Compliance@jetprive.com.br

Policy for the Prevention of Money Laundering, Terrorism Financing, and Proliferation Financing of Weapons of Mass Destruction (“PLD/FTP”)

Compliance

March/2023

Target audience:

This Policy applies to the JP GESTORA DE FUNDOS LTDA Group, its agencies and subsidiaries ("JETPRIVE ") and its employees. All Employees are required to comply with this policy and its detailed implementation in their respective locations.

Index

1. Overview

This Policy aims to establish the guidelines for the Policy for the Prevention of Money Laundering, Terrorism Financing, and the Financing of the Proliferation of Weapons of Mass Destruction (“AML/CFT”) and was developed according to the risk profiles of JETPRIVE, its Clients, the operations, transactions, products, and services it performs, as well as its Employees, partners, and outsourced service providers.

The term "Money Laundering" is broadly interpreted as (i) the insertion of the proceeds of crime or corruption into the financial system in order to give it the appearance of proceeds from a legitimate activity, as well as (ii) the financing of illegal activities, including terrorism, through financial systems. The prevention of such use is generally known as Anti-Money Laundering (“AML”) or Anti-Money Laundering (“AML”).

The money laundering process consists of three stages (not necessarily sequential):

- Placement - Introduction of money or other assets derived from illegal/criminal activities into financial or non-financial institutions.
- Layering - Separating the proceeds of criminal activities from their source through the use of layers of complex financial operations. These layers are intended to obscure the audit trail, mask the origin of the funds, and provide anonymity.
- Integration - Reintroducing the "cleaned" funds back into the economy in such a way that they re-enter the financial system as seemingly legitimate resources.

The term "Terrorism Financing" can be interpreted as the financing of terrorist acts, terrorists, or terrorist organizations. Brazilian law stipulates strict penalties for anyone who offers or receives, obtains, stores, keeps in deposit, requests, invests, or in any way contributes to the acquisition of assets, goods, or financial resources, with the purpose of financing, in whole or in part, a person, group of people, association, entity, or criminal organization whose main or secondary activity, even occasionally, is the practice of terrorist acts. The fight against this practice is referred to as Combating the Financing of Terrorism (“CFT”) or Combating the Financing of Terrorism (“CFT”).

Furthermore, the Security Council adopted measures to combat the proliferation of weapons of mass destruction. Thus, the Security Council required States to cease any support to non-state actors for the development, acquisition, production, possession, transport, transfer, or use of nuclear, biological, and chemical weapons and their means of delivery. In 2006, following international efforts to contain terrorism, the General Assembly unanimously adopted the UN Global Counter-Terrorism Strategy. This strategy outlines a series of specific measures to combat terrorism in all its forms, at the national, regional, and international levels.

Financial institutions can be used at any stage of the AML/CFT process. For this reason, Banks and other financial agents, as defined by current legislation, are

required to have mechanisms to prevent the aforementioned crimes, making it difficult, preventing and/or reporting the occurrence or suspicion of illegal activities.

With this, JETPRIVE has globally established the following guidelines:

- Do not accept funds that are or could be products of criminal activities;
- Do not accept funds used to finance illegal activities;
- Comply with laws and regulations related to AML/CFT;
- Fully cooperate with authorities in criminal investigations, in accordance with the law; and
- Protect its reputation by mitigating AML/CFT risks, recognizing that regulatory and reputational risks are critical and can cause permanent damage to the institution.

To manage the regulatory and reputational risks associated with money laundering, terrorist financing, and the proliferation of weapons of mass destruction, JETPRIVE has adopted a risk-based approach to implement controls aimed at the prevention, detection, and reporting of suspicious situations and activities, avoiding the use of the institution to facilitate criminal activities.

2. Abbreviations used in this Policy

 AML – Anti-Money Laundering - Prevention of Money Laundering (defined in Section 1 of this Policy).

 CFT - Combating the Financing of Terrorism (defined in Section 1 of this Policy). (defined in Section 1 of this Policy).

 AML/CFT Policy – Global Policy for the Prevention of Money Laundering, Terrorist Financing, and the Financing of Proliferation of Weapons of Mass Destruction. Terrorism and the Financing of Proliferation of Weapons of Mass Destruction.

 ML/TF – Money Laundering and Terrorist Financing Crimes.

 Business Sponsor – the person responsible for a business (business area).

 Client – is any party, entity, or organization including, but not limited to individuals, companies, business counterparts, governments, trusts, funds, consultants, legal representatives, or service providers with whom JETPRIVE agrees to initiate a business relationship. The Client may be acting on their own behalf or representing a third party. All requirements must be followed regarding the identification, qualification, and classification of Clients.

