Crown Digital:

AML and CFT Policy

TECHNICAL SHEET

TITLE: Policy on the Prevention of Money Laundering and the Financing of Terrorism and the Proliferation of Weapons of Mass Destruction ("Policy")

RESPONSIBLE AREA: Risk and Compliance

RESPONSIBLE DIRECTOR: COO

POLICY DESCRIPTION: Establishes Crown's guidelines, procedures, and internal controls to prevent its products and services from being used for the practice of money laundering, financing of terrorism, and the proliferation of weapons of mass destruction.

APPLICATION: CROWN SOCIEDADE PRESTADORA DE SERVIÇOS DE ATIVOS VIRTUAIS LTDA., its directors, employees, partners, and business partners.

APPROVED BY: CEO

VERSION CONTROL

VERSION	PUBLICATION DATE	DESCRIPTION OF CHANGES
1.0	October 28, 2025	Initial version created by converting and enhancing the previous Brazilian policy.
2.0	August 7, 2025	Policy enhanced with global best practices for risk assessment, partner due diligence, and transaction monitoring.

TABLE OF CONTENTS

1. Objective, Scope, and Fundamental Principles

The primary objective of this Policy is to establish the principles, governance structure, and internal controls that govern the efforts of CROWN SOCIEDADE PRESTADORA DE SERVIÇOS DE ATIVOS VIRTUAIS LTDA ("Crown") to prevent its products and services from being used for the practice of crimes of laundering or concealment of assets, rights, and values ("ML"), financing of terrorism ("FT"), and the proliferation of weapons of mass destruction ("PF").

This Policy aims to ensure compliance with applicable Brazilian legislation, notably Law No. 14,478/22 (Legal Framework for Cryptoassets) and BCB Circular No. 3,978/20, with the international standards established by the Financial Action Task Force (FATF), and with the best practices of the Brazilian financial sector, as recommended by entities such as the Brazilian Federation of Banks (FEBRABAN) and the Brazilian Association of Financial and Capital Markets Entities (ANBIMA).

1.1. Scope and Applicability

This Policy shall be in effect for an indefinite term, and its application is mandatory for all directors, employees, partners, and critical third-party service providers of Crown.

It is established that Crown directs its services exclusively to Legal Entities duly incorporated and domiciled in Brazil or abroad.

1.2. Senior Management Commitment

The Executive Board and the Board of Directors of Crown express their full and unequivocal commitment to the effectiveness and continuous improvement of the AML/CFT program.

Compliance is not viewed merely as a regulatory obligation but as a central component of Crown's business strategy and a fundamental pillar for building trust with clients, institutional partners, and regulators.

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

1.3. AML/CFT Documentary Structure

To ensure clarity, consistency, and auditability, Crown adopts a hierarchical documentation structure.

This Policy is the highest-level document, establishing the strategic principles and general guidelines ("what" and "why").

It is supported and detailed by a set of operational manuals that describe the step-by-step workflows ("how," "who," and "when"). The reference manuals include, but are not limited to :

- Onboarding and KYC Procedures Manual
- Monitoring and Atypicality Analysis Procedures Manual

The existence of these separate manuals mitigates the operational risk of processes depending on the tacit knowledge of key individuals, ensuring that controls are standardized, scalable, and auditable.

2. Governance Structure, Roles, and Responsibilities

Crown's AML/CFT governance is structured to ensure independence, effective supervision, and a clear segregation of duties, mitigating risks of conflict of interest and errors.

Crown's governance structure adopts the three lines of defense model, recognized as a best practice for risk management:

- **1st Line:** Business and operations areas, responsible for the initial execution of AML/CFT procedures, such as collecting client data and daily interaction.
- **2nd Line:** The Risk and Compliance function, which acts independently of the 1st line. It is responsible for defining this Policy, developing procedures, overseeing their implementation, conducting the Internal Risk Assessment, and performing transaction monitoring and analysis.
- **3rd Line:** Internal and/or External Audit, which provides an independent and objective assessment of the adequacy and effectiveness of the AML/CFT program

and the controls implemented by the first two lines.

