AML/CFT AND KNOW YOUR COUNTERPARTY POLICY

April 2026

RECORD OF CHANGES			
Version	**Modified Item**	**Modification**	**Date**
1	Original version	-	01/2024
2	General revision	Full review of the policy	04/2026

Table of Contents

758 Leopoldo Couto Magalhães Jr. Street, 2nd floor / 04542000 / Sao Paulo / Brazil

758 Leopoldo Couto Magalhães Jr. Street, 2nd floor / 04542000 / Sao Paulo / Brazil

1. General Definitions

1.1 Introduction

Due to its activities involving asset and wealth management, Tera Investimentos Ltda. ("Manager" or "TERA") maintains a direct relationship with its Clients (as defined below) and Partners (as defined below) (the "Counterparties"), which involves essential procedures such as registration and measures aimed at preventing and combating the use of the Manager's assets and systems for unlawful purposes, including money laundering, concealment of assets and values, and terrorist financing crimes, in accordance with the definitions established under applicable legislation.

TERA conducts its business in accordance with the highest standards of honesty, integrity, and transparency, and in full compliance with all applicable laws and regulations. Compliance with this Policy is essential to preserving the Manager's reputation and maintaining the trust of its Clients, Partners, and Employees (as defined below). For this reason, TERA does not tolerate, under any circumstances, acts of money laundering, terrorist financing, or corruption.

The Manager only maintains commercial and/or contractual relationships with Counterparties and Employees who demonstrate good reputation and ethical conduct, and who operate in compliance with applicable laws, the anti-money laundering and counter-terrorist financing regulations issued by the Brazilian Securities and Exchange Commission ("CVM"), and the guidelines established by the Brazilian Financial and Capital Markets Association ("ANBIMA"), especially those relating to Anti-Money Laundering and Counter-Terrorist Financing ("AML/CFT").

1.2 Regulatory Framework

This AML/CFT and Know Your Counterparty Policy ("Policy") is based on the rules and regulations listed below, without prejudice to any other laws or regulations whose subject matter relates to the matters addressed herein:

(i) Law No. 9,613, as amended ("Anti-Money Laundering Law");
(ii) Law No. 13,260 ("Anti-Terrorism Law");
(iii) Law No. 13,810 ("Sanctions Compliance Law);
(iv) CVM Resolution No. 50 ("CVM Resolution 50");
(v) CVM Resolution No. 175 ("CVM Resolution 175");
(vi) The AML/CFT Guide issued by ANBIMA;
(vii) CVM/SMI/CIN Circular Letter No. 1/2022; and
(viii) CVM/SMI Circular Letter No. 1/2024.

1.3 Governance and Responsibilities

The Manager's governance structure for matters related to AML/CFT, notwithstanding the general and common duty imposed on TERA's partners, officers, and employees ("Employees"), is primarily conducted by TERA's Compliance Department, composed of (a) the Director of Compliance, Internal Controls and AML/CFT ("Compliance Department") and, where applicable, (b) the analyst(s) of the Compliance Department.

758 Leopoldo Couto Magalhães Jr. Street, 2nd floor / 04542000 / Sao Paulo / Brazil

The Compliance Department shall have broad, unrestricted, and timely access to any information related to the Manager's activities, thereby enabling the data necessary for the performance of its duties — especially with respect to the effective management of AML/CFT risks related to this Policy — to be carried out effectively and comprehensively.

In this regard, the Manager and/or its Employees may not restrict access to any corporate data that may be requested by the Compliance Department, even where such restrictions are based on legal and/or commercial confidentiality issues or other legal limitations.

The responsibilities of the Director of Compliance include, without limitation to others set forth throughout this and other policies of the Manager:

(i) Implement and oversee compliance with this Policy by all Employees;

(ii) Promote the dissemination of this Policy and the AML/CFT culture among Employees and Partners, whether essential or otherwise, as applicable;

(iii) Review occurrences of potential suspicious transactions that may be reported by Employees;

(iv) Review the existing control methodologies and parameters, adopting national and international regulatory developments and AML/CFT best practices;

(v) Analyze potential cases of violations of the rules described in this Policy, in the Manager's other internal policies and manuals, in the applicable regulations or self-regulatory rules, as well as other relevant events;

(vi) Determine the appropriate measures in cases where Employees or Partners fail to comply with the procedures set forth in this and other policies of the Manager, in addition to applicable legislation;

(vii) Update the terms of this and other policies of the Manager in accordance with legislation or findings arising from internal or external audits that may be conducted;

(viii) Organize and implement ongoing training for Employees regarding AML/CFT and other matters required under applicable regulations.

