




MONEY LAUNDRY AND
TERRORISM FINANCING PREVENTION POLICY
IG4 CAPITAL INVESTIMENTOS LTDA.
("Manager")

Current version: June/2022

Previous version: June/2021

Document No.:	Review No.:	Effectiveness:
1	6 (June 2022)	11/30/2016, and, when applicable, as from obtainment of CVM consent to operate as fund manager

Approved by:  205EC3047D034CD...

Flávia Andraus Troyano

Compliance Officer

CHAPTER I - PURPOSE

1.1. The purpose of this Policy is to outline rules and procedures aiming at preventing money laundry and terrorism financing in operations involving the funds managed by the Manager and its counterparts in operations carried out by them, whenever their knowledge is possible. Furthermore, this instrument shall also guide the Manager in conducting the process of knowing and monitoring its workers and partners and relevant service providers.

1.2. The Manager does not carry out the activity of distribution of managed investment funds, so the controls of money laundry and terrorism financing prevention ("MLTFP") inherent to investors of managed funds are not applicable to the internal routines of the Manager. Notwithstanding, if the Manager is aware of any unusual situation, the Compliance and MLTFP Team will check the suitability of exchanging

information with the areas of internal controls of distributing institutions, following the rules of confidentiality and access restriction, enabling the reporting to competent authorities to happen as completely as possible.

1.3. This Policy applies to the workers of the Manager, defined as its (i) partners, (ii) associates; (iii) employees; (iv) officers; (v) interns; or (vi) any people who, due to their jobs, functions or positions in the Manager, have access to confidential information on the manager, its business or clients.

CHAPTER II - GOVERNANCE

2.1. The guidelines established in this document must be followed by all workers, with the following duties:

- (i) Executive Board: responsible for disseminating the Compliance culture and, thus, ensuring the enforcement of this Policy, as well as determining the institutional guidelines based on ethical values and principles that guide the workers' conduct, therefore directing the preparation and constant improvement of the procedures to prevent money laundry and terrorism financing adopted internally.
- (ii) Compliance and MLTFP Officer: responsible for guiding the conduct and checking the strict compliance with this Policy by the workers, also regarding the preparation and implementation of the risk-based approach process, storage of materials that document the analysis and decisions made for a minimum period of 5 (five) years.
- (ii) Compliance and MLTFP Team: execution of the procedures defined by this Policy, reporting to the Compliance and MLTFP Officer any indication of crime.

2.2. Professionals assigned to the area of Compliance and MLTFP have full independence and autonomy to perform their duties and make decisions in their scope of action, with no subordination to the other areas of the Manager, reporting directly to the Executive Board. Such professionals have broad and unrestricted access to information related to corporate activities, including operations performed, products, counterparts, service providers and other workers of the Manager, in order to enable the risk management this Policy is about.

2.3. Notwithstanding other routines defined by this Policy, the Compliance and MLTFP Team is responsible for:

- (a) preparing a previous analysis of new technologies, services and products for the purpose of mitigating the risk of the Manager engaging in operations aimed at money laundry and/or terrorism financing;
- (b) selecting and monitoring administrators, associates, employees and relevant service providers hired, with the purpose of guaranteeing high standards from its personnel, monitoring the reporting of operations or situations with indications of money laundry and/or terrorism financing involving the managed investment funds; and
- (c) maintenance of the Training Program which all workers are submitted to annually, aiming at disseminating the routines and procedures inherent to this Policy. Training may be promoted in a shorter periodicity, aiming at updating and extending the Workers' knowledge about normative and regulatory developments, as well as discussing concrete cases that happen inside and outside the institution.

CHAPTER III - RISK-BASED APPROACH

3.1. This methodology of risk-based approach is intended to ensure that the prevention and mitigation measures are proportional to the risks identified by the Manager due to the activity carried out, service providers, workers and products under management.

Risk Classification Criteria

3.2. The counterparts and service providers relevant for the activity of professional management of third party resources are classified as HIGH RISK in case they present any of the following characteristics:

- (i) Geographic location: people/companies domiciled/established in countries considered to be of high risk and/or non-residing investors, especially when they are established in the form of Trust and Managers of bearer securities. For that purpose, the Compliance, Risk and MLP Team follows up the communications approved by the Financial Action Group against Money Laundry and Terrorism Financing - GAFI/FATF, in order to enable to identify countries and jurisdictions that, in the assessment of the organism, have strategic deficiencies in money laundry prevention and in fighting terrorism financing and/or represent high corruption risks.

