POLICY FOR PREVENTION OF MONEY LAUNDERING, TERRORISM FINANCING AND FINANCING OF PROLIFERATION OF MASS DESTRUCTION WEAPONS

OF

LIGHTROCK GESTORA DE RECURSOS LTDA.

APRIL 17, 2023

INTRODUCTION

LIGHTROCK GESTORA DE RECURSOS LTDA. is a limited business company with its head office in the city of São Paulo, state of São Paulo, at Avenida Brigadeiro Faria Lima, No. 3477, Suite 42-A, Zip Code 04.538-133, Itaim Bibi, registered with the National Corporate Taxpayer's Register of the Ministry of Economy (" CNPJ/ME ") under No. 27.927.837/0001-37 ("Manager"), accredited by *Comissão de Valores Mobiliários* (the Brazilian Securities Commission) (" CVM ") to conduct the professional activity of securities portfolio management, as asset manager, pursuant to CVM Resolution No. 21, of February 25, 2021, as amended ("CVM Resolution 21").

The Manager is a member of the Lightrock group ("Lightrock Group"), a global asset and securities management group, acting as manager of specialized investment funds and other investment vehicles, which invest in a wide range of industries, geographies, classes of asset and investment strategies.

In view of the nature of the management activities it develops, the Manager is subject to an extensive legislation, regulation and self-regulation in the Brazilian market. In order to fully meet the applicable legislation, regulation and self-regulation requirements, as well as to adjust its activities to the best market practices, the Manager adopts the following internal policies: (i) code of ethics; (ii) securities trading policy; (iii) risk management and liquidity management policy; (iv) business plan; (v) information security policy; (vi) order division and apportionment policy; (vii) compliance and internal controls policy; (viii) this policy for prevention of money laundering, terrorism financing and financing of proliferation of mass destruction weapons ("AML/CFT"); (ix) third-party contracting policy; and (x) private credit management policy (jointly, the " Internal Policies").

All the Manager's partners, officers, directors, managers and employees directly involved in the securities portfolio management activities ("Associates"), related to the Manager on the date of preparation of the Internal Policies and/or who become part of the Manager's professionals body shall receive a copy (in printed and digital versions) of the Internal Policies.

The Manager establishes this AML/CFT policy ("Policy"), in order to establish the general provisions on AML/CFT and the fight against corruption acts ("Anti-Corruption Policy").

Upon receiving a copy of this Policy, the Associates shall sign an Instrument of Adhesion, according to the form of Exhibit I to the Manager's Compliance and Internal Controls Policy ("Instrument of Adhesion").

Associates may also consult this Policy at the Manager's website: www.lightrock.com.

This Policy shall be updated by the Manager's Chief Compliance, Risk and AML/CFT Officer, in order to reflect any changes in applicable legislation, regulation, self-regulation and best practices. Whenever this Policy is updated, Associates shall receive a new copy of the updated Policy (printed and scanned), and shall sign a new Instrument of Adhesion.

The Instruments of Adhesion signed by Associates shall be scanned and filed by the Chief Compliance, Risk and AML/CFT Officer, and shall be kept for the entire period of the professional relationship with the Associate, and for an additional period of at least five (5) years counted from the Associate's termination date, for any reason.

In addition to reading this Policy, all Associates shall read and understand the set of rules applicable to the Manager within the legal, regulatory and self-regulatory scope. In case of doubts on the rules to be analyzed and/or regarding the interpretation of the content thereof, Associates shall contact the Chief Compliance, Risk and AML/CFT Officer for the necessary clarifications.

The provisions of the Policy shall be interpreted in an integrated manner by Associates, who shall take into account the Manager's set of internal policies, as well as the applicable legislation, regulations, self-regulation and best market practices.

Organizational Structure of the Manager

The Manager was established to conduct the management of securities portfolio, and its organizational structure is divided into two (2) distinct areas, namely: (i) asset management, and (ii) compliance, risk management and AML/CFT. The Manager establishes and develops mechanisms to ensure the independent performance of all areas.