For the purposes of this and other internal policies and manuals of the Manager, "Senior Management," pursuant to Article 2, item I, of CVM Resolution 50, means the highest decision-making body or the individuals responsible for conducting TERA's strategic matters, represented by its managing partners, as provided for in its articles of incorporation.

The Manager's Senior Management shall:

i) Be aware of AML/CFT compliance risks, as well as national and international regulatory developments on the subject;

ii) Ensure that the Compliance Department has sufficient independence, autonomy, and technical knowledge for the full performance of its duties, as well as full access to all information it deems necessary for the proper implementation of AML/CFT risk governance;

iii) Ensure that transaction monitoring systems, as well as the identification of atypical situations, are aligned with the institution's risk appetite and may be promptly reviewed in the event of any change to the applicable AML/CFT risk matrix; and

iv) Ensure the effective allocation of sufficient human and financial resources to comply with the obligations and procedures established in this and other internal policies and manuals of the Manager.

2. Methodology

2.1 Commercial Counterparty Identification Process

Transactions carried out within the portfolios managed and/or investment vehicles administered by TERA shall be analyzed from an AML/CFT perspective independently from the risk analysis already conducted on the Client holding the portfolio. Knowledge of the Client does not replace the due diligence required with respect to the commercial counterparty of transactions carried out on the Client's behalf, with the purpose of preventing portfolios and/or investment vehicles under management from being used as instruments for AML/CFT practices.

Due diligence on commercial counterparties shall be calibrated according to the level of risk identified in each situation. For assets traded in the markets listed below, the nature of the commercial counterparty and the trading environment already provide an adequate level of verification, dispensing with additional due diligence:

(i) initial and follow-on public offerings registered with the CVM, as well as restricted offerings exempt from registration;
(ii) assets admitted for trading on stock exchanges, commodities and futures exchanges, or registered in custody or financial settlement systems supervised by a recognized authority, including abroad under the conditions set forth in CVM Resolution 50; and
(iii) assets whose counterparty is an authorized, registered, or equivalent financial institution.

For all other assets — especially privately distributed instruments, CRIs, CRAs, FIDC quotas, credit rights, and real estate developments — the Manager shall adopt due diligence measures proportional to the risk posed by the commercial counterparty, which may include on-site due diligence visits and verification of AML/CFT mechanisms.

2.2 Identification and Treatment of Politically Exposed Persons

For AML/CFT compliance purposes, the Manager shall undertake specific efforts in analyzing transactions involving counterparties that are considered politically exposed persons, as well as their family members, close associates, and legal entities in which they hold an interest ("PEPs"). Indeed, the participation of PEPs in any transaction in the financial market is regarded as a highly sensitive matter by regulatory and self-regulatory entities within the financial and capital markets.

758 Leopoldo Couto Magalhães Jr. Street, 2nd floor / 04542000 / Sao Paulo / Brazil

Pursuant to CVM Resolution 50, PEPs are individuals who hold a position, office, mandate, or any function classified as politically exposed under Annex A of CVM Resolution 50.

In the identification and treatment of PEPs, the Manager adopts internal procedures based on objective criteria aimed at conducting a cautious analysis and continuous risk monitoring with respect to:

(i) the personal documents of the PEP, their family members, spouse, close associates, and legal entities in which they hold an interest;
(ii) the corporate documents of legal entities and investment vehicles in which the PEP holds an interest, is the ultimate beneficial owner, or otherwise exercises significant influence (e.g., participation on the board of directors); and
(iii) contracts, agreements, and other documents relating to assets that the Manager intends to acquire for the fund's portfolio.

In transactions and assets involving PEPs, the Manager's analysis is not limited to the politically exposed person alone. The Compliance Department shall examine the relationship between the PEP and the specific transaction or asset, with particular attention to the issuers and guarantors of the asset, their shareholders, and other related parties involved in the issuance, distribution, commercialization, and circulation of the asset.

2.3 Third-Party Systems and Reputational Screening

The Manager shall adopt all possible and necessary precautions, in accordance with its capabilities, to obtain sufficient informational and documentary support to ensure that the Counterparty and/or Employee has a good reputation and is morally, financially, and legally reputable.

With respect to the investment funds managed by the Manager, the Manager shall rely on the efforts of fiduciary administrators, distributors, custodians, and other service providers to investment funds ("Service Providers") to:

(i) identify new and existing investors, including prior to the effective completion of investments; and
(ii) prevent, detect, and report any suspicious transactions to the Manager.

For purposes of complying with items (i) and (ii) above, the Manager's Compliance Department shall assess, through a due diligence process, whether the Service Providers comply with the minimum regulatory requirements necessary to satisfy the assumptions set forth above.

