryptocurrency transaction involves, or appears to involve, anonymising technologies, privacy-enhancing mechanisms, mixers, tumblers, obfuscation tools or other services designed to conceal transaction origin or ownership, the transaction may be declined, suspended, subject to Enhanced Due Diligence or escalated in accordance with the AML/CFT Policy.

Any attempted use of virtual assets or related services that prevent adequate transparency, traceability or compliance review may result in additional due diligence measures, transaction restrictions and/or the filing of an Unusual Transaction Report where appropriate.

The Company periodically reviews the categories of virtual assets considered acceptable to ensure continued alignment with regulatory expectations, international standards, emerging risk typologies and the Company's internal risk appetite.

3.9 Wallet Ownership and Withdrawal Rules

The Company applies withdrawal practices designed to preserve the integrity, transparency and traceability of cryptocurrency movements connected with customer activity. As a general principle, cryptocurrency withdrawals are processed to the wallet from which the relevant deposit originated or to another wallet that can be reasonably verified as belonging to, or being controlled by, the same customer.

This approach supports the Company's ability to confirm the legitimacy of the source and destination of funds and to ensure consistency with its AML/CFT, fraud prevention and transaction monitoring obligations.

The Company may require customers to demonstrate ownership or control over any wallet used in connection with deposits or withdrawals. The verification method applied may vary depending on the customer's risk profile, transaction history, blockchain indicators and other relevant circumstances. Such verification may include blockchain-based or non-blockchain-based methods that provide the Company with reasonable assurance regarding wallet ownership or control.

Where a wallet cannot be reliably attributed to the customer, shows indicators of third-party control, or presents other risk concerns, the Company may restrict or delay withdrawals, request additional information or supporting documentation, or escalate the matter for further review under the AML/CFT Policy.

3.10 Wallet Segregation and Custody Standards

The Company maintains an appropriate level of separation between different categories of wallets used in connection with its virtual asset operations. The specific manner in which wallets are structured, allocated or managed may vary depending on business requirements, technical considerations, operational arrangements and the use of external service providers.

The purpose of wallet segregation is to support operational efficiency, safeguard the integrity of virtual asset flows and ensure that cryptocurrency transactions can be monitored and reviewed in accordance with applicable compliance requirements.

The Company ensures that only wallets under its control, or wallets managed through service providers that meet the Company's compliance and security expectations, are used for business-related virtual asset operations. Wallets owned or controlled by private individuals, including employees, beneficial owners or any other natural persons, must not be used for Company operations involving virtual assets.

The Company periodically reviews its wallet management arrangements to confirm that they remain appropriate in light of regulatory expectations, operational risks, technical developments and industry practices. The Company may adjust its wallet structure as necessary to maintain effective oversight, transparency and compliance with AML/CFT obligations, without requiring any specific fixed operational configuration.

3.11 External Crypto Processing Framework and Travel Rule Compliance

The Company may rely on external service providers to facilitate the processing, settlement, transfer or custody-related handling of cryptocurrency transactions. Such providers operate within their own regulatory, technical and compliance frameworks and apply their own systems, controls and procedures to support the secure handling of virtual assets.

The Company's engagement with external providers is focused on ensuring that the services used by the Company support its own AML/CFT, record-keeping, transaction monitoring and regulatory compliance obligations. The Company does not assume or duplicate the internal compliance responsibilities of such providers, except to the extent required to satisfy its own obligations under applicable law and internal policies.

Where elements of the Travel Rule or equivalent virtual asset transfer information requirements apply to the Company's operations, the relevant information is handled through the processes, tools or mechanisms made available by the applicable external service provider. The Company retains such information only to the extent necessary to meet its own legal, regulatory and record-keeping requirements, as set out in this Policy and the AML/CFT Policy.

