

Encode Digital B.V.
Company Number: 158289

Cryptocurrency Risk Management and Compliance Policy



Approved by the Board of Directors

May 2025

Contents

Contents

- 1. Executive Summary**
- 2. Regulatory Compliance Framework for Cryptocurrency Operations**
 - 2.1 Curaçao Anti-Money Laundering Ordinances
 - 2.2 Gaming Control Board of Curaçao Guidelines
 - 2.3 FATF Virtual Asset Recommendations
 - 2.4 EU AML Directives (AMLD5 & AMLD6)
- 3. Administrative Framework**
 - 3.1 Executive Board
 - 3.2 Compliance Officer
 - 3.3 Risk Oversight Committee
 - 3.4 Internal Audit Team
- 4. Risk Detection**
 - 4.1 Market and Volatility Risk
 - 4.2 Regulatory and Compliance Risks
- 5. Anti-Money Laundering (AML) & Countering the Financing of Terrorism (CFT) Compliance**
 - 5.1 Know Your Customer (KYC) Protocols
 - 5.2 Real-Time Transaction Monitoring
 - 5.3 Suspicious Activity Reporting (SAR)
 - 5.4 Incident Handling Procedure
- 6. Enhanced AML/CFT Controls for Cryptocurrency Transactions**
 - 6.1 Enhanced Due Diligence (EDD)
 - 6.2 Continuous Monitoring of High-Risk Behavior
 - 6.3 EDD Escalation Procedure
- 7. Cryptocurrency Security & Asset Protection Measures**
 - 7.1 Cold Storage for Asset Reserves
 - 7.2 Hot Wallet Security & Real-Time Monitoring
 - 7.3 Security Process Overview
- 8. Operational Security for Cryptocurrency Management**
 - 8.1 Cold Wallets (Offline Reserves)

8.2 Hot Wallets (Operational Funds)

8.3 Operational Protocol

9. Transaction Monitoring and Review

9.1 Monitoring Flow

10. Red Flags

10.1 Identification of Tainted Wallets

10.2 Use of Privacy Tools and Anonymizers

11. Regular Audits and Compliance Reviews

12. Training and Staff Awareness

13. Policy Review and Update

1. Executive Summary

Encode Digital B.V., incorporated under registration number 158289, is officially registered at 10 Schottegatweg Oost, Unit 1-9, Bon Bini Business Centre, Curaçao, as of August 16, 2021. As part of our commitment to operational excellence and regulatory integrity, we have established this Cryptocurrency Risk Management and Compliance Policy to guide the secure and compliant integration of digital assets within our gaming ecosystem.

As cryptocurrencies continue to reshape the global financial landscape, particularly within the gaming and betting sectors, we recognize the critical importance of strong governance, comprehensive risk mitigation, and full regulatory alignment. This policy defines the framework through which Encode Digital B.V. manages the inherent risks associated with cryptocurrency transactions, ensuring alignment with Curaçao's regulatory requirements and internationally recognized Anti-Money Laundering (AML) standards.

Our approach includes robust internal controls, transaction monitoring protocols, and continuous due diligence across all customer touchpoints. We actively monitor user account activity and transaction patterns to ensure consistency with declared customer information, business operations, and individualized risk profiles. This ongoing oversight forms the cornerstone of our compliance posture, enabling us to detect anomalies and respond swiftly to potential threats.

This policy is binding on all stakeholders involved in our cryptocurrency operations, including employees, contractors, affiliates, and third-party service providers. Each individual and entity is expected to uphold the highest standards of transparency, accountability, and vigilance in line with this policy.

By implementing this framework, Encode Digital B.V. reaffirms its commitment to safeguarding digital asset operations, preserving customer trust, and promoting a secure, compliant gaming environment in the evolving world of decentralized finance.

2. Regulatory Compliance Framework for Cryptocurrency Operations

At Encode Digital B.V., our cryptocurrency operations are governed by a robust compliance framework designed to align seamlessly with both national and international regulatory standards. Our approach ensures the secure, lawful, and transparent use of digital assets across all aspects of our licensed gaming activities.

