

Version 2024.01 October 21, 2024

**ANTI-MONEY LAUNDERING AND COUNTER-TERRORISM
FINANCING POLICY
OF
MIRADOURO ASSET MANAGEMENT LTDA.**

This Policy aims to describe the principles and procedures adopted by MIRADOURO ASSET MANAGEMENT LTDA. ('Miradouro') in the conduct of its activities for purposes of preventing and combating money laundering, pursuant to applicable laws and regulations.

1. Brief History

The crime of 'money laundering' began to be defined in the 1980s in the context of combating drug trafficking.

The FATF-GAFI (Financial Action Task Force / Groupe d'Action Financière), one of the main international reference bodies in combating money laundering and the primary agent for integrating and coordinating international policies in this area, was created in 1989 at the initiative of the G-7 countries and the European Union.

In Brazil, the first law specifically addressing the crime of 'money laundering' dates from 1998 (Law No. 9,613/98), which was amended by Law No. 12,683/12. In the same year, COAF (Financial Activities Control Council) was also created, a government body specifically dedicated to combating money laundering. The crime of money laundering is classified, under Brazilian legislation, as a predicate offense, meaning it depends on an underlying illegal conduct, and is punishable by up to 10 (ten) years of imprisonment, with the penalty potentially increased if criminal organizations are involved. The law also establishes various control mechanisms and reporting duties, as well as a special supervisory body for such violations.

2. Legal Basis

Money laundering activities have been subject to repression by national and international authorities, which, through specific legislation and oversight, have been combating the problem and adopting preventive measures to prevent its escalation.

Brazil has distinguished itself internationally for the actions implemented to combat and prevent money laundering.

In addition to Law No. 9,613/98, as amended by Law No. 12,683/12, other rules governing 'Money Laundering' include: (i) BACEN Circular No. 3,461 and other BACEN regulations; (b) CVM Resolution No. 50 and other notices and communications; and (c) COAF Resolutions and other regulatory instruments.

Recently, Law No. 12,846, of August 1, 2013, which entered into force in February 2014, was enacted to combat unlawful acts against Brazilian and foreign public administrations. Said Law No. 12,846/13 imposes civil and administrative liability on companies for acts committed by their employees and executives involving crimes against the public administration.

Law No. 12,846 establishes various types of penalties, ranging from fines of up to 20% of the company's revenue, forfeiture of property, suspension of activities, and even compulsory dissolution of the company.

Miradouro is committed to complying with all Brazilian legislation and to taking all possible measures to prevent Miradouro or any of its subsidiaries, agents, Employees, or staff from acting in violation of Brazilian law. Brazilian anti-corruption law is in compliance with international anti-corruption standards (Groupe d'Action Financière/Financial Action Task Force – 'GAFI/FATF').

3. General Theory

Under the terms of Law No. 9,613/98, it is a crime to conceal or disguise the nature, origin, location, disposition, movement, or ownership of assets, rights, or values derived, directly or indirectly.

Thus, money laundering can be considered the process by which a criminal transforms resources from illegal activities into assets with an apparently lawful origin.

'Money laundering' is not characterized by a simple act, but rather by a process consisting essentially of three stages:

- (i) Placement;
- (ii) Layering, Diffusion, or Concealment; and
- (iii) Integration.

At times, the three stages mentioned above may be resolved in a single transaction, but in general, they are more likely to appear in well-separated forms, one at a time and over a certain period.

The three stages can be explained as follows:

During the placement stage, the form of the funds must be converted to conceal their illicit origins. Once funds enter the financial system, the placement phase is complete. Within the scope of Miradouro, this is the phase that must be combated to prevent the entry of illicit resources.

In Layering, Diffusion, or Concealment, the criminal attempts to further disguise the trail linking the assets to the criminal activity. These transactions must be disguised to be mixed with the numerous legitimate operations that occur every day.

The Integration stage is the criminal's ultimate goal. At this phase, the criminal moves the assets into common economic activities (typically commercial investments, real estate, or purchases of luxury goods).

