POLICY ON COMBATING AND PREVENTING MONEY LAUNDERING, FINANCING OF TERRORISM, AND FINANCING THE PROLIFERATION OF WEAPONS OF MASS DESTRUCTION (AML-CFT)

I. Introduction

According to Law no 9.613/1998, money laundering is the process by which the true origin and ownership of resources that are the product of illicit activities is hidden. If money laundering is successful, the interested parties are able to maintain control over such a product and ultimately give a veil of legitimacy to its illegitimate source.

The specialized literature breaks down the washing process into three very distinct stages, most of the time complex, which can develop over a certain period of time, or even simultaneously:

Placement of money: is the initial stage, as money is still close to its origins; is characterized by the introduction of illicitly obtained resources into the financial system;
Concealment or camouflage: is the stage at which the criminal seeks to break the chain of evidence before the possibility of investigations on the origin of the resources moved; and,
Integration: is the stage at which it is almost impossible to distinguish between legal and illegal wealth; illicit money is reintroduced into the economic-financial system, integrating with other assets.

Terrorism is already conceptualized in Law no 13.260/2016, and corresponds to the practice by one or more individuals of the acts of using, transporting and carrying harmful contents capable of causing damages of mass destruction, Cyber threat or threat to life and physical integrity for reasons of xenophobia, discrimination or prejudice of race, color, ethnicity, and religion, when committed with the purpose of provoking social or widespread terror, exposing person, property, public peace or public safety.

Procedures to combat and prevent money laundering, financing terrorism, and financing the proliferation of weapons of mass destruction will be led by the Director of Internal Controls and Compliance ("DoC"), with the involvement of the operational and registration areas.

II. Objective

This AML-CFT policy ("Policy") aims to establish the rules for, in compliance with applicable legislation, including regulatory resolutions, prevent the involuntary involvement of Managers in criminal activities, including the inadvertent use of (i) Perfin Resources Administration Ltd. ("Perfin Administration"); (ii) Perfin Equities Administração de Recursos Ltda. ("Perfin Equities"); and (iii) Perfin Wealth Management Ltda. ("Perfin Wealth Management"), which make up the "Perfin Group" ("Managers") as intermediaries in any type of process aimed at

concealing the true source of funds derived from criminal activities of money laundering and financing of terrorism and financing of proliferation of weapons of mass destruction, especially observed the provisions in Law 9.613/1998, amended by Law no 12.683/2012, Law no 13.260/2016, Law no 13.810/2019, as well as the regulatory provisions on the subject.

The AML-CFT legislation provides, in addition to the criminalization of money laundering and terrorism, the sectors required to comply with certain internal controls that will be detailed throughout this document.

III. Applicability

The rules in this Policy shall be applied to all partners, directors, officers, employees, trainees, consultants, and companies invested in investment funds managed by Perfin Group ("Employees").

IV. Registration and Opening of Accounts

The clients of the Managers must be duly registered before the start of activities. If the Collaborator suspects any data or information of a client, either by incompatibility of information about income, address, professional activity, resistance to submit personal information, or any other reason, shall report such event to the DOC so that it is determined whether or not the client should be accepted. If the customer refuses to provide certain information required by law, the customer's request may be denied. Required account documents may vary according to the type of account to be opened.

If any of the information provided by customers is incomplete or inconsistent with the documentation presented and other information publicly obtained by the Managers, the compliance area should describe the identified inconsistencies *and* suggest measures to be adopted for their sanitation.

If such inconsistencies cannot be remedied or there is a restriction or concern about the commission of crimes, the client in question shall be rejected or undergo the exceptional approval procedure by the Compliance Committee, including any reporting of associated operations.

If the KYC process is interrupted in these circumstances, the compliance area will necessarily be informed of the occurrence and will be responsible for assessing whether there is a need to report suspicious activity to regulatory bodies, including the Financial Activities Control Board ("COAF").

In addition, Employees may not accept transactions or conduct any type of business or activity with customers who are unable to attest to the origin of the resources they intend to deliver to the management of the Managers.

A. Managed Wallets and Exclusive Funds

As recommended by the Circular CVM/SIN/N. 5/2015, notwithstanding that the Managers carry out discretionary management of assets, without the influence of clients in their investment decision, in case the Managers have individual portfolios under management, or exclusive funds, for the customer identification policy ("know your customer" - "Know Your Client", "KYC"), these will be considered *high-risk* customers as defined below.