- (ii) Types of activities: activities related to types of business or industries known to be susceptible to money laundry are considered to be of high risk, such as: NGOs, churches or similar entities, bingo, real estate transactions, transactions involving large animals, lotteries, importation, group under investigation by PIC/PM/Police/Bacen;
- (iii) PEP: Politically Exposed People (“PEP”), as well as their relatives, close collaborators and legal entities they hold any equity interest.

3.3. The Compliance and MLTFP Team must monitor thoroughly the operations and relations held with counterparts and service providers considered to be of high risk, making sure that their register information is updated.

3.4. MEDIUM RISK relationships are those that present any type of connection with HIGH RISK people. And, finally, LOW RISK relationships are all the other relations.

Register – Identification of Final Beneficiaries

3.5. The Manager must prepare and keep a register of all identifiable counterparts, partners and relevant service providers, updating it in a maximum of:

Periodicity	Level of Risk
At every 1 (one) year	HIGH RISK
At every 3 (three) years	MEDIUM RISK
At every 5 (five) years	LOW RISK

3.6. Initial register and register updating may be done through alternative service channels, which may be by telephone, e-mail or other channel to be defined by the Manager. This process must be evidenced with signed registration forms, system logs, telephone recordings or any other proof of data confirmation.

3.7. It is a responsibility of the Compliance and MLTFP Team checking the information provided by the counterparts and service providers in the registration form, in order to identify indications of or suspected crime of money laundry and/or terrorism financing.

3.8. Register information of legal entities, including investment funds, must comprise individuals authorized to represent them, their controllers, direct and indirect, and the individuals who have significant influence on them, until reaching the individual characterized as final beneficiary, except for cases expressly listed in the standard. For that purpose, it is defined that the percentage of minimum interest that characterizes direct or indirect control is an interest of 25% (twenty-five percent).

3.9. In case it is not possible to identify the final beneficiary of the operation, the Manager must implement an enhanced monitoring in an attempt to identify unusual situations, regardless of risk classification, aiming at checking the need to communicate COAF (Brazilian Financial Activities Control Council) and of assessment by the Compliance and MLTFP Officer, subject to review regarding the interest on starting or keeping the relationship.

Know Your Client - KYC Procedure

3.10. The Know Your Client activity is a responsibility of the institutions hired to perform the distribution of quotas of investment funds, which have a direct relationship with the investors.

3.10.1. In case the Manager becomes aware of any unusual situation involving a quota holder of any investment fund, the Compliance and MLTFP Team shall assess the adequacy and possibility of exchanging information with the area of internal controls of the institution responsible for the distribution of the referred quota holder and with the fiduciary manager of such fund, according to the procedure defined in the portfolio management service agreement.

3.11. The funds managed by the Manager have trustworthy managers and distributors, which have their own Registration, Know Your Client, Suitability and Money Laundry and Terrorism Financing Policies.

Know Your Employee - KYE Procedure

3.12. Before a new worker is hired by the Manager, an analysis is carried out, not only regarding the resume, to check technical qualifications, but also looking at search sites and restrictive lists, in order to find occasional disparaging information.

3.13. The Manager has an internal procedure for hiring new workers, carrying out the required analysis and assessments, according to the position to be occupied by the worker.

3.14. All partners and service providers shall be classified with the method of Risk-Based Approach, both at the moment of hiring and during the continuous monitoring process, according to the classification defined above.

Know Your Partner - KYP Procedure

3.14. A premise of the Manager is to only do business with trustworthy third parties with excellent reputation and adequate technical qualification for the services to be provided. In that sense, hiring service providers that have been convicted, with a final judgement, in legal or administrative proceedings related to the practice of detrimental acts, infractions or crimes against the economic or tax order, money laundry or concealment of assets, rights and securities, or against the National Financial System, Capital Markets or public administration, domestic or foreign, including, without limitation, illegal acts that may lead to administrative, civil or criminal liability is prohibited, except for founded approval decision from the Executive Board.