2.1. The Responsible Statutory Director

Crown formally designates a statutory Director as responsible, before regulatory bodies, for complying with AML/CFT obligations. Their duties are exercised within the collegiate governance structure, ensuring the proper segregation of functions.

2.2. The Risk and Compliance Committee

The Risk and Compliance Committee is a collegiate body, chaired by the Responsible Director, which meets quarterly or whenever necessary. Its main duties are to deliberate on strategic risk issues, approve the Internal Risk Assessment (IRA), and decide on the approval of high-risk clients and on complex cases of suspicious transactions.

To ensure the robustness and transparency of the decision-making process, the minutes of the Committee's meetings will record all deliberations, decisions made, and, crucially, any dissenting votes and their respective justifications, as well as abstentions due to conflict of interest. This practice ensures that multiple perspectives are considered and that responsibility for decisions is properly allocated.

2.3. Responsibility Assignment Matrix (RACI)

To eliminate ambiguities and formalize the segregation of duties, the distribution of responsibilities for key AML/CFT activities follows the RACI (Responsible, Accountable, Consulted, Informed) model.

The previous concentration of decision-making power in a single individual represented a single point of failure and a risk of the absence of effective challenge. The RACI matrix distributes functions more granularly, ensuring that critical decisions, such as the approval of high-risk clients and reporting to COAF, are made collegially and with the necessary checks and balances.

Key AML/CFT Activity	Business Area	Risk & Compliance	Responsible Director	Risk Committee	Board of Directors
Conduct Internal Risk Assessment (IRA)	C	R	A	C	I
Client Onboarding (Data Collection/DDQ)	R	C	I	I	I
Client Risk Analysis and Classification	I	R	A	C (for High Risk)	I
Approval of Low/Medium Risk Client	I	R	A	I	I
Approval of High-Risk Client / PEP	I	C	R	A	I
Transaction Monitoring Alert Analysis	N/A	R	A	I (for complex cases)	I
Decision to Report to COAF (STR)	I	C	R	A	I

Legend: R=Responsible (Executes the task), A=Accountable (Owns the process, ultimately responsible), C=Consulted (Must be consulted before action), I=Informed (Must be informed after action)

3. The Risk-Based Approach (RBA)

3.1. Internal Risk Assessment (IRA) Methodology

Crown conducts and documents an Internal Risk Assessment (IRA) at least annually, or whenever significant changes occur in the institution's risk profile, its products, or the regulatory environment.

The IRA is the pillar that supports the entire AML/CFT program, serving as the basis for calibrating all controls. To ensure that Crown's risk assessment is not insular and is aligned with the vision of the Brazilian financial ecosystem, Crown's IRA incorporates, as one of its fundamental pillars, the analysis and addressing of the risks, vulnerabilities, and threats identified in the latest National Risk Assessment of AML/CFT (NRA) published by the Brazilian authorities.

3.2. Customer Risk Factors and Classification

The IRA evaluates a set of factors to classify clients into risk categories (Low, Medium, High), directing the intensity of due diligence and monitoring controls. The failure to include risk factors specific to the virtual assets business was a fundamental vulnerability, as the initial risk classification did not reflect the main source of risk for a VASP. To correct this deficiency, the risk matrix was expanded to include the client's on-chain activity profile, ensuring that the intensity of controls is proportional to the real risk the client represents to the platform.