 EDD – Enhanced Due Diligence - In-depth background checks used for higher-risk Clients. checks) used for higher-risk Clients.

 FATF – Financial Action Task Force or Financial Action Task Force (FATF) (http://www.fatf-gafi.org).

- KYC – Know Your Customer - Know Your Customer.
- KYP – Know Your Partner – Know Your Partner/Outsourced Service Provider.
- KYE – Know Your Employee – Know Your Employee.
- PEP – Politically Exposed Person - Politically Exposed Person.
- ABR – Risk Based Approach - controls proportional to the identified risk. The higher the greater the risk, the higher the level of control, analysis, approval, and monitoring.
- RBA – Risk Based Approach – see the concept of ABR.
- Employees – Partners, Associates, Employees, Temporary Workers, Contractors/Consultants and Interns of JETPRIVE.
- Third Parties – Partners, Outsourced Service Providers, Suppliers.

3. Roles and Responsibilities

a. All Employees of JETPRIVE

All Employees and Third Parties of JETPRIVE are responsible for conducting business in compliance with the terms of applicable legislation against money laundering and terrorist financing, the Code of Ethics, and this AML/CFT Policy ("AML Policy").

In addition to the specific obligations and responsibilities outlined below, all Employees and Third Parties (when applicable) of JETPRIVE, especially those dealing with Clients, are responsible for ensuring that the requirements of this Policy are respected. Failure to apply and/or observe compliance with such requirements may result in disciplinary measures.

b. Senior Management

The creation, maintenance, and implementation of an effective AML Policy are the responsibilities of senior management through the Compliance Committee, which in turn reports to the Board of Directors of JETPRIVE. The Compliance Committee is responsible for guiding the work of the Compliance team regarding:

- Timely and transparent disclosure of risks related to AML/CFT;
- Dissemination of AML/CFT standards (including this Policy) so that Employees are aware of and comply with all the rules set forth therein; and
- Keeping those responsible regularly informed about the status of their respective AML/CFT Programs and associated risks.

The Board of Directors is responsible for:

- Approving the present AML/CFT Policy; and
- Evaluating and approving, when applicable, the action plan and the respective follow-up report resulting from the Effectiveness Assessment.

c. Audit Committee and Risk Committee

- Informing about the Internal Risk Assessment.

d. Front Office Employees and Relationship Managers

The Front Office Employees and Relationship Managers or their equivalents (i.e.: business areas in general) are responsible for the relationships with their Clients and transactions carried out by them with JETPRIVE. Relationship Managers must be diligent regarding AML/CFT risks, reporting all atypical or suspicious situations to Compliance.

In addition, Front Office Employees are also responsible for involving Compliance in discussions regarding new products and services before their respective launch, as well as in discussions about substantial changes in existing products and services, so that an appropriate assessment of AML/CFT risks can be made.

It is the duty of the Relationship Manager to continuously assess the relationship and activity of the Clients under their responsibility and to inform the Onboarding and Compliance areas about any changes (such as changes related to registration information, financial situation, etc. of the Client) of which they become aware.

e. Onboarding

The Onboarding Area is responsible for managing the process related to the initiation of relationships with Clients at JETPRIVE (together with the Relationship Managers), as well as verifying whether the documentation/information provided by the Client complies with the rules established in this Policy and in the Relationship Opening Procedures. JETPRIVE has procedures aimed at knowing its clients. To this end, the Onboarding Area must:

- Request information that allows identifying and qualifying the Client, aiming at verifying and validating the authenticity of the information received from the Client (e.g.: requesting and analyzing the Client's shareholding structure and/or the identity of the respective beneficial owners, directors, and legal representatives - as determined by law and applicable relationship opening procedures);
- Obtain all necessary information and evidence for verifying the identity of the Client, including their Family Members and Close Persons (when applicable);

In addition, the Onboarding area coordinates the periodic review of the registration databases.

f. Compliance / AML Compliance

The Compliance Area leads JETPRIVE's global efforts in all aspects of AML/CFT. This includes:

