LUMINA CAPITAL MANAGEMENT LTDA.

COMPLIANCE MANUAL

2025

Version [3.0.]

Content

1. Definitions 4
2. Purpose of this Manual 8
3. Compliance, Risk Management and Data Protection Officers 9
4. Code of Ethics 11
5. AML/PTF 11
6. KYC Policy 15
7. Anti-Corruption Policy 16
8. Service Provider Selection, Contracting and Monitoring Policy 17
9. Expert Hiring Policy and Expert Network 27
10. Confidentiality and Information Security Policy 30
10.1 Data Classification 30
11. Risk 31
12 Privacy Policy 33
13. Cybersecurity Policy 38
14. Business Continuity Plan 45
15. Remote Work Policy 46
16. Segregation Policy 48
17. Personal Investment Policy 48
18. Principal Transactions 52
19. Risk Management Policy 53
A. Procedures Related to Risk Identification 53
B. Risk Management Governance 53
C. Market Risk 55
D. Concentration Risk 56
E. Credit and Counterparty Risk 56
F. Operational Risk 57
G. Liquidity Risk 58
20. Asset Selection and Allocation Policy. 63
21. Insider Trading Policy 66
A. Policy Statement on Insider Trading 66
B. Elements of Insider Trading 66
22. Abroad Investment Policy 70
23. Allocation Orders Policy 70
24. Voting Rights Exercise Policy 72
A. Compulsory Matters 72
B. Optional Matters 74
C. Exceptions to the Exercise of Voting Rights 74
D. Decision Making Process and Procedure for Exercising Voting Rights 75
E. Communication of Votes to Investors 76
25. Continuous Certification Policy 76
26. Training Policy 78
28. Penalties 79

29. Periodic Updates and Reviews 80
Appendix I – Code of Ethics 82
1. Responsibility 82
2. Relationship between Members and Anti-Harassment Policy 82
3. Relationship with the Team, Managers, and Colleagues 83
4. Relationship with Clients, the Market and Competitors 84
5. Relationship with Affiliate Companies 85
6. Relationship with Vendors and Service Providers 85
7. Relationship with Supervisory and Oversight Bodies 85
8. Conflicts of Interest 85
9. Gifts (*Soft Dollar*) 86
10. Understanding and Accepting Changes 87
11. Intellectual Property 87
12. Press Communication 87
13. Charity and Political Contributions and Donations 88
14. Impartiality in Business 88
15. Organization 88
16. Hot Line 88
17. Penalties 89
18. Violations to the Code 91
Appendix II - Statement of Compliance 92
Appendix III - Risk Assessment Methodology and AML/PTF Monitoring 93
Methodology and Assessment 93
Low Risk 93
Medium Risk 94
High Risk 94
Evidence of Suspicious Activities 94
Monitoring 96
Appendix IV – Statement for Contracting Third Parties 98
Appendix V – Holding Report 99

1. Definitions

The following terms shall have the meanings ascribed below:

"Administrator"	It is the Funds' administrator.
"AML/PTF"	anti-money laundering, prevention to the financing of terrorism and to the financing of the proliferation of mass destruction guns.
"ANBIMA"	the Brazilian Financial and Capital Markets Association, *Associação Brasileira das Entidades dos Mercados Financeiros* e de Capitais.
"ANPD"	Brazilian National Authority for Data Protection.
"Anti-Corruption Law"	Law No. 12,846 of August 1st, 2013, as amended.
"Classes"	These are the investment Classes of the Funds, as well as their subclasses, where applicable.
"CNPJ/ME"	National Registry of Legal Entities of the Brazilian Ministry of Economy, Cadastro Nacional da Pessoa Jurídica do Ministério da Economia.
"COAF"	the Brazilian Council of Control of Financial Activities, *Conselho de Controle de Atividades Financeiras*.
"Code of ART from ANBIMA"	Refers to the ANBIMA Code for the Administration and Management of Third-Party Resources, which establishes the principles, rules, and best practices for entities engaged in asset management and fiduciary administration activities in Brazil.
"Compliance Officer"	the statutory Compliance Officer at Lumina. The Compliance Officer is the same person appointed as AML/PTF Officer, Risk Management Officer and Data Protection Officer.
"Conglomerate" or "Economic Group"	means a set of entities that are directly or indirectly controlling, controlled, affiliated, or under common control.
"Confidential	Information deemed private, proprietary or confidential

Information"	received and/or made available by Lumina, including those received by Members, regarding customer activities or businesses (including Personal Data and Sensitive Personal Data, according to LGPD, as appropriate and as applicable). Confidential Information may be in physical format (written on paper, e-mail, or recorded to disk) or not, and marked or not as confidential. Confidential Information includes Lumina's Internal Information or information of its clients, which includes, but is not limited to: trade secrets, know-how, innovations, marketing plans, business plans, investor relations and investor information in general, as well as terms of limited partnership and limited liability company agreements, financial data, financial models, research and development, forecasts, processes, internal communications, legal advice, computer access codes, investment positions, trades intentions and strategies, investment strategies, software, source code, computer system configurations, and other system information and performance data, of which information derives independent economic value, actual or potential, for not being known.
"CPF/ME"	Individual Taxpayer Registry of the Brazilian Ministry of Economy, Cadastro de Pessoas Físicas do Ministério da Economia.
"CVM"	the Brazilian Securities Commission, *Comissão de Valores Mobiliários*.
"Data Protection Officer"	Person appointed by Lumina to act as a communication channel between Lumina, the holders of the Personal Data and the ANPD.
"Employee(s)" or "Member(s)"	All partners, officers, and members of Lumina.
"Funds"	means investment funds managed by Lumina, including their classes and subclasses, where applicable.
"General Personal Data Protection Law"	Law No. 13,709 of August 14th, 2018, as amended.
"Internal Information"	information related Lumina's business or operations that implies, by their nature, certain kind of care and privacy. Internal Information may be disclosed with the prior consent of the Compliance Officer. Examples include, but are not

	limited to, certain information regarding Lumina's internal controls or operational procedures, and information regarding sellers, service providers, contractors and investments or any information which the disclosure could be imposed by law or competent authority.
"IT"	Lumina's Information Technology department or group, including third-party services contracted for this purpose.
"KYC"	*Know Your Client.*
"Lumina" or "Manager"	Lumina Capital Management Ltda., a limited liability company registered as an asset manager ("administradora de recursos"), in the quality of "portfolio manager".
"Manual"	this compliance and risk manual.
"Person"	any individual, company, association or legal entity, or any other entity.
"Personal Data"	Information relating to an identified or identifiable natural person. The concept of personal data includes sensitive personal data.
"Portfolio Management Officer"	an individual certified as Asset Manager by the CVM Resolution No. 21/21 and the ANBIMA Code.
"Public Information"	information which Lumina and the Members could make available to the public in general. For example, information available in Lumina's website and accessible to public, content accessible to the public through social media or other pages managed by Lumina, and information accessible to the public in general in Lumina's regulatory files.
"RCVM 175/22"	CVM Resolution No. 175, dated 23 December 2022, including its regulatory annexes.
"RCVM 21/21"	CVM Resolution No. 21 of February 25th, 2021.
"RCVM 50/21"	CVM Resolution No. 50/21 of August 31st, 2021.
"Risk Management Officer"	the statutory Risk Management Officer at Lumina. The Risk Management Officer is the same person appointed as Operating Officer, AML/PTF Officer, Compliance Officer

	and Data Protection Officer.
"Sensitive Personal Data"	Personal data on racial or ethnic origin, religious belief, political opinion, membership of a trade union or organization of a religious, philosophical or political nature, data relating to health or sexual life, genetic or biometric data, when linked to a natural person.
"Subclasses"	means the investment subclasses of the Funds' Classes.

2. Purpose of this Manual

Lumina is an asset management company ("*administradora de recursos de terceiros*"), registered under Brazilian regulation in the category of "portfolio manager", specialized in independent management of investment funds. Lumina does not distribute shares of the Funds, provide securities advisory or manage "*carteiras administradas*" (a type of investment portfolio existing in Brazil) or wealth portfolios ("*gestão de patrimônio*") and therefore is not subject to the rules applicable to these activities under Brazilian regulation.

Lumina is not currently required to be, and is not, registered as an investment adviser with the Securities and Exchange Commission (the "SEC).

Lumina has adopted the Codes and Policies set forth in this Manual to comply with Brazilian law and applicable regulations (especially those of CVM and ANBIMA), and as a matter of best practice as part of a broader effort to ensure compliance with any applicable legal or regulatory obligations in the U.S.

The purpose of this Manual is to help all Members understand the legal and regulatory requirements applicable to them in the context of the activities performed by Lumina, as well as to inform all Members about the internal methods, controls and codes of conduct implemented by Lumina that they shall adhere to. If any Member becomes aware of any possible breach of any rules set forth in this Manual, such Member shall immediately notify the Compliance Officer thereof.

For the purposes of interpreting the provisions set out in this Manual and its annexes, unless expressly stated otherwise: (a) the terms used in this Manual shall have the meaning assigned in RCVM 175/22; (b) references to Funds shall include their Classes and Subclasses, if any; and (c) references to the bylaws shall include annexes and appendices, if any, in accordance with the provisions of RCVM 175/22.

This Manual is by no means exhaustive and is subject to changes, corrections, updates, and continuous revisions. If any Member becomes aware of any doubtful or relevant situations not dealt with in this Manual, such Member shall notify the Compliance Officer of such situation. The Compliance Officer, in the exercise of his/her competencies indicated below, shall be responsible for advising the Member as to any actions to be taken and if the case may be, shall arrange for amendment to this Manual in order to cover the specific case.

When new Members join Lumina, they shall receive a copy of this Manual and shall acknowledge in writing that they have read, agreed to, and shall not violate the rules set forth in this Manual. All Members are required to read this Manual thoroughly and carefully, including any periodic and extraordinary revisions published according to

item 27 of this Manual.

IN CASE OF DOUBTS, THE MEMBERS SHALL CONSULT THE COMPLIANCE OFFICER PRIOR TO TAKING ANY ACTION THAT MAY POTENTIALLY RESULT IN NON-COMPLIANCE WITH THE PROVISIONS HEREIN.

3. Compliance, Risk Management and Data Protection Officers

The Compliance Officer is responsible for the activities described below, in addition to the specific responsibilities provided in this Manual:

(a) ensuring compliance with the law and with all rules and regulations (internal or external) that govern Lumina's business;
(b) reviewing periodically, and under the terms provided for in this Manual, the internal rules and regulations of Lumina, in order to ensure that they are consistent with applicable law and regulations and that any doubts or issues that may arise during the course of Lumina's business may be dealt with;
(c) supervising compliance by Members of Lumina's internal rules and regulations through the adoption of specific internal measures to implement the policies in the daily routine of the company;
(d) Oversee the interactions of the management team with third parties, particularly in higher-risk scenarios, ensuring that the Compliance Department has visibility into meetings scheduled on behalf of the Manager and/or its investment vehicles. To this end, the Compliance Department shall be informed of the management team's activity calendar, containing basic information on asset due diligence meetings (such as date, participants, and purpose), so as to enable the prior identification of potential risks. Whenever possible, records or meeting notes of such interactions shall also be maintained for subsequent review, if necessary.
(e) investigating cases of violation or potential violation of this Manual by a Member and taking appropriate measures to promptly remedy the violation or potential violation and punish the Member, as applicable;
(f) filing a complaint about acts of fraud, misconduct, corruption, AML/PTF, to the relevant authorities, as applicable;
(g) evaluating operations that may be suspected of money laundering and terrorist financing and filing them to COAF, as applicable;
(h) advising Members about the rules contained in this Manual and the compliance and AML/PTF rules applicable to their roles;
(i) developing and supervise training for Members according to the Training Policy contained herein;
(j) ensuring that reports of actual or potential non-compliances with this Manual

or the applicable law or regulations are treated confidentially and impartially, except as provided for in this Manual;

(k) supporting and encouraging compliance activities and programs;
(l) ensuring that Lumina complies with the best AML/PTF practices..

