

Caecus N.V. Cryptocurrency Risk Management Policy

Company Number: 163779

Effective Date: 11/11/2024

1. Introduction

1.1 Purpose of the Policy

The purpose of this policy is to establish a comprehensive framework for the effective identification, management, and mitigation of risks associated with the use of cryptocurrency in the operations of Caecus N.V., incorporated in Curaçao and authorized under the license issued by the Curaçao Gaming Control Board to offer games of chance (License Number OGL/2024/1262/0493) (hereinafter referred to as "the Company"). This policy ensures compliance with the legal and regulatory requirements set forth by the Gaming Board Curaçao and other international standards related to anti-money laundering (AML), combating the financing of terrorism (CFT), and cryptocurrency usage.

1.2 Scope

This policy applies to all individuals and entities engaged with Caecus N.V., including employees, contractors, partners, and third parties who manage, transact, or store cryptocurrencies on behalf of the Company. It covers all aspects of cryptocurrency operations, including deposit handling, transactional processing, payouts, and custody of digital assets.

2. Regulatory Compliance and Legal Obligations

2.1 Curaçao Legislation

The Company adheres strictly to Curaçao's National Ordinance on Reporting Unusual Transactions (NORUT) and the National Ordinance on Identification of Clients for Services (NOIS). These laws mandate customer identification, the monitoring of unusual activities, and the timely reporting of suspicious transactions to the Financial Intelligence Unit (FIU Curaçao).



2.2 FATF Guidelines

As part of its commitment to international standards, Caecus N.V. follows the Financial Action Task Force (FATF) Recommendations, including Recommendation 15 on Virtual Assets (VAs) and Virtual Asset Service Providers (VASPs). The Company implements a risk-based approach to manage the specific challenges posed by cryptocurrencies, aligning with FATF's guidance.

2.3 Best Practices from Other Jurisdictions

While Curaçao is outside the European Union, the Company voluntarily incorporates measures from AMLD5 and AMLD6, particularly in areas such as customer due diligence (CDD), transaction recordkeeping, and enhanced due diligence (EDD) for high-risk activities. Additionally, principles from the Basel Committee on Banking Supervision are applied to address operational and market risks.

3. Governance and Oversight

3.1 Board of Directors

The Board of Directors holds ultimate responsibility for the oversight of cryptocurrency risk management. The Board ensures that the policy aligns with the Company's strategic objectives and regulatory obligations. Quarterly meetings are convened to review compliance reports and approve updates to the policy.

3.2 Compliance Officer

The Compliance Officer plays a pivotal role in the implementation and monitoring of this policy. Key responsibilities include liaising with the FIU Curaçao, overseeing audits, maintaining compliance documentation, and ensuring the timely reporting of suspicious activities.

3.3 Risk Management Team

The Risk Management Team is tasked with conducting periodic assessments of cryptocurrency-related risks. This team includes senior management and experts in digital assets, who evaluate transactional trends, identify vulnerabilities, and recommend risk mitigation strategies.

3.4 Internal Audit Function

An independent internal audit team performs quarterly reviews of the Company's cryptocurrency operations, ensuring that policies are effectively implemented and regulatory compliance is maintained. The team submits detailed reports to the Board for review.



4. Risk Assessment and Mitigation

4.1 Volatility and Market Risk

Cryptocurrency values are inherently volatile, posing financial risks for operations that involve deposits, payouts, or bets in digital currencies.

To address this, the Company:

- Uses stablecoins such as USDC or USDT for high-value payouts, minimizing exposure to price fluctuations.
- Implements payout limits and schedules, spreading large transactions across multiple intervals to mitigate sudden market shifts.

Additionally, the Financial Department actively monitors market conditions and updates internal pricing models to ensure payouts reflect real-time values. Adjustments are logged in the transaction ledger, ensuring transparency and traceability.

4.2 Regulatory Risk

Cryptocurrency regulations evolve rapidly, especially in sectors like online gaming. The Company mitigates this risk through:

- Continuous monitoring of global and Curaçao-specific regulatory developments by the Compliance Team.
- Maintaining robust records of all cryptocurrency transactions for at least five years, in line with AMLD5 and FIU Curaçao requirements.

Regular internal and external audits are conducted to ensure compliance with the latest legal requirements.

4.3 AML/CFT and Fraud Risk

The pseudo-anonymous nature of cryptocurrencies increases the risk of money laundering and fraudulent activities. To counteract this:

- Comprehensive customer verification (CDD) is mandatory, requiring government-issued IDs and proof of address.
- High-risk transactions, including those involving large amounts or high-risk jurisdictions, undergo enhanced due diligence. Additional documentation, such as proof of funds, is required for these cases.

Blockchain analysis tools are utilized to trace the origins of funds. Any flagged transactions are reviewed by the Compliance Team and reported to FIU Curaçao if necessary.



4.4 Cybersecurity Risks

Digital assets are vulnerable to hacking, phishing, and unauthorized access. To protect these assets, the Company employs:

- Cold storage wallets for long-term asset custody, with multi-signature security protocols.
- Hot wallets with strict operational limits and enhanced security features, including two-factor authentication and real-time monitoring.

Access to wallets is restricted to authorized personnel, with detailed logs maintained for every transaction and wallet access.

5. Operational Framework

5.1 Wallet Management

The Company maintains a clear segregation between cold and hot wallets. Cold wallets store the majority of cryptocurrency reserves offline, reducing exposure to cyber threats, while hot wallets are used exclusively for day-to-day operations.

Transfers between cold and hot wallets require multi-level authorization and are documented meticulously to ensure transparency.

5.2 Transaction Monitoring

A blockchain analytics platform monitors all transactions, identifying patterns that may indicate unusual or suspicious behavior. Transactions flagged by the system are escalated to the Compliance Team for further review.

6. Reporting and Documentation

6.1 Suspicious Activity Reports (SARs)

When a suspicious transaction is identified, it is reported to FIU Curaçao within 24 hours. The Compliance Officer ensures that the SAR includes all relevant details and retains a copy for at least five years, in compliance with NORUT regulations.

6.2 Documentation Standards



Comprehensive records of all cryptocurrency-related activities are maintained. These include customer verification documents, transaction logs, and audit reports, ensuring readiness for regulatory inspections.

7. Training and Capacity Building

To ensure compliance and operational efficiency, all employees involved in cryptocurrency handling undergo regular training sessions. These sessions cover:

- AML/CFT best practices tailored to cryptocurrency risks.
- Cybersecurity protocols for safeguarding digital assets.
- Incident response procedures for fraud or data breaches.

8. Policy Review and Amendments

This policy is subject to an annual review by the Risk Management Team. Updates necessitated by changes in regulations or operational requirements are approved by the Board and communicated to all relevant stakeholders.

Approved by:

Board of Directors, Caecus N.V.

Date: 11/11/2024