- Develop, maintain, supervise and (when applicable) test the implementation of a Global Anti-Money Laundering, Counter-Terrorism Financing, and Proliferation Financing Strategy, including appropriate Policies, Procedures, and Controls to ensure compliance with current laws and regulations;
- Monitor the evolution of AML/CFT legislation and market best practices;
- Promote awareness programs, training, and capacity building for Employees on AML/CFT topics;
- Promote an organizational culture of AML/CFT, encompassing not only Employees but also partners and outsourced service providers;
- Report AML/CFT issues to Senior Management through the Compliance Committee;
- Conduct proper analysis of new relationships, as well as verify that relationships with new Clients have been properly identified in the Onboarding registration process and that periodic reviews have been completed in accordance with AML/CFT Policies and procedures;
- Ensure that all standard checks (background checks) and sanctions-related checks are conducted.
- Classify Clients by risk categories, as defined in the Internal Risk Assessment;
- Assess the risks included in JETPRIVE's Internal Risk Assessment;
- Correct any deficiencies identified in the Effectiveness Assessment.

g. Internal Controls

- Verify compliance with this Policy, AML/CFT procedures, as well as internal controls related to AML/CFT, through the Effectiveness Assessment;
- Identify any deficiencies in AML/CFT processes and routines.

h. Internal Audit

- Monitor the implementation of any action plan resulting from the Effectiveness Assessment and issue a Monitoring Report.

The action plan and the Monitoring Report mentioned above must also be approved by the Audit Committee.

4. Corporate Governance of AML

a. Compliance Committee

The Compliance Committee reports to the Board of Directors of JETPRIVE and aims to assist it in performing its duties related to the adoption of strategies, Policies and

measures aimed at spreading the culture of Compliance, mitigating legal and regulatory risks (including reputational risk) and compliance with the applicable standards to JETPRIVE.

The Compliance Committee coordinates and supervises all Compliance matters, including AML/CFT, meeting at least quarterly or at a shorter frequency if necessary.

The main responsibilities of the Compliance Committee are:

- Formulate the strategies for managing Compliance Risk by supervising the development and implementation of the program;
- Examine situations that expose the Group to Compliance Risks;
- Review the annual budget proposal for the Compliance area;
- Approve the annual work plan;
- Receive and analyze Compliance reports;
- Approve and apply the global Compliance Policies;
- Promote investigations regarding received complaints;
- Analyze other matters related to Compliance; and
- Report to the Board of Directors the activities of the Compliance Committee.

At its discretion, the Compliance Committee may invite other Employees to participate in the meeting.

The details of the responsibilities of the Compliance Committee, including its composition, are available in the Global Risk Management and Control Structure Policy (COMP 003).

b. Board of Directors

The Board of Directors of JETPRIVE has a high degree of commitment to the effectiveness and continuous improvement of this Policy, the procedures, and the internal controls related to AML/CFT. Through the Compliance Committee, it monitors AML/CFT activities and periodically reviews and approves this Policy.

c. Compliance Officers

Each location/business must be under the responsibility of a formally designated Compliance Officer, who must:

- Understand the laws, rules, regulations, and best practices of AML applicable to the location(s) and business(es) under their responsibility;
- Understand the products and services offered by the area(s) under their responsibility;
- Conduct relevant AML/CFT training periodically;
- Hold any certifications/registrations that may be required according to the applicable regulations.

5. Risk-Based Approach

The risk-based approach ("RBA") adopted by JETPRIVE is the main governance tool for the institution's Anti-Money Laundering and Counter-Terrorism Financing process.

The AML Compliance is responsible for the analysis, development, and implementation of the RBA process in the institution, which has been mapped and developed to effectively manage the process of identifying, monitoring, analyzing, and mitigating Money Laundering and Terrorism Financing risks.

The RBA is a methodology used for the process of reviewing the rules and procedures contained in this Policy and other supporting documents.

The RBA is used to define the risk profiles of Clients, JETPRIVE itself (business model, geographical area of operation, among others), operations, transactions, products and services, covering all distribution channels and the use of new technologies, as well as Employees (at the time of hiring), partners, and outsourced service providers.

Internal risk categories are defined to allow for the adoption of enhanced management and mitigation controls for higher risk situations and simplified controls for lower risk situations.