3.15. In the event the service provider is being investigated or sued, with no unfavorable decision, the Department of Compliance must be consulted before the service is hired.

3.15. Every relevant service provider shall go through the registration process, KYP and due diligence, so that the Manager may have a complete register of its information and, therefore, may clear any doubts regarding its ethical values, probity, honesty and reputation, carefully checking any evidence that may indicate propensity or tolerance by the third party regarding acts of corruption.

3.16. The partners and service providers shall be classified with the method of Risk-Based Approach, both at the moment of hiring and during the continuous monitoring process, according to the classification defined above.

Restrictive Lists

3.17. For the purpose of completing the process of identification and knowledge of counterparts that enable to establish its identity, know the activity performed, find the origin and destination of resources, the Compliance and MLTFP Team shall look at restrictive lists and search sites to confirm data and/or identify disparaging information, such as:

- State Court of Law of the domicile of the counterpart of the operations;
- Federal Court of the Judiciary Section of the domicile of the counterpart of the operations;
- Google search tool (www.google.com.br);
- IEPTB-BR - Brazilian Institute of Study of Protested Notes;
- SERASA Experian Tool and SCPC (Credit Protection Service);

- Online search of the "Sanctions List Search" made available by OFAC - Office of Foreign Assets Control.

3.18. Such searches shall be applied, moreover, to the process of selecting and hiring service providers relevant for the activity of professional management of third party resources and workers, as defined above.

3.19. In case of any evidence of the crimes approached by the Law no. 9,613/98, including those arising from sudden change in the economic standard, the Executive Board shall assess the risks of keeping the professional among the personnel of the Manager or keeping the commercial relation with the service provider, requesting additional clarification when it is convenient.

3.20. The Manager shall demand that service providers relevant to the activity of management of third party resources and commercial partners have adequate money laundry and anticorruption prevention practices.

3.21. The diligence procedures defined herein must be applied to companies targeted for investment by the Equity Investment Funds managed by the Manager, as well as their controlling partners and key personnel in the team.

Relationship Acceptance, Refusal and Veto

3.22. In case of any suspicion or discomfort regarding the information reviewed, the Executive Board must be alerted, so that it may assess the adequacy of accepting the relationship. Relationships classified as HIGH RISK in the form of this Policy shall be automatically reported to the Executive Board.

3.23. The assessment regarding acceptance or refusal of a relationship shall be carried out by the Executive Board of the Manager, and the Compliance and MLTFP Officer has a power of veto. In the event of refusal, the interested party must be communicated that the information provided by it was not approved by the internal controls of the institution.

Definition of Criteria for Product Risk Classification

3.24. The Manager is an equity investment fund - FIP manager. As the transactions carried out by the FIP are traded out of the regulated environment, the risk of engaging the fund in operations with the purpose of money laundry and terrorism financing is MEDIUM. In order to mitigate such risk, the Manager adopts the criteria described in Chapter IV below.

3.25. The funds managed by the Manager are distributed by the fiduciary administrator/distributor, which has its own policies to prevent money laundry, being reviewed and classified by the Manager according to the methodology of Risk-Based Approach for the aforementioned risk classification.

CHAPTER IV - CRITERIA FOR ANALYSING AND MONITORING COUNTERPARTS

4.1. In order to complement the information obtained from the sources mentioned in the previous chapter, the Compliance and MLTFP Team is responsible for adopting the following mitigating measures related to using the Manager for money laundry purposes:

- (i) monitoring the diligence visits to institutions that appear as counterparts of operations carried out by managed funds, when it is possible to identify them, in order to ensure effective existence of the counterpart, identification of its operating market, origin and destination of resources, its economic-financial capability to acquire the traded asset, corporate structure, as well as the commitment of the institution with the prevention and fighting money laundry and corruption;
- (ii) checking the effective monitoring of the price range of traded assets and securities for the portfolio of managed investment funds. In case of illiquid assets, the price analysis shall be made by observing economic assessment metrics usually practiced in the market, such as asset value, EBITDA multiple and assessment by the discounted cash flow method;
- (iii) follow up the communications approved by the Financial Action Group against Money Laundry and Terrorism Financing – GAFI/FATF, in order to enable to identify operations with participation of individuals residing or entities established in countries and jurisdictions that, according to the assessment of that body, have strategic deficiencies in preventing money laundry and fighting terrorism financing.