In this sense, the shareholders of exclusive funds and clients of managed portfolios must undergo initial due diligence for KYC purposes before their acceptance, as well as their operations will be monitored periodically by the compliance area.

The Managers will seek information on the origin of resources invested in the Managers and their compatibility with the assets declared by the client in their registration, under CVM Resolution no 50.

V. Rules of Governance

As detailed below, as one of the controls adopted in the scope of this Policy, the area of Operations will value the compatibility of transactions made by clients versus their investor profile, defined through the suitability procedures detailed in the Perfin Group*'s* Distribution and Registration Manual. If there is any discrepancy in the movements made by the customers, the DOC should be notified immediately.

At the sole discretion of the DOC, a meeting of the Compliance Committee may be convened to deal with *any* evidence of money laundering, Financing of terrorism, and the proliferation of weapons of mass destruction, and assessment of reports on such operations to competent authorities.

In addition to the Operations Team's verification of investment compatibility according to the client profile, the risk-based approach, as specified above, will be conducted by the DOC, involving the operational and registration areas. If necessary, any reassessment may be discussed at the Compliance Committee.

Based on the Managers' business, which involves the management of investment funds and distribution of the quotas of these funds, there will be two fronts for AML-CFT.

(i) In the asset, any transactions carried out outside of market prices and without plausible justification must be identified, or transactions carried out with unsuitable counterparties, or for which it is not possible to obtain complete registration information; and

(ii) In the liabilities, when the Perfin Group acts as a distributor of the quotas of funds under management, movements of clients with suspicious behavior must be identified, or without due plausible economic justification, or incompatible with the financial situation/ source of resources declared in the register.

VI. The Risk-Based Approach

The Perfin Group has developed this risk-based approach to ensure that the prevention and mitigation measures described in this Policy are proportionate to the risks identified.

Below, we list all the services provided by the Perfin Group, as well as products offered and distribution channels, with their degree of risk, in compliance with the provisions of article 5 of CVM Resolution 50:

Products Offered	**Degree of Risk**	**Services provided**	**Degree of Risk**	**Distribution channels and trading and registration environments**	**Degree of Risk**
Shares of investment funds under management	Low	Management of third-party resources and distribution of shares of investment funds under management	Low	-Own Distribution -Investment Platform -Autonomous Agent -DTVMs	Low

In addition, still in compliance with article 5 of CVM Resolution no 50, we classify the customers of the Perfin Group, potential or existing:

Customers	**Degree of Risk**
Managed portfolios and exclusive funds	High
Customers from border regions or in places known to be at risk	High

Resident, incorporated or headquartered clients or, also use in their relationship with the funds bank accounts held in countries that do not implement or insufficiently implement the recommendations of the Financial Action Task Force on Money Laundering and Terrorist Financing - FATF	High
Customers with frequent occurrences of deviations from the established operating normal situation without due justification	High
Notes from the list called Specially Designated Nationals ("SDN List"), published by OFAC - Office of Foreign Assets Control (Office of Foreign Assets Control) of the Department of the Treasury of the United States of America, as mentioned in the Registration and Know Your Client Policy - KYC	High
Clients who present notes in the due diligence process relevant from the perspective of money laundering	High
Clients distributed by account and order without relevant notes from the AML-CFT perspective.	Low
Investment funds without relevant notes under the AML-CFT perspective	Low
Closed Supplementary Pension Entities without relevant notes under the AML-CFT perspective	Low

Other customers whose distributors are responsible for AML-CFT checks are financial institutions accepted by the Perfin Group in which there is no relevant information under the AML-CFT lens	Low
Other customers not listed above	The classification of the degree of risk must be ratified by the DoC

VI. Processes AML-CFT About the Passive (KYC - Know Your Client)

Not being identified points of attention in the information collected during the customer's registration process, your approval will be automatic.

In relation to clients classified as high risk according to the above criteria, they must be submitted for approval by the Compliance Committee.

The compliance area should make periodic checks and monitoring throughout the relationship that it maintains with customers, and at least every 24 months, should dispense semi-annual monitoring to clients classified as high risk.