Our compliance protocols encompass the following key regulatory pillars:

- **Curaçao Anti-Money Laundering Ordinances**

We fully comply with reporting obligations under the NORUT and NOIS frameworks, with a dedicated focus on identifying, documenting, and reporting unusual or suspicious transactions.

- **Gaming Control Board of Curaçao Guidelines**

Our digital asset practices strictly adhere to the Gaming Board's sector-specific regulations, ensuring responsible integration of cryptocurrencies within regulated gaming environments.

- **FATF Virtual Asset Recommendations**

We implement global best practices as outlined by the Financial Action Task Force (FATF), particularly in the oversight, risk assessment, and tracking of virtual asset activities.

- **EU Anti-Money Laundering Directives (AMLD5 & AMLD6)**

Encode Digital B.V. applies the highest standards of Know Your Customer (KYC) and risk-based monitoring as mandated by European AML directives, safeguarding customer interactions and financial integrity.

To maintain our leadership in compliance, our appointed Compliance Officer continuously monitors the evolving regulatory landscape, performs regular internal assessments, and delivers comprehensive quarterly reports to the Board of Directors. This proactive oversight ensures that our policies remain current, effective, and aligned with global regulatory developments.

3. Administrative framework

To ensure robust and accountable oversight of cryptocurrency-related activities, Encode Digital B.V. has established a structured governance model with clearly defined roles and responsibilities across key departments. This cross-functional approach enhances our ability to manage risk, maintain regulatory compliance, and uphold the integrity of our digital asset operations.

- **Executive Board**

Serving as the highest authority, the Executive Board holds ultimate responsibility for cryptocurrency governance. It approves all policy updates, reviews strategic compliance initiatives, and monitors organizational adherence to regulatory obligations.

- **Compliance Officer**

The Compliance Officer plays a central role in day-to-day regulatory oversight. This includes managing cryptocurrency compliance activities, ensuring timely regulatory reporting, and submitting suspicious transaction findings to the Curaçao Financial Intelligence Unit (FIU) as required.

- **Risk Oversight Committee**

Comprising senior leaders from multiple departments, this committee meets quarterly to evaluate the Company's exposure to cryptocurrency-related risks. It reviews the effectiveness of security measures, assesses compliance performance, and recommends risk mitigation strategies.

- **Internal Audit Team**

Operating independently, the Internal Audit Team conducts thorough quarterly audits of cryptocurrency operations. The team evaluates adherence to internal policies and external regulations, reporting findings directly to the Executive Board to support transparent governance.

Through this multi-tiered structure, Encode Digital B.V. reinforces its commitment to operational resilience, regulatory compliance, and responsible innovation in the evolving digital asset landscape.

4. Risk Detection

Market and Volatility Risk

Cryptocurrencies are known for significant value swings, which can impact payouts and deposits. To address this:

- **Preference for Stablecoins:** Where possible, the Company encourages high-value payouts in stablecoins to reduce volatility impact.
- **Scheduled Payout Intervals:** Large payouts are distributed across fixed intervals to buffer against sharp market drops.

The Financial Operations Team monitors cryptocurrency valuations daily, making adjustments to payouts to reflect real-time market values. Transaction values are documented, and any market-driven adjustments are reported to the Compliance Officer

Regulatory and Compliance Risks

Given the changing nature of crypto regulations, the Company commits to a proactive approach to compliance, including:

- **Real-Time Regulatory Monitoring:** Ongoing analysis of regulatory updates that could affect cryptocurrency operations, especially Curaçao-specific directives.
- **Comprehensive Documentation:** Full record-keeping of all transactions and customer interactions is maintained for five years, per Curaçao FIU requirements.

Process: Monthly audits of all crypto records ensure accuracy, while regulatory updates are tracked by the Legal Team. Any gaps in documentation are corrected immediately to ensure compliance.

