

CARLITTA N.V.

Crypto Usage Policy

- CONFIDENTIAL –

This Document is intended only for the following users:

<u>User Types</u>
General Users (All Employees)

Version Control:

<u>Document Version</u>	<u>Responsible Office:</u>	<u>Approving Official</u>	<u>Document Purpose</u>	<u>Release Date</u>	<u>Signature for Approval</u>
1.0	Campbell Gino Steven – Compliance Officer	Jorge Luis Castillo, FO Management LTD – Director	Initial Release	November 29, 2025	
			Next Review	November 29, 2026	

Table of Contents

1. INTRODUCTION4

2. SCOPE AND PURPOSE.....4

3. DEFINITIONS4

4. RISK MENAGEMENT MEASURES.....6

5. GOVERNANCE.....12

6. STAFF TRAINING AND AWARENESS13

7. REPORTING AND ESCALATION14

8. REGULATION COMPLIANCE AND SANCTIONS SCREENING.....15

1. INTRODUCTION

This Cryptocurrency Usage Policy (“the Policy”) defines the internal governance and control framework applied by Carlitta N.V. (“the Company”) to ensure that all activities involving virtual assets are conducted responsibly, transparently, and in accordance with applicable Anti-Money Laundering and Countering the Financing of Terrorism (AML/CFT) requirements. The Policy complements the Company’s AML/CFT Policy and sets out general principles for the management of virtual asset–related risks within the business.

The website <https://www.pin-up.casino/> is operated by **Carlitta N.V.**, a company registered under the laws of **Curaçao**, with registration number **162777** and an official address at **Zuikertuintjeweg Z/N (Zuikertuin Tower), Curaçao**. Carlitta N.V. is committed to providing a secure, transparent, and legally compliant environment for cryptocurrency transactions.

2. SCOPE AND PURPOSE

This Policy applies to all activities and processes within the Company that involve or may involve cryptocurrency transactions. It extends to all personnel engaged in oversight, monitoring, or compliance functions relating to virtual assets. The Policy ensures that every such activity is carried out in accordance with Anti-Money Laundering (AML) and Countering the Financing of Terrorism (CFT) standards, as well as applicable data protection and fraud prevention frameworks.

This Policy applies to all employees, contractors, partners, and third parties acting on behalf of the Company who may be involved in compliance, oversight, or risk management related to cryptocurrency transactions. It covers operational and procedural aspects of virtual asset governance, ensuring consistent application of internal controls and adherence to regulatory obligations.

3. DEFINITIONS

For this Policy purposes the below term will have the following meaning, unless the context prescribes otherwise:

“Business Risk Assessment” “(BRA)” – means a structured process aimed to identify, evaluate, and manage the risks the Company faces in the context of money laundering (ML), financing of terrorism (FT) and proliferation of weapons of mass destruction (FP).

“CDD” – procedures undertaken to identify and verify customers, assess their risk profile, and ensure ongoing compliance with AML/CFT obligations.

“Compliance Officer” – a senior management official with independent authority responsible for overseeing the Company’s AML/CFT framework, ensuring regulatory compliance, and reporting any identified risks or unusual activities.

“Customer” – means any natural person who interacts with the Company’s services, including real-money gaming, deposits, withdrawals, or other transactions.

“Customer Risk Assessment” “(CRA)” – an internal methodology used to assign risk ratings to customers based on predefined factors, including identity verification results, jurisdictional exposure, and behavioral patterns, to determine the level of due diligence to be applied.

“EDD” – additional verification and monitoring procedures applied to customers, transactions, or situations identified as high-risk. EDD may include senior management approval, verification of source of funds or wealth, and increased scrutiny of customer behavior.