The Company periodically reviews its reliance on external cryptocurrency service providers to confirm that the overall arrangement remains compatible with applicable regulatory expectations, the Company's operational needs and its internal compliance framework. Such review does not require the Company to conduct an independent audit or full assessment of the provider's internal AML/CFT systems, unless otherwise required by law, regulation or the Company's risk assessment.

3.12 Blockchain Analytics and On-Chain Risk Screening

The Company conducts blockchain analytics and on-chain risk screening as part of its cryptocurrency compliance framework. These measures are designed to identify potential exposure to illicit or high-risk typologies, including transactions connected to mixers, tumblers, anonymising services, darknet-linked entities, sanctioned wallets, high-risk exchanges, or other virtual asset sources associated with elevated financial crime risk.

On-chain analysis may include the review of transaction flows, wallet exposure, counterparty risk, transaction velocity, rapid value movement, proximity to known high-risk clusters and other indicators that may suggest layering, structuring, sanctions exposure, fraud or other suspicious activity.

The purpose of blockchain analytics is to assess whether cryptocurrency movements are consistent with the customer's known profile, expected activity, source of funds, transaction history and risk classification, as determined under the Company's AML/CFT Policy.

Risks identified through blockchain analytics are escalated for review in accordance with the investigation, escalation and reporting procedures set out in Section 6.8 of the AML/CFT Policy. Where appropriate, the

findings may result in Enhanced Due Diligence, transaction restrictions, account action or the submission of an Unusual Transaction Report to the Financial Intelligence Unit Curaçao.

3.13 Crypto-Specific Incident Response

The Company maintains procedures for identifying, assessing, escalating and responding to incidents specific to cryptocurrency operations. These procedures apply to events that may affect the integrity of customer funds, the continuity of cryptocurrency-related operations, the reliability of external service providers or the Company's ability to comply with applicable AML/CFT requirements.

Crypto-specific incidents may include, without limitation, blockchain network instability, delayed or failed confirmations, interruptions or failures at Virtual Asset Service Providers, unusual wallet activity, coordinated or abnormal deposit behaviour, suspected exploitation of transaction processes, or other events indicating potential fraud, money laundering, terrorist financing or operational risk.

Upon detection of a cryptocurrency-related incident, the responsible operational team escalates the matter to the Compliance Officer for further assessment where compliance, fraud, AML/CFT or financial crime risks may be involved. The Compliance Officer evaluates the nature and severity of the incident, determines whether containment or additional due diligence measures are required, and assesses whether the matter should be reported to the Financial Intelligence Unit Curaçao or another competent authority.

All actions, decisions and outcomes relating to cryptocurrency-specific incidents are documented and retained in accordance with the escalation, investigation and reporting procedures established under the AML/CFT Policy.

The Company reviews its crypto-specific incident response procedures periodically to ensure that they remain effective, proportionate and responsive to emerging virtual asset risks, technological developments and updated regulatory expectations.

4. GOVERNANCE

4.1 Independent Audit

Cryptocurrency compliance governance forms part of the Company's broader AML/CFT governance framework. Oversight responsibilities are allocated in accordance with the Company's Three Lines of Defence model to ensure clear accountability, appropriate operational independence and consistent application of internal controls.

The Compliance Officer is responsible for maintaining this Policy, coordinating relevant risk assessments and monitoring the effectiveness of cryptocurrency-related controls. Senior Management is responsible for regularly reviewing the implementation of AML/CFT measures and ensuring that adequate resources, systems and personnel are available to support effective supervision and compliance.

The Company's cryptocurrency compliance framework is subject to independent audit at least annually. The audit assesses the adequacy and effectiveness of cryptocurrency-related risk management, transaction monitoring, escalation procedures, reporting mechanisms and the integration of these controls into the Company's wider AML/CFT Program.

Audit findings are documented and submitted to the Board of Directors. Any identified gaps, weaknesses or deficiencies are addressed through corrective action plans and follow-up reviews. The Compliance Officer monitors the implementation of remediation measures and ensures that corrective actions are completed within appropriate timeframes.