The main functions of each of the executive boards are described below:

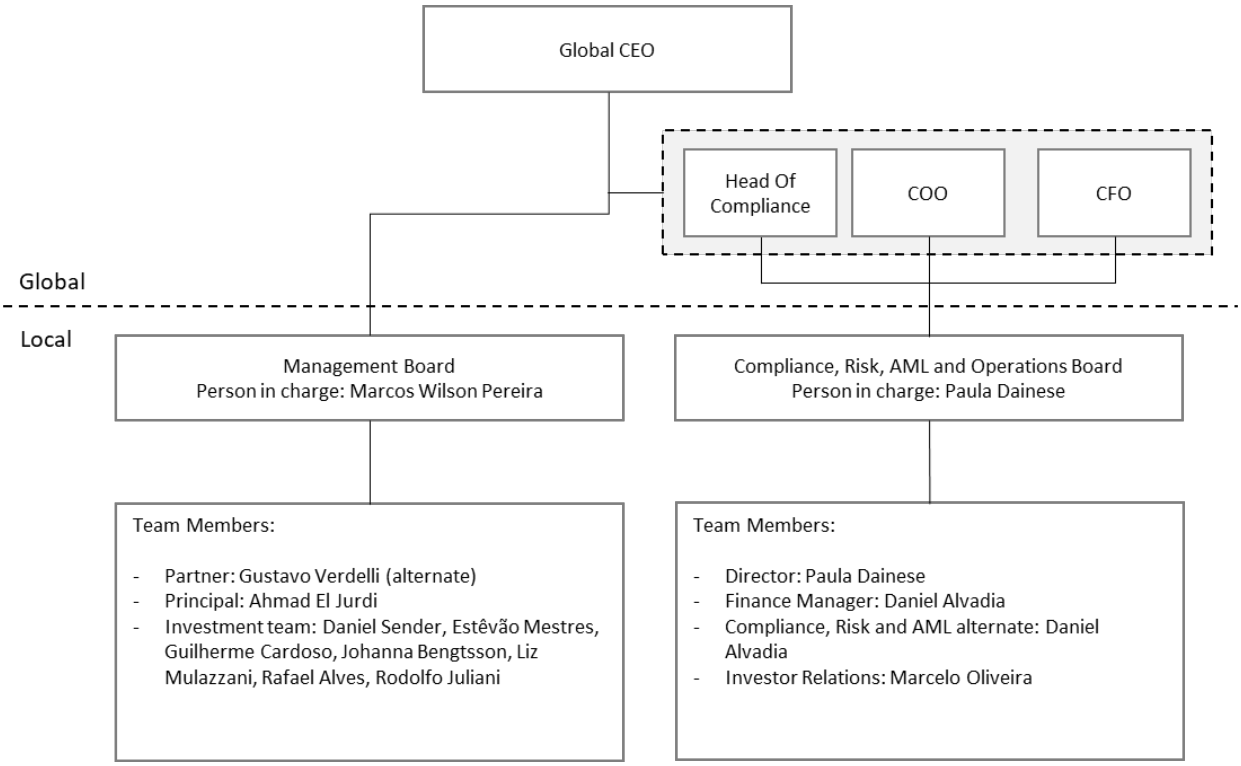
- Asset Management Board: responsible for the management of managed portfolios, which shall be carried out in accordance with the strategies and the industry, financial assets and private equity analysis. The executive board is leaded by a "Chief Management Officer", designated directly in the Manager's Articles of Association, pursuant to art. 4, item III, and paragraph 7, of CVM Resolution No. 21; and

- Compliance, Risk and AML/CFT Executive Board: responsible for (i) the risk management of portfolios administered by the Manager and the risk monitoring of financial assets, as described in the Manager's Risk Management and Liquidity Management Policy, (ii) developing, approving, implementing and monitoring rules, policies, procedures and internal controls adequate to the operational standards and

legal and regulatory conduct, and (iii) the compliance with policies, procedures and internal controls related to the prevention of money laundering, terrorism financing and financing of proliferation of mass destruction weapons. The executive board is leaded by a "Chief Compliance, Risk and AML/CFT Officer", designated directly in the Manager's Articles of Association, pursuant to art. 4, items IV and V, and paragraph 7 of CVM Resolution No. 21, CVM Resolution No. 50, of August 31, 2021, and Law No. 9.613.

As applicable, local experts and the global support team shall offer full support to the executive boards autonomously, performing tasks and operational procedures, and developing back office tasks essential to the development of the Manager's activities.

The organization chart of the organizational structure to be adopted by the Manager is as follows:



Without prejudice to the provisions of this Policy, as an entity member of the Lightrock Group, the Manager is subject to the provisions of the Lightrock Group's policies and codes of conduct, which establish guidelines and rules for AML/CFT and fighting of corruption acts, as applicable to all associates of the Lightrock Group and its affiliates.