Under the terms of RCVM 21/21 article 25, the Compliance Officer shall send to Lumina's management, by the last business day of April of each year, a report for the previous year containing:

(a) his/her conclusions about the supervisory activities of fulfilment of the codes of conduct and Policies contained herein, as well as the revisions undertaken in Lumina's internal policies;
(b) recommendations regarding any issues found in Lumina's internal policies, establishing a timeline for their solution, when applicable; and
(c) opinion of the Portfolio Management Officer regarding those issues and the measures planned (according to a specific timeline) or effectively taken to solve them.

O The Compliance Officer is the same person appointed as AML/PTF Officer, Risk Management Officer and Data Protection Officer.

The Compliance Officer performs his/her roles independently and shall not report directly to any other officer at Lumina.

The Risk Management Officer shall be responsible for the activities described below, in addition to the specific activities provided in this Manual:

(a) ensuring the compliance of the Risk Management Policy, according to item 14 of this Manual;
(b) managing market risks;
(c) managing liquidity risks;
(d) managing Concentration Risks;
(e) managing credit and counterparty risks;
(f) managing operational risks;
(g) creating risk management reports according to the law, regulations and this Manual; and
(h) implementing risk-related legal and regulatory frameworks.

The Data Protection Officer is responsible for the activities described below, in addition to those specific responsibilities provided for throughout this Manual and the other policies disclosed by Lumina:

(a) accept complaints and communications from the holders of Personal Data, provide

clarifications and take action;;
(b) receive communications from the ANPD and take action; and
(c) guide Lumina's Members and contracted third parties regarding the practices to be taken in relation to the protection of Personal Data.

4. Code of Ethics

Lumina has adopted a Code of Ethics that establishes certain standards of business conduct that Lumina and all its Members must follow. The Code of Ethics can be found in Appendix I hereto.

5. AML/PTF

The term "money laundering" includes several activities and processes intended to hide the ownership and precedence of unlawful activity, simulating a lawful origin. The term "financing of terrorism" is based on the existence of indications or evidence of the practice of terrorism, the financing of terrorism or correlated acts, by natural persons or entities. Article 2 of Law No. 13.260/2016 defines as terrorism the practice of certain acts pre-identified for reasons of xenophobia, discrimination or prejudice of race, color, ethnicity and religion, when practiced with the purpose of committing social or generalized terror, exposing people, assets, the public peace or the public safety to danger. Lumina and its Members are committed to the AML/PTF policy, aiming to detect and deter the occurrence of money laundering, financing of terrorism, and other illegal activities in connection to Lumina's business.

The practice of acts of financing of terrorism and the proliferation of weapons of mass destruction does not depend on the identification of a relevant or substantial financial amount for the understanding that the act is qualified as helping or financing such practices. The identification of any amounts connected to such practices shall trigger reporting and combating measures provided for in this AML/PFT Policy.

Lumina and its Members shall comply with all rules intended to prevent money laundering in investment fund management, including, but not limiting to, Law No. 9,613/1998, Law No. 13.260/16 and RCVM 50/21.

Lumina and its Members must also comply with the U.S. sanctions regimes administered by the U.S. Treasury Department's Office of Foreign Assets Control ("OFAC"). These sanctions restrict the ability of U.S. persons and entities from doing business with (i) individuals and entities the U.S. government believes are engaged in

terrorism, terrorist financing, drug trafficking, or other activities that could harm the United States, and (ii) jurisdictions (such as Iran, Cuba, North Korea, and Sudan) that pursue policies that are contrary to those of the United States. Failure to comply with these sanctions regimes can result in civil or criminal liability for Lumina and its Members.

Involvement in money laundering activity – even if inadvertently – could result in potential civil and criminal penalties for Lumina and its clients and/or its Members, as well as damages to their reputation.

The Compliance Officer, under the terms of RCVM 50/21, article 8, shall be responsible for this Policy and all provisions concerning AML/PTF. The Compliance Officer must provide training for all Members so that they can detect and fight against money laundering and the financing of terrorism and the proliferation of weapons of mass destruction, according to the Training Policy herein. The Compliance Officer shall arrange new trainings, if required, in case of changes to applicable law or regulations. Protecting Lumina from being inadvertently contaminated by money launderers is the responsibility of every Member. No Member may facilitate or participate in any money laundering activities. Non-compliance with this Policy will subject Members to disciplinary action, including, without limitation, the termination of employment, as well as potential civil or criminal penalties, under the terms of Lumina's Code of Ethics.

Lumina adopts an uncompromising stance when hiring its Members. Before joining the company, candidates must be interviewed by all Lumina's officers. Requirements such as their market reputation and profile are assessed, as well as their backgrounds, under the terms of Lumina's Privacy Policy.

Lumina employs a risk assessment methodology to check its exposure to money laundering and the financing of terrorism and the proliferation of weapons of mass destruction weapons activities in certain transactions. Appendix III herein outlines the general topics of this methodology, including analysis of order counterparties and pricing of traded assets.

Among other possibilities, an activity may be deemed suspicious if it is:

(a) a transaction with amounts that seem objectively incompatible with the occupation, revenue and/or the assets or financial situation of any of the parties involved, based on their available data;
(b) a transaction carried out between the same parties or for the benefit of the same parties, in which continuous gains or losses are verified in relation to any of the parties involved;
(c) a transaction that shows a significant oscillation in relation to the volume and/or frequency of deals of any of the parties involved;

(d) a transaction with consequences that include characteristics that may represent a mechanism to disguise the identification of the actual beneficial owners and parties involved;
(e) a transaction showing sudden changes, objectively unjustified in view of the operational characteristics typically used by the parties involved;
(f) a transaction performed for the purpose of generating loss or gain which objectively lacks economic basis;
(g) a transaction with the participation of individuals residing or entities organized in non-cooperative countries or territories, pursuant to the circular letters issued by the Financial Action Task Force (FATF);
(h) a transaction settled in cash, if and when permitted;
(i) a private transfer, for no apparent reason, of funds and amounts;
(j) a transaction with a level of complexity and risk that seems to be incompatible with the technical qualification of the client or its representative;
(k) a deposit or transfer made by third parties for settlement of transactions of clients or guarantee of transactions in future settlement markets;
(l) a payment to third parties, in any manner whatsoever, by way of settlement of transactions or redemption of amounts deposited in guarantee, registered on behalf of the client;
(m) a situation in which it is not possible to keep the client's record data updated; and/or
(n) a situation or transaction in which it is not possible to identify the beneficial owner.

Members shall pay special attention to transactions involving the following categories of investors:

(a) Ultimate beneficial owners of Funds under Lumina's Management;
(b) non-resident investors, especially those organized as trusts and companies with bearer bonds;
(c) high net worth investors whose funds are managed by areas of financial institutions focused on wealth management ("private banking"); and
(d) politically exposed persons, pursuant to the applicable law and regulations.

In no case will Lumina accept an investment from or on behalf of any investor who is deemed to be a Prohibited Investor. "Prohibited Investors" include the following:

- Any person who, or entity that, is a "specially designated national" and thus subject to sanctions by OFAC.
- Any person or entity subject to OFAC sanctions (such as Iran, Cuba, Russia or Venezuela); and
- Foreign shell banks (i.e., a foreign bank without a physical presence in any country).

Members shall analyze transactions together with other related transactions that may be part of the same group or in any manner related to each other.

Any Member who suspects the possibility of money laundering activities involving Lumina or its clients shall immediately report such activities to the Compliance Officer informing as many details as possible. The Compliance Officer should also be notified immediately if (i) there is any attempt by a Prohibited Investor to become an investor in a Fund, or (ii) any situation arises in which an existing investor becomes a Prohibited Investor. The Compliance Officer shall carry out additional investigations to determine whether the relevant authorities shall be informed of such activities, according to the applicable law and regulations. The Compliance Officer must also communicate such activities to COAF within 24 (twenty-four) hours from the conclusion of his/her analysis that uncovered the atypical transaction.

If no suspicious activities have been identified, the Compliance Officer shall also send a report to CVM by the last working day of April of each year informing that no suspicious activities have been identified in any concluded or proposed transactions, following the mechanisms established in the agreement between CVM and COAF.

Furthermore, the Compliance Officer shall send an internal AML/PTF risk assessment report by the last business day of April of each year, under the terms of RCVM 50/21, article 6.

This report shall also include, under the terms of RCVM 50/21, article 5:

(a) identification and analysis of AML/PTF risks, including their threats, vulnerabilities, and consequences;
(b) number of transactions analyzed, and atypical situations detected, as well as number of suspicious transaction reports and eventual negative statements;;
(c) effectiveness indicators, including timeliness of detection, analysis, and communication of atypical operations or situations;;
(d) recommendations to mitigate identified risks from the previous financial year that have not yet been adequately addressed, as applicable; and
(e) a report of the effectiveness of the recommendations adopted in relation to the risks identified in the previous year.

Subject to the Compliance Officer supervision, all Members shall keep books and records updated, including documents related to all transactions carried out in the last 5 (five) years. This period may be extended indefinitely if a formal investigation process is initiated and formally communicated by CVM. Each investment fund shall contain its own records, separate from the records of other funds under Lumina's management.

The Compliance Officer shall adopt procedures to ensure that Lumina prevents damage, forgery, destruction, or improper alteration of books and records..

6. KYC Policy

Lumina is not involved in distribution activities; therefore, it does not maintain a direct relationship with the investors of its Funds. Lumina does not intend to be involved in distribution activities and does not currently have the necessary legal and regulatory authorizations to do so.
Under the terms of article 5, § 3 and article 17, § 1, of RCVM 50/21, managers who have no direct relationship with investors shall identify, analyze, understand, and mitigate the AML/PTF and terrorist financing risks inherent in their activities, within the limits of their duties. Lumina does not perform any distribution activities and therefore has no direct relationship with the investors of the Funds it manages. For the purposes of the ANBIMA AML/PTF Guide (Edition IV, 2022), in relation to Lumina's relationship with the investors of the funds under its management, Lumina plays the role of "investment fund manager with multiple investors" and "exclusive fund manager".

In this context and within the limits of its role as an asset manager, the Manager shall periodically inquire the trustees about the tests they perform in the investor base of investment funds managed by the Manager, as well as the governance practices they implement for the prevention of money laundering and terrorist financing and the supervision of service providers, especially contracted distributors. Specifically, regarding exclusive funds under its management, Lumina shall (i) collect onboarding information of the ultimate beneficial owner of these vehicles from the respective distributors and/or administrators, and (ii) monitor such information, in line with the AML/PTF Policy.

In the event Lumina decides to undertake distribution activities of its Funds and establishes relationships with its investors, thus obtaining legal and regulatory permission to do so, this Manual shall be promptly updated to include specific and detailed KYC rules.