CHAPTER V - MONITORING WITH THE PURPOSE OF IDENTIFYING INDICATIONS OF CRIME

5.1. The following atypicalities may constitute indications of money laundry and terrorism financing:

- (i) situations deriving from the process of identifying counterparts, such as:

- a) situations where it is not possible to keep updated register information;
 - b) situations where it is not possible to identify the final beneficiary;
 - c) situations where the diligences provided for in this Policy cannot be concluded;
 - d) in case of legal entities, investment funds and other hypotheses, incompatibility of economic activity, corporate purpose or revenues informed with the operational standard presented by counterparts with the same profile;
- (ii) situations related to operations in the securities market, such as, but not limited to transactions:
- a) between the same parties or for the benefit of the same parties, where there are continuous gains or losses regarding one of the parties involved;
 - b) that evidence significant fluctuation regarding volume or frequency of business by any of the parties involved;
 - c) with developments that contemplate characteristics that may constitute deception to avoid identification of the parties effectively involved and respective beneficiaries;
 - d) with characteristics and developments that evidence operating, persistently, on behalf of third parties;
 - e) that evidence sudden and objectively unjustified change regarding the operational modalities usually used by the parties involved;
 - f) with a degree of complexity and risk incompatible with the profile, size and corporate purpose;
 - g) carried out with apparent purpose of generating gains or losses, for which there is no objective economic or legal basis;
 - h) that are private transfer of resources and securities with no apparent reason, such as:
 - 1. between current accounts of investors before the broker;
 - 2. ownership of securities with no financial activity; and
 - 3. securities out of the organized market environment;
 - i) deposits or transfers made by third parties, to settle operations or to provide guarantees for operations in future markets;
 - j) payments to third parties, in any form, by settlement of operations or redemption of values deposited as guarantee; and
 - k) operations out of the market price;
- (iii) operations and situations related to people suspected of engaging in terrorist actions, such as those that involve:
- (a) assets reached by sanctions imposed by UNSC resolutions;



- (b) assets reached by request of unavailability measure filed by foreign central authority, that the Manager becomes aware of;
- (c) transactions, regardless of value, by people who have committed or tried to commit terrorist actions, or have participated on them or facilitated their execution;
- (c) securities owned or controlled, directly or indirectly, by people who have committed or tried to commit terrorist actions, or have participated on them or facilitated their execution;
- (e) activity subject to be associated to terrorism financing.

(iv) transactions with participation of individuals, legal entities or other entities that reside, have their headquarters or are established in countries, jurisdictions, premises or locations:

- (a) that do not apply or insufficiently apply GAFI recommendations, according to the lists generated by that body;
- (b) with favored taxation and under privileged tax regimes, according to the standards issued by the Brazilian Revenue Service.

5.2. The operations or situations mentioned in the item above comprise:

- (i) those that are object of transaction or registration involving securities, regardless of their value or risk classification;
- (ii) unusual events identified in the scope of diligences conducted and respective monitoring that may be associated to operations and situations involving high risk of money laundry or terrorism financing.

5.3. Monitoring must comprise operations and situations that appear to be related to other connected operations and situations or that are part of the same group of operations.

CHAPTER VI - OPERATION REGISTER AND ARCHIVE MAINTENANCE

6.1. All documents, information and registers relevant for the processes described in this Policy are archived, either in electronic or physical media, for a minimum period of 5 (five) years, and must enable: (i) the internal risk assessment and the respective rules, procedures and internal controls defined by this Policy, as well as information obtained in the process of identifying the counterparts; (ii) the timely analysis and communications mentioned in this Policy.

6.2. The electronic systems used by the Manager must: (i) enable immediate access to documents and information; and (ii) fully comply with regulatory provisions regarding register.

CHAPTER VII - COMMUNICATION

7.1. COAF must be communicated, and the Manager must refrain from notifying any person of such action, including the one the information refers to, within 24 (twenty-four) hours after concluding the analysis that verified the atypicality of the operation, respective proposal or even occurrence of detected atypical situation, about all situations or operations, or operation proposals, comprised by the records mentioned by this Policy, which may constitute serious indications of money laundry and terrorism financing crimes.