The following are considered in the RBA, but not limited to:

- JETPRIVE's capacity to combat Money Laundering and Terrorism Financing, with the appropriate level of continuous monitoring that should be applied based on the risk presented by a specific Client, employee, or Third Party;
- The level of Money Laundering and Terrorism Financing risk that the Client presents to JETPRIVE;
- Risk by the type of client or third party, such as government entities, unregulated funds, trusts, foundations, among others;
- Function of the business activity, such as the assessment of activities more susceptible to illegal exploitation (Casinos, Betting Houses, and other Gambling-related Activities, religious and charitable entities, gas stations, among others), and the creation of a list of "Prohibited Activities";
- Risk to JETPRIVE's reputation;
- Risk by product, service, or activity, in addition to operations (foreign exchange, credit, pensions, insurance, stock market);
- Financial impacts;
- Reputational impacts;
- Impacts related to Environmental, Social and Governance (ESG);
- Distribution Channels;
- Trading and registration environments;
- Relevant media for AML;

- PEP - Politically Exposed Persons;
- SCAP - Clients residing in sensitive countries;
- SIAP - economic activities considered sensitive;
- Suitability Profile;
- Accounts opened by power of attorney;
- Geographic Factors, such as border cities;
- Position greater than the declared assets;
- Number of alerts in monitoring;
- Shareholder of structured funds;
- Client position - Private Clients;
- Dual citizenship / Foreigner;
- Time for registration review;
- Account registered for a Digital Bank;
- Judicial Blocking/Breach of bank secrecy;
- Reports made to COAF;
- Incomplete registration information;
- Identification of vulnerable populations.

Despite the harmonization between the deadlines for updating the investment profile and updating the registration data of clients, as provided in CVM Resolution No. 30/21 and CVM Resolution No. 50/21, JETPRIVE chooses to maintain a period of 24 (twenty-four months) for reviewing the information related to its clients' profiles, since, in JETPRIVE's understanding, the risk appetite in the securities market does not necessarily have a direct relationship with the propensity to engage in practices for money laundering purposes.

6. Internal Risk Assessment

The institution's ABR is evaluated through an internal process called Internal Risk Assessment, which contains the parameters and guidelines that underpin JETPRIVE's ABR, which are formalized in a specific document.

The Internal Risk Assessment document is approved by the AML/CFT Director and forwarded for the knowledge of the Compliance Committee, the institution's Risk Committee, the Audit Committee, as well as the Board of Directors. This document is reviewed every two years; however, if there are significant changes in the parameters and guidelines documented therein before the review period, the Assessment is forwarded for the knowledge of the aforementioned bodies.

The Statutory Director responsible for complying with the standards established by current regulations must prepare a report related to the Internal Risk Assessment by March 31 of the year following the report's base date.

The document that encompasses the Internal Risk Assessment is the responsibility of Compliance.

7. Effectiveness Assessment

The Internal Controls area must assess, in accordance with current regulations, the effectiveness of the Internal Risk Assessment, as well as this Policy and the procedures linked to it. This assessment must occur annually through a specific methodology adopted for verifying all related to AML/CFT procedures and must be formalized in the Effectiveness Report, by the last business day of March of the year following the base date of December 31 of the effectiveness assessment.

As a general rule, the Effectiveness Test must contain, among other determinations, information that describes: (i) the methodology adopted in the effectiveness assessment; (ii) the tests applied; (iii) the qualifications of the evaluators; and (iv) the deficiencies identified. In addition, it must contain, at a minimum, the assessment: (i) of the procedures aimed at knowing clients, including the verification and validation of client information and the adequacy of registration data; (ii) of the monitoring, selection, analysis, and communication procedures to Coaf, including the effectiveness assessment of the parameters for selecting operations and suspicious situations; (iii) of the governance of the Anti-Money Laundering and Counter-Terrorism Financing Policy; (iv) of the measures to develop the organizational culture aimed at Preventing Money Laundering and Terrorism Financing; (v) of the periodic training programs for personnel; (vi) of the procedures aimed at knowing Collaborators, partners, and outsourced service providers; and (vii) of the actions to regularize findings from internal audits and supervision by the Central Bank of Brazil.

An action plan aimed at addressing any deficiencies identified through the effectiveness assessment must be developed after the issuance of the Report, when applicable. The monitoring of the implementation of this action plan must be documented through a follow-up report, which is the responsibility of Internal Audit.

8. New Products and Services or Substantial Changes to Existing Ones

Following best market practices, rules, and regulations on AML/CFT, a senior Compliance representative must always be involved in the discussion and approval of new products and services, as well as in the eventual use of new technologies, so that they can assess and analyze potential AML/CFT risks in advance. It is emphasized that the assessment and analysis must be conducted before the launch/approval of these. For the same reason, it is also mandatory for a senior Compliance representative to be involved in discussions regarding any substantial changes to existing products and services.

9. Know Your Customer (KYC) Guidelines

The institution considers the beginning of the relationship the best opportunity to understand the Client and their business and, consequently, mitigate potential AML/CFT risks. Therefore, JETPRIVE has developed global standards to know its Clients, with proper identification, qualification, and classification of them, their ultimate beneficiaries, and administrators in the case of Individual Clients.

