Institutional Policy	
Management Area ***Compliance* and Risk Management**	Version **02**
Subject **Internal Controls Manual (*Compliance*)**	Publication Date **06/24/2025**
Scope **Limited to CapSigma Investment Partners Ltda.**	

INTERNAL CONTROLS MANUAL
(*COMPLIANCE*)

CONTENTS

1. INTRODUCTION AND OBJECTIVE

The term "*Compliance*" comes from the English verb "*to comply*" and means "*to* conform to rules, standards and procedures".

Therefore, **CAPSIGMA INVESTMENT PARTNERS LTDA.** ("Manager") has adopted "Internal Controls" or "Compliance" activities within its structure. The officer in charge of *compliance* ("Chief Compliance Officer") is responsible for ensuring compliance with the laws and regulations issued by the competent authorities applicable to Manager's activities, as well as Manager's policies and manuals, and obligations of trust, fiduciary duty and loyalty owed to investment funds and other clients whose securities portfolios are managed by Manager ("Clients"), preventing the occurrence of violations, detecting violations that occur and punishing or correcting any such non-compliance.

This Internal Controls *(*Compliance*)* Manual ("Compliance Manual") was prepared to specifically address the activities carried out by Manager, in accordance with their nature, complexity and inherent risks, subject to the obligation of periodic review and updating pursuant to item 2 below.

This Compliance Manual is applicable to all of Manager's partners, directors, officers, employees, trainees and other collaborators (jointly the "Employees" and, individually and without distinction, the "Employee").

This Compliance Manual should be read in conjunction with the Manager's Code of Ethics, which also contains rules aimed at meeting the objectives described here.

This Compliance Manual is in accordance with the ANBIMA codes and regulations, including, but not limited to, the "*Código de Administração e Gestão de Recursos de Terceiros*" and its "*Regras e Procedimentos do Código de Administração e Gestão de Recursos de Terceiros*" ("ANBIMA Code") , as well as the current regulations issued by the Brazilian Securities and Exchange Commission ("CVM") and the U.S. Securities and Exchange Commission ("SEC").

2. PROCEDURES

2.1. Appointment of a Director in Charge

The Manager's compliance area is headed by the Chief Compliance Officer, duly appointed in the Manager's articles of association.

The Chief Compliance Officer performs his duties with full independence and does not perform any duties that could affect his impartiality, either inside or outside the Manager. Likewise, the compliance area is not subject to any interference by the management team and has the autonomy to question the risks assumed in the operations carried out by Manager.

The Chief Compliance Officer is responsible for the general implementation of the procedures set out in this Compliance Manual, and if he has to be absent for a long period of time, he must be replaced or must appoint a temporary person to carry out his duties during this period of absence. If this appointment is not made, it will be up to the Manager's partners to do so.

The main duties and responsibilities of the Chief Compliance Officer are to provide support to all of the Manager's areas terms of clarifying all internal controls and regulations (compliance), as well as monitoring the compliance of the Manager's operations and activities with the regulatory standards (internal and external) in force, defining action plans, monitoring compliance with deadlines and the level of excellence of the work carried out and ensuring that any deviations identified can be promptly corrected (*enforcement*).

The Chief Compliance Officer's duties also include, without prejudice to others described in this
Compliance Manual:

(i) Implementing internal controls through a culture of compliance, with a view to improving controls;

(ii) Promote a broad knowledge and implementation of ethical values in the actions of all Employees;

(iii) Analyze all situations involving non-compliance with the procedures or ethical values established in this Compliance Manual, or in the Manager´s Code of Ethics, as well as evaluate other situations that have not been provided for in all of the Manager's internal policies ("Internal Policies");

(iv) Define strategies and policies by developing processes that identify, measure, monitor and control contingencies;

(v) Ensure the confidentiality of possible whistleblowers, even when they don't ask for it, except in the case of judicial testimony;

(vi) Request that the appropriate measures be taken in cases where conflicts of interest are identified;

(vii) Recognize new situations in the day-to-day of internal administration or in the Manager's business that were not planned, and analyze these situations;

(viii) Propose studies for possible structural changes to implement or guarantee compliance with the concept of segregation of activities carried out by the Manager;

(ix) To examine in confidence all matters that arise, preserving the image of the Manager as well as that of the people involved in the case.

2.2. Compliance Management System

The Manager adopts a third-party compliance system for compliance management. The system adopted by the Manager allows for the parametrization and execution of compliance testing routines. Monitoring of regulatory and self-regulatory updates, as well as the design and operation of internal controls, is carried out directly by the compliance team. The system does not provide a digital library or document storage functionality. All relevant documents are securely stored in the Manager's cloud environment, with access controls in place and retention periods observed in accordance with applicable legal and regulatory requirements.

Therefore, the Compliance area may store all documents and archives in the system, at its sole discretion. In addition, all activities, events and other records entered into this system have logs for auditing purposes and automatic backups.

2.3. Periodic review and report preparation

The Chief Compliance Officer shall review this Compliance Manual at least annually to verify the adequacy and effectiveness of the policies and procedures set forth herein. Such periodic reviews shall consider, among other factors, violations occurring in the previous period, and any other updates arising from changes in the activities carried out by Manager.

The Chief Compliance Officer shall prepare, at least once a year, a Compliance Review Report, in accordance with Rule 206(4)-7 under the U.S. Investment Advisers Act of 1940, CVM Resolution No. 21 of February 25, 2021 ("CVM Resolution 21"), and the applicable principles of the ANBIMA Code.

This report shall include, among other relevant matters:

(i) a summary of the tests and examinations carried out to assess the effectiveness of the Manager's compliance program;

(ii) the Chief Compliance Officer recommendations regarding any deficiencies identified and the respective timetables for their remediation; and

(iii) a statement issued by the Chief Compliance Officer, in his capacity as the individual responsible for overseeing the Manager's risk exposure and for ensuring effective implementation of the Manager's Risk Management Policy, regarding the identified findings and the corrective measures planned or implemented, in accordance with the established remediation timeline.

The Compliance Review Report shall be submitted to the Executive Committee and made available for inspection by the applicable regulatory authorities. All documentation supporting the report's conclusions shall be retained for a minimum of five (5) years, in accordance with Rule 204-2 of the Investment Advisers Act and Brazilian regulatory requirements.

2.4. Training

Manager has an initial training process and a continuous recycling program of knowledge about the Internal Policies, including this Compliance Manual, applicable to all Employees, especially those who have access to confidential information and/or participate in the investment decision-making process.

The Chief Compliance Officer shall conduct training sessions for Employees periodically, as he deems advisable, so that Employees understand and comply with the provisions set out in this manual and shall be frequently available to answer questions that may arise in relation to the terms of this Compliance Manual and any compliance-related rules.

The minimum periodicity of the continuous retraining process will be annual. Employees will sign a document attesting to their participation in each continuous retraining process and the Chief Compliance Officer shall retain all records for the legally required timeframe.

The materials, workload and timetable will be defined by the Chief Compliance Officer, who may even hire third parties to give classes and/or speakers on relevant subjects.

2.5. Presentation of the Compliance Manual and its modifications

The Chief Compliance Officer shall deliver a copy of this Compliance Manual and the Internal Policies to all Employees upon the commencement of their activities at Manager, and whenever these documents are amended. Upon receipt of this Compliance Manual, the Employee shall confirm that he/she has read, understood and complies with the terms of this Compliance Manual and the Internal Policies, by signing the term of adhesion which shall follow the format set forth in Annex I ("Adhesion Term").

2.6. External Activities

Employees must obtain the written approval of the Chief Compliance Officer before engaging in business outside the Manager. "External Activities" include being an officer, director or partner of a company or an employee or consultant of any entity or organization (whether on behalf of the Manager or not). Employees wishing to join or engage in such External Activities must obtain the prior written approval of the Chief Compliance Officer by means of the "Request for Performance of External Activity" in the form of Annex II to this Compliance Manual.

Prior authorization from the Chief Compliance Officer is not required for External Activities related to charity, non-profit organizations, clubs or civil associations so long as it does not represent a conflict of interest to the Manager and/or the role the Employee exercises at the Manager.

2.7. Supervision and responsibilities

All matters of violations of compliance obligations, or doubts relating thereto, which come to the attention of any Employee must be promptly reported to the Chief Compliance Officer, who must investigate any possible violations of compliance rules or procedures, and determine which sanctions are applicable.

2.8. Sanctions

Sanctions arising from non-compliance with the rules established in this Compliance Manual and/or the Internal Policies shall be defined and applied by the Chief Compliance Officer, at his reasonable discretion, guaranteeing the Employee, however, a broad right of defense. Penalties of warning, suspension, termination or dismissal for cause, if applicable, may be imposed, among others, under the terms of current legislation, without prejudice to the application of penalties by the CVM, the SEC and Manager's right to claim compensation for any losses incurred, damages and/or lost profits, through the appropriate legal procedures.

3. CONFIDENTIALITY, MNPI AND INFORMATION SECURITY POLICY

The manager adopts robust procedures to ensure the protection of confidential information and Material Non-Public Information (MNPI), in accordance with CVM Resolution 21, ANBIMA Code, Rule 204A-1 and Rule 204-2 under the Investment Advisers Act of 1940, and related SEC guidance.

