

# Public AML/CFT Policy Statement

This document serves as the public-facing summary of Crown's Anti-Money Laundering and Counter-Terrorism Financing (AML/CFT) framework. It is intended to inform our clients, partners, and the general public of our core compliance principles, governance structures, and regulatory commitments.

To protect the integrity of our security infrastructure and prevent the evasion of our controls by illicit actors, Crown maintains a comprehensive, highly detailed **Internal AML/CFT Operational Manual**. This internal document governs our proprietary risk-scoring algorithms, exact investigation SLAs, specific transaction monitoring typologies, and precise UBO dynamic thresholds. The complete Internal Manual remains strictly confidential but is readily available in its entirety to competent regulatory authorities, including the Central Bank of Brazil (BACEN) and the Financial Activities Control Council (COAF), upon official request.

---

## 1. Objective and Scope

The primary objective of this AML/CTFP Policy is to establish the principles, governance structure, and internal controls that govern the efforts of Crown to prevent its products and services from being used for the practice of crimes of laundering or concealment of assets, rights, and values, financing of terrorism, and the proliferation of weapons of mass destruction.

This framework applies to Crown, and all of its Employees, Partners, and Service Providers. It ensures compliance with applicable Brazilian legislation, notably the Legal Framework for Cryptoassets, relevant Central Bank of Brazil (BCB) resolutions governing Virtual Asset Service Providers (VASPs), and the international standards established by the Financial Action Task Force (FATF).

## 2. Governance and Responsibilities

### The Three Lines of Defense

Crown's AML/CTFP governance is structured to ensure independence, effective supervision, and a clear segregation of duties, mitigating risks of conflict of interest and errors. Crown adopts the three lines of defense model, recognized as a best practice for risk management:

- **1st Line of Defense (1LoD):** Comprises the Commercial, Business, and Onboarding Teams responsible for the initial execution of AML/CFTP procedures, such as collecting client data.
- **2nd Line of Defense (2LoD):** Includes the Head of Legal and Compliance, the Compliance Team, and Senior Management, acting independently to oversee implementation, conduct risk assessments, and perform transaction analysis.
- **3rd Line of Defense (3LoD):** Internal and/or External Audit provides an independent and objective assessment of the adequacy and effectiveness of the AML/CFTP program.

Senior management is fully committed to providing the necessary resources—technological, financial, and human—to ensure the full execution and success of this policy.

### 3. The Risk-Based Approach (RBA)

Crown conducts and documents an Internal Risk Assessment (IRA) at least annually to identify and mitigate risks. The RBA directs the intensity of due diligence and monitoring controls by classifying Clients into risk categories (Low, Medium, High) based on several factors. These risk factors include:

- **Industry Sector:** Assessing whether the client operates in traditional, regulated industries or inherently high-risk sectors.
- **Jurisdiction:** Evaluating exposure to FATF member countries versus countries on high-risk or sanctioned lists.
- **Corporate Structure:** Analyzing the complexity of the organization, including the use of trusts, offshore vehicles, or bearer shares.
- **Virtual Asset Activity Profile:** Reviewing intentions or histories of interaction with mixers/tumblers, privacy coins, or unregulated VASPs.

## 4. Client Due Diligence (CDD) and Know Your Customer (KYC)

Crown implements a robust and multi-phase KYC process to comprehensively assess each Client's risk profile.

- **Identification and Verification:** We collect comprehensive documentation guided by specific checklists, including proof of incorporation, tax identification, and corporate organizational charts.
- **Ultimate Beneficial Owner (UBO):** Crown identifies the natural persons who ultimately own or control the entity, specifically looking for individuals who own 25% or more of the share capital, or who in fact exercise control over the client's activities.
- **Politically Exposed Persons (PEPs):** Crown uses continuous screening tools to identify PEPs during onboarding and periodic reviews. The definition of a PEP strictly includes immediate family members and close associates. Clients identified as PEPs require Enhanced Due Diligence (EDD) and formal approval from the CEO.
- **Sanctions:** Crown adopts a zero-tolerance policy regarding transactions or relationships involving countries, individuals, or legal entities mentioned in sanctions lists, such as those from OFAC, the UN, and the European Union.

## 5. Monitoring, Controls, and Transaction Analysis

Crown employs a sophisticated dual-layered monitoring framework to ensure comprehensive oversight of financial activities.

- **Fiat Monitoring (Off-chain):** Focuses on the "cash-in" and "cash-out" phases, monitoring bank transfers and interactions with the traditional financial system to detect patterns like structuring or unexplained wealth.

- **On-chain Monitoring (Digital Assets):** Utilizes specialized Know Your Transaction (KYT) tools to monitor the lifecycle of our tokens, analyzing wallet-to-wallet transfers and exposure to high-risk digital asset entities.
- **Travel Rule Compliance:** Crown declares its full commitment to adhering to the principles of the FATF "Travel Rule". For applicable virtual asset transfers, Crown collects and securely transmits necessary information about the originator and beneficiary to the counterparty VASP.

Suspicious transactions that indicate involvement in money laundering, lack economic basis, or represent a sudden change in pattern are documented in a specific dossier. If applicable, these cases are communicated to COAF.

## 6. Comprehensive Due Diligence (KYE, KYP, KYA)

Crown's risk management is holistic and extends beyond Clients:

- **Know Your Employee (KYE):** We conduct background checks and verify professional histories to ensure alignment with Crown's values and compliance standards.
- **Know Your Partner (KYP):** Critical partners and service providers undergo risk-based due diligence, including regulatory status assessments and reviews of their internal AML/CFT programs.
- **Know Your Asset (KYA):** Crown maintains rigorous due diligence for the selection and monitoring of the financial institutions that custody the reserve assets, including independent audits.

## 7. Training and Record Retention

Crown maintains a continuous and mandatory AML/CFTP training program for all Employees to ensure awareness of the latest financial crime typologies and regulatory obligations.



Information collected during the KYC procedure, as well as the registry of operations, products hired, and suspicious transaction dossiers, are securely retained for a period of ten (10) years.

**\*Full Policy:** The detailed *AML/CFT Policy* is available upon request at [compliance@crowd-brlv.com](mailto:compliance@crowd-brlv.com).