Legal and representatives, in the case of Individual Clients, furthermore, the global rules encompass the verification and analysis of the source of funds and the parties involved in a transaction.

The established rules apply to all JETPRIVE Clients. From the perspective of AML/CFT, as mentioned at the beginning of this Policy, a Client is any party, entity, or organization including, but not limited to individuals, companies/businesses, business counterparts, governments, trusts, funds, consultants, legal representatives, or service providers with whom JETPRIVE agrees to initiate a business relationship. The Client may be acting on their own behalf or representing a third party. All requirements must be followed regarding the identification and verification of each Client.

The tools that make up the AML procedures allow JETPRIVE to conduct a risk-based assessment of its Clients, considering the history, professional activity, source of wealth and income as well as the expected transactional activity. To establish the "risk profile" associated with Clients and/or transactions, JETPRIVE assesses the activity and characteristics of the Client/transaction to conclude in which areas the likelihood of potentially suspicious or illegal situations may be higher. Based on this assessment, we determine the information, documents, and type of monitoring required for the Client. All parameters and guidelines used for classifying the Client's risk profile, in line with the ABR, are included in the Internal Risk Assessment.

Whenever the procedure to be applied is not clear, the issue should be forwarded to AML Compliance.

In summary, the principle of "Know Your Customer" is applied to know the true identity of the Client (up to the level of the ultimate beneficiary and/or controller whenever required by law and/or best market practices), their business profile, and their intentions regarding how to operate and use the banking products offered by JETPRIVE. For this purpose, it is necessary:

- Obtain the supporting/legal documents required by law; and
- Apply a risk-based approach to obtain sufficient information about each type of Client according to their respective situation and risk profile.

The obtaining and processing of the above data constitute the criteria for assessing the overall profile of the Client. Specific procedures will prevail whenever the applicable regulation is more stringent than the requirements of this Policy, and any conflicts/exceptions regarding this Policy must be evaluated by AML Compliance.

a. Identification and Verification of Clients' Identity

JETPRIVE seeks to identify and know its Clients (including, whenever applicable, their ultimate beneficiaries, controllers, representatives, attorneys, and agents – when applicable), applying consistent processes across various business segments and locations. Local laws and regulations regarding the type of documents and information necessary for satisfactory identification and verification of Clients, as well as the types of assessments or monitoring conducted, must always be observed as a minimum required standard.

Each location must establish, as part of its AML Policy, procedures to verify the identity of new Clients. Provided that the referred procedures include obtaining, verifying, and validating the authenticity of client identification information, including, if necessary, by cross-referencing this information with that available in public and private databases.

This Policy, together with the Know Your Customer Procedures, establishes the identification and verification requirements that must be applied to all potential Clients before opening an account or relationship. The identification requirements are as follows:

- Obtaining information about the Client's identity;
- Verification of identity;
- Establishment of the Client's ownership structure;
- Confirmation of the Client's intent and authorization to do business with JETPRIVE;
- Verification of any specific country requirement that needs to be addressed;
- Confirmation of the Client's business activities and the source of their funds.

The fundamental principle governing the KYC procedure is that JETPRIVE must be convinced that it has established and documented the true identity of the Client (up to the level of the ultimate beneficial owner when required by applicable regulations and/or best market practices) and that it understands their main activity and the source of their funds.

b. Client Qualification

Once identified and the minimum registration data verified, Clients are qualified, meaning that all characteristics that make up their risk profile are raised, so that it is possible to classify their risk at the end.

Among the characteristics that make up the profile of each Client are the geographical location, the risk level of the product or service they will operate, the assessment of possible negative media involving the Client, among other characteristics outlined in the Internal Risk Assessment.

c. Politically Exposed Person (“PEP”)

In addition to the characteristics that assist in the qualification of Clients, JETPRIVE has procedures that allow for the qualification of Clients, their representatives, family members, or close associates of Clients as Politically Exposed Persons (“PEP”).