Material Non-Public Information (MNPI) refers to any information not yet disclosed to the public and which a reasonable investor would consider important when making an investment decision. This includes, but is not limited to non-public earnings data, undisclosed investment decisions, significant corporate events, or confidential client information. The improper use or disclosure of MNPI is strictly prohibited and may result in disciplinary and legal consequences under Brazilian and U.S. securities law.

The information obtained as a result of the professional activity carried out by each Employee at the Manager is considered confidential and may not be transmitted in any way to third parties other than Employees or to unauthorized Employees on a "need to know" basis.

3.1. Information Security and Protection of MNPI

3.1.1 Access Controls and Confidentiality Principles

Manager maintains an up-to-date inventory which identifies and documents the existence and main characteristics of all information assets, such as internal databases, servers, models, cloud directories, reports and others. No confidential information should, under any circumstances, be disclosed to any person, inside or outside the Manager, who do not need or should not have access to such information for the performance of their professional activities.

Manager has implemented "information barriers" (also known as Chinese Walls) to restrict access between areas that may handle MNPI (e.g., investment team) and those responsible for client relations, compliance or back-office activities.

In the event that an Employee moves between areas, he/she shall only have access to the information relating to this area which he/she needs to carry out the new activity, and shall no longer be allowed access to the data, files, documents and other information restricted to the activity previously carried out. In the SharePoint directory, folders to which a user does not have access are not visible in the user's interface, ensuring confidentiality and limiting exposure to information. Access to folders, files, and internal systems is password-protected and tracked.

In the event of termination of employment with Manager, the Employee shall immediately cease to have access to any of Manager's internal information assets.

Any information about the Manager, or of any nature relating to the Manager's activities, its partners and Clients, obtained as a result of the performance of the Employee's normal activities at Manager, may only be provided to the public, the media or other bodies if authorized in writing by the Chief Compliance Officer.

3.1.2 Handling and Circulation of Confidential Information

All Employees, as well as all third parties hired by the Manager, must sign a confidentiality document regarding confidential, reserved or privileged information entrusted to them as a result of their professional activities.

It is strictly forbidden for Employees to make copies or print out the confidential files and MNPI and to circulate in environments outside Manager with these files, since such files contain information that is considered confidential information.

The above prohibition does not apply when the copies or printing of the files are for the benefit of the execution and development of the business and the interests of the Manager and its Clients. In such cases, the Employee in possession and custody of the copy or printing of the file containing the confidential information shall be directly responsible for its proper preservation, integrity and maintenance of its confidentiality.

3.1.3 Secure Disposal and Data Handling Procedures

In addition, any printouts of documents must be immediately removed from the printing machine, as they may contain restricted and confidential information, even in the Manager's internal environment.

Confidential information on digital media must be disposed of in such a way that it cannot be recovered. All files scanned into temporary folders will be deleted periodically, so that no files should remain there. Failure to comply with this rule will be considered an infraction and will be treated in the same way as someone who forgets material in the printing area.

Physical documents containing confidential information and MNPI or copies thereof must be disposed of immediately after use in such a way as to prevent their recovery.

In addition, Employees must refrain from using *hard drives*, *pen-drives*, floppy disks, tapes, disks or any other means that are not intended to be used exclusively for the performance of their activity at Manager.

3.1.4 Use of IT Resources and Communications Policy

Manager does not allow the use of personal cloud services, messaging apps, or private emails to store, transmit, or discuss confidential information.

It is forbidden to connect equipment to the Manager's network that has not been previously authorized by the Information Technology (IT) and the compliance departments.

Each Employee is responsible for maintaining control over the security of the information stored or made available on the equipment for which they are responsible.

The sending or forwarding by *e-mail* of material containing discriminatory, prejudiced, obscene, pornographic or offensive content is also strictly forbidden, as mentioned above, as well as the sending or forwarding of *e-mails* with opinions, comments or messages that may denigrate the image and/or affect the reputation of the Manager.

Under no circumstances may an Employee issue an opinion by *e-mail* on behalf of Manager, or use Manager's material, brand and logos for non-corporate matters or after the termination of his/her relationship with Manager, unless expressly authorized to do so.

3.1.5 Network Monitoring, Access Logs and Oversight

The Chief Compliance Officer will also monitor and be notified by e-mail in the event of an attempt to access the directories and virtual *logins* on the password-protected server. The Chief Compliance Officer will investigate the circumstances of this occurrence and

apply the appropriate sanctions.

Programs installed on computers, especially via the internet (downloads), whether for professional or personal use, must obtain prior authorization from, the person responsible for the Manager´s IT department. It is not permitted to install any *software* that is illegal or has copyright protection. The installation of new *software*, with the relevant license, must also be notified in advance to the IT manager. The IT manager must approve or veto the installation and use of employees' software for professional and personal purposes.

3.1.6 Backup, Retention and Electronic Records

Manager reserves the right to record any telephone call and/or any communication of its Employees made or received through the office fixed telephone lines or any other means made available by Manager for the professional activity of each Employee.

All the information on the Manager's server, the Clients database and the investment team’s models is sent to the Manager's cloud server. On this server, information is segregated by area and backed up. Backups of all systems are encrypted, performed daily, and stored in secure cloud infrastructure.

The backup routine ensures that all data is safeguarded, be it databases, documents, spreadsheets and various other items stored in the servers' storage area.

In the event of improper disclosure of any confidential information, the Chief Compliance Officer will investigate who is responsible for such disclosure and will be able to verify on the server who had access to said document through the individual access of each Employee. Manager will retain all digital records in accordance with SEC Rule 204-2 for a minimum of five years.

Security tests will be carried out on the information systems used by the Manager at least once a year to ensure the effectiveness of the internal controls mentioned in this Compliance Manual, especially information held electronically.

3.2. Intellectual property and external disclosures

All models, reports, systems, and methodologies developed by Employees during their time at the Manager remain the intellectual property of the firm. Any unauthorized disclosure or external use is strictly prohibited and subject to legal sanctions.

The use and disclosure of any confidential or proprietary information subject to the Manager’s intellectual property outside the scope of its activities or not intended for Clients shall be subject to the prior express written authorization of the Chief Compliance Officer.

Once the Employee's relationship with the Manager has been severed, he/she will

remain obliged to comply with the restrictions dealt with herein, subject to liability in the civil and criminal spheres.

3.3. Data Protection and Privacy

In compliance with Brazilian Law No. 13.709/2018 (*Lei Geral de Proteção de Dados – LGPD*) and with Regulation S-P under the U.S. Investment Advisers Act, the Manager implements measures to ensure the privacy and protection of nonpublic personal information related to its Clients, Employees, service providers, and other stakeholders.

All personal data is processed solely for purposes compatible with the Manager's activities and is subject to appropriate technical and administrative safeguards. Access is restricted to authorized personnel and governed by strict internal controls. Third parties engaged by the Manager who have access to personal data are contractually bound to equivalent data protection obligations.

Data subjects may exercise their rights under applicable data protection laws, including access, rectification, and deletion, by contacting the Compliance department. Any unauthorized access, loss, or suspected breach of personal information must be reported immediately to Compliance and will be handled pursuant to the Manager's incident response procedures.

4. INSIDE INFORMATION AND INSIDER TRADING

Inside information is considered to be any Material Information (as defined below) about a company that has not been published and that is obtained in a privileged manner as a result of the professional or personal relationship maintained with a Client, with employees of companies studied or invested in, or with third parties, or as a result of the status of Employee.

For the purposes of this Compliance Manual, Material Information shall mean any information, decision, resolution, or any other act or fact of a political-administrative, technical, business or economic-financial nature occurring or related to Manager's business that may have a significant influence on: **(a)** the profitability of the securities managed by Manager; **(b)** the decision of Clients to buy, sell or hold shares of investment funds managed by Manager; and **(c)** the decision of Clients to exercise any rights inherent to the condition of holder of shares of investment funds managed by Manager.

Privileged information needs to be kept confidential by all those who access it, whether as a result of professional activity or personal relationships.

If an Employee has access to Material Information that he or she should not have, he or she must promptly report it to the Chief Compliance Officer and may not communicate it to anyone, not even to other members of the Manager, market professionals, friends or

relatives, or use it for his or her own benefit or that of third parties. If you are uncertain about the privileged nature of the information, you must also report it to the Chief Compliance Officer.

4.1. Insider Trading Policy

The improper use or disclosure of MNPI is strictly prohibited under both U.S. and Brazilian law. In the United States, such conduct is addressed primarily under Section 10(b) and Rule 10b-5 of the Securities Exchange Act of 1934, as well as Section 204A of the Investment Advisers Act of 1940, which requires registered investment advisers to establish and implement written policies designed to prevent the misuse of MNPI. In Brazil, insider trading is regulated under Law No. 6.385/76, as amended ("Brazilian Capital Markets Law") and the CVM Resolution 44. In compliance with these regulatory frameworks, the Manager has adopted this Insider Trading Policy to ensure that its Employees act with integrity, maintain confidentiality, and uphold their fiduciary obligations when handling sensitive information.