In selecting Service Providers, the Manager shall require: (a) the existence of AML/CFT policies; and (b) the adoption of procedures demonstrating the existence and practical application of policies and processes related to know your client procedures, identification of areas and processes susceptible to risk, adequate employee training, maintenance of updated client records (within the legally required timeframes), and the implementation of procedures and routines for the investigation and detection of activities considered suspicious.

Lastly, the Compliance Department shall adopt a background screening system for the registration and reputational verification of its Counterparties, and any negative findings shall be immediately submitted to the Compliance Department for review and assessment.

758 Leopoldo Couto Magalhães Jr. Street, 2nd floor / 04542000 / Sao Paulo / Brazil

Currently, the Manager uses the registration screening system provided by BRE Assessoria de Investimentos ("BRE AI"), a well-known provider in the market, which issues registration and reputational screening reports containing reputational information regarding potential Counterparties and/or Employees.

After the issuance of the registration and reputational screening report, the Compliance Department shall assess the results and the risk classification indicated by the system, determining the appropriate measures according to the outcome.

3. Know Your Client

3.1 Definition of Client and Identification Practices

For the purposes of this Policy, a client shall mean any individual or legal entity that, following approval in the internal registration and reputational screening process and assessment of adherence to the Manager's client profile, has accepted the commercial terms proposed by TERA and formalized the relationship through the execution of an asset or wealth management agreement ("Client").

Approval of the registration and reputational screening process and the execution of the agreement are cumulative and indispensable conditions for an individual or legal entity to be recognized as a Client of the Manager for the purposes of this Policy.

In this context, the Manager shall observe the following practices in relation to all its Clients, in accordance with the ANBIMA AML/CFT Guide and CVM Resolution 50:

(i) verification of the true identity of all Clients through the procedures internally established by the Manager;

(ii) refusal to receive funds from or conduct activities with Clients whose investment funds, legal entities, foreign investment entities, or similar structures originate from criminal activities, even where there is only suspicion of such unlawful activities;

(iii) refusal to receive amounts incompatible with the Client's declared professional occupation and financial and asset situation;

(iv) refusal to carry out investments or transactions with Clients who refuse or create unjustified obstacles to providing the information necessary for registration or updating registration records and/or who have not been approved under the AML/CFT procedures described herein; and

(v) full cooperation with regulatory authorities, including reporting all identified suspicious activities, within the limits of applicable laws and regulations.

In cases where TERA acts as the manager of funds distributed by third parties, the KYC and investor registration obligations shall be operationally performed by the distributor, without prejudice to TERA's responsibilities to: (i) establish minimum registration and identification standards applicable to distribution activities; (ii) supervise compliance with such obligations by the contracted distributors; and (iii) maintain access to the registration information necessary for the proper performance of management activities and compliance with its regulatory obligations.

3.2 KYC Process and Onboarding Client

TERA's KYC and Client onboarding process is structured in sequential and interdependent stages, beginning at the prospecting phase and extending through the formalization of the contractual relationship and the receipt of assets under management. Each stage constitutes a condition precedent for proceeding to the next stage, and the commencement of the commercial relationship is prohibited without the completion and approval of the previous stages by the Compliance Department.

The process is conducted in a multidisciplinary manner by the Relationship, Compliance, Risk, Operations, and Management Departments, with responsibilities assigned at each stage as described below.

3.2.1 Step 1 — Registration and Reputational Screening

Once a potential Client has been identified, the Relationship Department shall provide the Compliance Department with the potential Client's full name and identification documents (CPF/RG for individuals or CNPJ for legal entities) so that the registration and reputational screening process may begin.

The Compliance Department shall conduct the screening through the registration and reputational verification system adopted by the Manager, as described in Section 2.3 of this Policy, and shall analyze the generated report to verify the existence of any findings that may prevent the continuation of the relationship process.

Upon completion of the analysis, the Compliance Department shall communicate its opinion to the Relationship Department:

> (i) **where no restrictive findings are identified:** the Relationship Department shall be authorized to proceed with negotiations and advance to the subsequent stages of the KYC process; or
> (ii) **where relevant findings are identified:** the Compliance Department shall submit the matter to the Compliance Director for assessment, who shall determine, with proper justification, whether the relationship process may continue under enhanced due diligence measures or whether it must be terminated.

The opinion issued by the Compliance Department shall be recorded and archived, regardless of the outcome, ensuring traceability of the process from the prospecting phase onward.