1. MONEY LAUNDERING PREVENTION AND FIGHTING POLICY

1.1. INTRODUCTION AND ORGANIZATIONAL STRUCTURE

"Money Laundering" is the process by which funds arising from illicit activities are entered into the financial system, seeking to apart them from their illegal origin. To that end, several and sophisticated transactions are carried out, with the financial system being one of the main business environments used.

For this reason, legal requirements were created (derived from Law No. 9.613, of March 3, 1998) and regulatory requirements that could be applied to individuals related to the financial and capital markets, among others, so that they have internal policies that allow the identification, tracking and communication of suspected money laundering transactions, providing for administrative sanctions for non-compliance.

The Manager is aware that, as a legal entity providing services within the capital market, it takes the risk of being used for Money Laundering purposes. To mitigate such risk, this Policy, in line with the applicable legislation and regulations, presents the AML/CFT guidelines for the purpose of preventing the securities portfolios and investment funds managed by the Manager from being used and/or acquired in money laundering processes.

In order to achieve the highest levels of corporate governance and to protect the Manager and its Associates, the Manager shall require everyone to adhere to this AML/CFT Policy and to observe the AML/CFT Guide in the Brazilian Capital Market, as prepared by Anbima ("Anbima AML/CFT Guide"), and any new version of the Anbima AML/CFT Guide that may be published, whenever the new rules are more comprehensive or stricter than the current rules.

1.2. REGULATORY BASIS

The main legal source of rules that regulate the prevention of money laundering consists of Federal Law No. 9.613/98, as amended by Laws No. 10.701/03 and No. 12.683/12 (jointly referred to as "Money Laundering Law"), which provides for the definition of the crime of money laundering, preventive measures, the suspicious transaction reporting system, the creation of a financial intelligence unit (Council for Financial Activities Control – "COAF") and several international cooperation mechanisms.

In addition, regulators (CVM, Central Bank of Brazil, Superintendence of Private Insurance, Federal Council of Real Estate Brokers and Supplementary Pension Secretariat) and COAF

from time to time issue infra-legal regulations (circulars, official letters, resolutions and instructions) establishing specific rules to prevent money laundering.

Concurrently, self-regulation bodies also contribute to the development of best practices to fight money laundering in the market. Among them, *Associação Brasileira das Entidades dos Mercados Financeiro e de Capitais* (the Brazilian Financial and Capital Market Association) ("Anbima") stands out, with summary legislation and a manual of minimum provisions to be observed by its members.

In addition to the Money Laundering Law, among the main disciplinary rules of the financial market with regard to the prevention and fighting of money laundering, it is worth mentioning:

(i) BACEN Circular No. 3.461/09 - Provides for the procedures to be adopted in the prevention and fighting activities related to the crimes provided for in Law No. 9.613/98;

(ii) BACEN Official Letter No. 3.430/10- Clarifies aspects related to the prevention and fighting activities related to the crimes provided for in Law No. 9.613, of March 3, 1998, addressed in Circular No. 3.461, of July 24, 2009;

(iii) BACEN Official Letter No. 3.542/2012 - Discloses a list of transactions and situations that may evidence the occurrence of crimes of money laundering, and establishes procedures for their report to the Central Bank of Brazil;

(iv) CVM Resolution No. 50, of August 31, 2021 – Provides for the prevention of money laundering, terrorist financing and financing of proliferation of mass destruction weapons – AML/CFT, within the scope of the securities market ("CVM Resolution 50");

(v) Rules issued by COAF – *Conselho de Controle de Atividades Financeiras* (the Brazilian Financial Activities Control Council); and

(vi) ANBIMA AML/CFT Guide.

In this regard, having in mind that: (i) the activity of securities portfolios administration and management is provided for in Federal Law No. 6.385/79, which activity is subject to a proper authorization and inspection by CVM, under the terms of CVM Resolution No. 21; and (ii) that the establishment, management and operation of the several types of investment funds are subject to specific regulation by CVM, including, without limitation, CVM Instruction 356/01, CVM Instruction 399/03, CVM Instruction 432/06, CVM Instruction

444/06, CVM Instruction 459/07, CVM Instruction 472/08, CVM Instruction 555/14 and CVM Instruction 578/16, as amended, and the provisions of CVM Resolution 50 apply to the foregoing activities, with regard to the prevention of money laundering.

1.3. MONEY LAUNDERING PREVENTION

The Money Laundering Law defines as Crimes of Laundering or Concealment of Assets, Rights and Resources to hide or disguise the nature, origin, location, disposition, operation or ownership of assets, rights or resources arising, directly or indirectly, from a criminal offense.

