

KREVETKA B.V. 166108
Chuchubiweg 17, Willemstad,
Curaçao

Crypto Risk Management
Policy

Approved by the Board of Directors



21/03/2025

Table of Contents

- 1. Overview and Strategic Context**
- 2. Applicable Legal and Regulatory Environment**
- 3. Governance and Oversight Structure**
- 4. Identification and Assessment of Risk Indicators**
- 5. AML Procedures: Due Diligence and Reporting**
- 6. Fraud Mitigation and Anti-Money Laundering Measures**
- 7. Cybersecurity and Digital Asset Protection**
- 8. Operational Controls for Cryptocurrency Handling**
- 9. Transaction Surveillance and Risk Triggers**

1. Overview and Strategic Context

This Cryptocurrency Risk Management and Compliance Policy forms an integral part of KREVETKA B.V.'s overarching Anti-Money Laundering (AML) framework and is to be read in conjunction with the company's AML/CFT Manual. It does not function as a standalone document but complements existing compliance protocols. KREVETKA B.V. is an authorized online gaming operator, holding license number OGL/2024/937/0857, issued on October 18, 2024, by the Curaçao Gaming Control Board under the National Ordinance on Offshore Games of Hazard (NOOGH, P.B. 1993, no. 63).

This policy outlines the internal procedures, controls, and protective measures that KREVETKA B.V. has established to integrate cryptocurrency into its gaming services responsibly. Recognizing the growing significance of digital currencies within the gambling and betting industry, the company emphasizes the importance of strong security measures, legal compliance, and effective risk mitigation tailored specifically to cryptocurrency use.

KREVETKA B.V. conducts continuous monitoring of customer account behavior and transactional activity, in line with regulatory standards. The monitoring process persists throughout the client relationship to ensure transactions align with the customer's stated information, declared business activity, and assigned risk profile.

This policy applies to all personnel, including employees, contractors, affiliates, and third-party service providers who play a role in managing, handling, or facilitating cryptocurrency-related operations within the company.

2. Applicable Legal and Regulatory Environment

Regulatory Framework

KREVETKA B.V. operates within a robust compliance structure that integrates both domestic legal obligations and international standards relevant to cryptocurrency use in the gaming sector. This framework includes:

- **Curaçao AML Legislation:** Full adherence to the National Ordinance on Reporting Unusual Transactions (NORUT) and the National Ordinance on Identification of Clients for Services (NOIS), ensuring all suspicious or irregular transactions are properly identified and reported.
- **Curaçao Gaming Control Board (GCB) Directives:** Compliance with regulatory guidelines specific to licensed gaming operators regarding the use and custody of digital assets.

- FATF Guidance on Virtual Assets: Implementation of global best practices issued by the Financial Action Task Force (FATF), particularly concerning the governance and risk management of virtual asset service providers (VASPs).
- EU AML Directives (5th and 6th): While Curaçao is not part of the European Union, KREVETKA B.V. adopts the AMLD5 and AMLD6 directives as global standards, applying strict KYC procedures and risk-based oversight to all customer interactions involving cryptocurrency.

The company's Compliance Officer is responsible for keeping the organization aligned with evolving crypto-related regulations. This includes conducting periodic regulatory assessments and presenting quarterly updates to the Board on compliance performance and emerging legal obligations.

3. Governance and Oversight Structure

To ensure effective governance and oversight of cryptocurrency-related risks, KREVETKA B.V. has implemented a structured administrative framework with clearly defined roles and responsibilities across the organization:

Executive Board: Holds ultimate authority over the policy, including the approval of updates and changes. The Board is also responsible for overseeing company-wide compliance with cryptocurrency risk management protocols.

Compliance Officer: Manages the day-to-day enforcement of cryptocurrency compliance measures. This includes handling regulatory reporting duties and submitting required disclosures or findings to the Curaçao Financial Intelligence Unit (FIU) when applicable.

Risk Oversight Committee: A multidisciplinary team of senior managers that convenes quarterly to evaluate the company's exposure to cryptocurrency-related risks. The committee is tasked with reviewing internal control mechanisms and ensuring that compliance standards are being met.