A PEP, for the purposes of current regulations, is considered to be a person who holds (or has held in the last 5 years) an important or prominent public position, namely, holders of elective mandates in the Executive and Legislative Powers of the Union, those occupying positions in the Executive Power of the Union, including, but not limited to:

a. holders of elective mandates in the Executive and Legislative Powers of the Union;

b. os ocupantes de cargo, no Poder Executivo da União, de:
    i. Ministro de Estado ou equiparado;
    ii. Natureza Especial ou equivalente;
    iii. presidente, vice-presidente e diretor, ou equivalentes, de entidades da administração pública indireta; e
    iv. Grupo Direção e Assessoramento Superiores (DAS), nível 6, ou equivalente;
c. os membros do Conselho Nacional de Justiça, do Supremo Tribunal Federal,
d. sos Tribunais Superiores, dos Tribunais Regionais Federais, dos Tribunais Regionais do Trabalho, dos Tribunais Regionais Eleitorais, do Conselho Superior da Justiça do Trabalho e do Conselho da Justiça Federal;
e. os membros do Conselho Nacional do Ministério Público, o Procurador-Geral da República, o Vice-Procurador-Geral da República, o Procurador-Geral do Trabalho, o Procurador-Geral da Justiça Militar, os Subprocuradores-Gerais da República e os Procuradores Gerais de Justiça dos Estados e do Distrito Federal;
f. os membros do Tribunal de Contas da União, o Procurador-Geral e os Subprocuradores-Gerais do Ministério Público junto ao Tribunal de Contas da União;
g. os presidentes e os tesoureiros nacionais, ou equivalentes, de partidos políticos;
h. os Governadores e os Secretários de Estado e do Distrito Federal, os
i. Deputados Estaduais e Distritais, os presidentes, ou equivalentes, de entidades da administração pública indireta estadual e distrital e os presidentes de Tribunais de Justiça, Tribunais Militares, Tribunais de Contas ou equivalentes dos Estados e do Distrito Federal; e
j. os Prefeitos, os Vereadores, os Secretários Municipais, os presidentes, ou
k. equivalentes, de entidades da administração pública indireta municipal e os Presidentes de Tribunais de Contas ou equivalentes dos Municípios.
l. chefes de estado ou de governo;
m. políticos de escalões superiores;
n. ocupantes de cargos governamentais de escalões superiores;
o. oficiais-generais e membros de escalões superiores do Poder Judiciário;
p. executivos de escalões superiores de empresas públicas; ou
q. dirigentes de partidos políticos.
r. dirigentes de escalões superiores de entidades de direito internacional público ou privado.

Familiares e Estreitos Colaboradores das pessoas acima definidas também são consideradas como PEPs, isso inclui:

- Familiar, os parentes, na linha reta ou colateral, até o segundo grau, o cônjuge, o companheiro, a companheira, o enteado e a enteada; e
- Estreito colaborador:
  a) pessoa natural conhecida por ter qualquer tipo de estreita relação com um PEP, inclusive por:
  1. ter participação conjunta em pessoa jurídica de direito privado;
  2. figurar como mandatária, ainda que por instrumento particular da pessoa mencionada no item 1 (acima); ou

3. to have joint participation in arrangements without legal personality; and b) a natural person who has control over legal entities or arrangements without legal personality, known to have been created for the benefit of PEP.

Compliance is responsible for coordinating the approval of accounts or relationships involving Politically Exposed Persons. Each location is responsible for establishing local procedures to properly identify and approve the relationship with Politically Exposed Persons.

Business relationships involving Politically Exposed Persons, including their Family Members and Close Associates, will always be considered high risk. These and/or other specific high-risk factors are also defined in the Internal Risk Assessment.

d. Client Classification

Compliance is responsible for defining the client acceptance procedures, including the description of the types of relationships considered more susceptible to present higher risks. Clients classified as High Risk (HRN - High Risk Name) undergo enhanced due diligence and monitoring, according to the risk-based approach adopted by JETPRIVE. To determine the client's risk, risk factors such as country, industry, type of client, family members and close relationships, product and transaction, or other types of risks are considered in the analysis. All parameters and guidelines used for risk classification, in line with ABR, for both Clients and Collaborators and third parties, are included in the Internal Risk Assessment and procedures, an internal document that is the responsibility of Compliance.

It is important to note that the classification of Clients is based on their risk profile as well as their business nature. Furthermore, this classification is dynamic and is changed whenever there are changes in the risk profile and business nature of the Clients.

e. Prohibited Relationships

Business units may not engage in transactions that may be apparent or linked to Money Laundering, Terrorist Financing, or other illegal activities. Specifically, the following types of business relationships are prohibited:

- Individuals or entities known/suspected of supporting or engaging in activities with criminal organizations, including terrorist activities or terrorist organizations;
- Shell banks or financial institutions that offer and/or provide services to shell banks;
- Unregulated Money Transfer Companies;
- Individuals or entities prohibited by law or applicable regulations, including sanctions and embargoes.
- Institutions designated as having "Primary Money Laundering Concern" by any recognized international body or authorities or government of a FATF member country, including the “Specially Designated Banks” subject to a final order under Sec. 311 (US PATRIOT ACT).