“Internal Suspicion Report” “(ISR)” – a confidential internal report prepared by an employee and submitted to the Compliance Officer when activity or behavior raises suspicion of money laundering, terrorist financing, or any other financial crime. The ISR serves as the basis for determining whether an Unusual Transaction Report (UTR) must be filed with the Financial Intelligence Unit (FIU). The ISR template and escalation workflow follow Annex D of the Company’s AML/CFT Policy.

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

“Politically Exposed Persons” “(PEPs)” – foreign PEPs are individuals who are or have been entrusted with prominent public functions by a foreign country, and the direct family members or close associates of such persons. Examples are Heads of State or of government, senior politicians, senior government officials, judicial or military officials, senior executives of state-owned corporations, and important political party officials. Domestic PEPs are individuals who are or have been entrusted domestically with prominent public functions, for example, Heads of State or government, senior politicians, senior government, judicial or military officials, senior executives of state-owned corporations, and important political party officials. Persons who are or have been entrusted with a prominent function by an international organization refer to members of senior management, i.e. directors, deputy directors, and members of the board or equivalent functions.

“Source of Funds” “(SoF)” – the origin of the specific funds used in a transaction, verified to ensure that assets originate from legitimate and identifiable sources. Acceptable documentation or evidence may include financial statements, transaction records, or other supporting information.

“Source of Wealth” “(SoW)” – means source of wealth is the origin of all the money a person has accumulated over their lifetime, like employment income, inheritances, investments, and business ownership interests.

Virtual Asset (VA) – 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” – any activity or transaction that deviates from a customer’s expected behavior or normal activity patterns.

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 clients whose activity involves or may involve cryptocurrency transactions. The verification process ensures that customer identity, legitimacy of activity, and risk classification are established in accordance with Curaçao AML/CFT Regulations and the Company’s internal policies.

Enhanced Due Diligence (EDD) is required for customers and transactions that present elevated risks, such as higher exposure jurisdictions or activity inconsistent with the customer's known profile. Depending on the assessment, additional verification steps and management approvals may be required.

The verification framework is periodically reviewed to ensure continued alignment with FATF Recommendations and applicable Curaçao standards and regulations. Verification measures are periodically reviewed to ensure compliance with evolving regulatory requirements and industry best practices.

3.2 Transaction Monitoring

The Company maintains targeted monitoring measures for cryptocurrency transactions, based strictly on the indicators and control mechanisms defined in its Anti-Money Laundering / Combating Financing of Terrorism Policy.

Cryptocurrency activity is classified as a high-risk delivery channel under the Company's Business Risk Assessment (BRA) and Trigger-Based Risk Scoring Table. Accordingly, enhanced transaction monitoring applies to all such activities.

In line with the AML/CFT Policy, the Company specifically monitors and investigates the following risk typologies:

- Use of unregulated or anonymous payment service providers (PSPs), including those facilitating crypto or voucher-based payments.
- Inflows of cryptocurrency immediately followed by withdrawal or conversion requests, which may indicate layering or rapid fund movement.
- Use of privacy-centric cryptocurrencies that may indicate attempts to obscure transaction details.
- Interaction with unlicensed or unverified cryptocurrency exchanges, mixers, or tumblers designed to conceal the origin of funds.

- Transactions involving Virtual Assets (VA) transferred through, or associated with, entities, wallets, or Virtual Asset Service Providers (VASPs) registered in high-risk jurisdictions, as defined under the Company's jurisdictional risk assessment and FATF listings.

Crypto is classified as a high-risk delivery channel in accordance with Annex B (Trigger-Based Risk Scoring Table) of the AML/CFT Policy.

The use of mixers, tumblers, or anonymising services is treated as a high-risk indicator and triggers Enhanced Due Diligence and/or UTR filing, in accordance with Annex B of the AML Policy.

Where activity is deemed to present potential money laundering or other financial crime risk, it is escalated to the Compliance Officer for further investigation and, if required, reported to the Financial Intelligence Unit (FIU) Curaçao in accordance with Section 6.8 of the AML/CFT Policy.