Internal Audit Function: Operates independently to carry out quarterly audits, examining the effectiveness of risk management procedures and verifying adherence to policy. The audit team reports its findings directly to the Executive Board to ensure transparency and accountability.

4. Identification and Assessment of Risk Indicators

Market Volatility Risk

Due to the inherent price instability of cryptocurrencies, fluctuations in market value can directly impact deposits, winnings, and payouts. To manage this risk effectively, KREVETKA B.V. applies the following safeguards:

- **Use of Stablecoins:** For substantial payouts, the company prioritizes the use of stablecoins (e.g., USDT, USDC) where feasible, helping to minimize exposure to sudden market shifts.
- **Timed Payout Structures:** Larger disbursements are scheduled in structured intervals, which helps reduce the impact of abrupt price movements.

The Financial Operations Team conducts daily assessments of crypto market conditions and adjusts payout amounts based on live pricing data. All transaction values and market-driven adjustments are thoroughly documented, with updates shared regularly with the Compliance Officer.

Regulatory and Compliance Risk

With cryptocurrency laws evolving frequently across jurisdictions, KREVETKA B.V. takes a proactive and preventive approach to compliance through:

- **Ongoing Regulatory Surveillance:** The company continuously monitors regulatory developments, with particular attention to Curaçao-specific guidance that could influence cryptocurrency usage in gaming.
- **Detailed Record Maintenance:** In accordance with FIU Curaçao obligations, the company maintains complete records of all transactions and client interactions for a minimum of five years.

Operational Process: Monthly internal reviews are conducted to verify the completeness and accuracy of cryptocurrency-related records. The Legal Team tracks legislative updates, and any discrepancies in documentation are addressed immediately to maintain full regulatory compliance.

5. AML Procedures: Due Diligence and Reporting

To uphold strict compliance with Anti-Money Laundering (AML) and Counter-Terrorist Financing (CFT) regulations, KREVETKA B.V. implements a structured and vigilant due diligence process, including the following key components:

Know Your Customer (KYC) Measures:

Every customer is required to undergo identity verification prior to engaging in any cryptocurrency-related activity. This includes validating government-issued identification and other necessary documentation to confirm the user's identity.

Ongoing Transaction Monitoring:

All cryptocurrency transactions are subject to continuous surveillance. The system detects irregular or suspicious activity patterns that may indicate potential money laundering, prompting further investigation.

Suspicious Activity Reporting (SAR):

When a transaction is flagged as suspicious, it is formally reported to the Financial Intelligence Unit (FIU) Curaçao, in alignment with local regulatory requirements.

Reporting Workflow:

Flagged transactions are automatically escalated within the compliance system. The Compliance Officer examines the transaction and, if deemed necessary, submits a Suspicious Activity Report (SAR) to FIU Curaçao within 24 hours. Documentation related to these incidents is securely archived and retained for audit and inspection purposes.

6. Fraud Mitigation and Anti-Money Laundering Measures

Recognizing the pseudo-anonymous characteristics of cryptocurrencies, KREVETKA B.V. has implemented reinforced AML and CFT protocols to reduce the risk of fraudulent activity and illicit financial behavior, including:

- **Enhanced Due Diligence (EDD):**
Customers whose transactions surpass predefined thresholds are required to undergo stricter verification processes, including the submission of additional documentation to validate the origin and legitimacy of funds.
- **Continuous Surveillance of High-Risk Transactions:**
All cryptocurrency activity is tracked in real time. The system is designed to identify suspicious behavior, such as unusually frequent deposits or rapid withdrawals, which could indicate potential abuse or money laundering.

EDD Process Flow:

When a transaction is flagged for further scrutiny, it is escalated to the Compliance Team. The team may request supplementary documentation and conduct a deeper

investigation using blockchain analysis tools. Any transaction deemed high-risk may be temporarily suspended until full verification is completed and the activity is cleared for processing.

