

Crypto Risk Management Policy

1. Introduction and Purpose

The purpose of this Crypto Risk Management Policy (CRMP) is to establish a comprehensive framework for identifying, assessing, mitigating, and monitoring risks associated with the acceptance, holding, processing, and transfer of cryptocurrencies (Virtual Assets) within the operations of the Licensee.

As an operator licensed under the Curaçao Gaming Authority (CGA), the Licensee recognizes its obligation to comply with all relevant local and international Anti-Money Laundering (AML) and Counter-Financing of Terrorism (CFT) legislation, including the FATF recommendations as implemented by the CGA.

This policy specifically addresses the unique risks posed by virtual assets, including, but not limited to, regulatory compliance, money laundering, financial crime, market volatility, and cybersecurity.

2. Risk Assessment Methodology

The Licensee adopts a risk-based approach (RBA) to all crypto activities, continuously assessing two primary risk areas: Regulatory & Financial Crime Risk, and Operational & Market Risk.

2.1. Regulatory and Financial Crime Risk (AML/CFT)

Cryptocurrency transactions are inherently viewed as higher risk due to their speed, global reach, and potential for pseudo-anonymity.

2.1.1. Customer Risk Assessment (CRA)

All players utilizing Virtual Assets must be subjected to enhanced Customer Due Diligence (CDD). Risk factors that trigger an elevated risk score include:

- Source of Funds (SOF): Inability to verify the legitimate source of cryptocurrency used for deposits.
- Wallet Origin: Transactions originating from or being sent to non-custodial (self-hosted) wallets, high-risk wallets (e.g., decentralized exchanges, mixers/tumblers), or unverified third-party wallets.
- Geographic Risk: Players residing in or transacting from high-risk or sanctioned jurisdictions (as designated by FATF or the CGA).
- Transaction Patterns: Frequent, high-volume transactions, rapid deposit-and-withdrawal patterns, or deposits from multiple unverified addresses.

2.1.2. Transaction Monitoring and Screening

- Blockchain Analysis: The Licensee shall utilize a certified blockchain analytics tool to screen all crypto transactions (deposits and withdrawals) for links to illicit activities (e.g., darknet markets, scams, sanctioned entities).
- Travel Rule Compliance: The Licensee is required to collect, hold, and transmit necessary originator and beneficiary information for all virtual asset transfers above the prescribed threshold, consistent with the FATF Travel Rule requirements.
- Suspicious Activity Reporting (SAR/NORUT): Any transaction or pattern deemed "unusual" or "suspicious" based on defined indicators will be immediately reported to the Financial Intelligence Unit (FIU) of Curaçao via the designated Compliance Officer, in accordance with the National Ordinance on the Reporting of Unusual Transactions (NORUT).

2.2. Operational and Market Risk

2.2.1. Market Volatility Risk

- Instantaneous Conversion: The Licensee shall implement technical controls to convert incoming Virtual Assets (e.g., Bitcoin, Ethereum) into a stable asset (e.g., Stablecoin or Fiat) immediately upon receipt or confirmation to minimize exposure to price fluctuations, protecting both the operator and the player's account balance.
- Risk Disclosure: Clear disclaimers and terms and conditions must be provided to players, outlining that the operator is not responsible for the market volatility of cryptocurrencies between the time of transaction initiation and network confirmation.

2.2.2. Cyber Security and Wallet Management Risk

- Wallet Segmentation: Assets shall be strictly segregated into hot (online) and cold (offline) storage wallets. A minimal amount of crypto necessary for daily operations and withdrawals shall be kept in hot storage.
- Multi-Signature Control: Access to all cold storage wallets must require a multi-signature process, requiring verification from multiple authorized internal parties (e.g., CFO, Security Director).
- Secure Infrastructure: All systems processing crypto transactions must utilize industry-standard encryption, firewalls, and intrusion detection systems, subject to regular penetration testing and audits by independent, CGA-approved third parties.
- Private Key Security: Private keys shall be handled with the highest level of security, never stored on systems connected to the internet, and backed up in geographically separated, encrypted locations.

3. Mitigation and Control Procedures

3.1. Designated Roles and Training

- **Compliance Officer:** The designated Compliance Officer is responsible for overseeing the CRMP, maintaining records of all due diligence performed on crypto transactions, and serving as the primary liaison with the CGA and FIU regarding unusual transactions.
- **Staff Training:** All relevant staff (Customer Support, Finance, Compliance, IT) shall receive mandatory, periodic training on the specific risks associated with Virtual Assets, including new ML/TF typologies, the implementation of blockchain analysis tools, and internal procedures for managing wallet security.

3.2. Withdrawal Protocol

- **Enhanced Scrutiny:** All crypto withdrawal requests exceeding a defined threshold (e.g., €2,000 or currency equivalent) are automatically flagged for Enhanced Due Diligence (EDD) review by the Compliance Officer prior to release.
- **Address Verification:** The Licensee reserves the right to request proof of ownership of the receiving crypto wallet address before processing a withdrawal.

3.3. Record Keeping

- The Licensee must maintain all records pertaining to crypto transactions, CDD/EDD findings, blockchain analysis results, risk ratings, and internal review decisions for a minimum of five (5) years, as required by Curaçao law.

4. Policy Review and Audit

This Crypto Risk Management Policy shall be reviewed and updated no less than annually, or immediately following any legislative changes announced by the CGA, the FIU, or international bodies like FATF. Compliance with this policy shall be included as a mandatory element in the Licensee's periodic independent compliance audits.