Anyone who, in order to hide or disguise the use of assets, rights or resources of criminal offense, performs the following, also commits the crime:

(i) Converts them into lawful assets;

(ii) Acquires, receives, exchanges, negotiates, gives or receives in guarantee, keeps, maintain in deposit, operates or transfers them;

(iii) Imports or exports assets at amounts not corresponding to the true amounts;

(iv) Uses, in economic or financial activity, assets, rights or resources, knowing that they are derived from a criminal offense;

(v) Participates in a group, association or office, knowing that its main or secondary activity is aimed at committing crimes provided for in the Money Laundering Law.

The purpose of money laundering is to try to hide the true origin of profits obtained from criminal activities, that is, to pretend that the money comes from a lawful activity. Offenders intend to launder the money obtained by illicit means before they can safely spend it or make an investment.

The money laundering process involves three stages, namely: placement, concealment and integration.

Placement is the stage in which an offender introduces money obtained illicitly into the economic system through deposits, purchase of negotiable instruments or purchase of assets. It consists of the removal of money from the place where it was illegally acquired and its inclusion, for example, in the financial market.

Concealment is the moment when an offender carries out suspicious transactions that characterize the crime of laundering. In this phase, the offender performs complex transactions used to disassociate themselves from the illegal source of the money.

By its integration, the illegal resource becomes definitively part of the economic and financial system. From this moment on, the money is given a legal appearance.

1.4. EVIDENCE OF MONEY LAUNDERING

In accordance with the provisions of the aforementioned Law, and with the provisions of the above "*Money Laundering Prevention*" section, it is of the utmost relevance that all Associates are aware of the transactions that characterize evidence of money laundering. The following transactions are considered evidence of money laundering:

(i) The amounts of which appear objectively incompatible with the declared professional occupation and financial situation;

(ii) Those carried out between the same parties or for the benefit of the same parties, in which there are successive gains or losses with regard to any of the parties involved;

(iii) Those showing significant fluctuation in relation to the volume and/or frequency of transactions of any of the parties involved;

(iv) The developments of which include characteristics that may represent an artifice to circumvent the identification of the staff involved and/or respective beneficiaries;

(v) The Which characteristics and/or developments of which show that they consistently act on behalf of third parties;

(vi) Those showing a sudden and objectively unjustified change in relation to the operational modalities normally used by the person(s) involved;

(vii) Those carried out for the purpose of generating loss or gain for which there is, objectively, no economic basis;

(viii) With the participation of individuals residing or entities organized in countries that do not apply or insufficiently apply the recommendations made by the Financial Action Task Force - FATF;

(ix) Private transfers of funds and securities, with no apparent reason;

(x) Those wherein it is not possible to identify the beneficial owner; and

(xi) Those which degree of complexity and risk appear to be incompatible with the technical qualification of a customer or their representative.

The following practices may also be configured as evidence of money laundering:

(i) Resistance in providing the necessary information for opening and updating an account;

(ii) Declaring bank accounts and/or modifying them on a regular basis; and

(iii) Designate an attorney who does not have an evident relationship.

Once identified, any events of suspected money laundering shall be reported to the Chief Compliance, Risk and AML/CFT Officer, who shall be responsible for respecting the secrecy of the report, providing proper fact-finding and sending a report to regulators detailing the facts and the measures that were taken.

1.5. CRIMES OF TERRORISM

Law No. 13.260/16 defines terrorism as the performance, by one or more individuals, of the acts described below for reasons of xenophobia, discrimination or prejudice based on race, color, ethnicity and religion, when committed for the purpose of causing social or widespread terror, exposing individuals, property, public peace or public safety to danger.

The following are acts of terrorism:

(i) Use or threaten to use, transport, store or carry explosives, toxic gases, poisons, biological, chemical, nuclear contents, or other means capable of causing damage or mass destruction;

(ii) Sabotage the operation or seize, using violence, serious threat to a person or cybernetic mechanisms, the total or partial control, even if temporarily, of means of communication or transport, ports, airports, railway stations or highways, hospitals, nursing homes, schools, sports stadiums, public facilities or places used to operate essential public services, energy generation or transmission facilities, military

facilities, oil and gas exploration, refining and processing facilities, and banking institutions and their service network;

(iii) Attempt against the life or physical integrity of an individual; and

(iv) Offer or receive, obtain, keep, maintain in deposit, request, invest or in any way contribute to obtain an asset, property or financial resource for the purpose of financing, in whole or in part, an individual, group of individuals, association, entity, criminal organization, having as main or secondary activity, even on an occasional basis (sic).

