Gameplay International B.V.
Company Number: 148409

Cryptocurrency Risk Management and Compliance Policy

Approved by the Board of Directors

March 2025

Contents

I. Executive Summary

II. Regulatory framework

III. Administrative framework

IV. Risk Detection

V. AML Due Diligence and Reporting Procedures

VI. Fraud and Money Laundering Protection

VII. Cybersecurity and Asset Security

VIII. Operational Security for Cryptocurrency Management

IX. Transaction Monitoring and Red Flags

I. Executive Summary

Cryptocurrency Risk Management and Compliance Policy Procedure is part of the Gameplay International B.V. with company registration number 148409 ('the Company' or 'we' or 'our') AML Framework and it must be read in conjunction with AML/CFT Manual. This is not a separate stand-alone document. Gameplay International B.V is licensed online gaming casino with License Number OGL/2024/511/0630 issued: January 14, 2025, by Curaçao Gaming Control Board.

This Cryptocurrency Risk Management Policy establishes the protocols and safeguards Gameplay International B.V. utilizes to securely integrate cryptocurrency into its gaming operations. As digital assets become increasingly relevant in the betting and gaming sectors, the Company recognizes the need for enhanced security, regulatory compliance, and vigilant risk oversight specific to crypto asset transactions. This policy details the steps required to meet Curaçao's regulatory expectations and global anti-money laundering (AML) requirements while protecting business integrity and customer trust.

The Company undertakes ongoing monitoring of account activities and transactions of all customers as required by the regulation. Monitoring of customer's activities is undertaken throughout the course of the relationship with the customer to ensure that the transactions being undertaken are consistent with the information provided by the customer, his/her business, and risk profile

The policy applies to all employees, affiliates, contractors, and third-party providers involved in cryptocurrency operations.

II. Regulatory framework

The Company 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.

The Compliance officer ensures Company remains up to date with evolving cryptocurrency regulations, conducting regular assessments and providing quarterly reports to the Board.

III. Administrative framework

To enforce cryptocurrency risk management effectively, Company has created a governance model with dedicated roles across departments:

Executive Board: 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 Oversight Committee: This committee, 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 Executive Board.

IV. 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.

V. AML Due Diligence and Reporting Procedures

To maintain compliance with AML/CFT standards, the Company applies rigorous due diligence procedures:

- Know Your Customer (KYC) Protocols: All customers must complete identity verification before engaging in crypto transactions, including verification of government-issued ID.
- Real-Time Transaction Monitoring: Transactions are continuously monitored for unusual patterns, flagged for review, and assessed for potential money laundering risks.
- Suspicious Activity Reporting (SAR): All flagged transactions are reported to FIU Curaçao, following regulatory standards.

Procedure Flow: 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.

VI. Fraud and Money Laundering Protection

Due to cryptocurrency's pseudo-anonymous nature, The Company has established strong AML/CFT controls to prevent fraudulent activities, 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.

Procedure Flow for EDD: 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.

VII. Cybersecurity and Asset Protection

With heightened cyber risk for digital assets, The Company's 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.

Process: 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.

VIII. Operational Security for Cryptocurrency Management

Separation of Cold and Hot Wallets

We ensure 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.

Process: 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.

IX. 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.

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 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

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.

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.

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.

Signature:

____

Vivian Ersilia o.b.o. (SMES) Solutions for
Management and Employment Support N.V.
Date: 16.04.2025