7. Anti-Corruption Policy

Pursuant to the Anti-Corruption Law, it shall be considered harmful to the Brazilian and any foreign public administration any and all acts practiced by legal entities against the Brazilian or any foreign public estate, against the principles that govern public administration, or against international commitments undertaken by Brazil, as defined by::

(a) promising, offering or giving, directly or indirectly, any improper advantage to a public official or a third party related to a public official;
(b) (b) financing, funding, sponsoring or otherwise promoting the practice of tortuous acts in violation of the Anti-Corruption Law;
(c) making improper use of third parties, either individual or legal entities, to conceal or disguise their real interests or the identity of the beneficial owners of the actions taken in violation of any law;
(d) in what concerns public bids and contracts: (i) frustrating or defrauding, by means of collusion or any other expedient, the competitive nature of a public bid; (ii) preventing, hindering or defrauding the performance of any act within the scope of a public bid; (iii)removing or seeking the removal of a bidder, by means of fraud or by offering advantage of any kind; (iv) defrauding a public bid or the contract resulting thereof; (v) creating, fraudulently or irregularly, a legal entity for the purpose of participating in a public bid or entering into administrative contracts; (vi) obtaining improper advantage or benefit, by means of fraud, concerning modifications or extensions of contracts entered into with the public administration, without authorization provided either by the law or by the invitation to bid or respective contractual instruments; or (vii) manipulating or defrauding the economic and financial balance of the contracts entered into with the public administration; and
(e) hindering the activities related to the investigation or inspection by public agencies, entities, or officials, or intervene in the performance of their duties, including in the context of regulatory agencies and agencies in charge of supervising the national financial system.

“Foreign public administration” means the governmental entities or diplomatic representations of a foreign country, of any level of the government, as well as entities directly or indirectly controlled by the government of a foreign country. Public international organizations are considered as foreign public administration.

Foreign public agent means, for the purposes of this Policy, those who, even if transitorily or without remuneration, exercises public employment or function in public entities or in diplomatic representations of foreign country, as well as entities directly or indirectly controlled by the government of a foreign country or by international public organizations.

No Member shall facilitate or participate in any corruption activities. Non-compliance

with this Policy will subject Members involved to disciplinary action, including the termination of employment agreement, as well as potential civil or criminal penalties. All Members are required to immediately report to the Compliance Officer any suspicious activities that fit the above description.

Lumina makes every effort to monitor all its Members in order to ensure that they act in compliance with the Anti-Corruption Law, while respecting and practicing, to the extent of their activities and possibilities, the acts referring to the Integrity Program provided in Decree No. 8,240 of March 18th, 2015.

Relationship with Public Agents

Members must act in a way to prevent and, if applicable, remedy situations of conflict of interests that could arise in relation to Lumina and its Members, as well as in relation to Lumina and the public sector.
In line with the forbidden practices described herein above and in accordance with Anticorruption Law, Members are forbidden from offering, promoting, doing, authorizing or proportionating, directly or through intermediates, any undoable advantage to public agents, with the intention of influencing or retributing any official action or decision of such agent, in favor of the Member and/or Lumina, as well as of consent with the receipt, in the name of the Member or Lumina's, any advantage that could be interpreted as a payment due to the practice of acts harmful to the public administration, manly those related to corruption practices.

In order to ensure the effectiveness and enforcement of the above prohibitions, any contacts with public officials, whether via email correspondence, telephone conferences, in-person meetings, or virtual meetings, may be supervised by the Compliance Officer, without prejudice to the compliance department monitoring other matters it deems necessary to oversee, in accordance with the provisions of item 3(d) above.

8. Service Provider Selection, Contracting and Monitoring Policy

By virtue of the regulations, Lumina, together with the administrator of each Fund, is considered an essential service provider of the Funds (together, the "Essential Service Providers").

Thus, within the scope of its asset management activities and on behalf of the Funds, Lumina has identified the service providers covered by this policy as follows:

- Execution of transactions for the asset portfolio (including brokers and foreign exchange intermediaries);

- Distribution of fund units;
- Investment advisory services;
- Closed-class market making;
- Co-management of the asset portfolio.

Given the operational dynamics among the Essential Service Providers, the Manager may also engage other services for the benefit of the Fund that are not listed above, provided that, in such cases:

- The engagement does not occur on behalf of the Class, except as provided in the relevant regulatory documents or approved at a quotaholders' meeting;
- Regarding to the service provider engaged that is not a participant in a CVM-regulated market, or whose services to the Class do not fall within the CVM's scope of oversight, Lumina must supervise the activities of the third party related to the Class, in accordance with applicable regulations.

The engagement and oversight process, where applicable, adopted by Lumina is carried out with a view to the best interests of the Funds and the mitigation of potential conflicts of interest, particularly in cases where there is a direct or indirect connection between the service provider and other service providers or investors.

In this regard, when engaging service providers that may belong to its Conglomerate or Economic Group, or to the Conglomerate or Economic Group of the investors of the Funds under its management, Lumina shall ensure that the transactions comply with strictly commutative conditions as established in this policy.

Prior to contracting service providers on behalf of the Funds or of Lumina, all Members shall provide the Compliance Officer with necessary information to perform a due diligence on such third party, in order to verify (i) its compliance with legal and regulatory requirements; (ii) eventual conflicts of interest; (iii) its capacity to provide the services; (iv) the costs to provide the services, always preserving the best interests of Lumina's investors.

To this end, the following shall be required:

(a) for all activities not subject to ANBIMA supervision and regulation::

a. complete qualification of the company;
b. evidence of power of representation;
c. name and qualification of partners and executives;
d. date of the beginning of the activity;
e. marketing research regarding the quality of the service provided by the third party, its experience in the contracted service, reputation, and cost

of the services compared with competitors;

f. f. demonstration of absence of conflicts of interest, even potential ones, with the third party; and
g. if necessary, meetings at the third party's office and with its main executives.

(b) for activities subject to ANBIMA supervision and regulation, in addition to the requirements described above, the completion of the ANBIMA Due Diligence Form.

All Members shall require that the third party fills out and agrees with the Statement in Appendix IV.B of this Manual, indicating that it is not involved in corruption, money laundering, and terrorist financing activities.

Once the Member completes the due diligence of the third party and has all the necessary documents, he/she shall send the documents and his/her conclusions to the Compliance Officer. The Compliance Officer will, in turn, verify the adequacy of the third party to provide the services and either approve or reject its contracting.

The contracting of third parties shall be formalized by means of a written contract, pursuant to applicable legal and regulatory requirements. The contracting of third parties on behalf of the Funds shall be formalized by means of a written contract, pursuant to applicable legal and regulatory requirements, especially the minimum content set forth in Article 19 of Code of ANBIMA ART. The third party shall not start providing the services before the formalization of the contract with Lumina, and no payments shall be made to the third party before the formalization of the contract.

Contracted third parties shall be monitored through periodic reviews, in which the criteria for the adequacy of the services provided will be verified again, as well as their quality. The Members who contracted the third party shall be responsible for its monitoring and shall be reported to the Compliance Officer by means of revision due diligences/update of documentation collected with the purpose of the initial contracting.

In addition to the general provisions detailed above, the following procedures shall be adopted in accordance with the scope of the engagement carried out by Lumina or the relationship maintained.

<u>Relationship among the Essential Service Providers</u>

Although there is no subordination or engagement relationship between the Administrator and Lumina, considering that both are Essential Service Providers, prior to the launch of a new Fund, the Manager must verify whether the Administrator:

- Is duly authorized to carry out such activity and is a member institution of ANBIMA; and
- Has adequate structure and procedures for performing its functions, including with respect to interaction with other service providers, especially distributors.

Additionally, Lumina shall contractually establish, in the instrument governing the relationship among the Fund's Essential Service Providers, the information flows and responsibilities of each Essential Service Provider, at a minimum with respect to the following aspects:

(i) The flow of provision and submission of information to regulatory and self-regulatory bodies, as well as in relation to the establishment of Funds, Classes, and Subclasses, if any;
(ii) Duties regarding concentration limits;
(iii) Controls for managing the liquidity of the Classes;
(iv) Absence of joint liability among the Essential Service Providers and other complementary service providers, as well as the parameters for assessing the responsibility of each party;
(v) Procedure for the disclosure of relevant facts of the Funds; and
(vi) Flow of information regarding service providers engaged by the Administrator or the Manager, on behalf of the Fund

The Manager shall also update the Administrator evaluation process periodically, in accordance with the risk rating assigned within the risk-based approach detailed in this policy.

Selection and Engagement of Co-Managers

When engaging a co-manager to operate alongside the Classes, the Manager must:

- Ensure that the engaged co-manager is a member or associate institution of ANBIMA, except where expressly exempted under the terms of the AGRT Code; and
- Clearly define the responsibilities of each manager in the respective service agreement, which shall include, at a minimum:
  a. The designation of the specific market in which each manager will operate;
  b. The Class or Classes subject to the co-management services; and
  c. Where applicable under the prevailing regulations, the limitation of orders to the specific market in which each manager operates with respect to the custodian of the contracting Class.

Selection and Engagement of Distributors

In addition to the engagement provisions set out above, in the event of engaging distributors of Fund units, Lumina shall verify:

- Regardless of the distribution method: That the distributor is duly authorized to carry out such activity and has adequate structure and procedures to perform its functions, including with respect to interaction with other service providers, especially the administrator; and
- If the distribution is carried out on a "proprietary and agency" basis: confirm that the distributor (i) is authorized to provide securities registration services, or will arrange for the deposit of the units in a central securities depository or their registration in an organized market, in order to enable identification of the beneficial unitholder; and (ii) will assume all burdens and responsibilities related to the clients, including their registration, identification, and other procedures that would originally fall to the administrator under the applicable regulations.

In addition to the provisions set out above, in the context of engaging distributors, Lumina shall also verify the provisions established in its Policy for the Prevention of Money Laundering, Terrorism Financing, and Financing of the Proliferation of Weapons of Mass Destruction – AML/CFT and Customer Onboarding Policy.

Selection and Engagement of Credit Rating Agencies

Without prejudice to the other requirements set forth in this policy, contracts entered into with credit rating agencies shall include the following additional provisions:

- A clause requiring the credit rating agency to immediately disclose on its website and notify the CVM and the Essential Service Providers of any change in the Class rating or the termination of the contract;
- The termination of the contract shall only be permitted upon observance of a 180 (one hundred and eighty) calendar-day notice period, with the mandatory submission, at the end of such period, of a risk rating report prepared by the same agency; and
- If the contract termination occurs by resolution of the quotaholders' meeting, the notice period referred to above shall be equivalent to 90 (ninety) calendar days.

The engagement of a credit rating agency, if not provided for in the Fund's bylaws, shall be subject to a Relevant Fact disclosure.

Selection and Engagement of Market Makers

Subject to the other provisions of this policy, when engaging or terminating the services of market makers for the Funds, Lumina shall disclose a Relevant Fact or, alternatively, inform the Administrator so that it may disclose a Relevant Fact.

Selection and Engagement of Securities Advisors

In the selection and engagement of securities advisors, Lumina shall verify that the advisor holds all necessary regulatory authorizations to carry out the contracted activity, as well as the policies and manuals required under the applicable regulations governing the advisor's activities.

The contract entered into with the advisor shall include a prohibition on the receipt by the advisor of any remuneration, benefit, or advantage, whether direct or indirect, that could potentially compromise their independence in the performance of their duties.