The results of independent audits, together with related remediation records, are retained and made available for inspection by the Curaçao Gaming Authority or any other competent authority where required.

4.2 Review and Updating of the Policy

This Policy is reviewed by the Compliance Officer at least annually to ensure that it remains effective, proportionate and aligned with the Company's cryptocurrency-related risk exposure and AML/CFT obligations.

The review takes into account, where relevant:

- changes in applicable laws, regulations or guidance issued by the Curaçao Gaming Authority, the Financial Intelligence Unit Curaçao, the Financial Action Task Force or any other competent authority;
- developments in blockchain technology, virtual asset regulation, transaction monitoring practices and emerging financial crime typologies;
- changes in the Company's business model, operational arrangements, use of external service providers or cryptocurrency-related processes;
- findings from internal reviews, independent audits, compliance testing, incident reviews or regulatory inspections.

Any updates to this Policy are approved by Senior Management and communicated to relevant employees, contractors and service providers where applicable. Personnel involved in cryptocurrency-related processes are required to acknowledge and comply with any new or revised requirements introduced as a result of the review.

5. STAFF TRAINING AND AWARENESS

5.1 Mandatory Training

The Company ensures that employees, contractors and relevant third-party service providers involved in cryptocurrency-related activities receive appropriate training on AML/CFT compliance, data protection, fraud prevention, sanctions awareness and cryptocurrency-specific risk indicators.

Training is mandatory for all new employees whose duties involve cryptocurrency operations, compliance, risk management, customer due diligence, transaction monitoring, payments, customer support or related control

functions. Training is repeated periodically to reflect changes in applicable regulatory requirements, emerging virtual asset risks and updates to the Company's internal procedures.

The training program covers, where relevant:

- identification of cryptocurrency-specific money laundering, terrorist financing and fraud indicators;
- recognition of suspicious or unusual transaction patterns involving virtual assets;
- internal escalation and reporting procedures under the AML/CFT framework;
- data security, confidentiality and record-keeping obligations;
- sanctions screening, jurisdictional risk awareness and high-risk counterparty exposure;
- the use of blockchain analytics, transaction monitoring tools and other relevant compliance systems, where applicable.

Training is tailored to the employee's role, department and level of responsibility. Personnel in compliance, risk, payments, security and monitoring functions may receive more advanced training covering blockchain analysis, crypto-related typologies, Travel Rule considerations, external provider risks and evolving regulatory expectations.

The Compliance Officer is responsible for maintaining records of training sessions, attendance, training materials and completion status. The effectiveness of training is reviewed periodically through assessments, internal reviews, compliance testing or audit findings to ensure that relevant personnel remain capable of identifying, escalating and mitigating risks associated with cryptocurrency operations.

5.2 Ongoing Awareness and Assessment

The Company maintains ongoing awareness measures to ensure that employees understand their responsibilities in relation to cryptocurrency-related AML/CFT controls, fraud prevention, data protection and internal reporting obligations.

Employees are required to promptly escalate any concerns, red flags, unusual activity or suspected financial crime indicators to the Compliance Officer through the Company's internal reporting channels.

Refresher training and awareness sessions are conducted at least annually, and additionally where significant regulatory, procedural, technological or risk-related changes occur. Such sessions are intended to reinforce understanding of cryptocurrency-related red flags, emerging typologies, monitoring expectations and reporting standards.

Employee awareness and understanding are assessed through knowledge checks, case studies, compliance reviews, internal testing or other appropriate evaluation methods conducted by the Compliance Department. Where gaps are identified, the Company implements additional training, guidance or corrective measures to support consistent application of compliance standards across all relevant functions.

6. REPORTING AND ESCALATION

Employees within the first line of defence are required to promptly report any suspicions, red flags or findings relating to cryptocurrency transactions that may indicate money laundering, terrorist financing, fraud, sanctions exposure or any other financial crime risk. Such reports must be submitted internally to the Compliance Officer through the Company's established reporting channels.