4. Precautions and Guidelines

According to international bodies, there are certain recommended practices to avoid involvement in money laundering operations. Thus, the following guidelines must be observed:

- (i) Refuse transactions of any kind involving cash receipts (sales, services, financing);
- (ii) Do not make cash payments;
- (iii) Always use receipts that transit through the banking system (TED, PIX);
- (iv) Do not execute any commercial or financial transaction on behalf of third parties unless it is transparent, justified, and solid, and carried out through banking channels;
- (v) Refuse transactions with persons or entities that cannot prove the origin of the funds involved and are not well known;
- (vi) Refuse transactions for large amounts that do not have a well-defined origin and a sound economic, commercial, and financial rationale;

- (vii) Refuse suspicious transactions or those that appear 'miraculously' and/or seem 'too good to be true'; and
- (viii) Avoid complex international financial transactions involving many money movements across different countries and/or between different banks.

It should be noted that, within the scope of Miradouro, cash deposits are expressly prohibited.

5. Know Your Customer

The Know Your Customer (KYC) concept relates to the identification of the Client, which must be established before completing the transaction. If the client refuses or makes it difficult to provide the required information, Miradouro must not accept them as a Client.

The best identification documents are those whose lawful acquisition is difficult.

Miradouro's client registration procedures must be widely disseminated to minimize legal risks and risks inherent in money laundering crimes.

To register as a Miradouro Client, the following minimum documents are required, pursuant to Annex B of CVM Resolution 50:

I – if a natural person:

- a) Full name;
- b) Date of birth;
- c) Place of birth;
- d) Nationality;
- e) Marital status;
- f) Mother's name;
- g) Identification document number and issuing authority;
- h) Individual taxpayer registration number (CPF/MF);
- i) Name and CPF/MF of spouse or domestic partner, if applicable;
- j) Place of residence (street, complement, neighborhood, city, state, and zip code) and phone number;
- k) Electronic address for correspondence;
- l) Professional occupation;
- m) Name and CNPJ of the employer, when applicable;
- n) Updated information on income and financial situation;
- o) Information on the client's profile, as per specific regulation on suitability verification, when applicable;
- p) Whether the client operates on behalf of third parties (fund and portfolio managers);
- q) Whether the client authorizes or not orders transmitted by attorney-in-fact;
- r) Place of residence of attorneys-in-fact, if any, and whether they are considered politically exposed persons;
- s) Qualifications of attorneys-in-fact and description of their powers, if any;

- t) Dates of registration updates;
- u) Client signature;
- v) Whether the client is considered a politically exposed person;
- w) Copies of the following documents: (1) identity document; and (2) proof of residence or domicile; and
- x) Copies of the following documents, if applicable: (1) power of attorney; and (2) identity documents of attorneys-in-fact and their CPF/MF numbers.

II – if a legal entity, except legal entities with securities admitted to trading on an organized market:

- a) Corporate name or trade name;
- b) Names and CPF/MF of direct controlling shareholders, or corporate name and CNPJ of direct controllers, indicating whether they are politically exposed persons;
- c) Names and CPF/MF of directors;
- d) Names and CPF/MF of attorneys-in-fact, if applicable;
- e) CNPJ registration number;
- f) Full address;
- g) Phone number;
- h) Electronic address for correspondence;
- i) Updated information on average monthly revenue for the past 12 months and financial situation;
- j) Client profile information, per applicable suitability regulation;
- k) Corporate name and CNPJ of controlling, controlled, or affiliated companies, when applicable;
- l) Whether the client operates on behalf of third parties;
- m) Whether the client authorizes orders transmitted by representative or attorney-in-fact;
- n) Qualifications of representatives or attorneys-in-fact and description of their powers;
- o) Dates of registration updates;
- p) Client signature;
- q) Copies of: (1) corporate documents duly updated and registered; and (2) corporate acts indicating the company's directors;
- r) Copies of: (1) power of attorney; and (2) identity documents of attorneys-in-fact and their CPF/MF numbers; and
- s) Full address of attorneys-in-fact, if any, and whether they are considered politically exposed persons.