1.6 OFFICER RESPONSIBLE FOR MONEY LAUNDERING PREVENTION

Pursuant to article 8 of CVM Resolution No. 50, and Official Letter No. 05/2015/SIN/CVM, the Manager emphasizes that the Officer responsible for this policy and for all provisions concerning the Prevention of Money Laundering is the Chief Compliance, Risk and AML/CFT Officer, a position assigned in accordance with the Manager's Articles of Association.

In case any Associate has doubts or does not fully understand the provisions contained in this Policy and/or the legislation and regulations in force, such Associate shall seek assistance from the Chief Compliance, Risk and AML/CFT Officer by email.

In case the Chief Compliance, Risk and AML/CFT Officer is replaced, such replacement shall be informed to CVM and other regulatory entities, as applicable to the Manager, within seven (7) business days counted from heir qualification.

In addition, all Associates shall be promptly informed and shall receive the nomination and contact details of the respective replacement.

1.7 RESPONSIBILITIES

The Chief Compliance, Risk and AML/CFT Officer is responsible for coordinating the implementation and periodic maintenance of the structure capable of promoting the activities resulting from this Policy, seeking to use corrective actions to remedy deficiencies or failures in this regard.

Pursuant to CVM Resolution 50, the Chief Compliance, Risk and AML/CFT Officer has the following main powers and duties:

(i) Evaluate possible events of suspicious transactions or operations;

(ii) Ensure that mechanisms are in place for the recording and appropriate monitoring of documents related to this Policy;

(iii) Prepare a report on the internal assessment of risk situations to be forwarded to senior management bodies, annually, by the last business day of April, explaining whether there are politically exposed persons and/or non-profit organizations;

(iv) Provide or promote training to ensure the appropriate methodology and communication of this Policy requirements to those responsible;

(v) Support the implementation, maintenance and improvement of this Policy;

(vi) Review and take measures, in case of occurrences of exceptions to this Policy;

(vii) Present recommendations to mitigate the identified risks;

(viii) Review and take measures, in case of occurrences of exceptions to this Policy; and

(ix) Ensure that appropriate corrective measures are taken to remedy any reported deficiencies or incidents.

The Chief Compliance, Risk and AML/CFT Officer shall be responsible for AML/CFT activities, and shall use all tools that are necessary and in compliance with this Policy and the applicable regulations.

The team responsible for analyzing the events described in this Policy, under the guidance of the Chief Compliance, Risk and AML/CFT Officer, is composed of professionals with the technical qualification and experience necessary to carry out activities related to the Prevention and Fighting of Money Laundering, being compatible with the size and complexity of its operations, and has absolute independence and autonomy from the Chief Portfolio Management Officer and his team.

The Chief Compliance, Risk and AML/CFT Officer may, if necessary: (i) determine the suspension of negotiations understood as suspicious transactions or operations; and (ii) contact the proper authorities, at their discretion, without prior authorization.

1.8 KNOW YOUR CLIENT - KYC

The Manager does not provide trust administration, custody, intermediation or securities distribution services, always acting in partnership with financial institutions or not, accredited by CVM for the provision of such services and, for this reason, it shall adopt individually, for each fund under its management, the KYC procedures defined by the respective fund administrator.

1.9 KNOW YOUR PARTNER – KYP

The principle of the Manager is, whenever it enters into agreements, negotiations or transactions necessary for maintenance of the asset portfolio of its investment funds under management, to identify the counterparty, in order to prevent such counterparty from using the management institution and/or the investment funds or managed portfolios for illegal or improper activities.

The Manager adopts the policy 'know the counterparty' of transactions selected by the Manager for investment by the investment funds under its management. In addition to identifying the counterparty and the respective beneficial owner of the transaction through the preparation of registration, such procedure shall also include the knowledge by the Manager of the activities of such counterparty and beneficial owner (as applicable), the potential of its businesses and the analysis of the underlying financial rationale to perform the transaction with funds managed by the Manager. Thus, the Manager protects its reputation and reduces the risk of its products and services being used to legitimize funds from illegal activities.

The Manager's counterparty analysis process is included within the scope of the manager's obligations, and the following issues shall be investigated:

(i) Establish the identity of each counterparty;

(ii) Know the activity and risks inherent to the activity of a counterparty;

(iii) Know the origin of the counterparty's equity;

(iv) Verify the origin and use of funds operated by a counterparty.