3.2.2 Step 2 — Information Collection and Preparation of the KYC Report

The Relationship Department shall be responsible for collecting the Client's preliminary documents and information, as well as information regarding the Client's assets, culminating in the preparation of the internal Know Your Client report ("KYC Report"). The KYC Report must be signed by the representative of the Relationship Department and submitted to the Compliance Department for review, approval, and filing.

The communication channel between the Relationship and Compliance Departments shall be direct, ensuring that the personal data of potential Clients is analyzed simultaneously and in a coordinated manner by both departments.

The registration of Client information shall be carried out and maintained in an electronic system or file,

758 Leopoldo Couto Magalhães Jr. Street, 2nd floor / 04542000 / Sao Paulo / Brazil

in which the expiration date of the registration, as well as the date and content of all amendments made, shall be recorded, ensuring traceability and integrity of the information.

The Client registration records shall include, where applicable: (a) the individuals authorized to represent the Client; (b) all direct and indirect controlling persons; and (c) the individuals who exercise significant influence over the Client, until the individual characterized as the ultimate beneficial owner is identified, pursuant to CVM Resolution 50.

In the case of ultimate beneficial owners within trust structures or similar vehicles, the Manager shall make efforts to identify:

(i) the person who established the trust or similar vehicle (settlor);
(ii) the supervisor of the investment vehicle, if any (protector);
(iii) the administrator or manager of the investment vehicle (custodian or trustee); and
(iv) the beneficiary of the trust, whether one or more individuals or legal entities.

3.2.3 Step 3 — Onboarding

Following the execution of the asset management services agreement between the Client and the Manager, the formal onboarding process shall begin, including the registration of managed portfolios and/or investment vehicles in TERA's operational systems.

The onboarding workflow is structured in a multidisciplinary manner by TERA's Relationship, Compliance, Risk, Operations, and Management Departments, with the duties and responsibilities of each department defined in an internal flowchart, which forms an integral part of the Manager's operational procedures. The Manager shall document all stages of the process, preferably through email records and internal files, in order to ensure full traceability.

The onboarding flowchart includes, among other aspects, the procedures adopted by each department for the orderly receipt of the Client's assets, as well as the mechanisms for the ongoing assessment of the assets received, including the identification of potential suspicious assets or inconsistencies between the assets received and the information declared by the Client during the previous stages of the process.

3.3 Updating Registration Information

Changes to the information contained in the registration records may be made either: (a) upon the Client's formal request, submitted in physical or electronic form and accompanied by the relevant supporting documentation; or (b) upon the Manager's initiative during the periodic renewal process provided for in this Policy.

The Manager shall maintain its registration records permanently updated, and direct contact with the Client shall be mandatory whenever any relevant change in registration information, inconsistency between the available data and the declared profile, or need for additional information for AML/CFT monitoring purposes is identified.

3.4 Termination of the Client Relationship

758 Leopoldo Couto Magalhães Jr. Street, 2nd floor / 04542000 / Sao Paulo / Brazil

The Manager may decide to terminate its relationship with a Client when: (i) the Client unjustifiably refuses to provide registration information; (ii) the Client is reclassified as High-Risk and the Compliance Director determines that the relationship should be terminated; or (iii) indications of the Client's involvement in AML/CFT-related crimes are identified.

The termination procedure shall observe the following requirements:

(i) the decision to terminate the relationship must be formalized in a document signed by the Compliance Director, including a record of the reasons supporting the decision;
(ii) the termination shall be communicated to the Client in an orderly manner, in compliance with the applicable contractual and regulatory deadlines;
(iii) the Manager shall take all necessary precautions to avoid alerting the Client about any ongoing investigation or imminent communication to COAF (prohibition of "tipping off," pursuant to Article 11, Paragraph 2, of Law No. 9,613/98); and
(iv) the documentation related to the termination process shall be archived for a minimum period of 5 (five) years following the termination of the relationship.

4. Know Your Partner

4.1 Definição de Parceiro e Escopo de Aplicação da Presente Política

For the purposes of this Policy, a Partner shall mean any individual or legal entity engaged or in the process of being engaged by TERA to provide services or perform activities in collaboration with the Manager, regardless of whether such activities are regulated by regulatory and/or self-regulatory authorities of the financial and capital markets ("Partner").

The KYP process begins with the identification of the need to engage a Partner by any department of TERA, and the Compliance Department shall be responsible for conducting and supervising the stages described in this section prior to the formalization of the contractual relationship.

4.2 Reputational Screening

The first stage of the KYP process consists of the reputational screening of the Partner by the Compliance Department through the registration and reputational verification system adopted by the Manager, currently provided by BRE AI, as described in Section 2.3 of this Policy.