Risk Factor	Low Level	Medium Level	High Level
Industry Sector	Traditional and regulated industries.	Sectors with some risk exposure (e.g., import/export).	Inherently high-risk sectors (e.g., gambling, other unregulated VASPs, precious metals dealers).
Jurisdiction (Client/UBO)	FATF member countries with positive evaluations.	Countries with some deficiencies noted by the FATF.	Countries on FATF high-risk lists or under sanctions.
Corporate Structure	Simple structure, with easily identifiable UBOs.	Structure with one or two levels of holdings.	Complex structure, with multiple layers, use of trusts, offshore vehicles, or bearer shares.
PEP and Adverse Media	No identification of PEPs or relevant adverse media.	Relationship with a low-ranking PEP or minor adverse media.	Client, UBO, or legal representative is a high-ranking PEP; negative and credible adverse media about financial crimes.
Virtual Asset Activity Profile	Exclusive transactions with other known and regulated VASPs in FATF member jurisdictions.	Interaction with established and audited DeFi protocols or use of self-hosted wallets with a clear purpose.	Intention or history of interaction with mixers/tumblers, privacy coins, high-risk DeFi protocols, or unregulated VASPs/based in high-risk jurisdictions.

4. Customer Due Diligence (CDD) Program

4.1. Overview of the KYC Process

Crown implements a robust and multi-phase Know Your Customer (KYC) process for all institutional clients. The process aims not only to comply with regulatory requirements but also to understand the nature of the client's business and to comprehensively assess their risk profile.

The detailed procedures, documentation checklists, and step-by-step workflows are formalized in the Onboarding and KYC Procedures Manual, which serves as an operational guide for the Risk and Compliance team.

4.2. Identification and Verification of the Client and the Ultimate Beneficial Owner (UBO)

The identification and verification process is the cornerstone of KYC and follows a rigorous and documented approach.

- **Documentation Collection:** The collection of documents is guided by specific checklists for each jurisdiction (Brazil, USA, Others), as detailed in the Due Diligence Questionnaires (DDQs). The documents include proof of incorporation (e.g., Articles of Association), tax identification (e.g., CNPJ, EIN), financial statements, corporate organizational chart, and identification documents of individuals (e.g., ID/Passport, CPF/SSN).
- **Identification of the Ultimate Beneficial Owner (UBO):** The concealment of real ownership is a classic money laundering typology. Therefore, the identification of the UBO goes beyond the client's simple declaration and follows a multifaceted approach to ensure the accuracy and veracity of the information. The process combines:
    - collecting the information declared by the client in the DDQ and the corporate organizational chart;
    - independently verifying this information against public and private data sources (e.g., commercial boards, Serasa Experian databases); and

    - for complex structures (holdings, trusts), requesting additional supporting documentation to map the control chain to the natural person(s) who ultimately own or control the entity.

- **Dynamic UBO Threshold:** The application of the UBO identification threshold is dynamic and risk-based. The standard threshold for identification is 25% of capital or control. However, this threshold is reduced to 10% for any entity classified as High Risk during the initial assessment, requiring a re-evaluation of the ownership structure to identify and verify additional individuals.

4.3. Politically Exposed Persons (PEPs)

The identification of Politically Exposed Persons (PEPs) is a mandatory field in all DDQs. Crown uses continuous screening tools to identify PEPs among the client's beneficial owners and administrators. Any relationship with a PEP, their family members, or close associates automatically triggers the application of Enhanced Due Diligence (EDD) and requires approval for the start of the relationship by the Risk and Compliance Committee.

4.4. Enhanced Due Diligence (EDD)

EDD is a set of additional and mandatory scrutiny measures applied to all clients classified as High Risk. The triggers for EDD include the risk classification, PEP status, operating in high-risk sectors, or the identification of the client as a financial institution or another VASP. EDD procedures include, at a minimum, obtaining and critically analyzing the client's own AML/CFT policy and their latest independent audit report on the AML program, as well as an in-depth investigation into the source of funds and wealth.

4.5. Sanctions and Restricted Lists Policy

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 (Office of Foreign Assets and Control), the United Nations (UN), and the European

Union.

Screening against restricted lists is performed at onboarding and continuously across the entire client base and for all incoming fund transfers.

5. Monitoring, Controls, and Transaction Analysis

5.1. Monitoring of Fiat Currency Transactions

All deposits and withdrawals of Brazilian Reais (BRL) must, mandatorily, occur between the client's account at Crown and bank accounts of the same ownership (same CNPJ). Transactions that violate this "same ownership" rule are automatically blocked to prevent the use of the platform as a pass-through for funds from unidentified third parties.

