

Cryptocurrency Risk Management Policy

Orakum N.V. (141651)

Approved by the Board of Directors



April, 2025

Abraham Mendez Chumaceiro Boulevard 03,
Willemstad, 4750, Curacao

Glossary

AML (Anti-Money Laundering):

A set of rules and practices designed to prevent illicit income generation, particularly by obscuring the origins of cryptocurrencies within gambling platforms.

AMLD5/AMLD6 (Fifth and Sixth Anti-Money Laundering Directives):

EU regulatory frameworks that outline obligations and standards for AML and CFT, including those specific to cryptocurrency activities.

CFT (Combatting the Financing of Terrorism):

A series of procedures aimed at stopping the misuse of financial systems—such as crypto assets—for funding terrorist operations.

Cold Wallet:

An offline cryptocurrency wallet used for securely storing the majority of the company's digital asset reserves.

Compliance Officer:

The appointed individual responsible for enforcing AML/CFT protocols and for filing reports of suspicious activity with the proper authorities.

Cryptocurrency:

A digital currency utilizing encryption for security, functioning independently from centralized banking systems.

Customer Due Diligence (CDD):

A verification process to confirm client identity and evaluate potential risk, particularly relevant for users handling crypto transactions.

Enhanced Due Diligence (EDD):

Stricter verification procedures applied to clients or transactions considered high-risk, often involving deeper scrutiny of identity and source of funds.

FIU Curaçao (Financial Intelligence Unit):

The Curaçao government body in charge of collecting and assessing reports of suspicious financial activity.

Hot Wallet:

A cryptocurrency wallet connected to the internet, used for routine transactions and safeguarded with advanced security features.

KYC (Know Your Customer):

An essential AML requirement obligating firms to confirm the identity, background, and financial origins of their customers.

NORUT (National Ordinance on Reporting Unusual Transactions):

A local Curaçao law requiring companies to report suspicious or abnormal financial transactions to the FIU.

NOIS (National Ordinance on Identification of Clients for Services):

Curaçao legislation mandating identity verification of customers before service provision.

PEP (Politically Exposed Person):

An individual holding a significant public role, often posing elevated risks for involvement in bribery or corruption.

Risk Management Committee:

A designated group within the company responsible for overseeing risk evaluations, regulatory adherence, and strategic response to crypto-related threats.

SAR (Suspicious Activity Report):

An official report filed with the FIU upon detecting transactions deemed potentially illicit or abnormal.

Stablecoin:

A cryptocurrency pegged to a stable asset (e.g., USD) designed to minimize price volatility in digital financial transactions.

Transaction Monitoring System:

A blockchain-based analytical tool that identifies suspicious or irregular crypto transaction patterns for further compliance review.

1. Statement

Orakum N.V. is a company legally incorporated in Curaçao under registration number 141651, and it operates from Abraham Mendez Chumaceiro Boulevard 03, Willemstad, 4750, Curaçao. The company conducts its business under license OGL/2024/586/0786, issued by the Curaçao Gaming Authority on 28 March 2025, in accordance with the National Ordinance on Games of Chance (P.B. 2024, no. 157). This license subjects the company to regulatory requirements, including restrictions that prohibit it from offering gaming services in certain jurisdictions such as the United States, Australia, Dutch West Indies (Aruba, Bonaire), Curaçao, France, Germany, the United Kingdom, Belize, and the Netherlands. Orakum N.V. strictly limits its operations to legally permitted markets and does not solicit or serve users located in restricted regions.

The company is obligated to adhere to legislation concerning the Prevention of Money Laundering and Terrorist Financing, and is supervised by the Curaçao Gaming Control Board (GCB), which oversees compliance with AML and CFT requirements within the gaming sector.

This document outlines Orakum N.V.'s internal policy framework for assessing, controlling, and reducing the risks related to the use of cryptocurrency in its operations. The policy aligns with the legal and regulatory standards mandated by the Curaçao Gaming Authority, as well as internationally recognized AML/CFT guidelines and standards applicable to virtual assets and financial technology.

This policy is applicable to all personnel, including employees, affiliates, contractors, subsidiaries, and external service providers, who are involved in the management, processing, or storage of cryptocurrency as part of Orakum N.V.'s business activities.

2. Applicable Legal and Regulatory Standards

Orakum N.V. is obligated to adhere to a range of legislative and regulatory instruments aimed at preventing money laundering and terrorist financing. The applicable frameworks include:

- **Curaçao AML and Gaming Legislation:** The company complies with all requirements set by the Curaçao Gaming Authority, particularly concerning the lawful and regulated use of cryptocurrencies within licensed gaming activities.
- **National Ordinances NORUT and NOIS:** Orakum N.V. abides by the National Ordinance on Reporting Unusual Transactions (NORUT) and the National Ordinance on Identification of Clients for Services (NOIS). These laws mandate robust client identification, transaction monitoring, and the timely reporting of any suspicious or unusual financial activity to the Financial

Intelligence Unit (FIU) Curaçao.