All crypto-related alerts, investigations, and outcomes are documented and maintained in the transaction monitoring records as part of the Company's ongoing compliance framework.

3.3 Anti-Money Laundering (AML) Compliance

The Company's AML compliance framework ensures that cryptocurrency-related activities are fully integrated into its overall Anti-Money Laundering and Countering the Financing of Terrorism (AML/CFT) Program. All principles, procedures, and controls established under the AML Policy apply equally to operations involving virtual assets.

The Compliance Officer is responsible for ensuring that cryptocurrency-related risks are identified, assessed, and mitigated in line with the Company's Business Risk Assessment (BRA) and Customer Risk Assessment (CRA). Any cryptocurrency activity considered high-risk is subject to enhanced due diligence (EDD), management approval, and continuous monitoring.

As part of AML oversight, the Compliance Officer:

- reviews alerts generated from crypto transaction monitoring systems and blockchain analysis tools;

- ensures that internal escalation and reporting procedures follow the requirements of the National Ordinance on the Reporting of Unusual Transactions (NORUT);
- verifies that all staff engaged in crypto-related processes receive adequate AML/CFT training;
- maintains a documented record of all reviews, investigations, and reports submitted to the Financial Intelligence Unit (FIU) Curaçao.

The Company's AML/CFT controls related to cryptocurrency transactions are reviewed at least annually as part of the independent audit process. Identified findings and recommendations are submitted to senior management to ensure continuous improvement and alignment with Curaçao regulatory requirements and FATF standards.

3.4 Data Security and Privacy

The Company safeguards all information related to cryptocurrency activities through appropriate technical and organizational measures. Customer data, verification documents, and blockchain monitoring records are stored securely and accessed only by authorized personnel for compliance purposes.

Information security controls include encryption, restricted access, and periodic system audits to ensure data integrity and protection from unauthorized use. Personal data obtained during AML/CFT procedures is processed in accordance with Curaçao data protection laws and the General Data Protection Regulation (GDPR).

All records associated with cryptocurrency compliance are retained for a minimum of five years in secure, access-controlled systems, after which they are deleted or anonymized in line with legal and regulatory requirements.

3.5 Anti-Fraud Measures

The Company implements targeted anti-fraud controls that address risks specific to cryptocurrency usage, as outlined in the AML/CFT Policy. Cryptocurrency-related fraud is treated as a high-risk exposure category and is subject to enhanced detection and escalation procedures.

Fraud indicators include the use of unregulated or anonymous payment providers (e.g., crypto systems). The Company also monitors for potential misuse of crypto assets to facilitate identity fraud, multiple account creation, or attempts to circumvent due diligence thresholds.

Fraud-related alerts are reviewed by the 1st line of defense and, if necessary, escalated to the Compliance Officer. Accounts suspected of fraudulent or deceptive activity may be suspended while an internal investigation is conducted. Where fraudulent conduct is confirmed, the Company takes appropriate measures, including reporting to the Financial Intelligence Unit (FIU) Curaçao or other competent authorities.

These controls are continuously evaluated through the Company's AML Program to ensure they remain effective against evolving typologies and emerging crypto-related threats.

3.6 Jurisdictional Restrictions

The Company applies a risk-based approach to jurisdictional exposure in cryptocurrency operations. In accordance with the Business Risk Assessment (BRA) and AML/CFT Policy, cryptocurrency transactions associated with prohibited or high-risk jurisdictions are restricted or rejected.

Activities involving virtual assets are not permitted when counterparties, wallets, or Virtual Asset Service Providers (VASPs) are located in or linked to:

- jurisdictions subject to UN, EU, or Kingdom of the Netherlands sanctions;
- 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 listed as prohibited or high-risk in Annex C of the AML/CFT Policy, including those demonstrating systemic AML/CFT deficiencies or high levels of corruption;
- any country where local regulations prohibit or restrict virtual asset transactions.