The Compliance Officer reviews all internal reports and assesses whether the relevant activity, transaction or behaviour meets the criteria for the filing of an Unusual Transaction Report ("UTR") with the Financial Intelligence Unit Curaçao. The assessment, decision-making process and any subsequent actions are documented in accordance with the procedures set out in the AML/CFT Policy.

All internal reports, supporting documentation, investigation records, decisions and outcomes are stored securely and handled on a strictly confidential basis. The Company ensures that reporting and escalation procedures are conducted in compliance with applicable anti-tipping-off obligations under Curaçao law.

The Company periodically reviews its internal reporting and escalation procedures to ensure that they remain effective, proportionate, consistently applied and aligned with applicable regulatory requirements, FATF Recommendations and Curaçao Gaming Authority guidance.

7. REGULATORY COMPLIANCE AND SANCTIONS SCREENING

The Company ensures that cryptocurrency-related activities are conducted in accordance with applicable Curaçao laws and regulations, FATF Recommendations, Curaçao Gaming Authority guidance and the Company's internal AML/CFT requirements.

All customers, transactions, wallets, counterparties, exchanges and Virtual Asset Service Providers connected to cryptocurrency operations are screened against applicable national and international sanctions lists. Such screening may include, where relevant, sanctions lists issued by the United Nations Security Council, the European Union, the Office of Foreign Assets Control of the United States Department of the Treasury, and sanctions measures applicable under the laws of the Kingdom of the Netherlands.

Sanctions screening is conducted during customer onboarding and on an ongoing or periodic basis throughout the business relationship, as appropriate to the customer's risk profile, transaction activity and applicable regulatory requirements.

The Company does not knowingly engage with, facilitate or process cryptocurrency transactions involving sanctioned individuals, entities, wallets, exchanges, Virtual Asset Service Providers or jurisdictions. Where a potential sanctions match or sanctions-related concern is identified, the relevant transaction may be halted, the account may be restricted or frozen, and the matter is escalated to the Compliance Officer for immediate review.

The Compliance Officer assesses the match, determines the appropriate internal and regulatory response, and, where required, reports the matter to the Financial Intelligence Unit Curaçao or any other competent authority in accordance with applicable laws and the Company's AML/CFT Policy.

The Company regularly reviews and updates its sanctions screening procedures to reflect changes in applicable sanctions regimes, regulatory expectations and emerging virtual asset risks. Audit trails of screening results, alerts, assessments, decisions and follow-up actions are securely retained as part of the Company's AML/CFT compliance records.

8. RECORD KEEPING

The Company maintains complete and accurate records of all activities relating to cryptocurrency compliance to support transparency, auditability and compliance with applicable regulatory obligations. Such records include documentation relating to customer identification and verification, due diligence measures, transaction monitoring, internal investigations, sanctions screening, blockchain analytics, risk assessments and any related findings or decisions.

Records are maintained in secure, access-controlled systems and are made available for inspection by competent authorities where required.

In addition to the Company's general AML/CFT record-keeping framework, the Company retains information specific to virtual asset activities, including blockchain analytics reports, on-chain tracing results, wallet screening outputs, transaction monitoring alerts and reconciliations between blockchain explorer data, exchange or Virtual Asset Service Provider account statements and the Company's internal ledger or operational systems.

Where applicable, information relating to Travel Rule or equivalent virtual asset transfer information requirements is retained for the applicable statutory retention period.

All cryptocurrency compliance records are retained for a minimum period of five years following the termination of the business relationship or completion of the relevant transaction, unless a longer retention period is required under Curaçao law, applicable regulatory requirements or an instruction from the Financial Intelligence Unit Curaçao or another competent authority.

The Company periodically reviews its record-keeping, data retention and information security practices to ensure continued alignment with legal requirements, regulatory expectations, internal policies and relevant international standards.