- **FATF Guidelines:** The company follows the recommendations issued by the Financial Action Task Force (FATF) regarding Virtual Assets and Virtual Asset Service Providers, with particular attention to Recommendation 15 and the FATF's guidance on applying a risk-based approach to the use of virtual assets.
- **EU AML Directives (AMLD5 and AMLD6):** While Curaçao is not an EU member state, Orakum N.V. incorporates these directives as international best practices. They provide essential procedures for Know Your Customer (KYC) verification, detailed recordkeeping, and mandatory transaction reporting in the context of crypto assets.
- **Basel Committee Standards:** The company also considers the Basel Committee on Banking Supervision's principles on cryptocurrency risk, which offer global benchmarks for addressing asset volatility and operational vulnerabilities within financial systems.

3. Roles, Responsibilities, and Governance

Board of Directors and Executive Management

The Board and senior leadership of Orakum N.V. are jointly accountable for defining the company's strategic goals, formulating approaches to meet those objectives, and establishing governance structures and risk control mechanisms to manage associated threats, particularly in relation to cryptocurrency usage.

Their duties include evaluating the risk of money laundering, ensuring this policy is enforced effectively, mandating regular staff training, and incorporating compliance adherence into employee performance assessments. The Board is also responsible for confirming that robust systems and controls are in place, especially in situations where functions are outsourced, to mitigate potential AML risks.

Additionally, the Board must ensure the Compliance Officer is granted sufficient authority, autonomy, and resources to perform his duties and maintain the company's compliance with anti-money laundering laws.

Compliance Officer

The Compliance Officer oversees the design and implementation of AML/CFT procedures and manages communication with regulatory bodies, including the FIU Curaçao. They coordinate internal and external audits and ensure the company's cryptocurrency-related activities comply with applicable laws and internal controls.

The Compliance Officer must possess an appropriate level of authority and operational independence and must have unrestricted access to relevant personnel, systems, and information. This role is subject to performance evaluations to ensure continued effectiveness and reports directly to the Board.

Key responsibilities include:

- Preparing an Annual Compliance Report for Board review, summarizing AML compliance and risk mitigation efforts.
- Delivering quarterly updates to the Board on the performance and adequacy of AML systems, along with recommendations for improvement.
- Cooperating with investigative authorities during AML inquiries by providing required data or access.
- Acting as the central figure within the company for all AML-related matters and ensuring internal alignment with current legal and regulatory developments.
- Managing staff AML/CFT training programs and ensuring training content remains current.
- Serving as the point of escalation for employee-reported concerns or suspicions of money laundering. All such incidents must be reviewed, documented, and, where applicable, reported to the FIU. If no report is submitted, the Compliance Officer must justify the decision and notify management.
- Maintaining active and transparent communication with law enforcement and relevant regulatory authorities as needed.

This policy is introduced during staff onboarding, and any revisions are communicated company-wide by the Compliance Officer.

Risk Management Committee

Orakum N.V. has formed a Risk Management Committee composed of senior management and specialists in digital finance. This committee meets on a quarterly basis to assess risk exposure related to cryptocurrency, evaluate transaction patterns, and review the effectiveness of control mechanisms.

The committee's responsibilities include:

- Leading the implementation of the regulatory compliance framework
- Acting as an escalation channel for serious internal issues, such as breaches or suspected misconduct
- Managing relationships with external regulators during audits, inspections, or inquiries
- Evaluating the overall adequacy of the company's compliance structure against its defined risk appetite
- Reviewing and analyzing the company's risk management processes, including how emerging threats are detected, assessed, and addressed
- Examining proposed operational changes—such as new products or services—for associated AML risks
- Reviewing significant breaches of internal AML protocols
- Supervising fraud detection and prevention mechanisms
- Overseeing the company's regulatory compliance performance through continuous monitoring
- Performing any additional risk oversight functions as needed

Internal Audit

The internal audit function is tasked with conducting quarterly reviews of the company's cryptocurrency operations. These assessments provide an objective evaluation of how well the company adheres to its risk policy and the broader regulatory framework.

The audit team evaluates the strength of existing AML procedures—including policies, controls, and infrastructure—and determines the company's level of compliance. Upon identifying areas for improvement, the audit team issues recommendations, which are implemented and formally documented by the Compliance Officer and the Board.