Insider trading is defined as the act of trading securities based on MNPI in violation of a duty of confidentiality, trust, or fiduciary obligation. Such information is considered material if a reasonable investor would consider it important when making an investment decision, and non-public if it has not been disclosed broadly to the market.

This conduct includes both:

(i) the use of MNPI for one's own benefit or for the benefit of third parties (directly or indirectly); and

(ii) the disclosure or transmission of MNPI to others (known as *tipping*), where the recipient may reasonably use the information to trade securities or further disseminate it.

It is forbidden for any Employee of the Manager to carry out the aforementioned acts for their own benefit, for the benefit of the Manager or for the benefit of third parties.

Insider trading and tipping are prohibited under:

- Brazilian Law No. 6.385/76, which classifies as a criminal offense the use of relevant, undisclosed information that must remain confidential and is capable of providing an undue advantage through securities trading; and

- U.S. federal securities law, including Section 10(b) of the Securities Exchange Act of 1934, Rule 10b-5, and Section 204A of the Investment Advisers Act of 1940, which require investment advisers to adopt policies designed to prevent the misuse or improper disclosure of MNPI.

Violations of these provisions may result in civil, administrative, and criminal liability, including fines, imprisonment, and regulatory sanctions.

It is the Chief Compliance Officer's responsibility to periodically check, and process notifications received regarding the use by Employees of inside information, insider trading and "tips". Cases involving the use of inside information, insider trading and "tips" must be analyzed not only during the term of the Employee's professional relationship with the Manager, but even after the termination of the relationship, with the incident being reported to the competent authorities.

5. SEGREGATION OF ACTIVITIES POLICY

5.1. Physical segregation

Given that the Manager engages exclusively in the activity of portfolio management, without performing fund administration or distribution services, physical segregation of office areas is not required under applicable regulation. Nevertheless, the Manager maintains adequate functional segregation, with clearly defined responsibilities and internal procedures to mitigate potential conflicts of interest.

Access to operational areas of the office is restricted to authorized Employees, based on their respective roles and responsibilities. The circulation of third parties, including Clients and service providers, is allowed only by prior appointment and limited to designated meeting rooms, ensuring the confidentiality of sensitive information.

The Chief Compliance Officer is responsible for overseeing adherence to internal access and segregation protocols. Any repeated or unjustified attempts by Employees to access restricted areas may result in the application of disciplinary measures, as provided in this Internal Controls Manual.

In addition, the Manager's accounting activities are outsourced, and such services are performed at the premises of the contracted third-party service provider, as an additional layer of independence and control.

5.2. Electronic segregation

In addition, the Manager will operationally segregate its areas by adopting the following procedures: each Employee will have a microcomputer and fixed telephone line for their exclusive use, to avoid sharing the same equipment and/or viewing the information of another Employee. Furthermore, there will be no sharing of equipment between Employees in the investment team and other Employees, and there will be a printer and fax machine exclusively for the use of the investment team.

Specifically with regard to the IT area and the safekeeping, conservation, restriction of use and access to technical information/files, among others, the access to files/technical information will be restricted and controlled, and that such restriction/segregation will be made in relation to (i) position/hierarchical level and (ii) team.

In addition, each Employee will have a user code and password to access the network, which is defined by the person in charge of each area, and only authorized Employees will be able to access information in the investment team. In addition, the Manager's computer network will allow the creation of users with different permission levels, by means of a logical segregation on the servers which ensures that each department has a separate data storage area on the server with access control by user. In addition, the computer network will keep a record of access to and viewing documents, which will make it possible to identify who have and have had access to a given document.

Each Employee will have an exclusive access folder for scanning their files, guaranteeing exclusive user access to the documents they are responsible for. In the event of an Employee leaving the company, all files saved in the respective folder will be transferred to the folder of their direct superior, in order to avoid loss of information.

5.3. Segregation from other companies in which the Manager's partners and/or directors have an interest

The Manager's partners and directors may hold equity stakes in other businesses. In this sense, in order to segregate the activity of asset management and avoid any sharing of information, the Manager determines that partners who have a shareholding in other companies operating in the financial and capital markets may not have a functional role in such a company and should only appear as equity partners. In addition to that, such Employees are required to disclose such participation to the Chief Compliance Officer and keep him updated of any changes in status.

5.4. Specifics of internal control mechanisms

The Manager, through the Chief Compliance Officer, makes any internal guidelines available to all Employees, which must always be complied with, and may address the following points, among others:

(i) Definition of responsibilities within the management company;

(ii) Means of identifying and evaluating internal and external factors that could adversely affect the achievement of the company's objectives;

(iii) Existence of communication channels that ensure that Employees, according to their level of activity, have access to reliable, timely and comprehensible information considered relevant to their tasks and responsibilities;

(iv) Continuous assessment of the various risks associated with the company's activities; and

(v) Systematic monitoring of the activities carried out, so that it can be assessed whether the Manager's objectives are being achieved, whether the established limits and applicable laws and regulations are being complied with, as well as ensuring that any deviations identified can be promptly corrected.

If any employee identifies situations that could be considered a conflict of interest, they must immediately submit them to the Chief Compliance Officer for analysis.

In addition, all Employees shall be provided with equipment and software for which Manager has a license to use, internet access, as well as the necessary materials and support, with the sole purpose of enabling the performance of all activities inherent to Manager's business. In this regard, the Chief Compliance Officer may make available the guideline for the use of technology resources, detailing all the rules that must be followed by each and every Employee, regardless of their hierarchical level within Manager.

6. *MARKETING* MATERIAL

All Employees must be aware that marketing materials must be disclosed strictly in accordance with the rules issued by the SEC, the CVM and the Brazilian Association of Financial and Capital Market Entities - ANBIMA, and that they must not contain any false information or information that could mislead the public.

Marketing materials shall mean any note, circular, letter or other type of written communication intended for people outside the Manager, or any note or advertisement in any publication, radio or television, offering any advisory or management service provided by the Manager, or an investment product of the Manager in the securities market (including managed funds). For purposes of compliance with SEC regulations, marketing materials also include any direct or indirect communication made by the Manager that offers investment advisory services to U.S. persons or investors in private funds, including communications via websites, emails, social media, podcasts, webinars and presentations.

Any marketing materials must be previously submitted to the Chief Compliance Officer, who shall verify whether or not it complies with the various applicable rules, including without limitation the SEC Marketing Rule[1], the CVM resolutions, and the ANBIMA Code. The Chief Compliance Officer shall, when necessary, make use of external advisors to verify compliance with these rules. Only with the written approval of the Chief Compliance Officer should any marketing material be used.

As part of its compliance program, the Manager has implemented specific controls to ensure that all marketing materials distributed to U.S. persons or related to U.S.

[1] *SEC, Rule 206(4)-1 under the Investment Advisers Act of 1940, 17 C.F.R. § 275.206(4)-1*

advisory activities are fully aligned with the SEC's Marketing Rule. These controls include a formal review and pre-approval process by the Chief Compliance Officer, who verifies the accuracy, consistency and completeness of all statements, particularly those related to performance, hypothetical or predecessor returns, and the use of testimonials or endorsements. The Manager may establish internal guidelines and procedures to support the appropriate use of such content, ensuring that it is suitable for the intended audience and does not present a misleading impression. All materials referencing past performance are presented net of fees, with the required disclosures and contextual information to avoid selective or unbalanced presentation. Additionally, any reference to third-party ratings or Client statements is carefully vetted to ensure the required transparency, including disclosure of compensation arrangements where applicable.

Below is a non-exhaustive list of rules applicable to Investment Vehicle marketing materials.

Under the terms of CVM Resolution of December 23, 2022 ("CVM Resolution 175"), any fund disclosure material must, subject to the exceptions provided for in the applicable rules:

(i) be consistent with the funds offering memorandum and the Investment Vehicle mandate, if any;

(ii) be written in calm and moderate language, warning its readers of the risks of the investment;

(iii) be identified as marketing material;

(iv) mention the existence of the Investment Vehicle documentation, as well as the addresses on the World Wide Web from which these documents can be obtained; and

(v) contain information: (a) that is true, complete, consistent and does not mislead the Client; (b) that is written in simple, clear, objective and concise language; and (c) that is useful for evaluating the investment; and (d) that does not ensure or suggest the existence of a guarantee of future results or is not risk- free for the Client.

Factual information must be accompanied by an indication of its source and must be distinguished from interpretations, opinions, projections and estimates.

Any disclosure of information on the fund's results may only be made, by any means, after a grace period of 6 (six) months from the date of the first issue of shares.

All information disclosed by any means, in which reference is made to the profitability of the Investment Vehicle, must be mandatory:

(i) mention the date on which it began operating;

(ii) in addition to the information disclosed, the monthly return and the accumulated return over the last 12 (twelve) months, in which case it is not compulsory to provide a breakdown on a month-by-month basis, or over the period since it was set up, if shorter, noting that the disclosure of returns must be accompanied by a comparison, over the same period, with a market index compatible with the fund's investment policy, if any;

(iii) be accompanied by the average monthly net worth for the last 12 (twelve) months or since its incorporation, if more recent;

(iv) disclose the administration fee and the performance fee, if any, expressed in the regulation in force in the last 12 (twelve) months or since its constitution, if more recent; and

(v) highlight the fund's target audience and the restrictions on fundraising, in order to emphasize any permanent or temporary impossibility of access to the fund by investors in general.