III – if a legal entity with securities admitted to trading on an organized market:

- a) Corporate name; b) Names and CPF/MF of directors; c) CNPJ; d) Full address; e) Phone number; f) Electronic address for correspondence; g) Dates of registration updates; and h) Client's agreement with the information.

IV – if investment funds registered with the CVM:

- a) Name; b) CNPJ; c) Full identification of the fiduciary administrator and manager; and d) Dates of registration updates.

V – in other cases:

- a) Full client identification; b) Full identification of representatives and administrators; c) Updated financial and asset information; d) Client profile information; e) Whether the client operates on behalf of third parties; f) Dates of registration updates; and g) Client signature.

For the KYC analysis of Legal Entities, the corporate control chain must be identified up to the natural person(s) who ultimately hold control over the client legal entity, referred to as the 'Ultimate Beneficial Owner.'

Regarding the identification of Ultimate Beneficial Owners, from a 10% representation of the share capital, it is necessary to obtain the registration data of persons related to the Legal Entity.

For Legal Entities incorporated as publicly held companies or non-profit entities, the natural persons exercising control of the company must be identified regardless of their shareholding percentage.

In addition to obtaining the documents described above, information searches on the respective Client must be conducted on the following websites/bodies:

- (i) Google (www.google.com.br);
- (ii) Federal Revenue Service (www.receita.fazenda.gov.br);
- (iii) SERASA;
- (iv) United Nations Security Council (<https://www.un.org/securitycouncil/content/un-sc-consolidated-list>);
- (v) Other research websites listed in Annex I of this Policy.

In addition to registration procedures, all Employees are advised to pay special attention to the following types of Clients:

- (i) Clients of questionable integrity or honesty;
- (ii) Clients who refuse or make it difficult to provide required information or documentation;
- (iii) Clients associated with commerce known to be of dubious origin or whose revenue attributed to the business is initially incompatible with the type of business;
- (iv) Clients who show disregard or are unconcerned about redemption dates, fees, and charges, resulting in losses in returns;
- (v) For legal entities, the production line should be observed, analyzing facilities, production volume, and equipment;
- (vi) For legal entities, whenever possible, it is important to visit Clients at their commercial offices to ascertain the nature of their activities and sources of revenue;
- (vii) Clients who offer bribes or gratuities for transactions to be carried out; and
- (viii) Elderly or naive client accounts controlled by non-family members.

After obtaining and analyzing all documentation provided, the Risk and Compliance Department will prepare an analysis report containing the information obtained, conclusions regarding the analysis, and the internal risk classification of the Client (1 – Low Risk; 2 – Medium Risk; and 3 – High Risk).

6. Counterparties

As set forth in Circular Letter No. 5/2015/SIN/CVM, even though Miradouro only operates in exchange markets, it cannot be exempt from maintaining its own routines for verifying suspicious transactions reportable to COAF.

Thus, it is not possible to endorse the argument that money laundering would be impossible for exchange transactions (given the infeasibility of determining the counterparty of transactions), either because (i) directing the counterparty of transactions is indeed possible in certain circumstances (e.g., for very low-liquidity securities), or because (ii) we already experience the sending of substantiated and consistent communications to COAF by obligated parties involving exchange transactions.

7. Verification, Registration, and Monitoring Process

Miradouro adopts this Policy, under which the following procedures will be carried out for client verification and registration:

- I – validate client registration information and keep such information updated;
- II – apply and evidence verification procedures proportional to the risk of using its products, services, and distribution channels for money laundering, terrorism financing, and proliferation financing of weapons of mass destruction;
- III – monitor operations and situations to permanently know its active Clients;
- IV – take all necessary measures and due diligence for the identification of the ultimate beneficial owner;
- V – classify active Clients by degree of money laundering or terrorism financing risk (low, medium, and high risk);
- VI – regarding active clients classified as PEP – Politically Exposed Persons or non-profit organizations: a) continuously and differentially monitor the business relationship; b) differentially monitor relationship initiation proposals; and c) identify clients who, after the start of the relationship, come to fall into this category;
- VII – in situations of higher risk of money laundering or terrorism financing involving active Clients: a) make additional efforts to identify the origin of resources involved; and b) more rigorously monitor the evolution of the relationship;
- VIII – identify possible clients and their respective ultimate beneficial owners who hold assets, values, and rights of possession or ownership related to the situations provided for in Articles 27 and 28 of CVM Resolution 50.