5.2. Monitoring of Virtual Asset Transactions (On-Chain)

As a VASP, on-chain monitoring is Crown's most critical and sophisticated control. A generic description of this process is insufficient and does not convey the depth of risk management. Therefore, Crown details the specific risk typologies that are monitored in real-time using advanced blockchain analysis tools. This transparent approach demonstrates that Crown not only possesses the technology but also masters the science behind it, aligning its controls with the risk typologies recognized globally by the FATF.

Risk Typology (Source: FATF, Market Reports)	Specific Red Flags Monitored	Immediate Action by the Compliance Analyst
Terrorism Financing/Sanctions	Direct or indirect interaction (one or more "hops") with digital wallet addresses on sanctions lists (OFAC, UN, etc.).	Immediate freezing of funds; Blocking of the client's account; Urgent escalation to the Responsible Director.
Laundering of Proceeds from Hacks/Ransomware	Receipt of funds with an origin traced to hacks of other platforms or known ransomware attacks.	Immediate freezing of funds; Preparation of a dossier for a Suspicious Transaction Report (STR) to COAF.
Obfuscation via Mixers/Tumblers	Funds that have recently passed through mixing or tumbling services (e.g., Tornado Cash) to break the trail.	Blocking of the transaction (if high risk) or escalation for EDD and request for information from the client (if medium risk).
Obfuscation via Chain Hopping	Pattern of rapid and multiple asset swaps between different blockchains without a clear economic purpose.	In-depth analysis of the end-to-end fund flow; Formal request for explanations from the client.
Interaction with Illegal Markets (Darknet)	Funds with origin or destination in wallet addresses associated with Darknet markets.	Blocking of the transaction; Analysis for a possible STR and termination of the relationship with the client.
Fraud/Ponzi Schemes	Receipt of funds from addresses associated with identified Ponzi schemes or crypto-asset investment frauds.	Blocking of the transaction; Analysis for a possible STR.

5.3. Atypicality Analysis and Resolution Times (SLAs)

The previous 45-day deadline for alert analysis was operationally indefensible and incompatible with the real-time nature of risks in crypto-assets. To ensure a rapid and risk-proportional response, each generated alert is classified by criticality level and handled by the Risk and Compliance team according to the following maximum resolution times (Service Level Agreements - SLAs):

- **Critical Risk Alert** (e.g., interaction with a sanctioned address): Analysis, containment, and escalation within 24 hours.
- **High-Risk Alert** (e.g., significant exposure to mixers): Analysis and decision within 72 hours.
- **Medium Risk Alert** (e.g., structured transactions): Analysis and conclusion within 7 business days.

5.4. Compliance with the "Travel Rule" (FATF Recommendation 16)

5.4.1. Commitment and Scope

Crown declares its full commitment to adhering to the principles of the "Travel Rule," as established by the FATF. This rule applies to all transfers of virtual assets to and from other VASPs that exceed the applicable regulatory threshold (e.g., USD 1,000 / EUR 1,000). The objective is to ensure the traceability of transactions to prevent the anonymous use of the crypto ecosystem for illicit purposes.

5.4.2. Procedure for Outbound Transfers

For outbound transfers that fall within the scope of the "Travel Rule," Crown will collect the necessary information about the originator (name, address, account identifier) and the beneficiary from its client and will transmit it securely to the counterparty VASP, using appropriate technological protocols.

5.4.3. Procedure for Inbound Transfers

To mitigate the risks associated with inbound transfers from unknown or non-compliant sources, the release of funds to the client's account is conditioned on prior confirmation

of the origin. Crown implements a risk-based approach that requires the client to:

A. perform a self-declaration of the origin wallet, providing sufficient information for its risk assessment; or
B. add the origin address to a list of pre-approved addresses (whitelisting).

Transfers received from undeclared or unapproved addresses will be automatically suspended and held in a quarantine wallet, pending an Enhanced Due Diligence analysis of the transaction and its origin, before any funds are released.