If the administrator hires the services of a risk rating company, it must present the most recent rating given to the fund in all its publicity material, as well as indicating how to obtain further information on the rating.

Also incorporated by reference are the provisions of Chapter VII of ANBIMA's *Regras e Procedimentos* of the ANBIMA´s Code ("ANBIMA Rules and Procedures"), publicly available on ANBIMA's website[2].

7. APPROVAL OF BROKERS AND *SOFT DOLLARS*

The compliance team will maintain a list of approved brokers based on the criteria established by the Manager. The trader will execute orders exclusively with brokers on said list, unless he receives prior authorization from the Chief Compliance Officer to use another broker. The Chief Compliance Officer will update the list of approved brokers as new relationships are established, or existing relationships are terminated or modified.

The most relevant transaction costs, such as brokerage, fees and custody, must be constantly monitored in order to minimize them. Every six months, the Manager's

[2] *https://www.anbima.com.br/pt_br/autorregular/codigos/administracao-de-recursos-de-terceiros.htm*

investment team shall draw up a ranking of brokers with objective criteria, taking into account the quality of service and price, with the aim of finding the best equation and respecting the fiduciary duty the Manager has towards the Clients.

The management and compliance teams should review the performance of each broker and consider, among other things: the quality of the executions provided; the cost of executions, soft dollar agreements, if applicable, and potential conflicts of interest.

7.1. Soft Dollar Policy

The Manager does not enter into any soft dollar arrangements and does not authorize the use of Client commission payments to actively obtain research, market data, or any other products or services from brokers. This practice is categorically prohibited under the Manager's internal policies, with no exceptions.

Soft dollars can be defined as any benefits offered by a broker to a manager who directs orders to the broker, which may include, without limitation*, research* and access to market information systems such as *Bloomberg*.

However, in the ordinary course of trading, the Manager may receive access to third-party research or market data systems provided by brokers through bundled commission arrangements. Such benefits are considered permissible under the safe harbor provision of Section 28(e) of the U.S. Securities Exchange Act of 1934. In all cases, the Manager exercises good faith in seeking best execution and acts solely in the best interests of its Clients.

All trading decisions are made in accordance with the Manager's duty of best execution and with the exclusive objective of serving the best interests of its Clients. No incentives, benefits, or services received from brokers affect the independence or objectivity of the Manager's investment decision-making process.

8. *KNOW YOUR CLIENT* ("KYC") POLICY AND PREVENTION OF MONEY LAUNDERING

8.1. KYC Program

The Manager maintains a comprehensive Know Your Client (KYC) and Anti-Money Laundering Program aligned with applicable Brazilian Law 9613/98, CVM Resolution 50 and U.S. Investment Advisers Act of 1940. The program is risk-based and proportional to the Manager's role as an investment manager, without engaging in distribution activities.

The Manager does not maintain a direct commercial relationship with investors in the pooled funds under its management. In such cases, it relies on the administrators and

distributors—formally engaged—to perform full KYC and AML duties, including UBO identification, transaction monitoring, and sanctions screening. These third parties are subject to Know Your Partner (KYP) due diligence under the Manager's service provider policy.

Non-exclusive vehicles

Manager´s role is limited to obtaining basic registration documentation through the contracted distributors, as required under CVM Resolution 50.

Administrators and distributors are contractually responsible for implementing adequate internal policies and controls to:

(i) maintain updated investor records;
(ii) monitor transaction consistency and detect potential ML/TF indicators;
(iii) identify and monitor politically exposed persons (PEPs);
(iv) detect high-risk structures (e.g., bearer shares, trusts, private banking);
(v) assess the adequacy of transactions in view of investor profile and declared economic capacity;
(vi) apply geographic, economic, and transactional risk factors in investor risk classification; and
(vii) report suspicious activity to the appropriate authorities, as per applicable regulation.

For Brazilian investment funds, the Manager conducts KYP due diligence through a local third-party service provider that helps to ensure that all contracted service providers adopt and enforce such standards and are equipped with the appropriate technological and human resources to do so.

Direct Relationship

The Manager considers that a direct commercial relationship exists in the following situations:

(i) managed accounts where Manager is directly contracted as investment adviser;
(ii) exclusive investment vehicles where Manager interacts directly with the investor and no distributor is involved.

In such cases, Manager performs full KYC and AML procedures, including:

- Identification and verification of the investor and its beneficial owners;
- Assessment of the investor's economic background, source of funds, and geographic risk factors;
- Sanctions and PEP screening;
- Risk-based classification and ongoing monitoring of the relationship.

The Manager is strictly prohibited from engaging in investment management services for any individual, entity, vessel, or jurisdiction listed on the OFAC Specially Designated Nationals (SDN) list or subject to sanctions by any applicable regulatory or governmental

authority.

8.2. Anti-Money Laundering Policy

The term "money laundering" covers various activities and processes with the purpose of concealing the owner and previous origin of illegal activity in order to simulate a legitimate origin. Manager and its Employees must comply with all money laundering prevention rules applicable to investment fund management activities, in particular Law No. 9613 of March 3, 1998, as amended ("Law 9613/98"), and CVM Resolution No. 50 of August 31, 2021 ("CVM Resolution 50"), the main terms of which are reflected in this Compliance Manual.

The Chief Compliance Officer shall be responsible to the CVM for complying with all rules and regulations in force relating to combating and preventing money laundering.

8.2.1. AML Control on the Asset Side

The negotiation of assets and securities on behalf of investment funds, vehicles, and managed accounts must also be subject to anti-money laundering and counter-terrorist financing (AML/CFT) analysis, assessment, and monitoring. The responsibility for conducting AML/CFT due diligence at the time of asset acquisition, as well as the ongoing monitoring of such positions, lies with the Portfolio Management and Investment teams as the first line of defense, and with the Compliance department as the second line of defense.

Transactions involving listed securities, private credit operations, and private equity investments, if applicable, shall be assessed under AML/CFT criteria based on the profile of the investee company, including its shareholders, officers, directors, corporate purpose, and transaction rationale—always considering the inherent risks of each deal and the respective mitigating factors.

Additionally, at the end of each trading day, the Portfolio Manager manually verifies the executed trades by comparing them to the market average price or the closing price provided by the fund administrator, with support from the back office team. If any indication arises that a transaction may have been executed at a price inconsistent with market conditions, the Compliance department will request supporting documentation and evidence to substantiate the pricing applied.

8.2.2. *Risk-Based Supervision*

As the main guideline of its money laundering and terrorist financing prevention program, the Manager has adopted the risk-based supervision method, which means that the Manager, within the limits of its powers, will identify, analyze, understand and seek to mitigate the money laundering and terrorist financing risks inherent in its

activities by adopting a risk-based approach to ensure that prevention measures are proportionate to the risks identified.

The Manager will classify all its products offered, services provided, distribution channels, trading environments and Clients, minimally segmenting them into low, medium and high risk. To this end, the following factors, among others, will be taken into account:

(i) The type of vehicle (i.e. investment fund / managed account);
(ii) Its activity;
(iii) The geographical location of the assets invested in by the investment vehicle;
(iv) Intermediary institutions (distributors) of fund shares;
(v) The fund's other service providers in the financial and capital market segment; and
(vi) The counterparty to the transactions carried out.

In addition, the Manager will act in a preventive manner based on the criteria listed above for the prior analysis of new technologies, services and products based on the risk they may expose in the future. The Manager adopts internal procedures for the selection and monitoring of Clients, Employees and relevant service providers. For more detailed information, see the applicable policies.

The Manager's risk-based supervision methodology will be analyzed by the Chief Compliance Officer in his annual report, in order to consider the effectiveness of internal controls, taking into account the following criteria: **(i)** the implementation of a continuous environment of knowledge of the operations of the funds managed by the Manager and the monitoring of their operations; and **(ii)** the prevention, detection and combat of atypical operations or those that may constitute money laundering or terrorist financing.

The Manager's senior management is responsible for approving the internal risk-based supervision methodology, as well as monitoring and reassessing it through the analysis of the annual report.

For the purposes of this Compliance Manual, the Chief Compliance Officer may request any documents and/or information that are necessary for the performance of his or her activities, and must do so in writing, with a deadline for response of up to 15 (fifteen) days, which may be extended, when necessary, at the discretion of the Chief Compliance Officer.