8. Tax Havens

For all purposes provided for in legal provisions, countries or dependencies that do not tax income or tax it at a rate lower than 20%, or whose internal legislation imposes secrecy regarding the corporate composition or ownership of legal entities, are considered tax havens in accordance with applicable tax legislation.

It should be noted that, in addition to Clients linked to the aforementioned countries, all suspicious cases must be immediately reported to the Risk and Compliance Department for appropriate action.

Given that tax havens are commonly used for money laundering crimes, when the Client is headquartered in such a jurisdiction, the Risk and Compliance Department must conduct a detailed investigation of the documentation presented for Client registration, and must ensure that there are no indications of practices that could characterize such crimes in the Client's relationship with Miradouro.

9. Suspicious Transactions

In addition to the process of verifying clients and the origin of resources to combat money laundering, the following situations will be considered suspicious and must be reported for analysis by the Risk and Compliance Department:

- (i) Resistance to providing information necessary for the start of a relationship or for registration updates, provision of false information, or provision of information that is difficult or costly to verify;
- (ii) Irregularities related to client identification (Know Your Client) procedures and transaction registration required by current regulations;
- (iii) Inducement of Miradouro professionals to not follow established procedures for transactions (buying and selling);
- (iv) Purchase and sale of assets for persons who are recognized as having committed crimes or facilitated terrorist acts;
- (v) Purchase and sale of assets outside 'normal' market standards;
- (vi) Purchase and sale of assets generating high returns but executed through intermediaries.

Furthermore, examples of atypical Client behavior that must be immediately reported to the Risk and Compliance Department include:

- (i) A public official who opens an account in a family member's name and begins making large deposits inconsistent with known sources of legitimate family income;
- (ii) Threats to an employee, attempting to dissuade them from filing required reports;
- (iii) Suggestions of payment of bonuses to an Employee;
- (iv) Apparent hidden purpose or unusual behavior. For example: refusal to obtain a higher interest rate on an account with high available funds;
- (v) Incompatibility of transactions with the asset situation; or
- (vi) Behavioral fluctuations in volume, frequency, and type.

10. Registration, Monitoring, and Reporting

Clients and transactions will be duly registered in accordance with the procedures previously described in this Policy and in CVM Resolution 50.

Additionally, Miradouro will register and monitor transactions to identify 'unusual' behavior, with special attention to:

- (i) Transactions of clients not residing in Brazil and incorporated as trusts;
- (ii) Investors with large fortunes managed by financial institutions;
- (iii) Politically exposed persons;
- (iv) Non-profit organizations.

If suspicious activity is detected, Miradouro, through the Risk and Compliance Department, will report it to the Financial Activities Control Council (COAF).

The communication with COAF will be made through a detailed individual report, containing:

- (i) Start date of the relationship with the client, employee, or third party involved in the transaction or situation;
- (ii) Explanation of indications of irregular activities;
- (iii) Description and/or details of the transactions and their characteristics;
- (iv) Presentation of information obtained through this Policy's activities, as well as details of the behavior of the reported person;
- (v) Conclusion of the analysis.

Communications must be made: (i) to the CVM within 24 hours of concluding the analysis that characterized the atypicality of the transaction, the respective proposal, or even the atypical situation detected, as a suspicion to be reported to COAF; and (ii) to BACEN: institutions must report to COAF suspicious ML/TF operations or situations pursuant to BACEN regulations.

Good-faith communications will not result in civil or administrative liability for the communicating parties. The communications made are confidential and must be restricted to employees involved in the analysis process. All records supporting the communication, or the decision not to communicate, must be archived for five years.

11. Consequences in the Event of Involvement

The dangers of involvement in money laundering operations, whether voluntary or involuntary, are quite evident. Persons involved in money laundering processes may be suspected of being accomplices of criminals. They may be prosecuted for these crimes and/or for others specifically related to 'money laundering.'