Contracting Broker-Dealers

Lumina has the duty to seek the best execution of client securities transactions. The SEC has described this requirement generally as a duty to execute securities transactions so that a client's total costs or proceeds in each transaction are the most favorable under the circumstances. The SEC also has stated that when seeking best execution a trader should consider the full range and quality of a broker-dealer's services in placing trades, and that best execution is not determined by the lowest possible commission costs, but by the best qualitative execution.

In addition to the rules described above, Lumina has adopted the following guidelines for evaluating brokerage services for Fund transactions. These guidelines are designed to enable Lumina to fairly evaluate the overall quality and costs of a broker-dealer's execution services, including factors other than prices, commissions and other expenses paid in connection with account transactions.

Best Execution Guidelines

The factors to be considered in selecting and approving brokers-dealers that may be used to execute trades for Fund accounts include, but are not limited to:

- Quality of execution - accurate and timely execution, clearance and error/dispute resolution
- Reputation, as obtained in the background check process;
- Willingness to execute difficult transactions;
- Access to underwritten offerings and secondary markets;

- Level of reliability;
- Overall costs of a trade (i.e., net price paid or received) including commissions, mark-ups, mark-downs or spreads in the context of Lumina's knowledge of negotiated commission rates currently available and other current transaction costs;
- Desired timing of the transaction and size of trade;
- Confidentiality of trading activity; and/o
- Market intelligence regarding trading activity.

Lumina shall not take the receipt of soft dollars into account when selecting broker-dealers, but the best interests of its investors.

Members shall not be allowed to benefit from returns on brokerage fees or discounts, which must always be received for the benefit of investors in Funds managed by Lumina or Lumina's shareholders.

Periodically, the Compliance Officer may sample trades completed to review execution of trades and ensure appropriate consideration of these guidelines.

Soft Dollar Arrangements

The use of soft dollars potentially raises an issue as to whether the trader has obtained best execution.

However, a "safe harbor" for purchases of eligible "brokerage and research services" with soft dollar commissions was created in Section 28(e) (the "28(e) safe harbor") of the Exchange Act. The 28(e) safe harbor provides that it shall not be deemed to have acted unlawfully or to have breached a fiduciary duty under state or federal law solely by reason of having paid more to a broker-dealer than the lowest available commission, provided that the trader has determined in good faith that the amount of the commission is reasonable in relation to the value of the brokerage and research services provided by the broker-dealer.

In respect to the provisions set forth in item 9 of the Code of Ethics, Lumina accepts the use of soft dollars to pay for proprietary and/or third-party research or certain brokerage products or services. It is Lumina's policy to only use soft dollar commissions to pay for products or services that qualify as eligible "brokerage and research services" under the 28 (e) safe harbor.

Soft dollar arrangements may be formal or informal. The research or brokerage products and services provided to Lumina by broker-dealers may include information on the economy, industries, groups of securities, individual companies, statistical information, accounting and tax law interpretations, political developments, legal

developments affecting portfolio securities, technical market action, pricing and appraisal services, credit analysis, risk measurement analysis, performance analysis, analysis of corporate responsibility issues and post-trade services, or communication services related to executing, clearing and settlement of transactions. Such research services are provided primarily in the form of written reports, telephone contacts, and personal meetings with securities analysts.

All proposed soft dollar agreements, whether formal or informal, are subject to prior approval by the Compliance Officer. In addition, the Compliance Officer is responsible for ensuring that appropriates disclosures of Lumina's soft dollar policies are made in the Funds' offering documents.

Post-Engagement Procedures for Third Parties

The reassessment of engagements in accordance with the risks associated with the activities performed shall be carried out throughout the duration of the contractual relationship. Monitoring shall be the responsibility of the Compliance Officer, who may be assisted by the Portfolio Management Director, where applicable.

Following the formalization of the contractual relationship, Lumina shall classify the third parties and the Administrator in accordance with the Risk-Based Approach detailed below, which shall be updated from time to time based on the outcome of such approach or if Lumina becomes aware of any adverse fact that, in Lumina's judgment, could affect the provision of services.

The reassessment of engagements in accordance with the risks associated with the activities performed shall be carried out throughout the duration of the contractual relationship. Monitoring shall be the responsibility of the Compliance Officer, who may be assisted by the Portfolio Management Director.

The analysis, for monitoring purposes, shall consider the contracted scope in relation to the services delivered, with emphasis on any discrepancies, timeliness, and expected quality. Furthermore, monitoring should be able to proactively identify activities that could pose risks to Lumina.

Given Lumina's organizational structure, the process for the continuous monitoring of the contracted third party shall be concise and objective. In general terms, the Compliance Officer with the assistance of the Portfolio Management Director where applicable, shall evaluate the third party's performance against the expectations and goals established at the time of engagement, the cost-benefit relationship, and the level of security applied in its tasks. Without prejudice, in specific cases, more stringent controls shall be adopted, as detailed below in the section addressing risk-based supervision of contracted third parties.

Except where expressly provided for under applicable regulation, updating KYP (Know Your Provider) should not be construed as supervision by Lumina over the Third Parties, given that such Third Parties usually:

- They are highly regulated by the CVM and, as applicable, also by the Central Bank of Brazil and/or self-regulated by ANBIMA;
- They have undergone increasingly robust and detailed accreditation and authorization processes for performing their activities, being required to demonstrate the existence of a suitably qualified technical team, clear manuals and policies, and compatible internal procedures (including periodic training for all Members);
- They are subject to continuous supervision, either through periodic routines established by the respective authorities and entities or as a result of specific events and demands;
- They are mostly subject to a robust institutional information regime regarding their activities, publicly available to the market; and
- Their responsibilities are clearly defined in the regulations applicable to their activities.

Duty of Oversight

In addition to applying the initial and periodic KYP process, Lumina shall supervise the engaged service provider exclusively if the provider is not a market participant regulated by the CVM, or if the service provided to the Class falls outside the scope of CVM regulation, in compliance with applicable regulations. Lumina shall also adopt the procedures outlined below, as applicable.

Selection and Engagement of Law Firms

Subject to regulatory provisions, Lumina shall be responsible for engaging law firms to defend the interests of the Classes, whether in or out of court, in matters related to the rights or assets held by the Classes.

In addition to the other provisions of this policy, Lumina shall take the following measures regarding the engagement and monitoring of legal services:

- Where applicable, for Classes that are parties to administrative or judicial proceedings, request the law firms to prepare explanatory notes for the financial statements, including the risk classification of such proceedings (i.e., probable, possible, or remote);
- Monitor the progress of judicial and administrative proceedings in which the Class is a party, together with the engaged lawyer, in order to identify potential contingencies

that may constitute a relevant fact for the Classes, informing the administrator of any need to establish provisions in the Classes' portfolio; and

• Request the preparation of periodic reports on the judicial or administrative proceedings and provide them to the administrator or the independent auditor of the Classes to comply with regulatory requirements applicable to the Classes' financial statements.

Selection and Hiring of Investment Advisors

In selecting and engaging specialist investment advisers, Lumina shall evaluate the following:

- the technical quality of the services provided;
- the existence of potential conflicts of interest;
- the credit risk/financial health of the consultant;
- any news and accusations in public administrative proceedings filed by regulatory or self-regulatory bodies that may discredit the reputation of the specialized investment advisor;
- the Anbima Due Diligence Questionnaire specific, if existing (i.e., real estate consultant and credit consultant).

In this way, the Manager may use its own mechanisms (e.g., internal questionnaire) for evaluation and subsequent inspection of the above requirements.

Delegation of Responsibilities of the Manager

Lumina may also contract or delegate the performance of certain obligations assigned to it, by virtue of the regulation, for example, the KYP process in relation to complementary service providers, the prior classification of operations, the verification of eligibility criteria and ballast, among others.

Such services may be delegated to other service providers of the Funds, including, but not limited to, the administrator or custodian, notwithstanding that the ultimate responsibility for approving and engaging the complementary service providers referred to in this Policy remains vested in Lumina, notwithstanding Lumina's right of recourse in relation to the conduct of the contracted service provider. as set forth in the contract.

In contracts entered into with Third Parties that are subject to Lumina's inspection, by virtue of the regulation, the Manager shall ensure the possibility of unilateral termination of the contract and at no cost to the Fund, in the event that the contracted Third Party is not approved by the internal contracting and monitoring processes, observing the curing periods for the remediation of inaccuracies identified by Lumina

in its monitoring process.

Subject to the provisions of the regulation, Lumina will be responsible for hiring law firms to defend the interests of the Classes, in or out of court, in cases related to rights or assets held by the Classes.

Risk-Based Supervision

Risk-based supervision aims to pay greater attention to third parties that demonstrate a greater probability of presenting failures in their performance or potentially represent greater damage to investors and to the integrity of the financial and capital markets.

Monitoring should include risk-based supervision, in order to pay greater attention to contracted third parties that demonstrate a greater probability of presenting failures in their performance or potentially represent greater damage to investors and to the integrity of the financial and capital markets, as classified below:

High risk: Mandatory service providers to the Funds, in accordance with applicable legislation; third parties who have access to Confidential Information in the performance of the contracted service; and/or third parties that are not associated with ANBIMA or adherent to ANBIMA codes. Third parties classified in this category must be monitored at least every twelve (12) months.

Medium risk: Providers of optional services to the Funds, under the terms of the respective applicable legislation; and/or third parties who have access to Internal Information in the execution of the contracted service. Third contractors classified in this category must be monitored at least every thirty-six (36) months.

Low risk: Other providers that do not fit into the other classifications. Third party contractors classified in this category must be monitored at least every sixty (60) months.

In the event of any new fact, or significant change that at the discretion of the Member responsible for monitoring third parties hired, the reassessment must be carried out immediately.

All documents related to the hiring of third parties will be filed or stored digitally by Lumina for a minimum period of 5 (five) years.

9. Expert Hiring Policy and Expert Network

This policy aims to regulate the hiring, use and monitoring of specialists and networks of specialists ("Expert" and "Expert Network", respectively) by Lumina.

Expert Networks are specialized platforms that promote the direct connection between investment managers and professionals with practical and in-depth knowledge in specific sectors, industries or topics ("Expert"), in order to support investment decisions by obtaining market information, sector and technical analysis. Such interactions must strictly respect the legal, ethical and regulatory limits in force, avoiding the obtaining, use or dissemination of **MNPI** (Material Non-Public Information).

A. Procedures for Contracting

The hiring of Expert Services or Expert Networks must be previously submitted to Lumina's compliance area for careful and detailed analysis, in order to mitigate risks related to the improper obtaining of **MNPI** (Material Non-Public Information), as well as to ensure compliance with applicable legal and regulatory requirements.

B. Prior Expert Evaluation or the Expert Network

Before formalizing the hiring of an Expert or an Expert Network, Lumina's Compliance area must carry out an evaluation of the provider or the provider company, as the case may be, in order to verify whether he/she adopts procedures, internal controls and compliance parameters compatible with the standards required by the Manager of its service providers.

The procedures adopted in the Policy for Selection, Hiring and Monitoring of Third Party Service Providers described above may be applied, as the compliance area deems them applicable, as well as the steps below:

- Verification of the integrity of the company or individual, history of operation in the area/sector of interest and involvement in litigation, criminal practices or relevant regulatory sanctions;
- Independent research on the expertise and experiences of the potential contractor for the topic or sector of interest;
- If company: checking for the existence of internal policies and controls, policies to prevent the use of privileged information and practices for monitoring interactions.
- If an individual: collection of the contracted person's commitment on the confidentiality of the information received from Lumina;
- If company: confirmation that the network conducts due diligence on professionals before hiring them and verification of the existence of internal or external audit processes.