In addition to risk-based supervision, the Manager adopts the following permanent

control and surveillance procedures to minimize the risk of money laundering in the various financial operations under its responsibility:

(i) Analysis by the Compliance area of financial transactions that may indicate the existence of a crime, due to their characteristics, amounts, forms of realization and instruments used, or that have no economic or legal basis;

(ii) Avoid carrying out any commercial or financial operation on behalf of third parties, unless it is transparent, justified and solid, and made possible or carried out through banking channels;

(iii) Avoid transactions with people or entities that cannot prove the origin of the money involved;

(iv) Avoid complex international financial transactions involving a lot of money movements in different countries and/or between different banks;

(v) Evaluation of the policies and practices for preventing and combating money laundering adopted by the Manager's third parties/partners;

(vi) Recording and storing information relating to Clients' financial transactions and services;

(vii) Reporting proposals and/or operations considered suspicious or atypical to the Financial Activities Control Board ("COAF") and the regulatory authorities, as applicable, within the legal timeframe, unless it is not objectively permitted to do so;

(viii) Communication to COAF and regulatory authorities of transactions in kind, or whose amount reaches the levels set by the regulators;

(ix) Periodic review of procedures and controls to prevent and combat money laundering and internal controls;

(x) Adoption of a special attention procedure for PEP, as defined below;

(xi) To have adequate knowledge of Employees and make them aware of the policies and regulations adhered to by the regulatory bodies;

(xii) Application of procedures to verify registration information in proportion to the risk of products, services and distribution channels being used for money laundering and terrorist financing;

(xiii) Classification of the active Investment Vehicles managed by the Manager by risk level, classifying them at least in low, medium and high levels;

(xiv) Reporting to COAF all situations and operations detected or proposed that could constitute serious evidence of money laundering or terrorist financing, as well as the non-existence of such operations and/or situations; and

(xv) Monitoring and compliance with sanctions imposed by UNSC resolutions, immediately and without prior notice to the recipients, following the procedures set out in CVM Resolution 50.

8.3. Procedures relating to counterparties

The Manager is responsible for taking all necessary measures, in accordance with applicable laws and regulations, including, but not limited to, Brazilian Law 9.613/98, CVM Resolution 50 and CVM Circular Letters, as applicable, the registration rules, *know your* client (KYC), *know your* employee (KYE) and *know your partner* (KYP) contained in this Compliance Manual and the best practices adopted by the market's self-regulatory entities, to establish and document the true and complete identity, financial situation and history of each counterparty in the transactions carried out by the investment vehicles.

Accordingly, in addition to the onboarding and monitoring of clients, the Manager conducts due diligence and risk-based analysis of counterparties involved in transactions carried out by the investment funds under its management. This includes assessing the counterparties' structure, background, and regulatory profile, when relevant, with the aim of identifying and mitigating any potential ML/TF risks associated with asset acquisition and negotiation activities.

8.4. Politically Exposed Person

The procedures for identifying and negotiating with persons considered politically exposed ("PEPs") are dealt with in CVM Resolution 50 and Brazilian Law 9.613/98, as amended, and other rules issued by BACEN, the National Monetary Council and GAFI/FATF.

Annex B of CVM Resolution 50 lists the individuals who are considered PEP, and it is possible to generically designate them as those who "hold or have held, in the last five (5) years, relevant public positions, jobs or functions, in Brazil or in other countries, territories and foreign dependencies, as well as their representatives, family members and other people closely related to them".

This includes occupants of relevant public positions, jobs or functions held by heads of state and government, high-ranking politicians, senior civil servants, high-ranking judges or military personnel, heads of public companies or political party leaders. It is also recommended to monitor the PEP's family members, their relatives in the direct line up to the first degree, as well as spouses, partners, stepchildren and close collaborators.

BACEN Circular No. 3.978, of January 23, 2020, and subsequent amendments, provides for the procedures to be observed by financial agents for establishing business relationships and monitoring the financial transactions of PEP, which must be structured in such a way as to make it possible to characterize people considered PPE and identify the origin of the funds involved in the transactions of the Clients thus identified.

Obliged parties are recommended to pay special, reinforced and continuous attention to examining and complying with the preventive measures, especially with regard to legal relations maintained with PPE, in the following terms:

(i) More rigorous supervision of the business relationship with PEP;

(ii) Special attention should be paid to proposals to start a relationship and to operations carried out with PEPs, including those from countries with which Brazil has a high number of financial and commercial transactions, common borders or ethnic, linguistic or political proximity;

(iii) Maintaining rules, procedures and internal controls to identify Clients who became PEPs after the start of the relationship with the institution or who are found to have already been PEPs at the start of the relationship with the institution and apply the same treatment as above; and

(iv) Maintenance of rules, procedures and internal controls to identify the origin of the funds involved in the transactions of Clients and beneficiaries identified as PEP.

8.5. Foreign Corrupt Practices Act (FCPA)

The Manager strictly prohibits any direct or indirect offer, promise, authorization, or payment of money or anything of value to foreign public officials, political figures, or entities, for the purpose of obtaining or retaining business, influencing decisions, or securing any improper advantage. This prohibition applies to all Employees and third parties acting on behalf of the Manager, regardless of the value involved or local customs.

For the purposes of this Policy, a "Covered Person" includes any officer or employee of a foreign government, agency, public company, central bank, sovereign fund, political

party, or any candidate for public office outside the United States.

Any such practice is considered a serious violation under the U.S. Foreign Corrupt Practices Act of 1977 and may result in criminal liability. No exceptions shall be applied without prior review and written approval from the Chief Compliance Officer.

8.6. Communications

If any Employee notices or suspects money laundering or other illegal activities on the part of any Client, they must immediately report their suspicions to the Chief Compliance Officer, who must then institute further investigations to determine whether the relevant authorities should be informed of the activities in question. Among other possibilities, an activity may be considered suspicious if:

(i) operations whose values appear objectively incompatible with the professional occupation, income and/or patrimonial or financial situation of any of the parties involved, based on the respective registration information;

(ii) transactions carried out between the same parties or for the benefit of the same parties, in which there are subsequent gains or losses for any of the parties involved;

(iii) operations that show significant fluctuations in the volume and/or frequency of business of any of the parties involved;

(iv) operations whose unfolding includes characteristics that may constitute a ruse to circumvent the identification of the personnel involved and/or the respective beneficiaries;

(v) operations whose characteristics and/or consequences show that the company is constantly acting on behalf of third parties;

(vi) operations that show a sudden and objectively unjustified change in relation to the operating methods usually used by the party or parties involved;

(vii) operations carried out with the aim of generating a loss or gain for which there is no objective economic basis;

(viii) operations with the participation of natural persons resident or entities incorporated in countries that do not apply or insufficiently apply the recommendations of the Financial Action Task Force against Money Laundering and Terrorist Financing - FATF;

(ix) transactions settled in kind, if and when permitted;

(x) private transfers of resources and securities without any apparent motive;

(xi) operations whose degree of complexity and risk appear incompatible with the technical qualifications of the Client or their representative;

(xii) deposits or transfers made by third parties, for the settlement of Client operations, or for the provision of guarantees in operations on the futures settlement markets;

(xiii) payments to third parties, in any form whatsoever, on account of the settlement of transactions or redemptions of amounts deposited in guarantee, registered in the Client's name;

(xiv) situations in which it is not possible to keep the registration information of its Clients up to date;

(xv) situations and operations in which it is not possible to identify the final beneficiary; and

(xvi) situations in which the steps to identify PPE cannot be completed; and

(xvii) all other operations that may constitute signs of money laundering or terrorist financing mentioned in article 20 of CVM Resolution 50 and in the applicable regulations;

The Manager must pay special attention to operations involving the following categories of Clients:

(i) non-resident clients, especially when constituted in the form of *trusts* and companies with bearer bonds;

(ii) clients with large fortunes managed by areas of financial institutions aimed at clients with this profile (*private banking*); and

(iii) politically exposed persons.

The Manager must analyze the operations together with other related operations that may form part of the same group of operations or have any kind of relationship with each other.

Employees must not disclose their suspicions or findings in relation to any activity to a person other than the Chief Compliance Officer. Any contact between the Manager and the relevant authority regarding suspicious activity should only be made by the Chief Compliance Officer. Employees must cooperate with the Chief Compliance Officer during the investigation of any suspicious activities.

The Manager must keep its books and records authentic, exact, complete and up to date, including documents relating to all transactions that have taken place in the last five (5) years, and this period may be extended indefinitely by the regulatory authorities in the event of administrative proceedings.

The Chief Compliance Officer shall ensure that the Manager prevents any damage, falsification, destruction or improper alteration of the books and records by adopting the necessary and prudent methods.

Operations related to terrorism or its financing are considered to be those carried out by persons who commit or plan to commit terrorist acts, who participate in them or facilitate their commission, as well as by entities owned or controlled, directly or indirectly, by such persons and the persons or entities acting under their command.

8.7. AML Training

The Chief Compliance Officer shall provide, at least every twelve (12) months, appropriate training to all Employees regarding the anti-money laundering rules set forth in this Policy and in the applicable laws and regulations. Such training is mandatory for all Employees and attendance is tracked through a sign-in sheet. Upon the onboarding of a new Employee, the Compliance department shall conduct individual training on this matter.

9. SENDING INFORMATION TO GOVERNMENT AUTHORITIES

Brazilian laws and regulations require the investment manager to submit periodic information and/or occasional information related to its asset management activity in the Brazilian capital markets. Some of this information will be submitted to the CVM or ANBIMA and some will be submitted to the companies in which the investment funds (or other investment vehicles) invest or to the shareholders of these investment funds.

This information includes, without limitation, (i) the communications provided for in CVM Resolution 44, on positions held in the companies that make up the portfolios of the investment vehicles, under the terms specified therein; (ii) annual updating of the reference form, as required by the CVM Resolution 21, which contains, without limitation, information on the funds managed, amounts under management and types of investors; (iii) periodic review of its manuals, codes and policies, which must be made

available on the Manager's website; and (iv) information required by the legislation and regulations dealing with the prevention of money laundering.