If the reputational screening results in relevant findings, the Compliance Department shall submit the matter to the Compliance Director for assessment, who shall determine the appropriate measures, including the recommendation not to engage the Partner.

In the absence of any relevant restrictive findings, the process shall proceed to the KYP Questionnaire stage described in Section 4.3 below.

4.3 KYP Questionnaire

Once the reputational screening stage has been completed without any restrictive findings, the Compliance Department shall send the internal Know Your Partner questionnaire ("KYP Questionnaire") to the Partner, through which the Partner shall:

758 Leopoldo Couto Magalhães Jr. Street, 2nd floor / 04542000 / Sao Paulo / Brazil

(i) provide the relevant registration and corporate information, including the identification of its ultimate beneficial owners, direct and indirect controlling persons, and individuals exercising significant influence; and

(ii) submit the documents requested by the Manager, in accordance with the list internally defined by the Compliance Department.

Completion of the KYP Questionnaire and submission of the requested documents are indispensable conditions for the approval and engagement of the Partner.

4.4 Assessment and Approval

Based on the results of the reputational screening and the information and documents obtained through the KYP Questionnaire, the Compliance Department shall conduct the Partner's risk assessment, classifying the Partner according to the criteria set forth in the Internal Risk Assessment described in Section 6 of this Policy.

Upon completion of the analysis of the KYP Questionnaire and the Partner's risk classification, the Compliance Department shall prepare the KYP Report and submit it to the Compliance Director for formal approval. Based on the KYP Report, the Compliance Director may:

(a) approve the continuation of the process for the contractual formalization provided for in Section 4.5 of this Policy;
(b) reject the engagement of the Partner, with formal record of the communication of such decision to the department involved in the negotiations; or
(c) temporarily suspend the decision, requesting additional information or documents necessary for the conclusion of the analysis.

The decision of the Compliance Director shall be recorded in the KYP Report and archived by the Compliance Department, regardless of the outcome, ensuring traceability of the process.

4.5 Contractual Formalization

TERA shall formalize its relationship with the Partner through a written agreement, executed by the parties involved in the provision of services, establishing the commercial and legal terms of the engagement, including, where applicable, compliance clauses relating to AML/CFT legislation.

4.6 Periodic Review

The registration records and risk assessment of Partners shall be reviewed periodically by the Compliance Department at intervals not exceeding 5 (five) years, or earlier whenever a relevant new fact is identified that may alter the assigned risk classification, such as a subsequent finding in a reputational screening, a change in the Partner's corporate structure, or a material change in the scope of services provided.

5. Know Your Employee

5.1 Scope of Application

758 Leopoldo Couto Magalhães Jr. Street, 2nd floor / 04542000 / Sao Paulo / Brazil

The Know Your Employee ("KYE") process begins prior to the formalization of the relationship with the Employee and continues on an ongoing basis throughout the entire duration of the relationship with the Manager, with the Compliance Department being responsible for conducting and supervising the stages described in this section.

5.2 Reputational Screening and Prior Assessment

Before the admission or engagement of any Employee, the Compliance Department shall conduct a reputational screening through the registration and reputational verification system adopted by the Manager, as described in Section 2.3 of this Policy, assessing, at a minimum:

(i) relevant criminal and civil records;
(ii) reputational background and adverse media history;
(iii) classification as a PEP or the existence of a relationship with a PEP, pursuant to Section 2.2 of this Policy; and
(iv) the existence of sanctions, restrictions, or convictions in administrative proceedings issued by the CVM, ANBIMA, or other regulatory authorities.

If the screening results in negative findings that reflect adversely on the Employee, the matter shall be reviewed by the Compliance Director, who shall determine the appropriate measures, including the recommendation not to admit or engage the Employee.

The scope and depth of the screening shall be proportional to the Employee's level of access to confidential information, investment decisions, and Client data, subject to the limitations imposed by labor legislation and the Brazilian General Data Protection Law ("LGPD").

5.3 Ongoing Monitoring

The Compliance Department shall ensure the ongoing monitoring of Employees throughout the entire duration of their relationship with the Manager, including the periodic renewal of reputational screenings at intervals not exceeding 5 (five) years, or whenever a relevant new fact is identified, such as:

(i) a subsequent finding identified in a reputational screening;
(ii) the initiation of administrative sanction proceedings against the Employee by a regulatory or self-regulatory authority;
(iii) a material change in the Employee's financial or professional situation that is incompatible with the Employee's compensation; or
(iv) the identification of a subsequent relationship with a PEP that had not been previously disclosed.