Even if it finds that customers have become part of the SDN List, the compliance area *must* adopt the necessary measures in relation to said customers according to the rules of the OFAC and the Brazilian regulation, reporting this fact to the COAF.

A. Routines in relation to Clients

With respect to clients, the Managers will carry out the following routines and procedures:

(i) Clients who are classified as "distributed by a third party", "investment funds", "Closed Entities of Complementary Pension Schemes" and other quota holders whose distributors responsible for the PLD-verifications are exempt from any AML-CFT analysis are financial institutions accepted by the Perfin Group (low-risk clients);

(ii) The *following* clients will be required to pass the Compliance Committee in advance:

(a) Those who opened accounts by proxy;

(b) Those who opened accounts on behalf of companies;

(c) Politically Exposed Persons, pursuant to Articles 1 to 5 of Annex A of CVM Resolution 50;

(d) Those that refer to countries considered of high risk (birth/constitution or address, including bank accounts for example);

(e) Those with high-risk occupations;

(f) Other *ad-hoc* filters, at the discretion of the *Compliance;* and

(g) Non-resident clients, in accordance with CVM Resolution 50;

B. Monitoring of typical situations

The monitoring of operations and situations is provided in art. 20 of CVM Resolution 50 will be carried out, which are:

(i) situations in which it is not possible to keep up to date the registration information of your customers;

(ii) situations where it is not possible to identify the final beneficiary;2

[1] "Art. 1o For the purposes of this Resolution, are considered politically exposed persons: I - the holders of elective mandates of the Executive and Legislative Powers of the Union; II - the holders of office, in the Executive Branch of the Union, of: a) Minister of State or equivalent; b) Special Nature or equivalent; c) the president, vice president and director, or equivalent, of entities of indirect public administration; and d) Senior Management and Advisory Group (DAS), level 6, or equivalent; III - the members of the National Council of Justice, the Supreme Federal Court, the Superior Courts, the Regional Federal Courts, the Regional Labor Courts, the Regional Electoral Courts, the Superior Council of Labor Justice and the Federal Justice Council; IV - the members of the National Council of the Public Prosecutor's Office, the Attorney-General of the Republic, the Deputy Attorney-General of the Republic, the Labor Attorney-General, the Military Justice Attorney-General, the Assistant Attorneys-General and the Prosecutors General of Justice of the States and the Federal District; V - the members of the Court of Auditors, the Attorney-General and the Deputy Attorneys-General of the Public Prosecutor's Office at the Court of Auditors; VI - the presidents and national treasurers, or equivalent, of political parties; VII - the Governors and the Secretaries of State and of the Federal District, the Deputies of the States and Districts, the presidents or their equivalents of entities of the indirect public administration of the States and Districts, and the presidents of the Courts of Justice, Military Courts, Courts of Accounts or equivalent of the States and the Federal District; and VIII - the Mayors, the Councilors, the Municipal Secretaries, the presidents, or equivalents, of entities of the indirect municipal public administration and the Presidents of Courts of Accounts or equivalents of the Municipalities.
Art. 2o Also considered politically exposed are persons who, abroad, are: I - heads of state or government; II - senior politicians; III - high-ranking government officials; IV - officers-generals and members of higher levels of the Judiciary; V - senior executives of public companies; or VI political parties managers.
Art. 3o Senior leaders of public or private international law entities are also considered to be politically exposed persons.
[...].
Art. 5th The condition of a politically exposed person lasts up to 5 (five) years from the date on which the person ceased to fall under the arts. 1 to 3 of this Annex A."

[2] According to Article 2, III, CVM Resolution 50, the final beneficiary shall be "a natural person or natural persons who together possess, control or significantly influence,

(iii) situations in which the procedures provided for in Section II of Chapter IV of CVM Resolution 50 cannot be completed;
(iv) in the case of customers classified under item I of art. 1 of Annex B of the CVM Resolution 50, operations whose values are incompatible with the professional occupation, income, or financial situation of any of the parties involved, based on the respective registration information;
(v) in the case of customers classified under Sections II to V of art. 1 of Annex B, of the CVM Resolution no 50, incompatibility of the economic activity, the social object or the billing informed with the operational standard presented by clients with the same profile;
(vi) transactions carried out between the same parties or for the benefit of the same parties, in which there are subsequent gains or losses with respect to any of the parties involved;
(vii) transactions that show significant variation in relation to the volume or frequency of transactions of any of the parties involved;
(viii) operations whose unfolding include features that may constitute a defacement to the identification of the personnel involved and the respective beneficiaries;
(ix) operations whose characteristics and developments show that they are acting, in a consistent manner, on behalf of third parties;
(x) operations that show a sudden and objectively unjustifiable change in the operating modalities usually used by those involved;
(xi) operations whose degree of complexity and risk appear incompatible with:

(a) the profile of the customer or his representative, in accordance with the specific regulation that provides for the duty to verify the suitability of products, services and operations to the customer's profile; and
(b) with the client's size and social object.

(xii) transactions carried out with the apparent purpose of generating loss or gain for which there is no objective economic or legal basis;
(xiii) Private transfers of resources and securities without apparent motivation, such as:

(a) between clients' current accounts with the intermediary;
(b) of holding securities without financial movement; and
(c) of securities outside the organized market environment.

(xiv) deposits or transfers made by third parties, for the settlement of customer transactions, or to provide collateral in transactions in future settlement markets;

---

directly or indirectly, a customer on whose behalf a transaction is being conducted or from which it benefits."

(xv) payments to third parties, in any form, for the settlement of transactions or redemptions of securities deposited on behalf of the client;
(xvi) transactions carried out outside the market price;
(xvii) assets achieved by sanctions imposed by the UNSC resolutions referred to in Law 13.810/2019;
(xviii) assets reached by request for a measure of unavailability from a foreign central authority that will be known;
(xix) the conduct of business, whatever its value, by persons who have committed or attempted to commit terrorist acts or participated in or facilitated their commission, as provided for in Law 13.260/2016;
(xx) securities owned or controlled, directly or indirectly, by persons who have committed or attempted to commit terrorist acts or participated in or facilitated their commission, as provided for in Law 13.260/2016;
(xxi) movement likely to be associated with the financing of terrorism, according to the provisions of Law 13.260/ 2016;
(xxii) operations involving natural persons, legal entities or other entities that reside, have their headquarters or are incorporated in countries, jurisdictions, dependencies or locations:

(a) that they do not apply or insufficiently apply the FATF recommendations, as listed by that body; and
(b) with favored taxation and subject to privileged tax regimes, according to the rules issued by the Federal Revenue of Brazil;

C. Systems Adopted

The information for the purposes of the AML-CFT program is obtained with the help of the specific tool contracted by the Manager, enabling the DoC and the operational and registration areas to adopt the appropriate process considering the factual situation. The Perfin Group, without prejudice to the verification procedures described in this Policy, applies the principle of presumption of veracity of the information obtained.

VII. Processes AML-CFT (Regarding the Asset)

A. Process of identification of counterparts

In case of transactions involving identifiable counterparties, the Managers may perform due diligence on the partner. A monitoring work is developed with brokers that operate for the funds and portfolios of Managers. The compliance area *has* a list of all counterparties that are authorized to operate for the Perfin Group. Only the compliance area can add new counterparties.

B. Third Party Distribution

In cases where the distribution of shares of the *funds* is outsourced to the Intermediary Institutions for a period not exceeding 36 (thirty-six) months, the compliance area must conduct due diligence procedures with the Intermediary Institutions of these funds to verify the adequacy of AML-CFT processes of these, in accordance with the procedures provided for in this Policy and in the Perfin Group's Third-Party Purchasing and Contracting Policy, in compliance with the rules of CVM Resolution no 50, including the use of the policy for registration and identification of customers, identification of areas and processes susceptible to risk, conduct appropriate training for its employees, maintenance of updated customer records, use of a specific system for investigation and detection of activities considered suspicious, and existence of high-level management bodies responsible for the AML-CFT initiatives. It will also be up to the DOC to know the policies and manuals for combating money laundering adopted by administrators, distributors, and custodians of funds that are or will be managed by the Perfin Group.

In addition, initiatives should be taken to implement the exchange of information with distributors and trustees of these funds, evaluating the opportunity and relevance of requesting more information on customers based on the internal risk assessment and other provisions of this Policy. The Perfin Group will rely on the efforts of the administrators, distributors, and custodians of the funds that are or will be managed by it to (i) identify new or existing clients, including prior to the effective realization of investments, and (ii) prevent, detect and report any suspicious transactions.