Similarly, under U.S. regulations, investment advisers registered with the SEC are subject to ongoing reporting, disclosure, and recordkeeping obligations pursuant to the Investment Advisers Act of 1940.

Annex III contains a non-exhaustive list of the periodic information required by law and by SEC, CVM and ANBIMA regulations on the date of this Compliance Manual.

10. OPERATIONAL PROCEDURES

The Manager acts in accordance with high ethical standards and values, mainly by observing and respecting the rules issued by the regulatory bodies and its Internal Policies. In conducting its operations, the Manager shall:

(i) observe the principle of probity in the conduct of its activities;

(ii) training for the performance of activities;

(iii) act diligently when carrying out orders, observing the criteria for dividing up orders (where applicable);

(iv) obtain and present to its clients the information necessary to fulfill orders;

(v) adopt measures to avoid transactions involving conflicts of interest, ensuring fair treatment for its clients; and

(vi) always keep the supporting documents for transactions available for both supervisory bodies and investors for the legal deadlines.

10.1. Recording of Investment Operations

All investment transactions are recorded in the systems of the administrators and custodians of the Investment Vehicles managed by the Manager. Manager also maintains a parallel and independent record of the portfolios via an outsourced portfolio control system to reconcile and validate the information made available by these service providers. These records are maintained in accordance with CVM Resolution 175 and ANBIMA rules, and are subject to periodic reconciliation, audit, and internal compliance review.

10.2. Recordkeeping of Electronic Communications Related to Operations

In compliance with Rule 204-2(a)(7) and (a)(10) under the Investment Advisers Act of 1940 and applicable Brazilian regulation, Manager also retains records of electronic communications that pertain to investment decisions, trading instructions, portfolio management activities, and any other communication relevant to advisory operations.

The scope of retention includes, but is not limited to:

- E-mails sent or received through the corporate domain;
- Bloomberg chat messages, if applicable;
- Internal or external communications over authorized messaging platforms;
- Corporate WhatsApp, if formally approved and archived;
- Meeting notes or chat logs where investment matters are discussed.

To ensure the integrity and availability of such communications:

- Only approved communication channels may be used for operational or investment-related matters;
- All communications are automatically archived, indexed, and stored in a secure system with search and audit capabilities;
- Access is restricted by role and monitored via access logs;
- Communications are retained for a minimum of five (5) years, in line with CVM and SEC requirements;
- Unauthorized use of personal messaging applications (e.g., personal WhatsApp, Telegram, private email) for business communications is strictly prohibited and subject to disciplinary action.

10.3. Settlement of Transactions

The settlement of investment transactions is carried out directly by the fund administrators, custodians, and financial institutions responsible for executing the trades, in accordance with the specific operational procedures and settlement cycles of each local market in which the vehicles invest.

The Manager does not perform custody or settlement functions. However, the Manager actively monitors the settlement process through daily reconciliation of trades, portfolio positions, and cash movements using its internal systems and third-party service providers. Any discrepancies identified between internal records and those of the administrators or custodians are promptly investigated and escalated to the Compliance and Operations teams.

All settlement procedures comply with the standards established by the relevant jurisdictions, including but not limited to Brazil, United States of America, Mexico, Chile, Colombia, and other countries in the region. The Manager also ensures that counterparties involved in settlement are duly authorized and reputable.

10.4. Order Allocation Policy

Manager maintains a separate, standalone Investment Selection and Allocation Policy that governs the principles, criteria, and procedures for selecting, allocating, and monitoring assets across the investment vehicles under management. This policy is designed to ensure fair and equitable treatment of all client accounts and to mitigate potential conflicts of interest arising from the management of multiple funds or accounts with similar investment strategies.

When appropriate, trade orders are aggregated ("bunched orders") to enhance execution efficiency and cost-effectiveness. The allocation of executed trades is carried out in accordance with pre-established, equitable, and verifiable criteria, ensuring that each participating account receives a fair portion of the trade based on its initial order size and other relevant factors. Manager does not favor any client or account over another and remains committed to its fiduciary duty to act in the best interest of all clients.

All documentation related to trade aggregation and allocation is retained by Manager for the minimum period required by applicable regulation and is available for review by supervisory authorities. The Compliance department monitors adherence to these procedures and conducts periodic reviews of the allocation process, as outlined in the standalone policy.

10.5. Custody of Client Assets

Manager does not maintain custody of client funds or securities as defined under Rule 206(4)-2 of the Investment Advisers Act of 1940 ("Custody Rule"), except where deemed to have custody due to its role as investment manager to Brazilian-domiciled pooled investment funds. In such cases, Manager is considered to have custody because it has the authority to instruct custodians to effect transactions and payments on behalf of the funds.

For these Brazilian-domiciled pooled investment funds, Manager ensures that:

- Each fund is audited annually by an independent public accountant registered with the Brazilian equivalent of the Public Company Accounting Oversight Board (PCAOB); and

- Financial statements are prepared in accordance with generally accepted accounting principles and distributed to fund investors within legally required timeframe;

- Manager does not maintain custody over any U.S.-based separately managed accounts. Specifically:

- Manager does not hold, directly or indirectly, client funds or securities;

- It does not have the authority to withdraw client funds or deduct advisory fees

directly from accounts;

- It does not act as general partner, trustee, or in any position that grants it legal ownership or access to client assets.

The Manager will immediately report to the Chief Compliance Officer any change in account structure, authority, or contractual terms that could result in a deemed custody relationship under SEC regulations. The Compliance department is responsible for periodically reviewing the firm's operational and contractual arrangements to ensure continued compliance with the Custody Rule and other applicable regulations.

10.6. Valuation of Client Assets

Manager primarily manages portfolios composed of publicly traded equity securities domiciled and/or listed in Latin American markets and/or generating more than 50% of their assets or revenues from Latin America, regardless of their listing venue. As such, asset valuation is generally based on observable market prices obtained from reputable and independent pricing sources, such as stock exchanges, custodians, or Bloomberg terminal data. The Manager does not invest in private securities or illiquid instruments that require discretionary fair value estimates.

All Client assets are valued daily using closing market prices in accordance with applicable fund documentation and local regulations. For Brazilian funds, valuations comply with the requirements of CVM Resolution 175, including the use of recognized pricing providers and methodologies consistent with the nature and liquidity of each asset class.

The Manager maintains internal controls to ensure that the pricing process is transparent, consistent, and free from conflicts of interest. In the event of pricing discrepancies or market disruptions, the Investment team, with input from the Compliance team, may determine whether alternative sources or valuation methods should be applied. Any such decisions must be fully documented and subject to review.

In accordance with SEC Rule 204-2, the Manager retains all records relating to asset valuation, including supporting data, pricing methodologies, and any adjustments made to market prices. The Chief Compliance Officer oversees the integrity of the valuation process and ensures that valuations are consistent with the firm's fiduciary obligations under Section 203(e)(6) of the Investment Advisers Act of 1940.

Although the Manager does not manage illiquid securities requiring subjective valuation, the firm remains committed to valuation oversight as part of its overall risk and compliance framework. Any future expansion into alternative or non-listed assets will require updates to the valuation policies and procedures, subject to approval by the Investment and Risk Committees.

10.7. Trade Error Policy

The Manager has established procedures for identifying, documenting, and correcting trading errors in portfolios under its management. A trade error is defined as any deviation from an investment instruction, policy, or restriction that results in an unintended transaction, including errors in asset selection, quantity, timing, pricing, or allocation.

When a trade error is identified, the Employee who notices it must immediately notify the Chief Compliance Officer. The Chief Compliance Officer will oversee the resolution of the error and ensure that:

- The affected client is restored to the position they would have held had the error not occurred, with no loss or gain retained by the Manager;
- Any gains resulting from the error are allocated to the fund or client account, as applicable, or transferred to a designated error account managed in accordance with internal controls;
- The error is documented in a dedicated register, including the date, nature, cause, remediation steps, and any financial impact;
- The root cause is assessed, and, where necessary, internal controls or systems are reviewed to prevent recurrence.

Errors are reported to senior management on a periodic basis, and records are retained for a minimum of five (5) years in accordance with applicable regulation.

10.8. Fee Transparency

The Manager is committed to full fee transparency and adherence to the fiduciary principles established under the Investment Advisers Act of 1940. In accordance with Section 205(a)(1), Manager does not enter into advisory contracts that provide for compensation based on a share of capital gains or capital appreciation of the funds of the client, unless such client qualifies as a "qualified client" under SEC Rule 205-3.

All fees, including management and performance fees, are fully disclosed to clients and investors prior to engagement, and are detailed in the advisory agreements, offering documents, and the firm’s Form ADV. These disclosures include the fee rate, calculation methodology, billing frequency, high-water marks, hurdle rates, and crystallization dates where applicable.

Manager does not receive any indirect or undisclosed fees, rebates, or soft dollar benefits from third parties that would compromise its independence or result in a conflict of interest not properly disclosed to clients. Any such arrangements, if applicable, are subject to prior approval and are disclosed pursuant to Section 28(e) of the Securities

Exchange Act of 1934 and the firm's Soft Dollar Policy.