The hiring of the Expert or Expert Network will only be authorized after final validation by the Compliance Department.

C. Evaluation and Selection of Experts

The evaluation and selection of Experts and Experts Network begins with a detailed verification of the professional history of the company or candidate, covering previous hires, performance and influence in the sector, academic background of the indicated individual and any relevant connections. Subsequently, potential conflicts of interest, whether personal, financial or institutional, are identified and analyzed, in order to ensure the impartiality and independence of the contractor.

To complement this analysis, public and internal databases are consulted in order to verify disciplinary records, regulatory investigations or administrative proceedings that may compromise the integrity or suitability of the contractor.

Special attention is given to professionals with a history in relevant public positions, in state owned companies, or in listed public companies, whether in Brazil or abroad. For these potential hires, a minimum legal quarantine applicable in the jurisdiction in which they have held the position, and, as the case may be, an additional minimum period to be established by the Compliance Department, counted from the end of the exercise of office, in accordance with the anti-corruption legislation and ethical standards in force. This measure aims to prevent conflicts of interest, misuse of privileged information and undue influence.

After completing this detailed analysis, the compliance area decides on the approval or rejection of the contractor, ensuring that only professionals with proven integrity and aligned with ethical and regulatory standards participate in the consultations made by Lumina.

Prohibitions and Monitoring

It is expressly forbidden, in the course of interactions with Experts, the following:

- Confidential, sensitive, or non-public information is requested or received;
- Questions are asked to obtain privileged information in the context of publicly-held companies or other situations subject to the regulation of the financial and capital markets.

Any identification of suspicious behavior attempts to obtain improper information or non-compliance with this policy must be reported immediately to the compliance area.

The compliance area will keep track of the contracts made with Expert Networks, with a record of the dates, participants, objectives and evidence that there was no exchange of privileged information. It may also carry out periodic audits to ensure adherence to this Policy.

10. Confidentiality and Information Security Policy

Lumina generates, receives, maintains, and possesses Confidential Information, Internal Information and Public Information, including information that is subject to non-disclosure agreements with third parties and shall treat such information in accordance with this Confidentiality Policy.

Members shall not use Confidential Information and/or Internal Information for their own benefit or for the benefit of any party other than Lumina. In addition, Members shall not disclose Confidential Information and/or Internal Information to anyone outside Lumina, except in furtherance of the business of Lumina and in a manner consistent with Lumina's interests after any appropriate procedural safeguards and any other applicable policies have been considered, or as required by applicable law after consulting with the Legal and Compliance Officers. Members are expressly prohibited from sharing physical or electronic copies of files that contain Confidential Information or posting or discussing Confidential Information on social media or professional networking sites, blogs, and chat rooms, considering that the disclose of Internal Information in these channels shall be authorized by the Compliance Officer and the Head of Legal. Failure to comply with this confidentiality requirement may pose serious detrimental consequences to Lumina, its investors, and the Member who breached the confidentiality.

10.1 Data Classification

All data classification must be carried out at the time the information is generated or, whenever necessary, at a later time. It is necessary to clearly know what data is being handled and its purpose, in addition to ensuring its protection.

- **Public** - all the content of all documents is viewed by any Member of the Manager
- **Restricted -** access to content is restricted to certain areas or functions within the Manager
- **Confidential -** Access to content is exclusive to people who are assigned specific permission.

Level of Confidentiality	**Impact caused by the breach of reliability**
Public	No impact
Restricted	Medium damage, which can lead to unwanted

	collateral damage
Confidential	Serious/severe damage, which can cause serious damage to the institution (affecting the image, generating financial loss, impacting operations and making strategic objectives unfeasible).

To carry out the classification, four important aspects must be considered, they are:

- **Integrity** - information that is up-to-date, complete and maintained by authorized person.
- **Availability** - constant availability and whenever necessary for authorized person.
- **Value -** the information must have an added value for the institution.
- **Confidentiality** - exclusive access by authorized person.

11. Risk

Lumina understands that information security risk management is a cyclical and dynamic process that requires constant participation by all people. Due to the fact that it is a cyclical process, it is constantly evolving and improving by comparing the results of the process with the expected results and making adjustments to improve the results.

The risk management process is based on the following steps:

- Identification of critical assets;
- Survey and assessment of the risks associated with these assets;
- Creation of a plan for the treatment of these risks;
- Execution of the risk treatment plan.

The process is cyclical, in the sense that, after the execution of the risk treatment plan, the new level of risk must be compared with the level initially assessed.

The information resulting from this comparison should be used to start the process again.

The process is also dynamic in the sense that critical information assets change over time and, therefore, must be evaluated periodically to keep their identification up to date with business processes.

In order to safeguard Confidential Information and Internal Information, Members are expected to abide by the following rules, guidelines, and any additional policies that may be adopted outside of this Manual by Lumina, Lumina's Information Technology group ("IT"), or any other group:

(a) o not remove or transmit any Confidential Information and/or Internal

Information from the Lumina premises, unless absolutely necessary for business purposes (and, if so, the Member must always keep the information in his/her possession or in a secure place and either destroy or return it promptly to the Lumina premises when its purpose is completed), and shall have authorization to dispose of such Confidential Information and/or Internal Information considering his/her professional attributions;

(b) exercise caution in displaying documents or discussing information in public places such as in elevators, restaurants, or airplanes, or in the presence of persons who are not Members (you should presume the bathrooms and office lobby are public places);

(c) exercise caution with documents containing Confidential Information and/or Internal Information when using them in conference rooms or leaving them in wastebaskets, on desktops, in bathrooms, or anywhere else where the information could be seen or retrieved;

(d) use methods approved by IT to copy or transmit data, particularly regarding large volumes of information;

(e) use caution when opening electronic communications and attachments to avoid picking up spyware and other malware;

(f) do not install software from any source without IT approval;

(g) review outgoing emails before sending them to confirm the recipients are correct (no "autofill" errors) and attachments are correctly selected;

(h) never disclose computer or voicemail passwords or website access codes to any unauthorized person;

(i) access only the Confidential Information needed to perform its duties and functions; and

(j) use caution in sharing Confidential Information with anyone at Lumina. A need-to-know basis should be the presumption.

Lumina restricts and controls the access to its offices and proprietary documents and information, stored physically or virtually, by providing login and password to each of its Members. All Members are required to keep their passwords in a safe place and not disclose them to third parties under any circumstances.

Electronic access to Confidential Information and Internal Information is controlled by the login assigned to each Member, according to its professional attributions. When assigning a login to any Member, the Compliance Officer shall decide on the Member's level of electronic access, which will be reviewed later if necessary. In addition, access shall be immediately canceled in case of termination of employment.

Lumina also uses Office 365 and Virtual Private Network (VPN) via firewall as multi-factor authentication methods for users to access its systems and files.

These confidentiality guidelines explain, but do not supersede, the Members'

confidentiality obligations under their respective employment agreements and as described in any other applicable policies. Lumina's restrictions on the disclosure and use of Confidential Information and Internal Information will continue in effect after termination or modification of a Member's employment with Lumina unless specific written permission is obtained from the Portfolio Management Officer or the Compliance Officer. Any questions regarding Lumina's policies and procedures on the disclosure and use of Confidential Information and Internal Information shall be clarified with the Compliance Officer.

With the exception of the information which is protected and considered, for lawful purposes, under the ownership of third-parties, such as their personal data, Lumina is the legitimate owner of all commercial information stored or transmitted through Lumina's systems, including the Confidential Information, the Internal Information and the Public Information, as applicable. Unless Lumina has entered into a specific agreement in writing, all commercial information developed while a Member works for Lumina are the exclusive property of Lumina.

Members, service providers and any other third-party are not authorized to copy the software furnished by Lumina for any way of storage, transfer such software to another computer or disclose such software to third parties without previous authorization of the Compliance Officer.

Under supervision of the Compliance Officer, the IT will conduct semi-annual tests to reexamine the reasonably foreseeable risks to the security and confidentiality of Confidential Information, reassess the sufficiency of the safeguards described herein and below, and ensure the due compliance of this Policy and the Cybersecurity Policy herein after.

12 Privacy Policy

Lumina is committed to the awareness of its owners regarding the personal data collected, used, stored and/or processed by Lumina in the context of the employment relationship between Lumina and the Member and in the scope of its business activities ("Holders"). Therefore, we present our privacy policy ("Privacy Policy"), which aims to provide clear and accurate information to the Holders about the handling of personal data processed by Lumina in the scope of the administration of securities portfolios, in the category of asset manager of investment funds governed by Brazilian law.

This Privacy Policy aims to present in an objective way the characteristics and hypotheses of treatment of personal data. For more information about the handling of personal data processed in the scope of Lumina's activities, please contact Lumina's

Compliance Officer.

Who is the controller of personal data?

Lumina Capital Management Ltda., headquartered at Professor Atílio Innocenti Street, Number. 165, room 1.301, Zip Code 04538-000, City of São Paulo, State of São Paulo, is the controller of personal data regarding the personal data handling activities described in this Privacy Policy. For the purposes of the applicable legislation, the "controller" is responsible for decisions regarding the handling of personal data. In addition, as will be detailed in this Privacy Policy, personal data may be shared by Lumina with other entities (including the other service providers of the investment funds under Lumina's management) for many purposes, in which case such entities may also be controllers of your personal data.

Personal data we may process and for what purposes

For personal data of Holders that are collected or otherwise processed within the scope of the portfolio management activities executed by Lumina, the types of personal data of the Holders that Lumina may handle include, but are not limited to:

- Full name, e-mail, telephone number, date of birth, nationality, identification documents, marital status, professional information, identification of politically exposed persons and other registration data that are voluntarily provide to Lumina and/or authorize to be shared with Lumina;
- Information about your investments, including information about equity and investor profile;
- Information related to lawsuits, protests and arrest warrants, as well as other information to that effect, for the purposes of Know Your Client due diligence; and
- Information about the Holders' relationship with Lumina and/or the administrator of the investment funds under Lumina's management, including, without limitation, customer identifier numbers, account identification details, investment statements and investment application validation, as well as personal data relating to the interactions with Lumina, through internet sites, social media pages, meetings, calls, chats, emails, and phone conversations.

Lumina informs you that it does not intend to collect personal data from individuals aged seventeen (17) years or less. If the Holder under the age of 17 (seventeen) years, please inform Lumina of this fact, so that Lumina may take the measures required by the applicable data protection legislation to process personal data in the scope of its activities.

The personal data of the Holders obtained by this source will be processed for the following purposes:

- For purposes related to the management activities of the investment fund in which the respective Holder is an investor, including the legal and regulatory obligations imputed to Lumina as a portfolio manager.

    ✓ It may include, but is not limited to, validation of the identity of the Holder, prevention and/or detection of illegal activities, compliance with requirements necessary for the maintenance of Lumina's registration with competent authorities, protection of the Holders, verification and monitoring of conflicts of interest, processing of personal data of members and administrators of third party service providers in the scope of the selection, hiring and monitoring of such providers, as well as compliance with judicial, arbitral and/or administrative orders and/or decisions.

    ✓ For the purpose of fulfilling contractual obligations assumed by Lumina, maintaining a relationship with the Holders, as well as defending their interests.

    ✓ It may include, but is not limited to, the development of new products and services, the development of commercial relations with the Holders, the defense of Lumina's rights and interests in judicial, arbitral and/or administrative proceedings.