The Manager understands that, in order to effectively prevent money laundering, it is necessary to assess the risk posed by its counterparties and their activities, prior to the actual transaction of the business. To help with such assessment, the Manager may use its own Due

Diligence Questionnaire, or even carry out due diligence visits, in order to ensure that business partners have adequate money laundering prevention practices.

1.10 KNOW YOUR EMPLOYEE - KYE

The Manager adopts a strict conduct in hiring its Employees.

Before joining the company, applicants shall be interviewed by officers. In addition to objective requirements, other requirements related to market reputation and profile shall be assessed, as well as applicant's professional background.

The Manager maintains an ongoing training program for its employees, aimed at disclosing its Policy, in order to avoid possible illicit practices.

The process ‘know your employees’ takes place upon the hiring, by checking information and obtaining personal documents, the delivery of the Code of Ethics and Conduct with the reading and subsequent signing of the Instrument of Adhesion by employees, ongoing monitoring processes to follow up on changes in the financial standard of employees, onboarding training.

Special attention shall be given to monitoring the conduct of employees, especially those who perform functions related to the handling of financial instruments, customer relations and information control.

In addition, any suspected or confirmed cases of employee involvement in transactions or operations considered uncommon shall be reported to the Chief Compliance, Risk and AML/CFT Officer, who shall adopt the necessary procedures.

1.11 MONITORING, ANALYSIS AND REPORT OF SUSPECT TRANSACTIONS AND SITUATIONS

The Manager monitors the activities and information under its knowledge, focusing on the compliance with its money laundering crime prevention policy.
Among the situations monitored, the Manager adopts specific procedures and care in the following situations:

The contracting of third-party intermediaries, acting on behalf of the Manager, especially upon dealing with Public Officials and Politically Exposed Persons, poses the risk of violations of anti-corruption legislation for which Manager may be responsible.

Any third party that may deal with Public officials, Politically Exposed Persons or with individuals or entities in a position capable of offering business advantages to the Manager shall not be contracted to provide services on behalf of the Manager or any of the funds under its management, without:

(i) carrying out an analysis, focusing on activities, reputation, integrity and policies and codes of conduct to address the issues of money laundering prevention and anti-corruption of such service provider, which analysis has to be properly documented and provide satisfactory results; and

(ii) formalizing the contracting by means of a written agreement, which includes an express section forbidding such service provider from offering or making payments, granting advantages or giving gifts to Public Officials or Politically Exposed Persons in an improper manner, which constitutes or may be understood as bribery, or which are in violation of anti-corruption legislation.

The scope of such analysis shall vary from case to case. For example, the analysis may be waived when a third party is a duly organized and regulated investment bank, or a law firm or an accounting firm recognized at national or international level, since, in general, it is presumed that such organizations maintain strict standards with regard to anti-corruption and anti-money laundering issues. However, if there is any suspicion about the integrity or unlawful conduct of an individual, acting as a representative of any of such entities, any reviews, audits and further inquiries may be carried out to solve such suspicions prior to the contracting.

In the case of a service provider based in countries clearly known to have a high level of corruption, the analysis shall be conducted more strictly, and shall have an exhaustive documentation of all issues analyzed.

The satisfaction of such analyzes shall be determined by the Chief Compliance, Risk and AML/CFT Officer.

In addition to the foregoing, the following events are considered red flags:

(i) Transactions carried out in the securities market:

(a) between the same parties or for the benefit of the same parties, in which there are successive gains or losses with regard to any of the parties involved;

(b) which show significant fluctuation in relation to the volume or frequency of transactions of any of the parties involved;

(c) which developments include characteristics that may be an artifice to circumvent the identification of the staff involved and respective beneficiaries;

(d) which characteristics and developments show performance, consistently, on behalf of third parties;

(e) which show a sudden and objectively unjustified change in relation to the operational modalities usually used by those involved;

(f) which degree of complexity and risk appear to be incompatible with: (a) the profile of a customer or their representative, under the terms of the specific regulation that provides for the duty to verify the adequacy of products, services and transactions to the customer's profile; and (b) with the client's size and corporate purpose;

(g) for the apparent purpose of generating loss or gain for which there is, objectively, no economic or legal basis;

(h) private transfers of funds and securities without apparent reason, such as: (a) between current accounts of investors with an intermediary; (b) ownership of securities without financial transactions; and (c) securities outside the organized market environment;

(i) deposits or transfers made by third parties for the settlement of customer transactions, or the provision of guarantee in transactions in the future settlement markets;

(j) payments to third parties, in any form, on account of the settlement of transactions or redemption of amounts deposited in guarantee, registered in the name of the client; and

(k) transactions carried out other than at their market price.