6. Communications to Regulatory Bodies (COAF)

When an analysis of an alert or an atypical situation concludes that there are indications of ML, FT, or PF, a complete dossier is prepared by the Risk and Compliance team and submitted for deliberation by the Risk and Compliance Committee. If the decision is to report, a Suspicious Transaction Report (STR) is prepared and submitted to the Financial Activities Control Council (COAF), via SISCOAF, within a maximum of 24 hours after the decision.

If there are no communications to be made in a calendar year, Crown will submit a "Declaration of Non-Occurrence" to COAF, when applicable.

7. Additional "Know Your" Procedures (KYE, KYP, KYA)

Crown's risk management is holistic and extends beyond clients.

7.1. Know Your Employee (KYE)

Crown implements due diligence procedures for its employees, from selection to termination.

At the time of application in a selection process, candidates will be asked to submit, at a minimum, a resume and/or LinkedIn profile page, with the aim of obtaining a professional and/or personal history, in compliance with Crown's privacy and personal data protection rules. The requested data aims to identify and qualify candidates according to the profile of the position they will occupy and the professional activities to be performed.

At this time, Crown will conduct an analysis to check for any potential conflict with

Crown's values, conduct, and compliance. In addition, during the selection process, Crown will promote the candidate's identification and qualification process, as well as search Restricted Lists and conduct background check procedures, as applicable.

If any inconsistency or risk factor is identified during the verification of the candidate's information, a specific analysis must be carried out before proceeding with the process.

Upon hiring, a copy of this Policy and Crown's other internal policies will be sent to the employee. Employees will also undergo training on the rules to be followed, aiming to promote an organizational culture of prevention.

If there is a vertical reclassification of a position, a new risk classification must be carried out. The areas and managers involved in the hiring or promotion procedure of employees must strictly follow the guidelines of this Policy and the specific KYE procedures. Additionally, the behavior of employees must be observed in order to detect and report possible suspicious behavior and/or behavior that is not in accordance with Crown's internal rules.

7.2. Know Your Partner and Service Provider (KYP)

Crown conducts specific, risk-based due diligence on all its critical partners and service providers. This process is essential to ensure the alignment of values and to protect the integrity of Crown's operations. The KYP process includes:

- **Identification and Verification:** Verifying the legal status, ownership structure, and identity of key principals of the partner entity.
- **Regulatory Status Assessment:** Confirming that the partner holds all necessary licenses and authorizations required for its business activities in its respective jurisdiction.
- **AML/CFT Program Review:** For partners involved in the financial flow or client-facing activities, a thorough review of their internal AML/CFT policies and controls is conducted to ensure they meet international best practices.
- **Risk Classification:** Partners are classified as high, medium, or low risk based on criteria such as the nature of the partnership, history of illicit activities, PEP status, and inclusion in restricted lists. High-risk partners are subject to EDD and require specific approval from senior management.
- **Contractual Obligations:** All contracts with critical partners must contain clauses establishing clear rights and obligations, division of responsibilities, and mechanisms for control and monitoring.

The risk classification of partners will be relevant for determining and better adapting monitoring procedures, selection, and analysis of suspicious situations and operations. In the event of verifying partners that present a higher risk, Crown will adopt complementary procedures and in-depth due diligence for evaluation and specific approval assignments, due to the criticality of the findings or the exceptions provided.
In this sense, the formalized contracts must contain clauses that establish, at a minimum:

- rights and obligations of the parties;
- detailed description of the services to be performed;
- deadlines and conditions of execution;
- the division of responsibilities and applicable penalties;
- termination hypotheses;
- declarations and guarantees; and
- control and monitoring mechanisms.

7.3. Know Your Asset (KYA)

The integrity of Crown's stablecoin depends on the quality and security of its reserve assets. Crown maintains a rigorous due diligence process for the selection and monitoring of the financial institution that custodies the reserves and conducts periodic and independent audits.