Any finding identified during the monitoring process shall be immediately brought to the attention of the Compliance Director, who shall determine the appropriate measures.

The risk classification and periodic monitoring of Employees shall be determined and carried out in accordance with the Risk Matrix set forth in Chapter 6.

5.5 Training

758 Leopoldo Couto Magalhães Jr. Street, 2nd floor / 04542000 / Sao Paulo / Brazil

All Employees are subject to the continuous AML/CFT training program conducted by the Compliance Department, pursuant to Section 1.3 of this Policy. Participation in such training is mandatory, and records thereof shall be maintained by the Compliance Department for a minimum period of 5 (five) years.

6. Internal Risk Assessment

6.1 Risk-Based Approach

TERA adopts the Risk-Based Approach ("RBA") as the central methodology of its AML/CFT governance framework, in accordance with CVM Resolution 50. Through the RBA, the Manager identifies, assesses, understands, and mitigates the AML/CFT risks inherent to its activities, calibrating the intensity of controls and procedures proportionally to the risks effectively identified.

The adoption of the RBA implies that the Manager's compliance, monitoring, and due diligence resources are allocated primarily where risks are higher, without prejudice to the maintenance of minimum controls applicable to all business relationships. This proportionality guides both the risk classification of Counterparties and Employees and the assessment of the Manager's products, services, and distribution channels.

6.2 Counterparty Risk Assessment Procedures

Upon completion of the Know Your Client and Know Your Partner procedures described in Chapters 3 and 4 of this Policy, the Compliance Department shall carry out the Counterparty's risk assessment, classifying the Counterparty as low, medium, or high-risk, based on the criteria established in Section 6.3 of this Policy.

The risk classification shall be formalized in the Counterparty Due Diligence Report, prepared by the Compliance Department and submitted for approval by the Compliance Director prior to the commencement or continuation of the relationship. The Due Diligence Report shall contain, at a minimum: (i) the identification of the Counterparty and a summary of the registration information collected; (ii) the results of the reputational screening; (iii) the assigned risk classification and its rationale; and (iv) the applicable review periodicity.

The Compliance Department shall ensure the periodic review of the Counterparty's information and documents, in accordance with the deadlines established for each risk level in the matrix set forth in Section 6.3 below. In the event of a change in the risk classification level (whether due to a new fact identified during ongoing monitoring or during a periodic review), the Compliance Department shall immediately adjust the applicable review periodicity and formally record the reasons for the reclassification in the updated Due Diligence Report.

6.3 Risk Classification and Risk Matrix

The classification of Counterparties by risk level is intended to guide monitoring procedures and the periodicity of registration updates, assigning greater attention to those more likely to be involved in AML/CFT activities. TERA adopts three classification levels (Low, Medium, and High-Risk), the classification criteria and associated obligations of which are consolidated in the matrix below:

Classification	Profile	Classification Criteria	Update Frequency	Monitoring Level
Low-Risk	Counterparties not classified as Medium or High-Risk.	Absence of any Medium or High-Risk criteria.	**Every 60 months**	Periodic routine monitoring
Medium-Risk	Specific Counterparty profiles	Non-resident Counterparties, except those classified as High-Risk.	**Every 36 months**	Enhanced attention
High-Risk	Classification under at least one of the criteria listed alongside is sufficient.	1.Impaired reputation: individuals accused or convicted in administrative sanction proceedings by the CVM or ANBIMA within the last 3 (three) years, deemed serious by the Compliance Director. 2.Politically Exposed Persons (PEPs), their family members, spouses, close associates, and legal entities in which they hold an interest. 3.Refusal to provide registration information, material inconsistencies, or receipt of amounts incompatible with the declared profile. 4.Exposure to offshore jurisdictions classified as non-cooperative by the FATF, included on a UN Security Council list, or lacking a capital markets regulator that is a signatory to IOSCO/OICV. 5.Non-profit organizations, pursuant to applicable legislation.	**At least annually**	**Continuous** Enhanced Monitoring

In addition to the periodic update intervals established in the matrix, the Manager shall promptly reassess the risk classification of any Counterparty whenever a relevant new fact is identified, including, without limitation, subsequent findings in reputational screenings, the initiation of administrative sanction proceedings, changes in the Counterparty's corporate structure, or material modifications to the Counterparty's operational profile.

Counterparties classified as High-Risk shall be subject to continuous and enhanced monitoring by the Compliance Department, which shall assess both the existing commercial relationship and any proposals for establishing a new relationship on a case-by-case basis. Classification within this category does not necessarily prevent the maintenance or engagement of the Counterparty, but it does require a reasoned analysis and formal record of the grounds justifying the continuation of the relationship.