To avoid conviction, they must, at a minimum, demonstrate that they took all possible precautions and measures to ascertain the nature of the transactions and the origin of the funds.

Therefore, it is necessary to follow a due diligence process before engaging in new and/or potentially suspicious transactions.

In addition to the risks of involvement in criminal activities, there are other more practical risks, such as:

- (i) Money of illicit origin may be seized or blocked, creating serious financial and economic problems; and
- (ii) It is worth noting the strong reputational risk associated with involvement in money laundering operations, even if involuntary.

In case of doubt or need for advice, the Risk and Compliance Department should be consulted.

12. Annual Report

The Compliance and Risk Director will issue an annual report on the internal AML/CFT risk assessment and forward it to the Managers by the last business day of May each year ('AML/CFT Report'), containing information relative to the prior year, including, as applicable:

- (i) All products offered, services rendered, and trading environments, categorized as low, medium, and high AML/CFT risk;
- (ii) Classification of Direct Clients by degree of AML/CFT risk;
- (iii) Identification and analysis of AML/CFT risk situations;
- (iv) If applicable, analysis of the performance of brokerage firms and/or intermediaries contracted for transactions;
- (v) Measures adopted for the treatment and mitigation of identified risks for active KYC clients, Employees, and relevant service providers;
- (vi) Data consolidation, as follows: consolidated number of atypical operations and situations detected, as well as those that may be considered AML/CFT; and number of reports made to COAF, including dates and outcomes.

13. Training and Validity

This Policy must be reviewed annually or whenever a prior need is identified for better support of risk and compliance requirements.

Additionally, after the policy review, the Risk and Compliance Department must conduct a training session with all Miradouro employees to keep them updated on AML/CFT practices.

14. Miradouro's Responsible Officer for Compliance with this Policy

The primary responsible party for compliance with this Policy is the Director of the Risk and Compliance Department of Miradouro, who will be supported by professionals from the Risk and Compliance team to fulfill the provisions of CVM Resolution No. 50 and other applicable rules and laws regarding the prevention and combating of money laundering.

In this regard, in addition to the responsibility of overseeing compliance with this Policy, the Risk and Compliance Department will also be responsible for promoting and sharing the practices and guidelines in this document, as well as investigating potential suspicious transactions that are reported. For this purpose, the Risk and Compliance Department must have full and unrestricted access to any information it deems necessary to carry out its periodic controls and to investigate potential suspicious transactions.

ANNEX I – SUGGESTED VERIFICATION LIST

- 1. <https://register.fca.org.uk/s/> – Financial Conduct Authority of the United Kingdom (FCA).
- 2. <https://sanctionssearch.ofac.treas.gov/> – U.S. Office of Foreign Assets Control (OFAC).
- 3. <https://www.fincen.gov/msb-state-selector> – U.S. Financial Crimes Enforcement Network (FINCEN).
- 4. <https://ec.europa.eu/transparencyregister/> – Committee against Money Laundering, Illicit Resources, and Terrorism Financing (MONEYVAL).
- 5. <https://www.worldbank.org/> – World Bank.
- 6. <https://siscoaf.coaf.gov.br/> – Police and regulatory authority agencies in each local jurisdiction, including forced labor lists.
- 7. <http://www.portaltransparencia.gov.br/download-de-dados/ceaf> – Expulsions from the federal administration (CEAF).
- 8. <http://www.portaltransparencia.gov.br/sancoes/ceis> – Ineligible and suspect companies (CEIS).
- 9. <https://servicos.ibama.gov.br/> – Environmental embargoes (IBAMA).
- 10. <http://www.portaltransparencia.gov.br/sancoes/cepim> – Barred non-profit entities (CEPIM).
- 11. <http://www.portaltransparencia.gov.br/sancoes/cnep> – Penalized companies (CNEP).
- 12. <https://www.interpol.int/How-we-work/Notices/View-Red-Notices> – INTERPOL.
- 13. <http://www.fazenda.gov.br/> – Other international AML/CFT bodies.
- 14. <https://www.un.org/securitycouncil/content/un-sc-consolidated-list> – United Nations Security Council.
- 15. <https://www.fatf-gafi.org/> – FATF list.