The personal data of Members need to be processed by Lumina for the purposes of compliance with legal or regulatory obligations, management of the employment contract, processing of remuneration, as well as for the administration of benefits to Members, spouses and/or dependents of Members, as the case may be. Lumina may also process personal data in accordance with Lumina's legitimate interests in the management of its Members and/or the administration of its business. The types of personal data that Lumina processes in this case may include, but are not limited to:

- Information about professional and academic trajectory and experience, details about personal life and habits, as well as skills indicated in the professional resume shared with Lumina or that was voluntarily made available on professional social networks.
- Information about professional and academic trajectory and experience, details about personal life and habits, as well as skills indicated in the professional resume shared with Lumina or that was voluntarily made available on professional social networks.
- Identification documents, such as RG, CPF, CNH and CTPS, for the purposes of registration of the Member and/or compliance with legal or regulatory obligations;
- Military certificate, copy of proof of residence, proof of education and other professional certificates for the purpose of registering the Member;
- Social identification documents (e.g. NIS, PIS, PASEP and NIT) for the purpose of registering the Member;

- Occupational health certificate and medical-admission examination for the purpose of registration and/or compliance with legal or regulatory obligations (which includes control of absences);
- Information about position/department, salary, enrollment, job performance, compensation and professional history for the purposes of monitoring the performance and managing the employment contract;
- Bank details for payroll management purposes; and
- Data of the Member and spouses and/or dependents of Members, such as full name, RG and CPF number, gender, date of birth, telephone, e-mail, for the purposes of managing benefits and fulfilling obligations under the applicable legislation and/or regulations related to the granting of such benefits.

The Member is aware that Lumina will collect the personal data of his/her spouse and/or dependents (as applicable) for the purposes of compliance with legal and/or regulatory obligations, as well as benefits management. In the case of data processing of children and adolescents, the Member declares that he is a parent or legal guardian and consents to the processing of the personal data of such holders to the extent required by applicable legislation. If you have any questions about the processing of data of spouses and dependents, please contact Lumina's Compliance Officer.

To whom do we share personal data?

Lumina may share personal data with third parties or business partners that are relevant to enable Lumina's business activities and for the purposes of providing information technology services (for example, service providers who manage Lumina's internal networks and computers). Such sharing takes place based on the following criteria and for the purposes described below.

- Service providers or business partners: We may share personal data with service providers or business partners engaged by Lumina for the purposes of providing information technology services (for example, service providers who manage Lumina’s internal networks and computers). Such agents receive personal data for the specific purpose of providing services to Lumina and do not have any rights to use personal data outside of this hypothesis.
- Service providers related to human resources management (in the case of members): We may share personal data with service providers hired by Lumina that are related to human resources management, such as: employment agencies specialized in selective processes, benefits management (such as meal and medical assistance), management of the payment of Members, background screening platforms (under the terms of the Compliance Manual), among others.
- Service providers of investment funds under Lumina's management: We may share personal data with the other service providers of investment funds under

Lumina's management, for purposes strictly related to the portfolio management activities of investment funds in which the Holder is (or will become) an investor.

- Request for competent authority: Lumina may still share personal data with third parties (including government agencies) in order to comply with legal or regulatory obligations, as well as to respond to investigations, judicial measures, judicial or arbitral proceedings, or to investigate, prevent or take action regarding illegal activities, suspected fraud or situations involving potential threats to the physical safety of any person or if otherwise required by the Applicable Law.
- New business: If Lumina is involved in a merger, acquisition or sale of all or part of its assets, personal data may be transferred to the person or entity involved in such corporate transaction.

Transfers of personal data outside of Brazil

Lumina may transfer some of the personal data to entities and service providers located abroad, including background check platforms and/or cloud storage service providers.

If the personal data is transferred outside of Brazil, Lumina will take appropriate measures to ensure adequate protection of the personal data in accordance with the requirements of applicable data protection legislation, including signing appropriate contracts for the transfer of personal data with third parties when required.

How long will we retain personal data?

We store and maintain information: (i) for as long as required by applicable law or regulation; (ii) until the end of the processing of personal data, as mentioned below; or (iii) for as long as necessary to preserve Lumina's legitimate interest. Thus, we will process personal data, for example, during the applicable limitation periods or as long as necessary to comply with a legal or regulatory obligation.

The termination of the processing of personal data will occur in the following cases:

- When the purpose for which the personal data of the Holder were collected is achieved and/or the personal data collected are no longer necessary or pertinent to the achievement of such purpose;
- When the Holder is within his/her right to request the termination of the treatment and the deletion of his personal data; or
- When there is a legal determination to that effect.

In these cases of termination of the processing of personal data, except for the hypotheses established by the applicable legislation, by this Privacy Policy or by the Lumina Compliance Manual (the latter, as appropriate and as applicable), personal data will be deleted.

Rights in relation to the personal data we process

Holders have certain rights in relation to personal data as set in the applicable law. Such rights include, but are not limited to:

- Receive clear and complete information about the processing of personal data, including about the hypotheses of sharing personal data;
- Request access to personal data and/or confirmation of the existence of personal data processing;
- Request that we rectify any inaccurate, incomplete and outdated personal data;
- Oppose the processing activities, request the anonymization and deletion of personal data, in specific circumstances;
- Request the portability of your personal data;
- Revoke consent at any time when Lumina processes personal data based on consent (if applicable); and
- Request review of automated decisions that may affect holders interests.

To exercise these rights, send a message to the Compliance Officer via e-mail compliance@luminacm.com.

Changes to this Privacy Policy

Lumina reserves the right to change this Privacy Policy at any time by posting the updated version at the address www.luminacm.com/. In case of material changes to this Privacy Policy, the Owner will receive a notice in this regard at the same address indicated above (as an informative pop-up).

13. Cybersecurity Policy

It is the responsibility of all Lumina Members, service providers, and system providers to protect the security and integrity of Lumina's information and computer equipment in compliance with this Policy.

Cyber threats can vary depending on the nature, vulnerability, information, or assets of involved. Cyber threats can cause damages to Lumina’s operations, image, financial data, and competitive advantage, and such damages may be irreparable.

In addition to malfunctions in its systems and electronic devices, Lumina may also be subject to cyber-attacks. The most common methods of cyber-attacks, according to the best practices on the subject, are as follows:

- *Malware: software designed to corrupt computers and networks;*
- *Virus: software that causes damage to the machine, network, software, and database;*
- *Trojan horse: mechanism that appears inside other software and creates a door for the computer to invade;*
- *Spyware: software to collect and monitor usage of information;*
- *Ransomware: software that locks access to systems and databases, demanding a ransom to restore access;*
- *Social Engineering: a method of manipulation to obtain confidential information such as passwords, personal data, and credit card numbers;*
- *Pharming: mechanism of directing the user to a fraudulent website, without his/her knowledge;*
- *Phishing: links transmitted by emails, pretending to be a trusted person or company that sends official electronic communication to obtain confidential information;*
- *Vishing: pretends to be a trustworthy person or company and, by means of telephone calls, tries to obtain confidential information;*
- *Smishing: pretends to be a trustworthy person or company and, through text messages, tries to obtain confidential information;*
- *Personal access: people located in public places such as bars, cafes and restaurants who capture any kind of information that can later be used for an attack;*
- *DDoS (distributed denial of services) and botnet attacks: attacks aimed at denying or delaying access to the institution's services or systems; in the case of botnets, the attack comes from numerous infected computers used to create and send spam or viruses, or flood a network with messages resulting in denial of service;*
- *Invasions (advanced persistent threats): attacks carried out by sophisticated attackers, using knowledge and tools to detect and exploit specific weaknesses in a technological environment.*

Safe Environment

- Local area network
  - Servers, workstations, networking and digital security equipment located in Lumina's office;
- Virtual Network
  - Virtual servers, virtual workstations, virtual digital file storage devices, located at a public cloud service provider partner;
- Mobile apps
  - Applications for accessing Lumina information that may be installed on Members' personal mobile devices;
- Web applications for information dissemination

    - Authenticated access by username and password should be used to ensure that only Members will have access to this information
- Counterparty servers for information exchange
    - For the exchange of messages, the counterparties' servers will be considered part of the digital security area. Such servers must be cataloged and accessed through a secure channel.

Security Perimeter Boundary

- Corporate email
    - Running on the local network, virtual network, or mobile apps. It is an important information frontier. It will be monitored and if confidential information crosses this border, the Compliance Officer may take the appropriate measures regarding the leakage of confidential data.

- Internet
    - Access to the internet through the local network or the virtual network.
    - Mobile applications within the perimeter will not be able to access the internet.
    - Access should be through a firewall, and access that allows unsupervised flow of confidential information should be blocked. Below is a non-exhaustive list of what will be blocked:
        - Messaging apps and websites, e.g. WhatsApp, Facebook messenger, WeChat, etc.
        - Non-corporate email, e.g. Gmail, Hotmail, etc.
        - Social media: Facebook, Instagram
            - In this case, an exception may be made for the corporate communication team to promote Lumina.
    - Messaging service connections (e.g. automated trade sending). In this modality, a secure way to exchange information should be used, for example:
        - Encrypted VPN Channel
        - SSL connection with TLS 1.2 protocol
- Corporate phone
    - Will be recorded for compliance and audit purposes.
- Access ports on the workstation
    - CD or DVD players, USB ports, Bluetooth, must be disabled.
- Remote Desktop access to virtual workstations that will be in the cloud
    - Each Member will receive a certificate that can be used to connect any personal computer with an internet connection to our virtual workstations.
    - On this border members will not be able to transit anything other than keyboard, mouse, sound and video information. Copying files and text will not be possible.

Lumina disclaims any and all liability arising from the improper, negligent or reckless use of the resources and services granted to its Members, reserving the right to analyze data and

evidence to obtain evidence to be used in the investigative processes, as well as to adopt the appropriate legal measures.

Lumina has several data prevention and information security procedures, including:

(a) all computers and mobile devices used by Members are either owned by Lumina or approved by Lumina's IT;
(b) all systems used by Members have been acquired by Lumina;
(c) personal laptops, tablets, or other hardware are not allowed to perform Lumina's business, except with express permission of the Compliance Officer, who will grant his/her permission only after IT approves and registers the device in Lumina's systems;
(d) all computers used by Members are intended for the performance of professional activities of the Manager;
(e) procedures for the availability and use of computers, including the following rules:
    a. the Compliance Officer shall authorize, upon request, the creation of a new username and the technical resources that will be available to each new Member;
    b. all equipment, software, and access permissions shall be tested, approved, and authorized by IT, under supervision and approval of the Compliance Officer;
    c. the Compliance Officer shall authorize, upon request, the removal or replacement of the computer made available to the user;
    d. each computer has its own user manager, who shall be responsible for that equipment. Control of the machines is the responsibility of IT, under supervision and approval of the Compliance Officer;
    e. user identification is made through login and password, which are created for each Member through the log record used by Lumina and serve as electronic signature on Lumina's server. Members shall not share his/her password with third parties or other Members;
    f. only 3 (three) maximum password authentication attempts are allowed, and if all are unsuccessful, access will be blocked, which can only be reestablished upon request to the Compliance Officer;
    g. all login and password change events are auditable and traceable, and may be requested to Lumina's IT by the Compliance Officer; and
    h. Members access to personal e-mails and social medial through the computers used for the purposes of their professional activities in Lumina is monitored, with control over exported documents.