5. Anti-Money Laundering (AML) & Countering the Financing of Terrorism (CFT) Compliance

Encode Digital B.V. is firmly committed to upholding the highest standards in Anti-Money Laundering (AML) and Countering the Financing of Terrorism (CFT). To that end, we implement

a rigorous due diligence framework designed to identify, prevent, and report any illicit financial activity related to cryptocurrency use.

Our compliance process includes the following core components:

- **Know Your Customer (KYC) Protocols**

Every customer must undergo a strict identity verification process before being allowed to participate in cryptocurrency transactions. This includes submission and verification of a valid, government-issued photo ID to ensure the legitimacy of the user.

- **Real-Time Transaction Monitoring**

All crypto transactions are actively monitored through an automated system that flags suspicious or unusual activity. These alerts are analyzed to assess potential money laundering or terrorism financing risks in real time.

- **Suspicious Activity Reporting (SAR)**

Any transaction flagged as potentially suspicious is escalated immediately. In accordance with regulatory requirements, all reportable incidents are submitted to the Financial Intelligence Unit (FIU) Curaçao within 24 hours.

Incident Handling Procedure:

When a suspicious transaction is detected, an automatic alert is triggered within the compliance monitoring system. The Compliance Officer conducts a detailed review and, if the activity meets the threshold for concern, initiates the SAR filing process. All related documentation is securely stored for future audits and regulatory review.

This layered approach ensures that Encode Digital B.V. remains fully compliant with AML/CFT mandates, reinforces its commitment to financial transparency, and maintains a secure, trusted environment for cryptocurrency transactions.

6. Enhanced AML/CFT Controls for Cryptocurrency Transactions

Recognizing the pseudo-anonymous nature of cryptocurrency and its associated risks, Encode Digital B.V. has implemented robust Anti-Money Laundering (AML) and Countering the

Financing of Terrorism (CFT) controls to detect and prevent fraudulent activity across its platform.

Key measures include:

- **Enhanced Due Diligence (EDD)**

For customers who exceed predefined transaction thresholds, additional layers of verification are required. This may include submission of financial statements, proof of source of funds, or other supporting documentation to validate the legitimacy of transactions.

- **Continuous Monitoring of High-Risk Behavior**

All cryptocurrency transactions are subject to real-time monitoring, with a particular focus on identifying high-risk patterns—such as rapid or large-volume deposits and withdrawals—that could indicate illicit activity.

EDD Escalation Procedure:

When a transaction is flagged for Enhanced Due Diligence, it is immediately referred to the Compliance Team for in-depth review. The team may request further documentation from the customer and utilize advanced blockchain analytics tools to trace the transaction's origin and flow. Any transaction deemed high-risk may be temporarily suspended until all due diligence checks are completed and clearance is granted.

Through these stringent protocols, Encode Digital B.V. reinforces its commitment to regulatory compliance, operational transparency, and the secure management of cryptocurrency activities.

7. Cryptocurrency Security & Asset Protection Measures

In light of the elevated cybersecurity risks associated with digital assets, Encode Digital B.V. has implemented a comprehensive security framework to safeguard cryptocurrency holdings and ensure the integrity of all transactions.

Key protective measures include:

- **Cold Storage for Asset Reserves**

The majority of the Company's digital assets are securely stored offline in cold wallets,

protected by multi-factor authentication and restricted access protocols. This minimizes exposure to online threats and unauthorized access.

- **Hot Wallet Security & Real-Time Monitoring**

Operational (hot) wallets—used for daily transaction processing—are safeguarded through continuous monitoring, strict withdrawal thresholds, and advanced security protocols. These wallets are configured to limit exposure while maintaining operational efficiency.

Security Process Overview:

Daily reconciliation is performed across all cryptocurrency wallets—both hot and cold—to ensure accuracy and detect any discrepancies. Transactions involving cold wallets are subject to elevated scrutiny, requiring approval from senior management and full documentation. Each transaction is logged and archived for audit purposes, ensuring transparency and accountability.