The Company reserves the right to terminate or block any cryptocurrency-related activity that exposes it to unacceptable jurisdictional risk. The jurisdictional list is reviewed periodically and updated in line with FATF and Curaçao Gaming Authority (CGA) guidance. Jurisdiction classification is aligned with Annex C of the AML/CFT Policy (Prohibited, High, Medium, Standard risk jurisdictions).

3.7 Technology and System Integrity

The Company recognises the technological risks associated with the use of cryptocurrencies and virtual assets. It maintains secure and segregated infrastructure to ensure the integrity and resilience of systems used for cryptocurrency monitoring and compliance.

Regular internal reviews, penetration testing, and technology risk assessments are performed to validate system effectiveness and safeguard data from unauthorised access or tampering.

The Company collaborates with reputable technology and cybersecurity providers that implement industry-leading software and continuously monitor for phishing activity, identity fraud, or other misuse of technological systems for financial crime purposes.

Ongoing evaluation of system performance and cybersecurity measures ensures that the Company's technological framework remains effective, reliable, and aligned with AML/CFT compliance obligations.

4. GOVERNANCE

4.1 Independent Audit

The governance of cryptocurrency compliance forms an integral part of the Company's overall AML/CFT structure. Oversight responsibilities are assigned in accordance with the Company's Three Lines of Defense model, ensuring clear accountability, operational independence, and consistent application of internal controls.

The Compliance Officer is responsible for maintaining this Policy, coordinating risk assessments, and ensuring that crypto-related controls operate effectively. Senior Management reviews the implementation of AML/CFT measures on a regular basis and provides the resources necessary to maintain effective supervision and compliance.

An independent audit of the Company's cryptocurrency compliance framework is conducted at least annually. The audit assesses the adequacy of crypto-related risk management, monitoring procedures, and reporting mechanisms, as well as the integration of these controls within the broader AML/CFT Program.

Audit findings are documented and presented to the Board of Directors. Identified gaps or deficiencies are addressed through corrective action plans and follow-up reviews. The Compliance Officer ensures that all remediation steps are completed in a timely manner and that the results of the audit are available for inspection by the Curaçao Gaming Authority (CGA) or other competent authorities.

4.2 Review and Updating of the Policy

This Policy is reviewed at least annually by the Compliance Officer to ensure its continued relevance and effectiveness in addressing cryptocurrency-related AML/CFT risks. The review also considers:

- changes in regulatory requirements or guidance issued by the Curaçao Gaming Authority (CGA) and the Financial Action Task Force (FATF);
- developments in blockchain technology, virtual asset regulation, and risk typologies;
- operational changes or findings from internal audits and independent reviews.

Policy updates are approved by Senior Management and communicated to all relevant employees and service providers. All staff must acknowledge and comply with new or revised requirements introduced as a result of the review.

5. STAFF TRAINING AND AWARENESS

5.1 Mandatory Training

The Company ensures that all employees and third-party providers involved in cryptocurrency-related activities receive regular training on AML/CFT compliance, data protection, and risk awareness. Training is mandatory for all new employees and is repeated periodically to reflect regulatory developments, emerging risks, and changes in internal procedures.

The training program covers:

- identification of crypto-specific money laundering and fraud indicators;
- recognition of suspicious or unusual transaction patterns associated with virtual assets;
- escalation and internal reporting procedures under the AML/CFT framework;
- data security and confidentiality obligations;
- sanctions screening and jurisdictional risk awareness.

Training is tailored to each department's function and level of responsibility. Compliance, risk, and security teams receive advanced modules focusing on blockchain analysis, crypto typologies, and emerging regulatory expectations.

The training framework includes structured induction modules for new employees and annual refresher sessions for existing staff. Targeted ad hoc training is also provided to compliance and technology teams when new monitoring tools or regulatory requirements are introduced.