(ii) Transactions and events related to individuals suspected of involvement in terrorist acts, such as those involving:

(a) assets affected by sanctions imposed by the UNSC resolutions under Law No. 13.810, of March 8, 2019;

(b) assets subject to a request for unavailability issued by a foreign central authority, which request becomes known;

(c) the carrying out of business, regardless of the amount, by individuals who have committed or attempted to commit terrorist acts, or have participated in or facilitated their commission, pursuant to the provisions of Law No. 13.260, of March 16, 2016;

(d) securities owned or controlled, directly or indirectly, by individuals who have committed or attempted to commit terrorist acts, or have participated in or facilitated their commission, pursuant to the provisions of Law No. 13.260/2016;

(e) operation likely to be associated with the terrorism financing, pursuant to the provisions of Law No. 13.260/ 2016; and

(iii) Transactions with the participation of individuals, legal entities or other entities resident, with their head offices located or organized in countries, jurisdictions, dependencies or locations:

(a) which do not apply or apply improperly the FATF recommendations, according to lists issued by that body;

(b) with favored taxation and subject to privileged tax regimes, according to rules issued by the Federal Revenue Office of Brazil;

(c) with a reputation for involvement in acts of corruption and money laundering;

(d) which have refused to guarantee compliance with anti-corruption and anti-money laundering laws;

(e) which have requested an excessive fee to be paid in cash or otherwise;

(f) which only make and receive payments through offshore accounts;

(g) which have a Public Official or a Politically Exposed Person as their controlling shareholder, or have relations with government entities, Public Officials or a Politically Exposed Person;

(h) contracting a consultant specifically appointed by a Public Official to obtain a government contract under the responsibility of such Public Officials;

(i) a service provider who has requested the issuance of notes, invoices or any other false or tampered documents;

(j) service providers who insist on keeping their identity secret from any Public Official, Politically Exposed Person or government entity;

(k) service providers who refuse, when requested, to disclose the identity of their partners, officers, directors or representatives;

(l) service provider who requests the diversion of the agreed terms of payment to "secret" accounts;

(m) lack of documentation supporting the transactions carried out, including invoices and payment receipts;

(n) the contracting of useless service providers;

(o) commercially unreasonable travel expenses; and

(p) Politically Exposed Persons included in the list of paid employees.

Such guidelines shall be checked on an ongoing, timely and regular basis by the Manager and, whenever there is any suspicion, it shall be reported to the regulators and to the trustee of the funds under the Manager's management, with the evidence of money laundering or the performance of corruption acts.

The Manager shall pay special attention upon contracting portfolio management services by clients, which are (i) non-resident investors, especially when organized as trusts and companies issuing bearer securities; (ii) investors with wealth managed by the areas of financial institutions; and (iii) politically exposed persons.

The Manager shall, through an informed analysis, report to the Financial Intelligence Unit all suspicious situations and transactions identified, or proposals for transactions that may be serious evidence of crimes, such as "laundering" or concealment of assets, rights and resources arising from the crimes listed in the applicable legislation.

The report above mentioned shall be made within twenty-four (24) hours from the conclusion of the analysis that characterized the uncommon transaction, the respective proposal, or even

the uncommon situation identified as a suspicion to be reported to the Intelligence Unit Financial.

1.12 RELATIONSHIPS WITH PUBLIC OFFICIALS AND POLITICALLY EXPOSED PERSONS

The Manager has no political alignment with any party, party entity, political representative or any person holding an elective position in the public administration, acting in the provision of its portfolio management services in line with a strong sense of integrity and business-oriented experience, regardless of any political considerations or "advantages".

Associates shall act in order to prevent and remedy any situations of conflict of interest that may occur, both in relation to the Manager and Associates themselves and the public authorities.

Accordingly, all Associates and contracted service providers are forbidden, in the exercise of their activities and in defense of the interests of the Manager from: (i) offering, promising, making, authorizing or providing, directly or through intermediaries, any undue advantage to public officials with the intention of influencing or compensating any official action or decision of such official in favor of the Associates themselves or a service provider and/or the Manager; and (ii) consenting to the receipt, in their own name or on behalf of the Manager, of any type of advantage that may be seen as a payment resulting from acts harmful to the public administration, mainly those related to the practice of corruption.