All questions regarding prohibited relationships must be directed to AML Compliance before taking any action.

f. Acceptance of assets or funds

No fund or asset may be received by JETPRIVE before proper identification and verification have been completed and the relationship approved (or exception granted) by Compliance. Failure to comply with this requirement may result in the return and/or blocking of funds/assets.

The specific procedures related to the KYC Process are described in the document Know Your Customer Procedures.

10. Know Your Employee (KYE) Guidelines

All JETPRIVE Employees, at the time of their hiring, including the final candidates from the selection processes, undergo Compliance evaluation to identify facts that may discredit the candidate and, consequently, pose a risk to the institution's reputation or, additionally, risks of AML/CTF, corruption, among others.

Upon starting their relationship with JETPRIVE, Employees are properly trained for AML/CTF purposes and must, mandatorily, undergo training annually. Additionally, they receive Compliance alerts periodically to reinforce internal rules.

JETPRIVE monitors the personal investments of its Employees through a specific form for declaring these investments. Therefore, it is possible to monitor potential atypical behaviors of the Employee, as well as mitigate the risk of possible conflicts of interest between the Employee and the institution's business. Additionally, it monitors all external activities of employees, aiming to similarly avoid any potential conflicts of interest, as well as monitoring the behavior of Employees.

11. Know Your Partner (KYP) Guidelines

All Partners, before having any relationship with JETPRIVE, must undergo Due Diligence analysis by the Compliance area. Additionally, all Suppliers and Service Providers undergo Compliance analysis through the Background check system before the relationship.

Research checks are intended to ensure that, before accepting the Third Party, JETPRIVE identifies and analyzes the negative information available about it and its controllers.

Background Checks must be conducted on the names of all Suppliers (up to the level of the ultimate beneficiary if applicable, according to regulatory requirements and best market practices); and

The AML area is responsible for conducting the verification of Supplier surveys. The relationship should not proceed until the verification of the surveys is completed.

The Internal Risk Assessment discusses the risk classification of Third Parties; furthermore, Compliance has specific procedures for the KYP process, in addition to this Policy.

12. Registration, Monitoring, Selection, and Analysis of Operations

To comply with the requirements of current legislation and regulations aimed at combating financial crimes as well as to meet JETPRIVE's internal policies, the transactions carried out by all Clients, including Clients holding checking accounts, brokerage account holders, and investors in investment funds managed by JETPRIVE, even if presented to JETPRIVE by third parties among others, are monitored with the aim of identifying transactions that may constitute indications of AML/CTF crimes.

Transactions are considered suspicious if they present, for example, the following characteristics:

- Show any signs of the client's involvement in money laundering crimes;
- Have no economic or legal basis;
- Are not habitually carried out by the client and do not present any reasonable cause for a sudden change in pattern; and/or
- Raise any suspicion that JETPRIVE is dealing with resources from criminal activities.

The operational processes at JETPRIVE have been created so that, as a rule, all transactions of its clients are carried out through their accounts, for all contracted products. The detailed procedures regarding the registration of operations and financial services, as well as the monitoring, selection, and analysis of operations and suspicious situations are in the Transaction Monitoring Procedures Manual.

a. Communication of Operations to COAF

JETPRIVE must report to the Financial Activities Control Council (“COAF”) the operations or situations suspected of Money Laundering and Terrorism Financing of Clients, prospects, or operations carried out by non-clients. The decision to report the operation or situation to COAF must be based on the information contained in the Client's, prospect's, or non-client's file, and must be recorded in detail in the respective file.

Communications must be made by the next business day following the decision to report.

Cases involving initially suspicious transactions and the AML/CTF area understand the need for communication, this will proceed with the report to the Financial Activities Control Council (“COAF”) and will subsequently inform the Compliance Committee of the respective report.

b. Sanctions Imposed by Resolutions of the United Nations Security Council (UNSC)

The monitoring of sanctions imposed by UNSC Resolutions consists of daily screening where updates to the UNSC list are compared with the institution's registry database (clients, assets, partners, employees), in addition to incoming and outgoing transactions (TED, DOC, SWIFT, PIX, among others).

There is also monitoring of alerts from the federal government and other authorities that may contain determinations of unavailability of assets of individuals and legal entities, and the national designation of individuals investigated or accused of terrorism, its financing, or related acts.

