

PREVAILER B.V.
149548

Cryptocurrency Risk Management Policy

Approved by the Board of Directors

A handwritten signature in blue ink, consisting of a large, stylized 'R' followed by a horizontal line and a small flourish.

21/03/2025

Contents

- 1. Overview and Strategic Objectives**
- 2. Applicable Regulatory Landscape**
- 3. Governance and Oversight Structure**
- 4. Risk Identification and Assessment**
- 5. AML Compliance, Due Diligence, and Reporting Measures**
- 6. Mechanisms Against Fraud and Money Laundering**
- 7. Cybersecurity and Asset Safeguarding**
- 8. Operational Controls in Crypto Asset Handling**
- 9. Transaction Monitoring and Risk Indicators**

A handwritten signature in blue ink, consisting of a stylized 'A' or '4' shape.

1. Overview and Strategic Objectives

This Crypto Risk Management Policy forms an integral component of Prevailer B.V.'s overarching Anti-Money Laundering (AML) and Countering the Financing of Terrorism (CFT) compliance framework. It must be interpreted in conjunction with the company's AML/CFT Manual, as it is not intended to operate as an independent document.

Prevailer B.V., a company incorporated under the laws of Curaçao with Company Number 149548, is licensed by the Curaçao Gaming Authority under license number OGL/2024/341/0759, in accordance with the National Ordinance on Games of Chance (*Landsverordening op de kansspelen*, P.B. 2024, no. 157).

This policy outlines the governance measures and internal protocols adopted by the Company to responsibly integrate cryptocurrency into its online igaming ecosystem. As digital assets continue to reshape financial services and payment modalities, Prevailer B.V. acknowledges the strategic importance of addressing the unique compliance, operational, and security challenges presented by crypto asset usage within the iGaming space.

The policy reflects the Company's commitment to maintaining regulatory compliance with Curaçao's legal framework and international AML obligations. It defines robust safeguards to detect, prevent, and respond to financial crime risks associated with cryptocurrency transactions. This includes rigorous transaction monitoring, customer risk profiling, and continuous surveillance throughout the business relationship to ensure that activity remains consistent with declared customer information, source of funds, and expected behavioral patterns.

This policy applies universally to all individuals and entities engaged in the Company's crypto-related operations, including employees, consultants, affiliates, and external service providers. All relevant parties are expected to uphold these standards to maintain the integrity of operations and foster customer trust.

2. Applicable Regulatory Landscape

Prevailer B.V. operates within a robust regulatory framework that incorporates both domestic and international standards for cryptocurrency usage in the igaming sector. The Company ensures full compliance with the following legal instruments and best practice guidelines:

- Curaçao AML Legislation

Prevailer B.V. adheres to national anti-money laundering requirements, including the National Ordinance Reporting of Unusual Transactions (NORUT) and the National Ordinance Identification for Services (NOIS). This includes

fulfilling obligations related to the identification, documentation, and timely reporting of unusual or suspicious transactions to the relevant authorities.

- **Guidance from the Curaçao Gaming Authority**
The Company complies with all sector-specific guidance and requirements issued by the Curaçao Gaming Control Board (GCB) pertaining to the responsible management of cryptocurrencies and virtual assets within licensed igaming operations.
- **FATF Standards on Virtual Assets and VASPs**
The Company integrates relevant principles from the Financial Action Task Force (FATF) recommendations, particularly those addressing virtual assets and virtual asset service providers (VASPs), to reinforce its transaction monitoring and due diligence processes.
- **European AML Directives (AMLD5 and AMLD6)**
While not directly bound by EU law, Prevalier B.V. voluntarily adopts key elements of the Fifth and Sixth Anti-Money Laundering Directives, specifically around enhanced Know Your Customer (KYC) protocols and risk-based monitoring for virtual asset activity.

The Company's Compliance Officer is tasked with maintaining alignment with evolving global and local regulatory expectations. This includes conducting regular reviews of the legal landscape, implementing necessary updates to internal procedures, and submitting quarterly compliance reports to the Board of Directors to ensure continuous oversight.