Through these rigorous controls, Encode Digital B.V. ensures the secure management of digital assets while maintaining trust, regulatory compliance, and operational resilience in a fast-evolving threat landscape.

8. Operational Security for Cryptocurrency Management

To maintain the highest level of security in managing digital assets, Encode Digital B.V. enforces a strict separation between operational and reserve cryptocurrency holdings. This structured approach minimizes risk exposure while ensuring efficient day-to-day functionality.

- **Cold Wallets (Offline Reserves)**

Designed for long-term asset storage, cold wallets are kept completely offline and isolated from external networks, significantly reducing the risk of unauthorized access or cyberattacks.

- **Hot Wallets (Operational Funds)**

Hot wallets are used exclusively for routine transactions and hold only the minimal amount necessary to support daily operations. These wallets are safeguarded with advanced encryption, real-time monitoring, and layered security protocols.

Operational Protocol:

Transfers from cold to hot wallets are tightly controlled and require explicit approval from senior management. All movement of funds is logged in real-time and reconciled daily. Any discrepancies in wallet balances are immediately flagged, escalated, and investigated to ensure full transparency and security.

This dual-wallet structure forms a core pillar of Encode Digital B.V.'s digital asset security strategy—balancing accessibility with rigorous risk management to protect the integrity of our financial ecosystem.

9. Transaction Monitoring and Review

The Company leverages a blockchain analytics system to monitor transaction patterns in real-time and post transaction monitoring, identifying potential fraudulent or unusual activities.

Monitoring Flow: Transactions exceeding predefined limits or displaying irregular frequency are flagged for review, prompting an investigation by the Compliance Team. Legitimate transactions are cleared, while suspicious activities are logged and monitored further.

10. Red Flags

When performing ongoing monitoring of the crypto pay-ins and pay-outs, some transactions will need to be reviewed manually. This review will be conducted by the Compliance Team.

In most cases, the Company traces the origin of the coins by going back multiple steps to fully understand the coin flow between different entities and addresses and to make sure there are no direct connections with illicit sources.

Crypto assets can be traced on the blockchain from the first moment of creation (usually through mining) until the last time they were spent. It is possible to trace coins back to the original source to minimize the risk of coins that were stored or passed through “tainted” wallets. Tainted wallets or high-risk wallets are the following:

Wallets that were hacked

Wallets that were used to fund or are the proceeds of illegal or terrorist activity

Wallets that were used to pay for services or goods on the dark web

Wallets that were used to obfuscate the origins of the coins, i.e. mixers and tumblers

Wallets that have otherwise suspicious origins

A significant proportion of the crypto assets held or used in a transaction is associated with privacy-enhancing features or products and services that potentially obfuscate transactions or undermine a Company's ability to know its customers and implement effective AML/CTF controls, such as:

Mixers or tumblers

Obfuscated ledger technology

Internet Protocol (IP) anonymizers

Ring signatures

Stealth addresses

Ring confidential transactions

Atomic swaps

Non-interactive zero-knowledge proofs

Privacy coins

A significant proportion of the crypto assets held or used in a transaction is associated with second-party escrow services

The crypto asset comes from, or is associated with, the darknet or other illegal/high-risk sources, such as an unregulated exchange, or is associated with market abuse, ransomware, hacking, fraud, Ponzi schemes, sanctioned bitcoin addresses, or unregulated gambling sites

11. Regular Audits and Compliance Reviews

Internal audits are conducted quarterly, complemented by an annual independent third-party audit. These reviews assess compliance with established protocols, and all findings are reported directly to the Executive Board.

12. Training and Staff Awareness

All staff managing cryptocurrency transactions undergo regular training on:

- AML/CFT regulations specific to cryptocurrency
- Cybersecurity standards
- Incident management for handling suspected fraud or breaches.

13. Policy Review

This policy is reviewed annually or as required by regulatory developments. Approved changes are communicated to all relevant employees to ensure ongoing compliance and operational alignment.