6.4 Red Flags and Monitoring of Atypical Transactions

In accordance with Article 20 of CVM Resolution 50, the Manager shall continuously monitor all transactions and situations, observing the following red flags that may indicate AML/CFT-related activities:

(i) transactions or contributions incompatible with the Client's profile, declared assets, or transaction history, without a plausible economic justification;

(ii) investment structures that hinder or prevent the identification of the ultimate beneficial owner, including multi-layered corporate structures or participation of vehicles located in low-

transparency jurisdictions;
(iii) fragmented contributions or transactions structured to circumvent regulatory reporting thresholds ("smurfing");
(iv) frequent transfers to or from jurisdictions listed by the FATF as non-cooperative, without apparent economic justification;
(v) unjustified resistance to registration updates or refusal to provide documents requested by the Compliance Department;
(vi) material inconsistencies between declared registration information and data obtained from other sources;
(vii) abrupt changes in the Client's transaction patterns without any identifiable economic justification;
(viii) attempts to conduct transactions involving Clients or Counterparties sanctioned by the UN Security Council ("UNSC") or the Office of Foreign Assets Control ("OFAC"); and
(ix) any other situations that, in the reasoned judgment of the Compliance Department, present indications of AML/CFT-related activities.
(x) upon identification of any red flag, the Compliance Department shall adopt enhanced monitoring measures and assess the need to report the matter to COAF pursuant to Section 7.1.

6.5 Annual Report

The Compliance Director shall issue an annual report regarding the internal AML/CFT risk assessment and submit it to Senior Management by the last business day of April of each year ("Annual AML/CFT Report"), containing information relating to the previous year, including, as applicable:

(i) All products offered, services provided, respective distribution channels, and trading and registration environments in which the Manager operated, segmented into low, medium, and high AML/CFT risk, in accordance with the classification set forth in this Policy;

(ii) The identification and analysis of AML/CFT risk situations, considering their respective threats, vulnerabilities, and consequences;

(iii) where applicable, the analysis of the performance of securities brokerage firms and/or intermediaries engaged to execute transactions for the portfolios;

(iv) Table relating to the previous year containing:

(a) The consolidated number of atypical transactions and situations detected, segregated by each category, pursuant to CVM Resolution 50;

(b) The number of analyses of atypical transactions and situations that may constitute indications of AML/CFT-related activities, pursuant to CVM Resolution 50;

(c) the number of suspicious transaction reports submitted to the Financial Activities Control Council ("COAF"), in accordance with CVM Resolution 50; and

(d) The date of submission of the negative declaration regarding the absence of situations, transactions, or proposed transactions subject to reporting, where applicable, pursuant to CVM Resolution 50;

758 Leopoldo Couto Magalhães Jr. Street, 2nd floor / 04542000 / Sao Paulo / Brazil

(e) The measures adopted for the treatment and mitigation of identified risks in order to maintain continuous knowledge of Clients, Partners, and Employees, in compliance with CVM Resolution 50; and

(f) The presentation of indicators regarding the effectiveness of this Policy, including the timeliness of activities related to the detection, analysis, and reporting of atypical transactions or situations.

(v) Where applicable, the presentation of recommendations aimed at mitigating risks identified in the previous year that have not yet been adequately addressed, including:

(a) Possible amendments to the guidelines set forth in this Policy;
(b) Improvements to the rules, procedures, and internal controls established under this Policy, including remediation timelines; and
(c) An indication of the effectiveness of the recommendations adopted as referred to above in relation to the immediately preceding report, in accordance with the methodology for the treatment and mitigation of identified risks, with results recorded individually.

The Annual AML/CFT Report shall remain available at the Manager's headquarters for inspection by the CVM and, where applicable, by the relevant self-regulatory entity. Additionally, the Annual AML/CFT Report may be prepared as a standalone document or incorporated into the annual internal controls report, subject to the requirements of applicable regulations.

7. Final Considerations

7.1 COAF Obligations

The Manager is subject to the reporting obligations to COAF set forth in the Anti-Money Laundering Law and CVM Resolution 50, which comprise two distinct categories:

(i) **Reporting suspicious transactions.** The Manager shall report to COAF, based on a reasoned analysis, all transactions or situations that, pursuant to Article 22 of CVM Resolution 50, present indications of constituting money laundering, terrorist financing, or the financing of the proliferation of weapons of mass destruction. Such reporting shall be made within 24 (twenty-four) hours from the conclusion of the analysis that characterized the atypical nature of the transaction, related proposal, or detected atypical situation;

(ii) **Negative declaration of occurrence.** If, during the previous calendar year, there were no situations, transactions, or proposed transactions subject to reporting to COAF, the Manager and/or its directors shall communicate such non-occurrence to the CVM, pursuant to Article 23 of CVM Resolution 50, by the last business day of April of the following year, through the mechanisms established under the agreement between the CVM and COAF. The obligation to submit a negative declaration to the CVM shall not apply if the Manager has already submitted at least one suspicious transaction report to COAF during the relevant reporting period.