4. Identifying Cryptocurrency-Specific Risks

4.1. Price Volatility and Market Instability

The inherent volatility of cryptocurrency prices can lead to significant financial exposure, especially in online gaming where crypto is used for deposits, wagers, and withdrawals. Orakum N.V. mitigates this risk through the following measures:

- **Use of Stablecoins for Large Payouts:** Whenever feasible, high-value disbursements are made using stablecoins such as USDC or USDT to maintain value consistency and reduce exposure to price swings.
- **Payout Thresholds and Timing Controls:** Transactions that exceed predefined limits are reviewed for potential market impact. Large payouts are broken into smaller, scheduled tranches to reduce financial exposure during volatile periods.
- **Operational Procedure:** The Finance Department actively monitors cryptocurrency market conditions and adjusts payout values to reflect current market rates. Daily reconciliations are conducted to ensure all crypto transactions comply with internal limits, with all changes meticulously recorded in the transaction ledger.

4.2. Regulatory and Legal Risk

Because cryptocurrency regulations differ between jurisdictions and may change rapidly—particularly in the gaming sector—Orakum N.V. proactively manages regulatory risk through:

- **Continuous Legal Surveillance:** The Compliance Officer is responsible for tracking updates to legislation and regulatory frameworks that apply to crypto activities in online gaming, with special attention to guidelines issued by the Curaçao Gaming Authority.
- **Record Maintenance:** The company ensures that detailed documentation of all crypto-related transactions, including KYC records, is securely retained for at least five years, in line with requirements from FIU Curaçao and AMLD5.
- **Operational Procedure:** Routine internal audits are conducted to verify the accuracy and completeness of transaction documentation. The Compliance Team prepares monthly reports for the Risk Management Committee, highlighting any compliance issues and initiating corrective actions as needed.

4.3. AML/CFT and Fraud Prevention

Given the semi-anonymous nature of cryptocurrencies, Orakum N.V. enforces strict AML/CFT controls to reduce the risk of fraud and illicit financial activities. These include:

- **KYC Protocols:** Every customer conducting cryptocurrency transactions must undergo identity verification, including government-issued ID checks and proof of residence.
- **EDD for High-Risk Scenarios:** Enhanced verification is triggered for transactions above specific thresholds or those involving jurisdictions considered high risk. This includes requiring documentation on the source of funds.
- **Operational Procedure for High-Risk Transactions:** When flagged by the transaction monitoring system, such transactions are reviewed by the Compliance Officer. The Compliance Team collects supporting documents and traces the origin of the funds using blockchain analysis tools. If risks remain unresolved, the transaction is suspended until a decision is reached.

4.4. Cybersecurity and Asset Protection

Due to their digital nature, cryptocurrencies are vulnerable to cyber threats, including unauthorized access and fraud. Orakum N.V. applies robust security practices to protect its crypto assets and transaction integrity:

- **Cold Wallets for Reserves:** The majority of non-operational cryptocurrency funds are stored in offline cold wallets, safeguarded by multi-signature authorization protocols.
- **Hot Wallet Security:** Wallets used for daily operations are protected by two-factor authentication (2FA), strict transaction limits, and real-time monitoring tools to prevent unauthorized access.
- **Operational Procedure:** Each day, balances in hot wallets are cross-checked against the transaction ledger. Any discrepancies are immediately flagged and investigated. Wallet access is restricted to authorized personnel, with all transactions requiring dual approvals. Additionally, automated alerts are generated for any wallet activity occurring outside of normal business hours.

5. Transaction Monitoring

Monitoring Infrastructure

Orakum N.V. employs a blockchain analytics platform to continuously track all incoming and outgoing cryptocurrency activity. This system identifies anomalies—such as unusually rapid transfers or large-scale withdrawals—that may indicate suspicious behavior and triggers further investigation by the compliance function.

Examples of Potentially Suspicious Activity

The following scenarios are considered red flags and are subject to heightened scrutiny:

- Transactions that diverge significantly from the user's typical betting patterns or differ from peer-group behavior.
- Payments made from a single account using an excessive number of different small-denomination coins.
- Multiple payments made with a single type of cryptocurrency in a way that deviates from normal usage.
- Transactions that are flagged as spam by the blockchain network.
- Transactions linked to individuals classified as high-risk by Orakum N.V. (e.g., Politically Exposed Persons).
- Transfers to or from wallet addresses that are marked as high-risk by the analytics tool.
- Deposits made shortly after account creation followed by swift withdrawals without utilizing the platform's services.
- Customer accounts that receive deposits in fiat or crypto but remain inactive afterward.
- Withdrawals executed within two months of deposit without any associated betting activity.
- Funds identified as stolen or tied to illegal activities.