3. Governance and Oversight Structure

To ensure effective oversight and execution of its cryptocurrency risk management strategy, Prevalier B.V. has established a structured governance framework that distributes responsibility across key internal functions:

- **Executive Board**
The Executive Board holds ultimate accountability for the Company's crypto-related risk management efforts. It is responsible for approving policy revisions, overseeing strategic direction, and ensuring comprehensive compliance with all applicable regulations.
- **Compliance Officer**
The designated Compliance Officer is responsible for the day-to-day implementation and supervision of cryptocurrency-related compliance measures. This includes monitoring regulatory obligations, managing internal controls, and submitting reports to the Financial Intelligence Unit of Curaçao

(FIU Curaçao) when suspicious or unusual activity is detected.

- **Risk Oversight Committee**

This multidisciplinary committee, composed of senior representatives from relevant departments, convenes on a quarterly basis to evaluate the Company's exposure to cryptocurrency-related risks. The committee reviews technical safeguards, assesses regulatory developments, and ensures that existing protocols remain aligned with compliance benchmarks.

- **Internal Audit Function**

An independent audit function operates under the direct mandate of the Executive Board. It conducts quarterly reviews of cryptocurrency-related operations, assessing adherence to internal policies and the effectiveness of implemented risk controls. The audit findings are reported directly to the Board to support transparent oversight and timely corrective action.

4. Risk Identification and Assessment

Prevailer B.V. acknowledges the dynamic risk landscape associated with cryptocurrency usage in igaming operations. The Company applies a structured approach to identifying and mitigating both market-related and regulatory risks associated with digital assets.

Market and Volatility Risk

Cryptocurrency valuations are highly susceptible to rapid fluctuations, which may directly affect the accuracy and stability of customer deposits and payout settlements. To reduce this exposure, the Company implements the following measures:

- **Prioritization of Stablecoins**

Where feasible, high-value transactions—particularly customer withdrawals—are settled using stablecoins. This mitigates volatility risk by anchoring transaction values to fiat-equivalent benchmarks.

- **Time-Staggered Payout Strategy**

For large transactions, payouts are executed in scheduled intervals, minimizing the financial impact of sudden price shifts in underlying crypto assets.

- **Active Market Surveillance**

The Financial Operations Team conducts daily reviews of cryptocurrency price trends to adjust the value of incoming and outgoing transactions. All

valuation-based modifications are transparently recorded and reviewed by the Compliance Officer to ensure consistency with internal policies.

Regulatory and Compliance Risk

Given the evolving nature of digital asset regulation—especially within Curaçao's iGaming context—Prevailer B.V. adopts a proactive compliance posture through the following mechanisms:

- **Continuous Regulatory Surveillance**
The Company's Legal and Compliance functions jointly monitor regulatory updates, particularly those issued by the Curaçao Gaming Control Board and international AML bodies, to ensure cryptocurrency activities remain compliant.
- **Record-Keeping Obligations**
In accordance with FIU Curaçao standards, all cryptocurrency transactions, customer engagements, and related records are securely maintained for a minimum period of five (5) years.
- **Routine Compliance Audits**
The Legal and Compliance teams conduct monthly internal audits of cryptocurrency transaction logs and customer records. Any deficiencies in documentation or procedural adherence are addressed promptly to safeguard compliance integrity.

5. AML Compliance, Due Diligence, and Reporting Measures

In alignment with national and international anti-money laundering (AML) and counter-terrorism financing (CFT) standards, Prevailer B.V. enforces stringent due diligence and reporting protocols specific to cryptocurrency-related activities. These measures are designed to detect, prevent, and report potential illicit activity, ensuring that the Company's crypto operations are fully compliant and secure.

Customer Due Diligence (CDD) and KYC Controls

Before engaging in any cryptocurrency transactions, all customers must undergo a robust Know Your Customer (KYC) verification process. This includes the mandatory submission and validation of a government-issued identification document, with additional checks performed based on the customer's risk profile and transaction behavior.