Furthermore, in compliance with current regulations, JETPRIVE has a procedure to immediately report the unavailability of assets and attempts to transfer them related to individuals, legal entities, or entities sanctioned by resolutions of the United Nations Security Council or by designations of its sanctions committees, to:

I - Central Bank of Brazil, through the BC Correio system; II - Ministry of Justice and Public Security (via email csnu@mj.gov.br); and III - Council for the Control of Financial Activities (COAF).

Finally, it is noteworthy that JETPRIVE does not accept clients listed in the aforementioned list.

c. Retention, Backup, and Recovery of Data related to the processes of AML/FTP

JETPRIVE has a specific Policy for Retention, Backup, and Recovery of Data, which details the subject. The document states that JETPRIVE must retain for a minimum period of 10 years: (i) - the information collected in procedures aimed at knowing the clients (AML KYC), counted from the first day of the year following the end of the relationship with the client; (ii) the information collected in procedures aimed at knowing employees, partners, and outsourced service providers, counted from the date of termination of the contractual relationship; (iii) the information and records of all operations carried out, products and services contracted, including withdrawals, deposits, contributions, payments, receipts, and transfers of funds; and (iv) the file related to the analysis of operations and situations selected through monitoring and selection procedures.

13. Training, Education, and Organizational Culture of AML/FTP

All employees, regardless of their roles and areas of activity, receive practical and theoretical training aimed at maximizing their professional development.

The formal training program includes practices of in-person training, online training, courses, and external conferences. Such training is provided and required depending on the

position and role of the employee, always aiming to empower them according to their activity and level of seniority.

All employees are required to complete Compliance training, including the annual AML/CFT training. Such training is mandatory regardless of the employee's area of activity and their level of seniority.

In the training process, Compliance Alerts are also used, sent periodically by Compliance, which address relevant topics on AML/CFT matters. Additionally, monitors in common office spaces and the screensavers on employees' computers are used as channels to reinforce communication on these aspects.

Furthermore, there are targeted trainings, personalized according to the activity performed by each business area, so that the employee has practical examples and can relate AML/CFT practices to their daily activities in the institution.

Whenever possible, we invite law firms or specialists from regulatory bodies to give lectures in the most sensitive business areas.

Annually, the Compliance area conducts specific AML/CFT training for the Executive Committee.

In addition, each area has initiatives aimed at training and updating employees, promoting lectures on various topics.

It is worth noting that such training is established across all JETPRIVE locations. Special attention should be given to the training of employees who deal directly with the Client and to employees in control functions with responsibilities in the AML/CFT Policy, including the staff of correspondents in the Country.

The AML/CFT Training Program must be repeated annually, and may use complementary solutions, for example:

- E-learning platform through which all employees will have access to the content of the AML/CFT training;
- In-person training offered by senior Compliance employees to complement the e-learning;
- Training by external consultants for employees with direct client relationships, employees in the Registration area, Compliance team, and for senior management.

Finally, regarding Third Parties, annual training (in-person or via Live) is provided for all Third Parties. Additionally, all are subject to receiving periodic Compliance Alerts.

14. Monitoring of this Policy

JETPRIVE adopts various internal control mechanisms to monitor compliance with laws, regulations, and internal standards (including this Policy). Various areas of internal controls, such as Compliance itself, Internal Audit, and Operational Risk, monitor and test the compliance of processes concerning the requirements of the various applicable regulations. Evaluation reports are issued and kept on file for a period of at least five years.

15. Record Keeping

All locations must, at a minimum, maintain records of customer identification data obtained through their Customer Identification Programs, including account files and related correspondence for the period set by applicable local law or regulation.

The names of Customers and former Customers must be kept in a format or medium that can be electronically searched.

The maintenance of records of suspicious activity or transaction reports must comply with applicable laws and regulations.

16. Exceptions to the Policy

There may be a justifiable need for exceptions to this AML Policy. However, the primary principle is that such exceptions are only granted if they comply with legal and regulatory requirements and with the overarching goal of the AML Policy.

17. Disciplinary Measures

Employees who are negligent, omit, or collude with Money Laundering and Terrorism Financing crimes are subject to disciplinary measures from JETPRIVE, as well as the application of administrative and civil sanctions by the authorities, regardless of the activity they perform in the institution. It is the responsibility of each Employee to comply with the laws and regulations regarding the crimes discussed here and, if they become aware of suspicious operations, to immediately inform Compliance.