8. Training and Dissemination of the AML/CFT Culture

Crown maintains a continuous and mandatory AML/CFT training program for all directors and employees. The objective is to ensure that everyone understands their responsibilities under this Policy, is aware of the latest financial crime typologies, and actively contributes to maintaining a strong compliance culture throughout the organization. Training is provided upon hiring and on an ongoing annual basis, covering:

- Applicable AML/CFT laws and regulations.
- The contents of this Policy and related procedures.
- Money laundering and terrorist financing typologies relevant to stablecoins.
- The recognition and reporting of suspicious activity.

9. Effectiveness Assessment and Performance Indicators

9.1. Annual Effectiveness Assessment

Annually, the Risk and Compliance area will conduct a complete assessment of the effectiveness of the AML/CFT program. The result will be consolidated into a report to be presented to and approved by the Risk and Compliance Committee and the Executive Board.

9.2. Performance Indicators

Measuring the performance of the AML/CFT program is crucial for its continuous improvement. The previous indicators focused on process metrics (efficiency) but did not measure the outcome (effectiveness) in risk reduction. To correct this flaw, Crown adopts a dual dashboard that clearly distinguishes between operational efficiency and program effectiveness. Measuring effectiveness, through KPIs such as the false positive rate, demonstrates a level of sophistication and self-criticism that is standard in mature financial institutions, showing that Crown is not just performing tasks, but actively managing the quality and outcome of its risk controls.

Table 1: Operational Efficiency Indicators

ITEM	INDICATOR	FREQ.	MINIMUM TARGET
Alert Monitoring	Average time to complete alert analysis.	Quarterly	< 30 days (for low/medium risk alerts)
Third-Party Due Diligence	Weaknesses identified and addressed in critical	Annual	100% of action plans implemented within 6 months.

	partners (KYP).		
Training	Participation and approval rate in annual training.	Annual	80%

Table 2: Key Effectiveness Indicators (KPIs) Dashboard

Category	Effectiveness KPI	Calculation Formula	Frequency	Proposed Target	Corrective Action for Deviation
Monitoring Quality	False Positive Rate	(Total Alerts Closed Without Action / Total Alerts Generated) %	Monthly	< 90%	Recalibrate monitoring rules and thresholds; Enhance client risk profiles.
Intelligence and Decision	Alert to STR Conversion Rate	(Total STRs Sent / Total Alerts Analyzed) %	Quarterly	Between 1% and 5%	Review the quality of generated alerts; Advanced typology training for the team.
Client Risk Management	EDD Effectiveness	(% of High-Risk Clients with Mitigants Applied / Total High-Risk Clients) %	Semiannual	100%	Implement an action plan for all high-risk clients without mitigating controls.
KYC Effectiveness	Onboarding Rejection Rate for AML Risk	(Clients Rejected for AML Risk / Total Onboarding Attempts) %	Quarterly	> 2%	If the rate is near zero, review the client acceptance policy as it may be too permissive.
Compliance Culture	Number of Valid Internal Whistleblowing Reports	Count of valid reports received through the Whistleblowing Channel.	Annual	Increasing	If zero, promote awareness campaigns about the channel and ensure anonymity.

10. Record Keeping, Confidentiality, and General Provisions

All documents and records related to KYC processes, risk analyses, transaction monitoring, and communications to COAF will be kept in a secure format for a minimum period of 10 (ten) years, starting from the end of the client relationship.

The absolute duty of confidentiality over all AML/CFT analyses and communications is reiterated. It is strictly forbidden to communicate to clients or third parties about the conduct of suspicion analyses or the filing of reports with COAF, a practice known as "tipping-off".

This Policy will be reviewed annually by the Risk and Compliance area and approved by the Board of Directors, or whenever there are relevant changes in legislation, regulation, or Crown's risk profile.

11. NON-COMPLIANCE AND SANCTIONS

Failure to comply with any provision of this Policy will subject offenders to disciplinary measures, which may range from a warning to termination of the contractual relationship, without prejudice to applicable legal sanctions. Crown provides a confidential Whistleblowing Channel.

12. GENERAL PROVISIONS

This Policy will be reviewed annually or whenever there are relevant changes.