The Manager's internal controls include regular testing and review of fee disclosures, billing processes, and contract terms to ensure consistency with SEC enforcement guidance on fee transparency and prevention of deceptive practices.

10.9. Management Agreements and U.S. Regulatory Requirements

In accordance with Sections 205 and 206 of the U.S. Investment Advisers Act of 1940, all portfolio management agreements entered into with U.S. clients — including managed accounts and private funds, where applicable — must be executed in writing and are subject to review and approval by the Chief Compliance Officer.

Such agreements shall include, at a minimum:

a) express provisions requiring prior written consent in the event of an assignment of the contract, including in cases of direct or indirect change of control;

b) clear notice obligations for any material organizational changes that may affect the Manager's ability to fulfil his obligations; and

c) a provision ensuring the pro rata refund of any prepaid fees in the event of early termination of the agreement.

11. BUSINESS CONTINUITY PLAN

In carrying out its activities, the Manager is subject to risks related to the occurrence of events that may compromise, hinder or even prevent the continuity of the Manager's operations, such as natural disasters, cyber-attacks, sabotage, theft, vandalism and structural problems.

This business continuity plan seeks to describe the procedures, strategies, actions and infrastructure employed by the Manager to guarantee the continuity of its activities in contingency situations.

The Chief Compliance Officer is responsible for complying with the business continuity plan and activating the contingency plan.

11.1. Contingency structure and procedures

The Manager will guarantee the continuity of its operations in the event of a disaster or any other drastic business interruption.

The Manager's servers can be accessed virtually via the cloud, so that all information can be accessed remotely from anywhere with internet access.

In the event of an emergency at the Manager's head office that makes it impossible to use it, the Employees will work remotely, from their home environment or a place to be defined at the time by the Compliance and Management Officers.

All employees have a copy of the business continuity plan which describes all the actions to be taken in the event of a disaster.

11.2. Contingency plan

The contingency plan will be activated in any event that materially disrupts the Manager's ability to operate in the ordinary course of business, including, but not limited to, physical inaccessibility of the office premises, cybersecurity incidents, widespread infrastructure outages (such as power, internet, or telecom failures), natural disasters, pandemics, acts of terrorism, or any other emergency or crisis that compromises the availability of personnel, systems, or critical third-party services. This plan is designed to ensure the continuity of key operations, the protection of client data, and the fulfillment of the Manager's fiduciary duties in accordance with applicable regulations.

In such cases, the Compliance and Management Officers, by mutual agreement, shall determine the application of contingency procedures, authorizing Employees to work remotely, in the Employee's home environment, or in a place to be defined at the time by the Compliance and Management Officers, which has its own secure connection. The Employees will use the Manager's notebooks and will have access to all the necessary data and information via the cloud server, in order to maintain the regular exercise of their activities.

Once access to the Manager has been normalized, Employees must submit a report on the activities carried out during the contingency period to the Chief Compliance Officer.

11.3. Updating the business continuity plan

The procedures, strategies and actions contained in the business continuity plan will be tested and validated at least every 12 (twelve) months, or less if required by current regulations. Test registration will be filled at the Manager´s office.

12. CYBERSECURITY

The Manager adopts cyber security mechanisms to ensure the confidentiality, integrity and availability of the data and information systems used in its operations. These mechanisms follow the standards set forth in Rule 206(4)-7 of the Investment Advisers

Act of 1940 and the guidelines of the Brazilian *Lei Geral de Proteção de Dados* ("LGPD") and ANBIMA's Cybersecurity Guide.

The Chief Compliance Officer is responsible for the governance and oversight of the cybersecurity program, in coordination with an external information technology (IT) service provider engaged by the Manager. This provider is responsible for the implementation, monitoring, and continuous improvement of technical and procedural safeguards, as well as ensuring compliance with cybersecurity rules and procedures.

12.1. Risk assessment

In carrying out its activities, the Manager may be subject to cyber risks that threaten the confidentiality, integrity and availability of the data and information systems used. Among the most common risks are:

(i) Malware: software designed to corrupt computers and networks:
   a. Virus: software that causes damage to the machine, network, other software and databases;
   b. Trojan horse: appears inside other software and creates a gateway for computer intrusion;
   c. *Spyware*: malicious software to collect and monitor the use of information; and
   d. *Ransomware*: malicious software that blocks access to systems and databases, demanding a ransom to re-establish access.

(ii) Social engineering: manipulation methods to obtain confidential information such as passwords, personal data and credit card numbers:
   a. *Pharming*: directs the user to a fraudulent website without their knowledge;
   b. *Phishing*: links transmitted by e-mail, pretending to be a trustworthy person or company sending official electronic communication in order to obtain confidential information;
   c. *Vishing*: pretends to be a trustworthy person or company and tries to obtain confidential information through phone calls;
   d. *Smishing*: pretending to be a trustworthy person or company and, through text messages, trying to obtain confidential information; and
   e. Personal access: people located in public places such as bars, cafés and restaurants who capture any kind of information that could later be used for an attack.

(iii) DDoS (*distributed denial of services*) attacks and *botnets*: attacks aimed at denying or delaying access to the institution's services or systems; in the case of *botnets*, the attack comes from a large number of infected computers used to create and send spam or viruses, or flood a network with messages

resulting in the denial of services; and

(iv) Intrusions (*advanced persistent threats*): attacks carried out by sophisticated attackers, using knowledge and tools to detect and exploit specific weaknesses in a technological environment.

The Manager periodically conducts a formal risk assessment that includes: (i) mapping of collected and stored data (e.g., investor, employee, client, and partner data); (ii) classification by sensitivity and criticality; (iii) identification of technological assets and systems; (iv) analysis of internal and external cyber threats and vulnerabilities; (v) current controls in place and their effectiveness; (vi) potential operational and reputational impacts; and (vii) assessment of the governance structure related to cybersecurity risk management. This assessment is updated at least annually or whenever relevant structural or regulatory changes occur.

12.1.1. *Third-Party Risk and Data Sharing*

Vendors and service providers with access to sensitive data undergo due diligence and must contractually commit to adequate cybersecurity standards, including breach notification and LGPD compliance. The Manager ensures revocation of access promptly upon contract termination.

12.2. Safeguards and protection actions

In order to mitigate cyber risks and protect its systems, information, database, equipment and the conduct of its business, the Manager adopts the following prevention and protection measures:

(i) Adequate access control to the Manager's assets, by means of procedures for identifying, authenticating and authorizing users, or systems, to the Manager's assets;

(ii) Establishment of minimum rules (complexity, periodicity and multi-factor authentication) when defining passwords for access to corporate devices, systems and the network, depending on the relevance of the asset being accessed. In addition, login and password change events are auditable and traceable;

(iii) Limiting each Employee's access to only resources relevant to the performance of their activities and restricting physical access to areas with critical/sensitive information;

(iv) Backup routines;

(v) Creation of logs and audit trails whenever permitted by the systems;

(vi) Carrying out due diligence when contracting services from third parties, making sure, whenever necessary, that a confidentiality agreement is signed and that security controls are required in the third party's own structure;

(vii) Implementation of anti-malware resources on network stations and servers, such as antivirus and personal firewalls; and

(viii) Restricting the installation and execution of unauthorized software and applications through process execution controls (e.g. *whitelisting*).

12.2.1 Bring Your Own Device (BYOD) Policy

The configuration of a Manager´s corporate email account on any personal device (such as mobile phones or tablets) by an Employee is conditional upon the prior installation of a security application approved by the technology team. This application enables the Manager to perform a remote wipe of all corporate data stored on the device in the event of theft, loss, or misplacement.

In addition to remote wiping capabilities, the application continuously monitors specific device security parameters—such as operating system patch level and password protection status—and may trigger an automatic restriction of corporate data access if minimum security standards are not met.

Employees are instructed during both onboarding and annual compliance training on best practices for securing personal devices. These include, but are not limited to, the installation of antivirus software, use of a virtual private network (VPN), and activation of multi-factor authentication on all personal accounts. Compliance with these practices is essential to maintaining Manager's information security standards and mitigating cybersecurity risks.

12.3. Monitoring

The Manager has mechanisms in place to monitor the protection actions implemented in order to guarantee their proper functioning and effectiveness.

In this regard, the Manager keeps up-to-date inventories of hardware and software, as well as carrying out periodic checks in order to identify elements foreign to the Manager, such as unauthorized computers or unlicensed software.

In addition, the Manager always keeps the operating systems and application software up to date, installing updates whenever they become available. Backup routines are monitored on a daily basis, with regular data restoration tests carried out.

External invasion and phishing tests are carried out periodically, as well as analysis of

vulnerabilities in the technological structure, whenever there is a significant change in this structure.

In addition, the Manager regularly analyzes the logs and audit trails created in order to enable the rapid identification of attacks, whether internal or external.

12.4. Incident Response plan

If a potential incident related to cyber security is identified, the Chief Compliance Officer must be notified immediately.

Initially, the Chief Compliance Officer will meet with the other directors of the Manager to understand the event that has occurred, the reasons and immediate consequences, as well as the seriousness of the situation. The Chief Compliance Officer may involve the IT service provider if it deems it necessary.

