

Infusion Tech B.V.

120001

Chuchubiweg 17, Curacao

Risk Policy for Cryptocurrency Usage

1. Purpose and Scope

This policy outlines the framework for identifying, managing, and mitigating risks associated with cryptocurrency usage by Infusion Tech B.V., hereinafter referred to as "the Company." This Risk Policy is established in compliance with applicable laws and regulations as required by the Gaming Board Curaçao, relevant international AML standards, and other regulatory bodies overseeing financial technology and cryptocurrency use.

This policy applies to all employees, contractors, subsidiaries, and third-party partners associated with Infusion Tech B.V. who engage in the handling, transaction, or storage of cryptocurrency in any form within business operations.

2. Legal and Regulatory Compliance

Infusion Tech B.V. adheres to all relevant legal frameworks governing cryptocurrency use, with specific focus on:

- **Curaçao Gambling and AML Regulations:** Compliance with the Gaming Board Curaçao's mandates for the use of cryptocurrency within licensed gaming operations.
- **Curaçao National Ordinance on Reporting Unusual Transactions (NORUT) and National Ordinance on Identification of Clients for Services (NOIS):** Ensuring identification, monitoring, and reporting of unusual or suspicious transactions as stipulated by Curaçao's Financial Intelligence Unit (FIU).
- **Financial Action Task Force (FATF) Recommendations:** Following the FATF guidelines on Virtual Assets (VAs) and Virtual Asset Service Providers (VASPs), specifically FATF Recommendation 15 and the FATF Guidance on a Risk-Based Approach to Virtual Assets.
- **European Union's 5th and 6th Anti-Money Laundering Directives (AMLD5 and AMLD6):** Although Curaçao is outside the EU, these directives provide critical guidance for best practices in crypto-related AML, including KYC measures, recordkeeping, and transaction reporting.
- **The Basel Committee on Banking Supervision's Principles** for handling cryptocurrency risk in financial institutions, providing global standards for mitigating volatility and operational risk.



3. Governance and Roles

To effectively manage cryptocurrency risk, Infusion Tech B.V. has established a governance structure, with clearly defined roles and responsibilities at each level.

Board of Directors: The Board provides oversight, reviews quarterly compliance reports, and approves all cryptocurrency policies and updates. The Board also ensures that policies align with corporate strategy and legal requirements.

Compliance Officer: The Compliance Officer is responsible for implementing AML controls, liaising with FIU Curaçao, and coordinating audits. They monitor adherence to both internal and external regulations, managing cryptocurrency compliance documentation.

Risk Management Committee: The Risk Management Committee, comprising senior management and experts in digital assets, oversees risk assessments specific to cryptocurrency. This committee convenes quarterly to evaluate transaction activity, analyze risk exposure, and review control effectiveness.

Internal Audit Function: The audit team conducts quarterly evaluations of the cryptocurrency management process, providing independent assessments to the Board and ensuring compliance with both the policy and regulatory standards.

4. Cryptocurrency-Specific Risk Identification

4.1 Volatility and Market Risk

Cryptocurrency values can fluctuate significantly, posing a financial risk in gaming operations where deposits, bets, and winnings are transacted in crypto. Infusion Tech B.V. mitigates these risks by:

- **Stablecoin Usage for High-Value Winnings:** Where feasible, Infusion Tech B.V. uses stablecoins (e.g., USDC or USDT) for larger payouts to provide stability and minimize exposure to price fluctuations.
- **Payout Limits and Frequency Controls:** Payouts over specific thresholds are reviewed for volatility impact. All payouts are segmented across predefined time intervals to prevent large financial losses during extreme price swings.

Procedure: The Financial Department monitors cryptocurrency markets and adjusts payout values to reflect real-time prices. Daily checks are conducted to confirm that all cryptocurrency payouts adhere to the established thresholds, and any adjustments are logged in the transaction ledger.

4.2 Regulatory and Compliance Risk

Cryptocurrency regulation varies across jurisdictions and can shift rapidly, especially in the gaming sector. To address regulatory risk:



- **Ongoing Compliance Monitoring:** The Compliance Officer tracks regulatory developments affecting cryptocurrency in online gaming, particularly those imposed by the Gaming Board Curaçao.
- **Documentation and Record-Keeping:** Comprehensive records of all transactions, including KYC documentation, are maintained for a minimum of five years, as mandated by the AMLD5 and Curaçao FIU standards.

Procedure: Regular audits are conducted on documentation and records related to cryptocurrency transactions. The Compliance Team issues monthly reports to the Risk Management Committee and immediately flags any regulatory deviations for corrective action.