7.2. It is not a condition to report a suspicious operation that the Manager is convinced of its illegality; being able to build a solid and well-based confidence about its atypicality is a sufficiently good foundation. Such reporting must be developed individually and based with the following information:

- (i) date of start of the relationship with the person who has caused or is engaged in the operation or situation;
- (ii) grounded explanation of the warning signs identified;
- (iii) description and detail of the characteristics of the operations performed;
- (iv) presentation of the information obtained by the diligences provided for in this Policy, which qualify the engaged individuals, including reporting whether it is the case of politically exposed people, and that detail the behavior of the reported person; and
- (v) conclusion of the analysis, including the grounded report that characterizes the warning signs identified as a suspicious situation to be reported to COAF.

7.3. The records of the conclusions of the analysis of operations or proposals that based the decision of reporting or not, must be held by a period of 5 (five) years, or for a longer period by express decision by CVM, in the event of administrative proceedings.

7.4. In case no communication is made under the terms of item 7.1 above, the Manager must communicate COAF annually, until the last working day of April, through an electronic system available at the website of COAF, in the World Wide Web, non-occurrence, in the previous calendar year, of transactions or proposals of transactions subject to be reported, by sending the negative statement.

7.5. In the event of receiving a court order, the Manager must forward it immediately to the managing or brokerage institution, as the case may be, in order to perform the blocking of identified assets.

7.6. CVM, COAF and the Ministry of Justice and Public Safety must be communicated about the unavailability decreed by UNSC, as well as about any attempts of the holders to transfer unavailable assets.

7.7. In case of failing to comply with UNSC measures, the Manager must report to CVM and the Ministry of Justice and Public Safety, stating its reasons.

CHAPTER VIII - TRAINING

8.1. The Manager has a training program for workers who have access to confidential information and participate on the investment decision process.

8.2. The procedures and routines defined in this Policy shall be approached in an annual training, coordinated by the Compliance and MLTFP Officer or an third party hired for that purpose, aiming at its dissemination throughout the team of the Manager.

8.3. Training may be promoted in a shorter periodicity, aiming at updating and extending the Workers' knowledge about normative and regulatory developments, as well as discussing concrete cases that happen inside and outside the institution.

CHAPTER IX - INTERNAL CONTROLS

9.1. The Manager counts on a professional responsible for the implementation and enforcement of internal rules, policies, procedures and controls, whose duties and routines, notwithstanding the responsibilities pointed out in this Policy, are provided for in the Compliance and Internal Controls Manual.

9.2. The Compliance and MLTFP Officer must prepare a report related to the internal risk assessment until the last working day of April, containing:

- (i) identification and analysis of risk situations, considering respective threats, vulnerabilities and consequences;
- (ii) analysis of the work of partners and service providers;
- (iii) table related to the previous year, containing the number of atypical operations or situations identified, number of analyses prepared, number of suspicious

- operations reported to COAF and the date of reporting of the negative statement to COAF, if applicable;
- (iv) measures adopted to identify and know the counterparts and final beneficiaries;
 - (v) presentation of indicators of the effectiveness of the risk-based approach, including the timeliness of detection, analysis and reporting of atypical operations or situations;
 - (vi) recommendations, if applicable, aiming at mitigating the risks identified in the previous fiscal years and that have not yet been handled, including possible changes in this Policy, improvement of internal controls with definition of correction schedules;
 - (vii) indication of the effectiveness of the recommendations adopted regarding the previous report, recording the results individually.

9.3. This report may be prepared in an individual manner or jointly with the Conformity Report provided for by art. 25 of CVM Resolution no. 21.

9.4. The Manager shall monitor, directly and permanently, the unavailability decisions issued by the UNSC, as well as occasional information to be followed for proper compliance with them, including total or partial search of such decisions regarding people, legal entities or assets, aiming at complying immediately with the decision, following up, notwithstanding the adoption of other monitoring procedures, information disclosed at the UNSC website in the World Wide Web.

CHAPTER X - GENERAL PROVISIONS

10.1. This Policy prevails over any previous oral or written understandings, binding the workers of the Manager to its terms and conditions.

10.2. Failing to comply with the provisions of this Policy shall result in warning, suspension, termination of contract or exclusion with due cause, according to the severity and recurrence of the violation, notwithstanding civil and criminal penalties.