Any expenses with travel, accommodation and meals shall always be paid by the Manager, even if the invitation comes from a public official, and any gifts received shall expressly follow the provisions of the Manager's Code of Ethics.

The treatment given to investment funds established exclusively or mainly by individuals classified as politically exposed person, Private Banking investors and non-resident investors, in particular companies organized as issuer of bearer shares and trusts, shall receive special care in the relationship, registration, monitoring and following-up of information, data and transactions, compared to other clients, investors and investment funds.

When registering a client, an analysis shall be carried out in order to identify whether the registered individual falls into the category of politically exposed person. Such analysis shall be repeated from time to time for the purpose of identifying whether, after the beginning of the relationship, the client has taken a position or function that may classify them as a PPE. The relationship with PPEs shall be directly supervised by the Chief Compliance, Risk and AML/CFT Officer.

A politically exposed person shall mean an individual who holds or has held in the last five (5) years:

(i) positions, jobs or relevant public functions, in Brazil or in other countries, territories and foreign dependencies, as well as their representatives, family members and other individuals of their close relationship;

(ii) position, job or relevant public function exercised by heads of state and government, high-level politicians, senior civil servants of public authorities, judges or high-level military personnel, directors of public companies or leaders of political parties; and

(iii) family members of an individual who performs the functions defined above, their relatives in the direct line up to the first degree, as well as their spouse, civil partner and stepchildren.

The following are examples of politically exposed persons in Brazil, according to CVM Resolution 50:

(i) holders of elective terms of office of the Executive and Legislative Branches of the Federal Union;

(ii) holders of office in the Executive Branch of the Federal Union:

(a) Minister of State or equivalent;
(b) of a special nature or equivalent;
(c) President, Vice-President and director, or their equivalent, of indirect public administration entities; or
(d) the Senior Management and Advisory Group - DAS, level 6, and equivalent.

(iii) the members of the National Council of Justice, the Federal Supreme Court, the State Superior Courts, the Federal Regional 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 Prosecutors' Office, the Federal Attorney General, the Deputy Federal Attorney General, the Attorney General for Labor, the Attorney General of Military Justice, the Deputy-Federal Attorneys General and the Public Prosecutors General Courts of the States and the Federal District;

(v) the members of the Federal Court of Auditors, the Attorney General and the Deputy Attorneys General of the Public Prosecutor's Office at the Federal Court of Auditors;

(vi) the presidents and national treasurers, or their equivalent, of political parties;

(vii) Governors and Secretaries of State and of the Federal District, State and District Congressperson, presidents, or their equivalent, of state and district indirect public administration entities, and presidents of Courts of Justice, Military Courts, Courts of Accounts, or their equivalent, of States and the Federal District; and

(viii) Mayors, Municipal Councilors, Municipal Secretaries, presidents, or their equivalent, of municipal indirect public administration entities and Presidents of Courts of Auditors, or their equivalent, of Municipalities.

The five-year period shall be counted retroactively from the initial date of the business relationship or the date on which client became a PPE.

Relatives, in the straight line up to the first degree, the spouse, civil partner, and stepchildren are considered family members.

In addition, the following are examples of situations that characterize a close relationship and lead to the classification of a client as a politically exposed person:

- Appointment of a politically exposed person as attorney or agent; and
- Direct or indirect control of a corporate client by a politically exposed person.

Thus, the client is required to make a self-declaration, in case they are or shall become a politically exposed person, at the time of their registration or updating thereof.

1.13 REGISTRATION OF TRANSACTIONS AND DOCUMENT STORAGE

The following documents shall be kept for five (5) years counted from the first day of the year following the end of the relationship or the conclusion of the transactions:

(i) Registration of operations/transactions;

(ii) Payments made in connection with the provision of portfolio management services;

(iii) Report of unusual transactions forwarded to the regulators; and

(iv) Client dossier.

The obligation to preserve documents is irrespective of those imposed by other rules, such as tax legislation.

In addition to preserving information, the Manager has a control system to ensure that (i) the transactions are carried out in accordance with the authorization of the responsible person; (ii) the transactions are recorded with the format and content necessary for the preparation of financial statements in accordance with accounting rules; (iii) the files are only accessed by authorized persons; and (iv) the records are checked from time to time against the assets and any discrepancies are immediately remedied.