

LOTOSTORM B.V. (163G10)

Abraham Mendez Chumaceiro Boulevard 03, Curacao



***Cryptocurrency Risk Management
and Compliance Policy***

February 2025

Approved by the Board of Directors

A handwritten signature in blue ink, appearing to be "Waaigat", written over a horizontal line.

Waaigat Directors B.V.

GENERAL PROVISIONS

Lotostorm B.V is a legally registered entity in Curaçao that owns and operates the website <https://clickpari.com>. The company holds an online gaming license issued by the Curaçao Gaming Control Board, specifically OGL/2024/303/0300, and complies with all licensing regulations and regional restrictions established by the Curaçao regulatory authorities.

Managing Cryptocurrency risk effectively in a Company operating in a continuously changing risk environment, requires a strong risk management culture. As a result, the Lotostorm B.V registration number 163910 has established an effective risk oversight structure and the necessary internal organisational controls to ensure that the Company undertakes the following:

- ☐ Compliance with the applicable legislation.
- ☐ The establishment of the necessary policies and procedures.
- ☐ The setting and monitoring of the relevant limits.
- ☐ The adequate identification and management of risks.

The Board meets on a regular basis and receives updates on risk and regulatory matters from management. More than that, the Board receives and reviews regularly (at least annually) written reports concerning compliance, Cryptocurrency Risk Management and Internal audit policies.

Risk culture is a critical element in the Company's Lotostorm B.V Cryptocurrency Risk management framework and procedures. Management considers risk awareness and risk culture within the Company as an important part of the effective risk management process. Ethical behaviour is a key component of the strong risk culture, and its importance is also continuously emphasised by the management.

The Company is committed to embedding a strong risk culture throughout the business where everyone understands the risks they personally manage and are empowered and qualified to take accountability for them. The Company embraces a culture where each of the business areas is encouraged to take risk-based decisions, while knowing when to escalate or seek advice.

Lotostorm B.V. adheres to a comprehensive framework that aligns with national and international cryptocurrency regulations, specifically:

- ☐ Curaçao Anti-Money Laundering Ordinances: Adherence to reporting obligations under NORUT and NOIS, focusing on unusual and suspicious transactions.
- ☐ Gaming Board Curaçao Guidelines: Compliance with industry-specific guidelines for the management of digital assets in licensed gaming activities.
- ☐ FATF Virtual Asset Recommendations: Incorporation of international best practices for monitoring virtual assets.
- ☐ EU Anti-Money Laundering Directives (AMLD5 & AMLD6): Ensuring all customer interactions and transactions meet stringent KYC and risk-based monitoring criteria.

GOVERNANCE STRUCTURE

To enforce Cryptocurrency Risk Management effectively, Lotostorm B.V. has created a governance model with dedicated roles across departments:

The Board of Directors: Ultimate oversight, responsible for approving policy changes and monitoring overall compliance.

Compliance Officer: Oversees daily compliance with cryptocurrency usage, regulatory reporting, and submission of audit findings to the Curaçao FIU when necessary.

Risk Department: This department, comprising cross-functional leaders, assesses risk exposures quarterly, reviewing security controls and compliance benchmarks.

Internal Audit Team: Conducts independent audits quarterly, reviewing policy adherence and reporting directly to the Board of Directors.

RISK IDENTIFICATION AND MANAGEMENT

Market and Volatility Risk

Cryptocurrencies are characterized by significant price fluctuations, which can affect both payouts and deposits. To mitigate this risk, Lotostorm B.V. implements the following strategies:

- **Preference for Stablecoins:** Where possible, Lotostorm B.V. 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, adjusting 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

With the evolving landscape of cryptocurrency regulations, Lotostorm B.V. is dedicated to maintaining a proactive and thorough compliance framework, 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.

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.