Even in cases where the distribution of quotas is outsourced, if the Managers come to have access to the cadastral information of quota holders, they may carry out KYC procedures under the terms of the Policy in order to enable the correct identification of their customers and the mitigation of the risk of evidence of illicit activities related to money laundering, notwithstanding the responsibility of the respective external distributor.

C. Monitoring: Price control of assets and securities traded

The Managers will establish a counterparty identification process appropriate to the characteristics and specificities of their businesses. It is noteworthy that the assets and securities listed below, depending on their counterparty and the market in which they are traded, have already passed through the AML-CFT process, thus excluding the Managers from additional due diligence regarding the control of the counterparty, namely:

(i) Initial and secondary public offerings of securities, registered in accordance with the rules issued by the CVM;
(ii) Public offers of restricted efforts, exempted from registration in accordance with the rules issued by the CVM;

(iii) Assets and securities admitted to trading in stock exchanges, commodities, and futures, or registered in registration, custody, or financial settlement system, duly authorized in their countries of origin, and supervised by a recognized local authority, except low liquidity shares;
(iv) Assets and securities whose counterparty is a financial or equivalent institution; and
(v) Assets and securities of the same economic nature as those listed above, when traded abroad, provided that (a) they are admitted to trading on stock exchanges, commodities, and futures or registered in registration, custody, or financial settlement systems, duly licensed in their home countries and supervised by a local authority recognized by the CVM, or (b) whose existence has been ensured by third parties duly authorized to carry out the custody activity in countries signatory to the Treaty of Asunción or other jurisdictions, or supervised by a local authority recognized by the CVM, except for low-liquidity shares.

As an exception to the above provisions and in accordance with the recommendations of the CVM/SIN/N. 5/2015 Circular, the Managers will pay special attention to suspicious transactions that may be reported to the COAF in cases of trades carried out on a stock exchange where it is possible, considering the specific circumstances of the transaction, determine the counterparty of the transactions, such as when trading low liquidity assets or when it is a transaction between investment funds managed by Perfin Group.

In addition, the Managers adopt their own routines to verify suspicious transactions made on organized OTC markets due to the possibility of determining the counterparty of the transaction (whenever possible) and, consequently, the possibility of detecting a possible targeting to gains or losses.

For the other assets and securities, such as securities and securities subject to private distribution (fixed income or shares), credit rights, real estate developments, etc., the Managers will adopt, in addition to the process of identification of counterparties, other procedures, in accordance with the Policy's premises, to ensure compliance with the minimum standard of AML-CFT, or verify that the counterparty has minimum mechanisms for such analysis.

The strategies of the entities of the Perfin Group that involve the asset management segment *and that carry out* all their operations in the organized market (stock exchange mainly) are outside the orbit of AML-CFT processes on assets.

The funds and portfolios of the Perfin Group entity's area that involves the wealth management segment *are required* to carry out such processes mainly in relation to private credit assets. In fact, the credit analysis process also involves due diligence of the *issuer and documentary* due diligence of the asset, which allows the identification of problems for FTP-PLD purposes.

VIII. Detection of suspected activities

Any suspicion of financial and non-financial transactions that may involve activities related to money laundering, concealment of assets and values, terrorism, proliferation of weapons of mass destruction, as well as incorporating gains in an illicit manner, for the Managers, customers or employees, must be communicated immediately to the DoC. The analysis will be made on a case-by-case basis, subject to disciplinary sanctions and legal consequences.

IX. Internal Report on the Internal Evaluation of Risk

The DoC will prepare an annual report on the internal risk assessment of AML-CFT, which will be forwarded to the Compliance Committee and the Strategic Council, in their capacity as senior management bodies of the Managers, by the last working day of the month of April[3], containing the information required in I and II of art. 6o of CVM Resolution 50, namely:

(i) Identification and analysis of situations at risk of money laundering or financing of terrorism or the proliferation of weapons of mass destruction, considering their threats, vulnerabilities, and consequences;
(ii) table for the previous year, containing:
  (a) the consolidated number of transactions and atypical situations detected, separated by each hypothesis;
  (b) the number of analyses carried out;
  (c) the number of suspicious transactions reported to COAF; and
  (d) the date of the negative statement report.
(iii) the measures adopted to comply with the provisions of paragraphs "b" and "c" of paragraph II of Art. 4 of CVM Resolution no 50;
(iv) the presentation of effectiveness indicators, including the timing of activities for the detection, analysis and reporting of operations or atypical situations;
(v) the presentation, where appropriate, of recommendations to mitigate the identified risks from the previous year that have not yet been properly addressed, containing: (a) possible changes in the guidelines provided for in the Policy;
(b) improvement of the rules, procedures and internal controls referred to in

[3] Your content will refer to the year preceding the delivery date.

art. 7o of CVM Resolution no 50, with the establishment of sanitation schedules; and

(vi) the indication of the effectiveness of the recommendations adopted referred to in the item above in relation to the respective previous report, according to the methodology addressed by Article II. 4o of the CVM Resolution no 50, recording the results in an individual way.

X. Communication with COAF

The Managers shall notify the COAF, refraining from giving knowledge of such act to any person, including to which the information refers, within 24 (twenty-four) hours after completion of the analysis that characterized the atypicality of the operation, proposed or atypical situation, understood as those that can be considered serious evidence of crimes of laundering or concealment of assets, rights and values arising from criminal offenses, as provided for in Article 1 of Law 9.613/1998, including terrorism or its financing, or relate to them, in which (i) there are exceptional characteristics with respect to the parties involved, method of implementation or instruments used; or (ii) objectively lacks an economic or legal basis.

The records of the conclusions of its analysis about operations or proposals that have supported the decision to make or not, communications, and that deals with this item, must be kept for a period of 5 (five) years, or longer, by determination of the CVM.

The Managers, as long as no communication has been provided to COAF, must communicate to the CVM annually until the last working day of the month of April through the mechanisms established in the agreement concluded between the CVM and the COAF.

The DOC will be responsible for the communications described in this item, with support from the Compliance Committee, whenever necessary.

XI. Suitability and Customer Profile

The objective of the suitability policy is to analyze, understand, and determine the investment profile of its clients in order to determine an individualized investment policy for each client, specifically and directly reflecting their profile, in the case of the wealth management segment, and offering suitable products in the case of the asset management segment.

The employees of the Perfin Group entity focused on the *wealth management* segment work closer to prospective customers in order to, in addition to the suitability process described in the Distribution and Registration Manual of the Perfin Group, Collect data on current portfolio, investment goals assessment, and propensity to take risks. In these cases, the manager has its own methodology and policy defined for the client's profile.

The objective is to identify and understand the characteristics of each of our clients in order to suggest the appropriate investment for their profile. The process will be guided by a form filled in by the client and together with the sales representative responsible for the client.

The determination of the profile will be made by obtaining various information from the client, such as (i) the current portfolio of the client, (ii) the percentage of loss in relation to the equity that you are willing to incur, (iii) the expected average annual return on your investments;(iv) the expected degree of liquidity of the investments;(v) reaction in the case of devaluation of investments;(vi) investment history by asset class;(vii) familiarity and experience with investments;(viii) investment in private issuers' securities;(ix) evaluation of the client's objectives.

The Employee responsible for the client collects completed and signed documents, and the Perfin Group analyzes them to identify the client's profile. At least every two years, this analysis is redone. Any change in the profile is communicated to the client and its consent is requested and filed. The change is communicated in writing and can be sent by e-mail.

The details of the suitability process can be found in the Perfin Group's Distribution and Registration Manual.

XI. Whistleblower Channel

All suspicions or violations of the provisions provided for in this Code or in the other policies of the Perfin Group must be reported through its Reporting Channel, which the internal and external public can access through the website: https://denuncia.perfin.com.br/, or through the following contact channels (11) 2526-2427 or compliance@perfin.com.br. Perfin Group ensures the confidentiality of reports received, certifying that retaliation in the face of good faith whistleblowers will not be allowed.

XII. Final Provisions

This Policy will be reviewed at least annually. Notwithstanding the stipulated revisions, they may be changed without prior notice and defined periodicity due to circumstances that require such action.

The compliance area *will inform* the Employees in due time about the entry into force of a new version of this document and make it available on the Managers' page on the World Wide Web.

The Compliance Committee has approved this Policy and revoked all previous versions, and it becomes effective on the date of its approval.