4.3 AML/CFT and Fraud Risk

Due to the pseudo-anonymous nature of cryptocurrencies, Infusion Tech B.V. is committed to strong AML and CFT controls to prevent fraud and money laundering. These include:

- **Advanced KYC Procedures:** All customers engaging in cryptocurrency transactions undergo rigorous verification, including government-issued ID checks and proof of address verification.
- **Enhanced Due Diligence (EDD) for High-Risk Transactions:** For transactions above certain thresholds or involving high-risk jurisdictions, additional due diligence measures are applied, such as gathering source of funds documentation.

Procedure Flow for High-Risk Transactions: When a transaction exceeds the high-risk threshold, it is flagged by the monitoring system and forwarded to the Compliance Officer. The Compliance Team reviews additional documentation and performs blockchain tracing on the funds' origins. If further investigation is warranted, the transaction is temporarily suspended pending clearance.

4.4 Cybersecurity and Asset Protection Risk

Cryptocurrencies, being digital assets, are susceptible to cybersecurity threats such as hacking, phishing, and unauthorized access. Infusion Tech B.V. employs comprehensive security protocols to protect crypto holdings and transactional integrity.

- **Cold Storage for Long-Term Holdings:** All non-transactional crypto reserves are stored in cold storage wallets, with multi-signature protection.
- **Hot Wallet Security Measures:** Operational wallets used for transactions are secured with two-factor authentication (2FA), real-time monitoring, and transaction limits to minimize exposure.

Procedure: Each day, cryptocurrency holdings in hot wallets are reconciled against the transaction ledger, with any discrepancies flagged for immediate investigation. Access to wallets requires multiple sign-offs by authorized personnel, and transaction attempts outside of standard hours trigger automated alerts.

5. AML/CFT Due Diligence and Reporting

Infusion Tech B.V. follows a robust AML/CFT framework tailored to cryptocurrency's unique risks:

- **Customer Due Diligence (CDD):** All users are required to complete CDD checks, including identity verification, address confirmation, and source of funds.
- **Ongoing Monitoring:** Real-time transaction monitoring systems analyze patterns and flag unusual behavior, such as high-frequency deposits and withdrawals that indicate potential layering or structuring.
- **Suspicious Activity Reporting (SAR):** Any flagged transactions are reported to FIU Curaçao as per NORUT requirements.

Flow of Reporting Suspicious Activity: Upon detecting a suspicious transaction, the system automatically notifies the Compliance Team. The Compliance Officer reviews the transaction and compiles a SAR report. If confirmed, the report is submitted to FIU Curaçao within 24 hours. Documentation of the transaction and SAR report is retained for five years, accessible for audit purposes.

6. Security Protocols for Cryptocurrency Transactions

6.1 Cold Wallet and Hot Wallet Segregation

To enhance security and limit risk, Infusion Tech B.V. distinguishes between hot and cold wallets:

- **Cold Wallets:** Hold 90% of the company's crypto assets in offline, secure storage.
- **Hot Wallets:** Retain only necessary operational funds for daily transactions, with 24-hour limits on maximum value thresholds.

Procedure: Each transfer from cold to hot storage requires multi-level authorization from senior management. Monthly reconciliations validate balances against transaction records, ensuring accuracy and preventing unauthorized transfers.

6.2 Access Control and Authentication

Only authorized personnel have access to cryptocurrency wallets, secured by multi-factor authentication and hardware security modules (HSMs).

7. Operational Controls and Transaction Monitoring

7.1 Transaction Monitoring System

Infusion Tech B.V. uses a blockchain analytics system to monitor all incoming and outgoing cryptocurrency transactions. The system flags irregular activity, such as rapid transactions or large withdrawals, prompting further investigation.

Procedure Flow for Monitoring: When a transaction is flagged, it enters the compliance review process, where the Compliance Team assesses whether it aligns with known customer activity. Transactions deemed suspicious undergo enhanced scrutiny, while legitimate activity is cleared and documented.

7.2 Quarterly and Annual Audits

The Compliance Officer and Internal Audit conduct quarterly reviews on cryptocurrency processes, validating transaction records and confirming adherence to AML protocols. An annual audit includes third-party verification to assess operational controls and cybersecurity standards.

8. Training and Employee Awareness

To ensure robust internal knowledge, all employees involved in cryptocurrency handling receive ongoing training covering:

- **AML/CFT standards specific to cryptocurrency**
- **Cybersecurity practices and secure handling of crypto assets**
- **Incident response protocols** for suspected fraud or breaches.

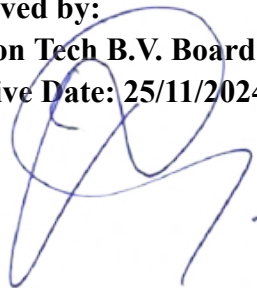
9. Policy Review and Amendments

This policy is reviewed annually by the Risk Management Committee. Any amendments, driven by regulatory changes or operational requirements, are approved by the Board and disseminated to all relevant personnel.

Approved by:

Infusion Tech B.V. Board of Directors

Effective Date: 25/11/2024

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