If the directors consider that the incident may cause imminent damage to the Manager, the appropriate immediate cybersecurity measures will be taken together with the Manager's IT service provider, which may include IT redundancy, redirecting telephone lines to cell phones, and instructing the telephone provider to divert data lines and e-mails, among others.

In the event that the incident compromises, hinders or even prevents the continuity of the Manager's operations, the procedures set out in the business continuity plan described in item 12 above shall be observed.

In addition, the directors will assess the pertinence of adopting measures such as **(i)** filing a police report or criminal complaint; **(ii)** reporting the incident to the regulatory and self- regulatory bodies; and **(iii)** consulting a lawyer to assess the legal risks and appropriate legal measures to ensure the rights of the Manager.

The Chief Compliance Officer will oversee the cybersecurity report preparation which shall include:

- Identification and classification of the incident;
- Immediate containment measures;
- Legal and contractual assessment of impacts and obligations;
- Activation of the Business Continuity Plan if operational integrity is affected;
- Root cause analysis and documentation;
- A post-incident review.

12.5. Training and Awareness

Cybersecurity training is mandatory for all Employees upon hiring and annually thereafter. Training covers:

- Social engineering and phishing threats;
- Use of secure passwords and multifactor authentication;
- Secure handling of devices and sensitive information;
- Reporting procedures for suspected incidents;
- Responsibilities under the cybersecurity policy.

Additional awareness initiatives include:

- Simulated phishing campaigns

12.6. Recycling and revision

The Manager will keep the cyber security program continuously updated, identifying new risks, assets and processes and reassessing residual risks.

The Chief Compliance Officer, who is responsible for implementing the cyber security procedures, will review and update this cyber security plan every 24 (twenty-four) months, or in a shorter period whenever any relevant fact or event motivates its early review, according to results from the risk assessment, penetration tests, incident records, and regulatory updates. Documentation of reviews, decisions, and improvements is retained.

***

ANNEX I

Adhesion Term

I, _____, bearer of Identity Card No. _____hereby declare for all intents and purposes that:

1. I am aware of the existence of the "Internal Controls Manual *(compliance)*" of **CAPSIGMA INVESTMENT PARTNERS LTDA.** ("Compliance Manual" and "Manager", respectively) and of all the internal policies of the Manager, including the "Code of Ethics", the "Personal Investment Policy" and the "Risk Management Policy" (together with the Compliance Manual, the "Internal Policies"), which I have received, read and have in my possession.

2. I am aware of the full content of the Internal Policies, with which I declare that I agree, which shall become part of my obligations as an Employee (as defined in the Compliance Manual), in addition to the rules set forth in the Individual Employment Contract, if applicable, and the other rules of behavior established by Manager, and I undertake to immediately notify Manager's directors of any breach of ethical conduct of the rules and procedures that comes to my attention, either directly or by third parties.

3. I am aware of and undertake to fully comply with the terms of the confidentiality policy established in Manager's Internal Policies, under penalty of the application of the applicable sanctions, pursuant to item 4 below.

4. Failure to comply with the Internal Policies, as of this date, implies serious misconduct and may be subject to the application of the applicable sanctions, including dismissal for cause, if applicable. Notwithstanding this, I undertake to reimburse any damage and/or loss suffered by the Manager and/or its partners and directors as a result of non-compliance with the Compliance Manual and/or Internal Policies, subjecting myself to liability in the civil and criminal spheres.

5. I took part in the Manager's onboarding and initial training process, where I learned about the principles and rules applicable to my activities and those of the Manager, notably those relating to the segregation of activities, and had the opportunity to clarify doubts relating to these principles and rules, so that I understood them and undertake to observe them when carrying out my activities, as well as to participate assiduously in the ongoing training program.

6. The rules stipulated in the Manager´s Internal Policies do not invalidate any provision of the Individual Employment Contract, if applicable, nor of any other rule mentioned by the Manager, but serve as a complement and clarify how to deal with certain situations

related to my professional activity.

7. I authorize the disclosure of my telephone contact details to other Employees, and I will inform the Manager of any changes to this information, as well as any other registration data about me, as soon as such changes occur.

8. I hereby declare that I am fully aware that non-compliance with this term may result in my immediate dismissal from the Manager, without prejudice to any damage that may have been caused by such non-compliance.

I hereby inform you of the situations that exist today that could occasionally be classified as infractions or conflicts of interest, in accordance with the terms of the Compliance Manual, except for conflicts arising from shareholdings in other companies, described in the "Personal Investment Policy", which I am aware will have to be specified in accordance with the terms of the Compliance Manual:

_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____

São Paulo, _____ of _____ of 20_____.

_____

[Employee]

ANNEX II

Request to Perform an External Activity

1. Name of the institution where the External Activity will take place / description of the External Activity:

_____

_____

2. Will you have a director or administrator position? [ ] yes [ ] no

3. Describe your responsibilities in External Activity:_____

_____

4. Estimated time that will be required of you to carry out the External Activity (on an annual basis): _____

5. Will you or any related party receive any remuneration or consideration for the Outside Activity: [ ] yes [ ] no
If yes, describe: _____

The Employee declares that the External Activity he/she intends to perform, as described above, does not violate any applicable law or regulation, or the manuals and codes of **CAPSIGMA INVESTMENT PARTNERS LTDA.** ("Manager"), and that it does not interfere with his/her activities at Manager, does not compete or conflict with any interests of Manager. The Employee further declares and warrants that he/she will notify the Manager's Chief *C*ompliance Officer of any conflicts of interest that may arise in connection with the External Activity described above.

São Paulo, _____ of _____ of 20_____.

_____

[Employee]

Chief Compliance Officer's reply*:* [ ] Request Accepted [ ] Request Denied

_____

Chief Compliance Officer

ANNEX III - Periodic Information Required by Regulation

Information	Deadline	Recipient	Filing Form
Send CVM Annex E of CVM Resolution 21 duly completed, containing information on the Investment Vehicles under management, professionals, administrative and operational structure, etc.	By March 31 of each year, based on positions as at December 31 of the previous year	CVM	Internet (via the CVM website)
The Chief Compliance Officer must submit a report on the internal controls, rules and procedures established in this Compliance Manual (e.g. security tests on systems, measures to keep information confidential, training programs).	By the last working day of April each year, based on information from the immediately preceding calendar year	*Executive Committee*	Physical or Electronic
Confirm that the registration information is still valid.	Between May 1st and 31st of each year	CVM	CVM website
Report on your investment management team, especially any changes made.	Monthly	ANBIMA	Internet (through the ANBIMA database)
Confirm that the professionals in the investment management team are certified by ANBIMA and that the NAV and value information of the investment fund shares have been sent.	By March 31, based on information from December 31 of the previous year	ANBIMA	ANBIMA website
Report to COAF and CVM, if applicable, the non-occurrence of proposals, transactions or operations that may be reported under the terms of Law 9.613/98, based on the immediately preceding year.	By the last working day of April each year, based on the immediately preceding year	COAF	SISCOAF
Voting adopted at the shareholders' meetings of investment vehicles.	5 days after signing	Administrator	Form and times previously established by the Administrator

Information	**Deadline**	**Recipient**	**Filing Form**
Each time the group of investment vehicles managed by the same investment manager exceeds, upwards or downwards, the thresholds of 5%, 10%, 15%, and so on, of any class of securities issued by a listed company.	Immediately after the event	Listed company that issued the securities	Letter or any other way defined by the management of the investment fund(s)
Suspicion of money laundering or terrorist financing activities, as defined in Law 9.613/98.	24 hours after the event occurred	COAF	SISCOAF
Register the most complete and up-to-date version of the Voting Policy with ANBIMA.	At the time of joining and whenever updated	ANBIMA	Via ANBIMA's SSM System
Register the most complete and up-to-date version of the Liquidity Management Manual with ANBIMA.	At the time of joining and within 15 (fifteen) days whenever there is an update	ANBIMA	Via ANBIMA's SSM System
Prepare an Annual Compliance Review report to assess the adequacy of the policies and procedures and the effectiveness of their implementation (Rule 206 (4)-7)	Annually by March 31	*Executive Committee*	Physical or Electronic
Form ADV	Annually by March 31	SEC	Via IARD (Investment Adviser Registration Depository) System
Form 13F Reports U.S. listed equity holdings if over $100 million	Quarterly (within 45 days of quarter-end)	SEC	Via EDGAR System
Form 13D Filed when acquiring >5% of a voting class of a public company's stock with intent to influence control	Within 10 days of acquisition	SEC	Via EDGAR System
Form 13G Passive alternative to 13D for >5% beneficial ownership without intent to influence control	Initial, annual and amendments as needed	SEC	Via EDGAR System

Form 13H "Large Trader", defined as any person or entity that trades (for its own account or on behalf of others) ≥ 2 million shares or $20 million in National Market System securities during any calendar day, or ≥ 20 million shares or $200 million during any calendar month	Initial upon crossing threshold; Annual (by Feb 14); Amendments as needed	SEC	Via EDGAR System

* * *

VERSION LOG

Date	Version	Approved by
03/28/2023	01	CCO