758 Leopoldo Couto Magalhães Jr. Street, 2nd floor / 04542000 / Sao Paulo / Brazil

7.2 Compliance with Sanctions Imposed by United Nations Security Council Resolutions

The Manager shall identify Counterparties subject to asset-freezing determinations pursuant to the Sanctions Compliance Law and as provided under CVM Resolution 50, and shall comply, to the extent applicable to its asset management activities, with the measures established by sanction resolutions of the United Nations Security Council ("UNSC") or the designations issued by its sanctions committees.

The Manager shall directly and continuously monitor asset-freezing determinations, as well as any information relevant to their proper implementation, including the total or partial lifting of such determinations in relation to sanctioned Counterparties, with the aim of ensuring immediate compliance with the applicable measures. For this purpose, and without prejudice to the adoption of additional monitoring procedures, the Manager shall monitor the information disclosed on the UNSC website.

The Manager shall also:

(i) Inform the Ministry of Justice and Public Security ("MJSP") and the CVM of the existence of persons and assets subject to asset-freezing determinations that were not immediately complied with, providing the reasons for such non-compliance;

(ii) Immediately report the freezing of assets and any attempts to transfer such assets involving sanctioned Clients to the MJSP, the CVM, and COAF;

(iii) Maintain ongoing verification of the existence or emergence, within its scope of activities, of assets subject to asset-freezing determinations, for purposes of implementing the measures established by the relevant sanctioning authorities; and

(iv) Promptly implement the total or partial lifting of sanctions measures whenever authorized by the competent authorities.

7.3 Compliance with Regulations of Different Jurisdictions

The Manager conducts the management of investment vehicles established in foreign jurisdictions and is therefore subject to compliance obligations under the laws of all countries in which such vehicles are domiciled.

Such investment vehicles maintain specific policies and procedures in force, subject to the laws of the jurisdictions to which they are subject, for the prevention and detection of money laundering and the combating of terrorist financing.

7.4 Whistleblowing Channel

The Manager shall maintain a formal whistleblowing channel ("Whistleblowing Channel"), with direct access and preferably anonymous reporting, through which any Employee, Partner, or third party may report suspected violations of this Policy, AML/CFT legislation, or any improper conduct related to money laundering, terrorist financing, or corruption. The Whistleblowing Channel shall be the email address compliance@teracapital.com.br.

The Whistleblowing Channel shall observe the following minimum requirements:

(i) assurance of confidentiality and anonymity of the whistleblower, secured through appropriate technical or operational mechanisms;
(ii) express prohibition of any form of retaliation against whistleblowers acting in good faith;
(iii) a maximum period of 15 (fifteen) business days to acknowledge receipt of the report and initiate investigation by the Compliance Department; and
(iv) registration and archiving of all reports received, including indication of the outcome of the investigation, for a minimum period of 5 (five) years.

The submission of false reports containing fabricated information or made with deliberate knowledge of their falsity constitutes a violation of this Policy and shall subject the offender to the penalties provided for in Section 7.6.

7.4 Sanções Aplicáveis por Descumprimento da Presente Política

Failure to comply with this Policy shall subject the offender to penalties including warning, suspension, contractual termination, disengagement, and/or dismissal for cause, depending on the severity of the misconduct committed.

Employees are required to report to the Manager's Compliance Department all actions or omissions suspected of violating any provision of this Policy. Deliberate failure to report such conduct may be considered serious misconduct, giving rise to the penalties provided for by law and under the Manager's other internal policies. The submission of false reports containing fabricated information or made with deliberate knowledge of their falsity shall also constitute a violation of this Policy.

7.6 Applicable Sanctions for Non-Compliance

Failure to comply with this Policy shall subject the offender to penalties including warning, suspension, contractual termination, disengagement, and/or dismissal for cause, depending on the severity of the misconduct committed.

Employees are required to report to the Compliance Department all actions or omissions suspected of violating this Policy. Deliberate failure to make such report may be considered serious misconduct, giving rise to the penalties provided for by law and under the Manager's other internal policies.

758 Leopoldo Couto Magalhães Jr. Street, 2nd floor / 04542000 / Sao Paulo / Brazil