(f) Members are oriented to not open messages of unknown origin and suspicious links, the latter even if they come from a known source;
(g) procedures for the protection of Confidential Information and Internal

Information, according to the Confidentiality and Information Securities Policy in this Manual;

(h) computers shall use screen savers, and the system is locked after a user absence, requiring a new login with password;

(i) members shall avoid entering websites from unsafe sources whenever they communicate through Lumina's technology assets;

(j) periodic blocking of access to internet addresses that are not in line with this Policy and may pose any risks to the Manager;

(k) use of an individual and untransferable electronic address for each Member, whereas all electronic addresses and their associated messages shall be property of Lumina. Proper use of electronic addresses and messages sent shall be the responsibility of each Member;

(l) he best cybersecurity standards shall be required when contracting cloud systems, such as documents that attest to the cybersecurity procedures and prove the technical capacity of the service provider. The contracting of cloud systems shall be approved by IT and the Compliance Officer;

(m) all software, basic programs (operating system and tools), and physical components shall be deployed and configured by IT, under supervision and approval of the Compliance Officer;

(n) users are not allowed to deploy new programs or change settings without formal permission from IT and the Compliance Officer;

(o) users are not allowed to deploy or change physical components on their computers;

(p) continuous and non-periodic monitoring of the controls provided in this Policy, which shall be carried out by IT under supervision of the Compliance Officer;

(q) annual contingency tests and security tests focusing on logical segregation, penetration tests, response to security incident events involving Personal Data, traceability of Personal Data processing logs, outperformed by an external audit under supervision of the Compliance Officer and IT.

In accordance with best practices, Lumina has developed a response plan for evidence, substantiated suspicion, or security incident events of Confidential Information and/or Internal Information or other security breaches. The response plan consists of:

(a) IT, under supervision of the Compliance Officer, shall, as applicable, among others, (i) check and audit logs; (ii) create an expert report containing the information that potentially leaked; (iii) run applications to eliminate unwanted applications; (iv) uninstall software; (v) run offline scans to discover any additional threats; (vi) format and rebuild the operating system; (vii) replace storage devices; (viii) rebuild network systems; and (ix) restore data from the backup performed daily;

(b) the Compliance Officer shall, as applicable, create a report based on the expert report prepared by IT, verifying eventual damages, suggesting possible

solutions, as well as classifying the severity of the event;

(c) the Risk and Operating Officer shall, as applicable, analyze data and information that may have been lost and its impact on accounting planning and asset value;

(d) if necessary, a specialized company shall be contracted to solve the event and/or respond to possible damages; and

(e) filing of materials and documents related to the event and measures adopted to solve it.

Specifically for security incidents involving unauthorized access or accidental or unlawful situations of destruction, loss, alteration, communication or any form of improper or unlawful processing of Personal Data, Lumina will proceed the following incident response plan:

(a) Any member who has knowledge or suspicion that an incident has occurred should report the situation immediately, in as much detail as possible, to the Data Protection Officer.

(b) In the event of reasonable indications that the security incident did in fact occur, IT shall: (i) collect the initial information it deems appropriate for an initial assessment of the scope and severity of the potential incident, including which systems; networks; equipment and Personal Data have been compromised; (ii) identify the type of vulnerability/attack and the initial extent of any loss (e.g., affected systems; source; misconfiguration; malware used, location where the information was sent); (iii) identify compromised digital information sources (e.g., systems, equipment, and files); (iv) determine whether the event is internal or external and whether any partner company has been affected.

(c) Once the initial assessment has been made, immediate steps should be taken to contain the incident and prevent further compromises and/or new unauthorized access. These measures include: (i) isolating the perimeter, limiting access to systems, equipment, and environments if necessary; (ii) monitor the servers to ensure that the technical failure has been corrected; (iii) preserve evidence whenever possible; and (iv) ensure impartiality in the analyses through the advice of internal and external experts.

(d) As soon as it becomes aware of an incident of medium or high severity, the Data Protection Officer shall act in conjunction with IT in order to: (i) evaluate the incident and preserve evidence of the facts; (ii) define the corrective and other actions they consider relevant to address the incident and its implications, whether legal, regulatory, corporate or public relations; (iii) assess the need for third-party support, such as the hiring of specialized experts, external legal advice, communication agency, etc.; and (iv) assess the need to make a communication to the Fund's investors and/or other affected Personal Data holders.

(e) Throughout the response to the incident, from the initial assessment, one should collect all relevant documents and information in a manner that preserves them

as potential evidence. It should also be done, as appropriate and as applicable::

- Keep record of a) who identified the incident; b) who reported; c) to whom it was reported; d) who else is aware of the incident; e) what type of violation; f) which data and equipment are compromised and other pertinent information.
- Acquire a forensic image through the hard drive of the identified computers and preserve the available chain of custody.
- Collect information and record all accesses that occurred during the exposure period and its related IP;
- Collect all relevant data that may clarify the incident, including a description of the technical information about firewall, proxy, antivirus, active directory and webmail server, for example;
- Describe in detail the technical failure, including the risks, who was responsible for it, how it was used to grant access to the server, and what data was compromised;
- Review and describe all precautionary controls that were available at the time of the incident;
- Create a document recording all the security measures taken after the identification of the flaw, both to contain it and to correct it; and
- Prepare a report presenting all the procedures of collection, identification and analysis implemented. In this report, it is important to list conclusions about the incident.

(f) The Data Protection Officer shall: (i) assess legal obligations, including incident notification requirements for affected authorities and regulatory bodies and Personal Data subjects; (ii) review the contracts of customers, suppliers, service providers and business partners to identify the existence of contractual notification obligations; and (iii)assess the need or feasibility of taking civil or criminal action against third parties related to the incident.

(f) Once the response to the incident has been completed, the Data Protection Officer shall prepare a report indicating: (i) the root cause of the incident; (b) measures taken to respond to the incident; (c) points in the response plan that may not have functioned properly, and measures to be taken for improvement; (d) reaction time between the discovery of the incident and the start of incident management; (e) whether there were notices and communications about the incident and to whom they were sent; and (f) the financial, image, and operational impact of the incident.

Monitoring of the controls established in this Policy will be executed by IT under supervision of the Compliance Officer. Monitoring will be continuous, not at defined intervals.

Lumina must ensure the correct and continuous operation of the control mechanisms

described above.

Furthermore, periodic security tests shall be carried out focusing on logical segregation, penetration tests, response to security incident events involving Personal Data, traceability of access logs to confidential information, among others, always aiming to safeguard the data and information held by the Manager, especially the confidential information. These tests shall be performed at least two times a year by an outsourced IT and their results shall be consolidated in the Manager's annual reports of internal controls. This Policy will be updated, at least, each 24 (twenty-four) months, or when there is any change in the applicable regulation and/or autoregulation that demand updates.

Lumina maintains inventories of hardware and software, checking them frequently to identify elements foreign to the institution. The IT Area must strive to keep operating systems and application software up to date.

The IT area is also responsible for monitoring backup routines on a daily basis, performing regular data restoration tests.

14. Business Continuity Plan

To continue its business operations following the occurrence of a disaster, Lumina has implemented the following procedures in its Business Continuity Plan.

Lumina's Business Continuity Plan anticipates two kinds of Significant Business Disruptions: those that are internal and those that are external. Internal Significant Business Disruptions affect Lumina's ability to communicate and do business, such as a fire in the building, cybernetic attacks or unavailability of essential systems to Lumina regularly performs its activity. External Significant Business Disruptions interrupt the operation of the securities markets or of a significant number of financial services firms, such as a terrorist attack, a city flood, or a wide-scale, regional disruption.

The Compliance Officer, the Portfolio Management Officer, and an IT representative shall be responsible for approving and conducting an annual review of the Business Continuity Plan.

Lumina has implemented an encrypted cloud-based backup and storage solution, which is scheduled to run daily, at night. All data in the cloud backup is password-protected and encrypted.

Technical support is provided by the company Tecnoqualify, through the e-mail clayton@tecnoqualify.com.br.

Copies of Lumina's transactional documents are saved in the cloud, as well as at the offices of external counsels who worked on Lumina's transactions.

In the event of a Significant Business Disruption, Lumina shall immediately identify what means will permit communication with Members, critical businesses, critical counterparties, and regulators. Depending on the effects of a Significant Business Disruption, Lumina shall follow the communication options described below.

All investment professionals shall have a laptop or home desktop and mobile devices approved by IT in order to access the network remotely from their homes or other locations. These connections are used regularly by Members and shall be also available in the event of a Significant Business Disruption. Lumina has redundant routes to the internet. In addition, its telephone links are also redundant.

Contingency tests will be performed annually in order to prepare the Manager for the continuation of its activities in case of any disruptions.

These tests will include:

a) no-break testing, checking operating status and support time of charged batteries;
b) remote access to systems and emails from laptops and/or other contingency computers;
c) access to stored data; and
d) other tests necessary for business continuity.

The test results shall be recorded in a document named Contingency Test and will be part of the Manager's Annual Report of Internal Controls, according to RCVM 21/21.

Should Lumina's principal place of business become inaccessible, Lumina has implemented the following communication procedures for its Members, clients, and others..

a) Clients: the Portfolio Management Officer shall be responsible for contacting Lumina's clients to update them on the current state of operations when necessary;
b) Members: the Compliance Officer and/or the Portfolio Management Officer shall be responsible for contacting the other Members to update them on the current state of operations;
c) Funds and other service providers: the Operating Officer shall be responsible for contacting the other Members to update them on the current state of operations.

15. Remote Work Policy

This policy aims to mitigate potential failures in information security due to the activities developed in remote work model, providing additional rules of information security and access to the manager’s systems in this work model.

All Lumina members are eligible for remote work and must request approval from their immediate head of department, who will have the autonomy to evaluate the request. Remote work must also follow all other rules set forth in this manual.

Lumina provides notebooks for all its Members, but the rest of the infrastructure necessary for remote work (for example, the existence of internet service) is under the responsibility of the member. The devices used by members are under supervision of the manager, who takes steps to ensure that they are safe and reliable. The manager does not authorize the use of public or third parties’ devices to access the manager's network.

Access to the manager's network occurs through an encrypted virtual private network (VPN), enabling access to systems and maintaining security in information traffic. The manager provides official communication tools through Microsoft Outlook (for external communications) and Microsoft Teams (for phone calls, virtual meetings and message exchange) and Microsoft One Drive (for file exchange).

To perform remote work, the member must ensure that there are minimum requirements in the place where they are working remotely to stay connected in a stable way. In addition, it is necessary to be in an environment where they can conduct video conferences in a presentable way and in a place where they can speak without external interference.

The member must also check the security of the network to which they are connecting. It’s also important to check if it is impossible for others to view sensitive information on their computer screen or listen to confidential conversations before they start the access.

If the member shares the residence with other people who work in activities related to the one of the manager, should be verified the possibility of segregating the work environments so that confidential information is not shared.

All members have a personal and non-transferable user account, with the respective authorized accesses in Lumina's systems, which must be kept safe and hidden when performing the access.

Violations of the recommendations in this policy may be punished, including taking disciplinary action if necessary.