Anti-Money Laundering (AML) and Fraud Prevention

To address the pseudo-anonymous nature of cryptocurrencies and prevent fraudulent activities, Lotostorm B.V. has implemented robust AML/CFT measures, including:

- ☐ *Enhanced Due Diligence (EDD)*: Customers exceeding transaction thresholds must provide additional documentation for verification.
- ☐ *Ongoing Monitoring for High-Risk Activity*: All crypto transactions are monitored in real-time to detect anomalies such as rapid deposits and withdrawals.

If a transaction is flagged for enhanced due diligence, it is escalated to the Compliance Team, who may request additional documents and investigate further using blockchain tracing tools. High-risk transactions may be paused until clearance is confirmed.

Cybersecurity and Asset Security

With heightened cyber risk for digital assets, Lotostorm B.V. employs extensive security measures:

- ☐ *Cold Storage for Reserves*: Most digital assets are stored offline in cold wallets, secured with multi-factor authentication.
- ☐ *Hot Wallet Security and Monitoring*: Operational wallets used for daily transactions are secured with real-time monitoring and strict transaction limits.

Cryptocurrency balances in both cold and hot wallets are reconciled daily. Transactions from cold wallets require approval from senior management and are logged for audit review.

AML DUE DILIGENCE AND REPORTING PROCEDURES

Client Due Diligence (“due diligence” or “CDD”) process must comply with procedures as detailed herein. These include the identification of the Client, ML/TF risk assessment, assessment of the financial position of the Client, validity of identity and the source of funds.

The following procedures which constitute the ML/TF prevention measures shall be carried out in order to perform customer due diligence at inception of a Business relationship with a Client

- (1) identification of persons who apply to the Company as the potential Clients
- (2) verification if the potential Clients acts as a principal, if the potential Clients is represented by other person (agent), the identification and verification of the representative (agent) applies as well
- (3) obtaining information on the Client’s management structure and the nature of its activity, if applicable
- (4) obtaining information on purpose and intended nature of the relationship with the Company; the above steps are essential prior to initiation of a business relationship with the potential Client and after the Client is engaged in the Business relationship, the following ML/TF prevention measure must be taken:

(5) ongoing monitoring of the Business relationship with the Client and the Monetary operations and Transactions of the Client.

(6) Suspicious Activity Reporting (SAR): All flagged transactions are reported to FIU Curaçao, following regulatory standards. When suspicious transactions trigger an alert in the compliance system. The Compliance Officer reviews these alerts, and a SAR is submitted to FIU Curaçao within 24 hours if warranted. Records of suspicious transactions are stored securely for audit purposes.

CRYPTOCURRENCY MANAGEMENT AND OPERATIONAL SECURITY

Cold and Hot Wallets

Lotostorm B.V. ensures the secure handling of assets by separating operational and reserve holdings:

- ☐ Cold Wallets: Used exclusively for long-term storage and held offline to prevent unauthorized access.
- ☐ Hot Wallets: Contain limited funds to fulfill daily transactions and are protected with robust security layers.

Transfers from cold storage to hot wallets require senior-level approvals, and any adjustments are documented daily. Discrepancies in wallet balances are flagged for immediate investigation.

Controlled Access and Authentication

Only authorized personnel with multi-factor authentication can access digital asset storage. Any transfer outside standard procedures triggers immediate review.

TRANSACTION MONITORING

Lotostorm B.V. leverages a blockchain analytics system to monitor transaction patterns in real time and post-transactions identifying potential fraudulent or unusual activities.

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.

All transaction monitoring alerts will be reviewed by the Compliance Officer immediately.

RED FLAGS AND HIGH-RISK TRANSACTIONS

Whilst 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, Lotostorm B.V. 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 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 firm’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

REGULAR AUDITS AND COMPLIANCE REVIEWS

Quarterly internal audits and an annual third-party audit verify adherence to compliance protocols, with findings reported to the Board of Directors.

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.

POLICY REVIEW AND AMENDMENTS

This policy is reviewed annually, or more frequently as required by regulatory developments. Updates are disseminated to all relevant personal to ensure continued compliance and operational efficiency.