Continuous Transaction Surveillance

The Company employs an automated compliance monitoring system that conducts real-time surveillance of all crypto-related transactions. This system is designed to detect irregular transaction patterns, deviations from expected customer behavior, and indicators of potential money laundering activities. Flagged transactions are escalated for further review.

Suspicious Activity Reporting (SAR)

When a transaction is identified as suspicious:

- An automated alert is generated by the monitoring system.
- The Compliance Officer conducts an immediate review of the flagged transaction.
- If deemed necessary, a Suspicious Activity Report (SAR) is submitted to the Financial Intelligence Unit (FIU) Curaçao within 24 hours, in accordance with statutory obligations.

All flagged transactions, investigations, and SARs are securely archived to support regulatory audits and facilitate retrospective reviews.

6. Mechanisms Against Fraud and Money Laundering

Recognizing the inherent risks posed by the pseudo-anonymous nature of cryptocurrency transactions, Prevalier B.V. has implemented robust anti-fraud and AML controls to mitigate the misuse of digital assets for illicit purposes.

Enhanced Due Diligence (EDD) Procedures

For customers whose crypto transaction volumes exceed predefined risk thresholds, the Company enforces Enhanced Due Diligence (EDD) measures. These clients are required to submit supplementary documentation to verify the legitimacy of their activity and the source of their funds.

Advanced Monitoring for High-Risk Behavior

All cryptocurrency transactions are continuously monitored using real-time systems to identify patterns associated with suspicious or high-risk behavior, including but not limited to:

- Unusually rapid or large-value deposit and withdrawal cycles
- Activity inconsistent with known customer profiles
- Structuring patterns intended to evade reporting thresholds

EDD Escalation Workflow

When a transaction triggers EDD criteria:

1. The transaction is immediately flagged and escalated to the Compliance Team.
2. The customer may be asked to provide additional identification or financial documentation.
3. The Compliance Team performs further investigation, which may include the use of blockchain analytics and tracing tools to verify transaction history and wallet ownership.
4. Pending verification, high-risk transactions may be suspended or delayed until a risk clearance is issued.

These measures reinforce the Company's risk-based approach and support its commitment to financial crime prevention within the cryptocurrency environment.

7. Cybersecurity and Asset Safeguarding

Given the elevated cybersecurity threats associated with digital assets, Prevaler B.V. has adopted a layered security architecture to protect its cryptocurrency holdings and ensure operational integrity across its igaming platform.

Cold Wallet Custody for Asset Reserves

The majority of the Company's cryptocurrency reserves are held in cold storage—offline wallets not connected to the internet—to minimize exposure to cyberattacks. These wallets are protected using multi-factor authentication (MFA) and are only accessible by authorized personnel with elevated clearance.

Secured Hot Wallet Operations

Digital assets used for routine transactional purposes are stored in hot wallets, which are subject to:

- Real-time monitoring for unauthorized access or anomalous activity
- Strict transaction limits to minimize potential exposure in the event of compromise
- Segregated access privileges to ensure operational control and traceability

Daily Reconciliation and Transaction Controls

To maintain full visibility and accountability:

- Cryptocurrency balances across both hot and cold wallets are reconciled daily by the Financial Operations Team.
- Withdrawals or transfers from cold storage require senior management approval and are recorded in a secure audit log.
- All crypto movements are subject to procedural oversight and internal audit verification to ensure alignment with the Company's risk management standards.

8. Operational Controls in Crypto Asset Handling

Prevailer B.V. enforces strict operational security procedures to govern the management, storage, and movement of cryptocurrency assets. A clear segregation of duties and wallet types is maintained to minimize risk and ensure system integrity.