The Compliance Officer maintains detailed records of training sessions, attendance, and content delivered. Training effectiveness is periodically reviewed through assessments and internal audits to ensure that all staff remain capable of identifying and mitigating AML/CFT risks associated with cryptocurrency operations.

5.2 Ongoing Awareness and Assessment

The Company ensures that employees remain continuously aware of their responsibilities regarding cryptocurrency-related AML/CFT controls and reporting obligations. Staff are encouraged to escalate any concerns or suspicions promptly to the Compliance Officer through the internal reporting channels.

Refresher sessions are conducted at least annually or whenever significant regulatory or procedural changes occur. These sessions reinforce understanding of red flags, risk typologies, and reporting standards relevant to cryptocurrency operations.

The effectiveness of employee awareness is assessed through knowledge checks, case studies, and periodic reviews performed by the Compliance Department. Where gaps are identified, additional training and corrective actions are implemented to ensure consistent application of compliance standards across all levels of the Company.

6. REPORTING AND ESCALATION

The employees from the 1st line of defense are required to report any suspicions or findings related to cryptocurrency transactions that may indicate potential money laundering, terrorist financing, or other financial crimes. Reports are submitted internally through the established reporting channels to the Compliance Officer.

The Compliance Officer reviews all internal reports and determines whether the activity meets the criteria for submission of an Unusual Transaction Report (UTR) to the Financial Intelligence Unit (FIU) Curaçao. The decision and subsequent actions are documented in accordance with the procedures defined in the AML/CFT Policy.

Reports, supporting documentation, and investigation outcomes are stored securely and handled with strict confidentiality. The Company ensures that all reporting procedures are compliant with anti-tipping-off obligations under Curaçao law.

Periodic reviews of reporting and escalation procedures are conducted to ensure that they remain effective, proportionate, and consistent with FATF recommendations and CGA guidance.

7. REGULATORY COMPLIANCE AND SANCTIONS SCREENING

The Company ensures that all cryptocurrency-related activities comply with applicable Curaçao laws, FATF Recommendations, and the guidance issued by the Curaçao Gaming Authority (CGA).

All customers, transactions, and counterparties connected to cryptocurrency operations are screened against relevant international and national sanctions lists, including those issued by the United Nations Security Council (UNSC), the European Union (EU), the U.S. Office of Foreign Assets Control (OFAC), and the Kingdom Sanctions Act. Screening is conducted at onboarding and periodically throughout the business relationship.

The Company does not engage with or process cryptocurrency transactions involving wallets, exchanges, or Virtual Asset Service Providers (VASPs) linked to sanctioned individuals, entities, or jurisdictions. In cases where a sanctions match is identified, the transaction is halted, the related account is frozen, and the Compliance Officer immediately reports the finding to the Financial Intelligence Unit (FIU) Curaçao in accordance with applicable regulations.

The sanctions screening process is regularly reviewed and updated to reflect changes in international sanction regimes and regulatory expectations. Audit trails of all screening results and follow-up actions are securely maintained as part of the Company's AML/CFT compliance documentation.

8. RECORD KEEPING

The Company maintains comprehensive and accurate records of all cryptocurrency-related compliance activities to ensure full transparency and accountability.

All documents and data relating to customer identification, due diligence, transaction monitoring, investigations, and reporting are securely retained for a minimum of five (5) years after the termination of the business relationship or completion of the transaction.

This includes, but is not limited to:

- KYC and CDD documentation;
- records of blockchain screening results and risk assessments;
- internal suspicion reports and related investigations;
- copies of Unusual Transaction Reports (UTRs) and related correspondence with the FIU;

- audit reports and compliance reviews.

Records are stored in encrypted systems with restricted access, ensuring data confidentiality and integrity. The Compliance Officer oversees adherence to record-keeping obligations and ensures that all records remain accessible for inspection by competent authorities upon request.

The Company periodically reviews data retention and security protocols to ensure compliance with evolving legal requirements and international best practices.