- Transfers involving unusually large sums or frequent movements that do not align with standard transaction patterns.
- Accounts funded through financial institutions in unstable or high-risk jurisdictions.
- Trading activity that reflects non-standard timing, volume, or strategy, inconsistent with accepted industry behavior.
- Transactions whose metadata, references, or scripts suggest illegal purposes.
- Customers directly or indirectly involved in crypto mining operations located in high-risk jurisdictions, or those using high-risk crypto assets like privacy coins.
- Customers who fail to provide required KYC documentation.
- Use of anonymizing tools such as VPNs, TOR browsers, or disposable/randomized email services.
- Requests to convert crypto into cash, privacy coins, or untraceable electronic currencies.
- Transfers to newly created wallet addresses with no transaction history.
- Repeated micro-transactions that appear designed to stay below KYC thresholds.
- Attempts to exchange to or from state-issued digital currencies possibly intended to circumvent international sanctions.
- Exploitation of system vulnerabilities or technical glitches for personal gain.

Monitoring Procedure

When a transaction meets any red flag criteria, it is automatically routed to the Compliance Team for assessment. The team reviews the transaction against the customer's profile and historical behavior. If deemed suspicious, the case is escalated for enhanced review. If the transaction is found to be legitimate, it is approved and logged as part of the compliance records.

6. Due Diligence and Reporting Protocols (Paraphrased)

Orakum N.V. maintains a comprehensive AML/CFT program specifically adapted to address the distinctive challenges posed by cryptocurrency use.

- **Customer Due Diligence (CDD):**
All platform users must undergo mandatory identity checks, including verification of personal identification, proof of address, and confirmation of the source of funds prior to conducting cryptocurrency transactions.
- **Continuous Transaction Surveillance:**
The company employs real-time monitoring tools to detect irregular activity patterns—such as frequent deposits or withdrawals in rapid succession—that may suggest money laundering tactics like layering or structuring.
- **Suspicious Activity Reporting (SAR):**
Transactions that raise red flags are escalated and formally reported to the FIU Curaçao, in compliance with the National Ordinance on Reporting Unusual Transactions (NORUT).
- **SAR Reporting Workflow:**
When suspicious behavior is identified, the monitoring system instantly alerts the Compliance Team. The Compliance Officer examines the flagged transaction and prepares a Suspicious Activity Report (SAR), which—if the concerns are substantiated—is filed with FIU Curaçao within a 24-hour window. All related documentation, including the SAR and transaction history, is securely stored for a period of five years and made available for regulatory audits when required.

7. Audit Processes

Orakum N.V.'s Compliance Officer and Internal Audit team carry out quarterly assessments of the company's cryptocurrency operations. These reviews ensure that transaction records are accurate and that all procedures align with established anti-money laundering (AML) requirements.

In addition, the company performs an annual audit, which includes an independent third-party review to evaluate the effectiveness of internal controls, particularly in relation to operational integrity and cybersecurity safeguards.

8. Cryptocurrency Security Protocols

Segregation of Cold and Hot Wallets

To maintain a high level of asset protection, Orakum N.V. employs a clear separation between cold and hot wallets:

- Cold Wallets are used to store approximately 90% of the company's crypto holdings in offline, highly secure environments, minimizing exposure to online threats.
- Hot Wallets contain only the necessary funds needed for daily operations, and are subject to strict 24-hour value limits to manage transactional risk.

Operational Safeguard:

All transfers from cold to hot wallets require multi-tier approval from senior management. At the end of each month, a full reconciliation is performed to ensure that recorded balances match actual holdings, helping to detect and prevent unauthorized activity.

Access and Authentication Controls

Access to cryptocurrency wallets is strictly limited to authorized individuals. These wallets are protected using multi-factor authentication (MFA) and hardware security modules (HSMs) to guard against breaches and unauthorized usage.

9. Staff Training and Awareness

Orakum N.V. is dedicated to providing all relevant employees with comprehensive AML/CFT training tailored to their responsibilities. Training is conducted at the start of employment and then repeated annually to ensure ongoing awareness and compliance.

Following each training session, employees are required to complete a knowledge assessment to verify their understanding of the material. The curriculum focuses on the legal obligations and responsibilities related to anti-money laundering and counter-terrorist financing, as outlined in applicable laws and regulations.

This policy undergoes a formal review at least once per year, or sooner if prompted by regulatory updates or internal operational changes. Any modifications are subject to Board approval and are promptly communicated to all affected personnel.