Cold and Hot Wallet Segregation

To safeguard digital asset reserves and facilitate efficient transaction processing, the Company utilizes a dual-wallet structure:

- Cold Wallets (Offline Custody):
Reserved exclusively for long-term asset storage, these wallets remain offline and inaccessible via the internet. Their isolation serves as a primary defense against hacking or unauthorized access.
- Hot Wallets (Operational Liquidity):
These wallets hold limited balances for the sole purpose of processing day-to-day transactions, including customer deposits and withdrawals. They are fortified with multiple layers of security and access control.

Transfer Authorization and Audit Trail

To maintain transparency and control over internal fund movements:

- Transfers from cold to hot wallets require explicit authorization from senior management, ensuring dual oversight.
- Each movement of funds is logged in real time and subject to daily reconciliation.
- Any discrepancies or irregularities in wallet balances are immediately escalated to the Compliance and Financial Operations teams for investigation and resolution.

These safeguards ensure that cryptocurrency operations are conducted with discipline, auditability, and minimal exposure to operational risk.

9. Transaction Monitoring and Risk Indicators

Prevailer B.V. employs an advanced blockchain analytics system to oversee and analyze cryptocurrency transactions in both real time and post-settlement review. The objective is to detect anomalous activity, trace the origin of funds, and prevent the inflow or outflow of digital assets linked to illicit conduct.

Transaction Monitoring Workflow

- Transactions that exceed predefined thresholds or display atypical frequency or structure are automatically flagged by the system.
- Flagged transactions undergo manual review by the Compliance Team, who investigate the source, flow, and legitimacy of the crypto activity.
- Transactions deemed legitimate are cleared for processing, while suspicious cases are documented, escalated, and subjected to ongoing monitoring or reporting procedures.

Red Flags and Investigative Tracing

Manual reviews are periodically required during the monitoring of crypto deposits and withdrawals. In such cases, the Company conducts in-depth tracing of the asset's journey across the blockchain to:

- Identify any direct or indirect links to illicit or high-risk wallets

- Map out coin movement from its origin point (e.g., mining event) to the most recent transfer
- Ensure the digital asset has not passed through wallets with reputational or regulatory red flags

Indicators of “Tainted” or High-Risk Wallets Include:

- Wallets involved in hacking or theft
- Wallets linked to terrorist financing or illegal activities
- Wallets used for dark web purchases
- Wallets connected to mixers, tumblers, or anonymizing services
- Wallets exhibiting obscured or untraceable transaction origins

Red Flags Associated with Privacy Features and Obfuscation Techniques

The use of certain privacy-enhancing tools or blockchain anonymity mechanisms may undermine the Company’s ability to implement effective KYC and AML controls. These include:

- Mixers/Tumblers
- Obfuscating ledger technologies
- IP anonymizers (e.g., Tor)
- Ring signatures / Ring Confidential Transactions
- Stealth addresses
- Atomic swaps
- Non-interactive zero-knowledge proofs
- Privacy coins (e.g., Monero, Zcash)

Transactions involving assets that utilize such techniques are treated with heightened scrutiny.

Escrow and Darknet Associations

Further red flags include:

- Crypto assets that originate from or are linked to second-party escrow services
- Assets traced to darknet markets, unregulated exchanges, or entities associated with:
 - Ransomware, market abuse, Ponzi schemes, or fraud
 - Sanctioned addresses
 - Unlicensed gambling platforms

Such assets may trigger immediate escalation, restriction, or SAR filing with the FIU Curaçao.

Regular Auditing and Policy Oversight

To ensure operational integrity and regulatory compliance:

- Quarterly internal audits are performed by the Company's audit function
- An independent third-party audit is conducted annually
- All audit outcomes are reported directly to the Executive Board

Training and Employee Awareness

All personnel involved in cryptocurrency-related operations receive periodic training on:

- Applicable AML/CFT regulations for crypto assets
- Cybersecurity standards relevant to crypto custody
- Incident response protocols for addressing suspected fraud or breaches

Policy Maintenance and Updates

This Crypto Risk Management Policy is reviewed annually, or earlier if required by regulatory developments. All updates are formally approved and communicated to

relevant stakeholders to ensure full alignment with compliance and operational standards.