7. Cybersecurity and Digital Asset Protection

Given the increased cybersecurity threats associated with handling digital currencies, KREVETKA B.V. implements a comprehensive set of protective measures to safeguard its cryptocurrency holdings:

- **Cold Wallet Storage for Reserves:**
The majority of the company's crypto assets are maintained in cold wallets, which are completely offline and protected using multi-factor authentication (MFA) to prevent unauthorized access.
- **Hot Wallet Safeguards:**
Wallets used for day-to-day operational transactions are protected through real-time monitoring, strict access controls, and daily transaction limits to reduce exposure.

Operational Protocol:

All cryptocurrency balances—both cold and hot—are reconciled on a daily basis to ensure accuracy and detect anomalies. Transfers from cold storage require senior management authorization and are fully documented for auditing purposes.

8. Operational Controls for Cryptocurrency Handling

To ensure secure management of cryptocurrency assets, KREVETKA B.V. maintains a clear separation between operational and reserve holdings:

- **Cold Wallets:**
Designated for long-term asset storage, these wallets are kept offline to mitigate the risk of unauthorized access or external breaches.
- **Hot Wallets:**
Configured for daily transactional use, these wallets hold only limited balances and are protected by multiple layers of advanced security protocols.

Operational Procedure:

Transfers from cold storage to hot wallets must be approved by senior management. All such movements are logged and reviewed daily. Any inconsistencies in wallet balances are immediately flagged for investigation and resolution.

9. Transaction Surveillance and Risk Triggers

KREVETKA B.V. utilizes a blockchain analytics platform to conduct both real-time and post-transaction monitoring of cryptocurrency activity. This system is designed to detect irregular patterns and flag potentially fraudulent or suspicious behavior.

Monitoring Workflow:

Transactions that exceed set thresholds or show unusual frequency are automatically flagged for internal review. These alerts are escalated to the Compliance Team, which investigates the nature of the transaction. If deemed legitimate, the activity is approved and logged. If suspicious, the transaction is monitored further and documented for ongoing oversight.

Manual Transaction Review

Certain crypto pay-ins and pay-outs may require manual examination by the Compliance Team. During such reviews, the company traces the origin and movement of the digital assets, often tracking back several transaction layers to identify potential links to high-risk or illicit entities.

Cryptocurrency can be traced from its creation—such as mining events—through all subsequent transfers. This enables the company to identify if the assets interacted with tainted wallets, including:

- Wallets linked to hacks or unauthorized access
- Wallets associated with criminal or terrorist financing
- Wallets involved in dark web transactions
- Wallets that utilized mixers or tumblers to hide asset origin
- Wallets flagged for other suspicious behavior

Indicators of Elevated Risk

Transactions are considered high-risk when:

- A substantial portion of the crypto asset is linked to privacy-enhancing technologies that hinder traceability, such as:
 - Mixing services / tumblers
 - Stealth addresses

- Ring signatures or confidential transactions
- Zero-knowledge proofs (ZKPs)
- IP masking tools or anonymizers
- Atomic swaps
- Privacy coins
- Funds originate from or are associated with:
 - Escrow services involving unknown second parties
 - Darknet marketplaces or high-risk exchanges
 - Unregulated gambling platforms
 - Activities like ransomware, hacking, Ponzi schemes, fraud, or links to sanctioned wallet addresses

Audit and Oversight

KREVETKA B.V. carries out quarterly internal audits to verify adherence to cryptocurrency risk controls and AML/CFT standards. These internal checks are reinforced by an annual independent third-party audit, with all audit findings formally submitted to the Executive Board for review and action.

Training and Staff Awareness

Personnel involved in cryptocurrency handling receive ongoing training tailored to:

- AML and CFT regulatory requirements specific to virtual assets
- Cybersecurity protocols applicable to crypto asset management
- Incident response procedures for addressing suspected fraud or breaches

Policy Review and Updates

This policy undergoes a formal review at least once per year, or sooner if required by regulatory changes or emerging risks. Any updates are approved by the Executive Board and promptly communicated to relevant staff to ensure continued compliance and operational effectiveness.