16. Segregation Policy

Lumina neither acts in activities other than the administration of third-party assets, in the its role of "portfolio manager", nor does it distributes the shares of the Funds. Notwithstanding, Lumina deals with conflicts of interest and ensures institutional and hierarchical segregation of its activities by adopting measures such as, but not limited to:

(a) implementation of access controls to folders and virtual directories according to the area and function of each Member and restriction of access to certain information;
(b) discussion of matters that could potentially generate conflicts of interest only in appropriate places;
(c) non-reporting of the Compliance Officer to the portfolio management area;
(d) prohibition of accumulation of functions with any area that may cause a conflict of interest for Members responsible for the portfolio management area;
(e) rules for preserving and maintaining the secrecy of Confidential Information and/or restriction to disclose Internal Information;
(f) implementation and maintenance of a training program for Members;
(g) implementation of controls that allow the identification of people who have access to files and Confidential Information, Internal Information and the Personal Data processed by Lumina;
(h) information to investors about other companies that will compose Lumina's economic group;
(i) periodic security tests for information systems; and
(j) creation of a Personal Investment Policy for Members.

Access control to Lumina's information systems consists, among others, of: (i) creation of individual usernames and passwords for all Members to access network data; and (ii) implementation and control of minimum requirements for creating passwords.

Lumina also segregates its activities physically. Meetings with third parties at Lumina's site shall occur exclusively in the meeting rooms.

In the event that Lumina decides to share its facilities with other institutions, the following measures shall be adopted: (i) physical segregation; (ii) functional segregation; (iii) informational segregation; and (iv) technological and systemic segregation

17. Personal Investment Policy

This Policy seeks to enable all Members to invest their resources safety, while avoiding any inappropriate use of Confidential Information and/or Internal Information, speculation and, primarily, that their personal interests are not put ahead of those of Lumina and its investors.

Before starting their activities at Lumina, all Members shall provide the Compliance Officer with information related to their investments and shareholdings in Brazil and abroad.

Pursuant to the General Part of RCVM 175/22, and in line with Lumina's Compliance Manual, the use of relevant information not yet disclosed, by any person who has had access to it, for the purpose of obtaining an advantage, for themselves or for others, through the trading of quotas in organized markets, is prohibited.

In order to establish the crime of trading quotas of the fund through the use **MNPI** (Material Non-Public Information), the following presumptions are observed in relation to Lumina, in its capacity as fund manager

I. the person who negotiated quotas of the fund with MNPI made use of such information in said negotiation;
II. Lumina Members who participate in decisions related to the management of the asset portfolio of funds under management have access to all MNPI about the fund;
III. if applicable, the quotaholders who participate in the decisions related to the management of the fund's asset portfolio have access to all MNPI regarding the fund of which they are quotaholders;
IV. the persons listed in items II and III above, as well as those who have a commercial, professional or trust relationship with Lumina, upon having had access to MNPI know that it is privileged information; and
V. if the Manager, as an Essential Service Provider, withdraws or is removed from the fund with MNPI, it uses such information in the negotiation of quotas within a period of three (3) months from its withdrawal.

The presumptions described above (a) are relative and must be analyzed together with other elements that indicate whether or not the unlawful trading through the use of MNPI was in fact practiced; and (b) may, where appropriate, be used in combination

The prohibition on trading of the fund's quotas does not apply to subscriptions of new quotas, without prejudice to the incidence of the rules that provide for the disclosure of information in the context of the issuance and distribution of quotas, notably CVM Resolution No. 160, of July 13, 2022.

Without prejudice to the foregoing, Lumina's Directors, as defined in Lumina's

Operating Agreement, and their Members may formalize an individual investment and divestment plan, in order to remove the applicability of the presumptions provided for in the regulations ("Investment and Divestment Plan"), which must:

I. be formalized in writing;
II. be subject to verification, including with regard to its formalization and the making of any change in its content;
III. establish, irrevocably and irreversibly, the dates or events and the amounts or quantities of the trades to be carried out by the participants, and may even use consistent and verifiable methodologies to determine such values or quantities of trades; and
IV. provide for a minimum period of three (3) months for the Investment and Divestment Plan itself, its eventual modifications and its cancellation to take effect.

Members declare that they are aware of and agree to send or have their brokers send directly to the Compliance Officer annually (i) when possible, brokerage notes and statements, and (ii) a report stating personal investments in stocks and other securities equivalent to shares held in Brazil or abroad, with the exception of those assets exempt from approval by the Compliance Officer (under the terms set forth below), in order to verify compliance with the premises established in this Policy. The Compliance Officer will be responsible for storing these documents, ensuring their confidentiality.

For the acquisition or any trading of debt securities, quotas in the Brazilian or foreign securities market (in equivalent securities), or quotas of investment funds located in Brazil or abroad (in equivalent securities), the Member must request authorization from the Compliance Officer, except for the assets listed below that are waived.

The Compliance Officer, after consulting the Portfolio Management Director, will authorize or not the requested trading, as the case may be, and will advise the Member on any specific periods of restriction or prohibition on the trading of the securities in question that are known to him. The authorization granted will be valid for up to 2 (two) business days from the date of approval, and will be automatically considered invalid after this period or if the asset is included in Lumina's restriction list.

The maintenance of investment portfolios managed at the discretion of independent third parties, called exempt accounts, will be allowed, at the discretion of the Compliance Officer provided that there is no influence, guidance or prior knowledge of the Member on the investment orders executed. In such cases, direct communication between the Compliance Officer and the manager or advisor responsible for the portfolio may be authorized, in order to ensure full compliance with this Policy, especially with regard to the mitigation of conflicts of interest.

Only the assets listed below are exempt from prior authorization from the Compliance Officer:

- Treasury securities;
- Investments in fixed income securities issued by S1 financial institutions;
- Investments in Pension plans "VGBL" or "PGBL";
- Investments in open-ended fixed income investment funds managed by S1 financial institutions;
- Savings investments;
- ETFs

Except if otherwise approved by the Compliance Officer, all Members shall hold investments in debt securities and stock exchanges within the securities market of Brazil or any foreign country (or other equivalent securities), as well with share of investment funds in Brazil or any foreign country (or other equivalent securities) for a minimum period of thirty (30) consecutive days counting from the date of each acquisition (holding period), within which the Member shall not perform any transaction related thereto.

In addition to the rules set out above, all Members shall comply with specific procedures that serve as examples in order to protect Lumina and its Members from the assumption of impropriety in their transactions:

(a) adherence to the Confidentiality and Security of Information Policy set forth in this Manual;
(b) adherence to the Firm's Restricted List (see Lumina's Insider Trading Policy);
(c) notification to the Compliance Officer of receipt of materials with potential Confidential Information and/or Internal Information;
(d) notification to and authorization from the Compliance Officer for any role as advisor or member of any creditors' committee or a similar capacity with respect to any for-profit company or other outside entity, and the Compliance Officer shall take action with respect to access to and sharing of Confidential Information and/or Internal Information;
(e) attendance at periodic compliance trainings set forth herein.

Whenever a situation of actual or potential conflict of interest exists, Members will not be allowed to enter into a transaction or will be required to sell their personal investments. In this case, they shall immediately send a written notification to the Compliance Officer.

Lumina shall not actively manage its own assets. Lumina's cash resources shall be allocated exclusively for the payment of expenses and distribution of profits to its

partners, and will be invested exclusively in government securities, third-party Interbank Deposit (***Depósito Interbancário – DI***) funds with immediate liquidity and first-tier Certificates of Bank Deposit (***Certificados de Depósito Bancário – CDBs***).

18. Principal Transactions

A principal transaction occurs when a trader, acting for its own account (or the account of an affiliated entity) buys a security from, or sells a security to, a related account. For instance, a principal transaction would arise if:

- A trade occurs between an investor and a proprietary account of Lumina (this example includes transactions between an investor and accounts pertaining to the family office of any Member).
- A trade occurs between two or more of the Funds depending on the percentage of ownership, directly or indirectly, held by the Firm and its personnel in the Funds at the time of the transaction.

Section 206(3) of the Advisers Act places restrictions to the principal transactions. The primary purpose for this restriction is to prevent a trader from transferring unwanted securities from its own accounts or those of its affiliates or from transferring very desirable securities to its own accounts or those of an affiliate.

Section 206(3) requires that prior to the settlement of any principal transaction, the trader must provide written disclosure and obtain consent, consistent with the applicable language in the Fund's governing documents. The written disclosure must state that the trader would be acting as a principal in the transaction and must describe the material terms of the transaction, which generally include (i) the original purchase price for any security; (ii) the price the trader expects to receive on the resale of any security; and (iii) the price at which a security could be bought or sold elsewhere. In addition, a trader must determine whether the proposed principal transaction is in the best interests of all.

The application of Section 206(3) can be challenging when applied to the Funds. Some of the potential challenges include (i) determining whether a Fund should be viewed as a principal account of the Firm and (ii) determining who on behalf of the Fund can receive the written disclosure and provide the necessary consent. Accordingly, the Portfolio Management Officer must identify any potential principal transaction, including any cross trade between two or more of the Funds, prior to effecting the transaction and must contact the Compliance Officer. The Compliance Officer, in consultation with outside counsel as appropriate, will determine whether the trade would constitute a principal transaction, and if so, determine how to ensure that all required notice and consent requirements are satisfied. The Compliance Officer will

then inform the Portfolio Management Officer whether and when to proceed with the trade.

19. Risk Management Policy

A. Procedures Related to Risk Identification

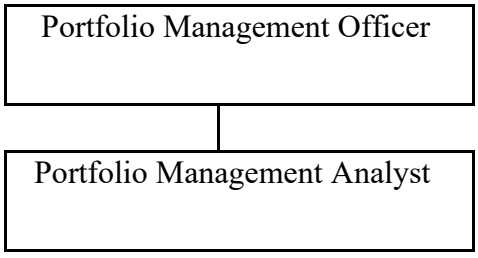
A Lumina defines risk as the potential for permanent loss of invested capital. The goal of risk management is to obtain control and knowledge about the risks inherent to the asset management activity, aiming to adapt the strategies to the objectives of the investment funds and seeking to mitigate or reduce potential negative results.

Lumina's risk management team adopts industry-established metrics to monitor exposure to the risks inherent to its activities, including market, concentration, credit and counterparty, operational, and liquidity risks.

Lumina monitors continuously (at least, every 12 (twelve) months), the effectiveness of these metrics through adherence tests led by the Risk Management Officer. The revision of the stablished methodologies shall occur, at least, every 24 (twenty-four) months, or more frequently in case the adherence tests evidence inconsistencies that demand revision.

B. Risk Management Governance

Initially, a Lumina analyst evaluates the risk of a specific position under supervision of the Risk Management Officer. The Risk Management Officer will then perform his/her analysis before and after the transaction, according to the organizational chart below:



The Risk Management Officer prepares monthly reports on risk exposure for the portfolio under management, which shall be sent to the Portfolio Management Officer. The limits of risk exposure, as well as the requirements for issuing the reports, shall be determined and agreed upon with Lumina, which will have permanent access to all such

data and reports through an integrated electronic system. In addition to the monthly review of reports, unusual activities or special circumstances may also prompt a review on a case-by-case basis.
These and other reports used to assess portfolio risks shall be generated and/or reviewed by the Risk Management Officer as applicable.
The Risk Management Officer shall meet with the Compliance Officer and the Portfolio Management Officer every two months or whenever necessary to review the investment exposure to risks.
Lumina also maintains an in-house technical department with a team of specialized analysts with academic and professional experience and qualifications for the analysis of securities, who provide technical support for Lumina's investment decisions. The technical department also has the necessary infrastructure, suitable for its size and area of operation, having access to a wide database and information, including access to research reports from main investment banks.

The Risk Management Director has the power to order the readjustment or reframing of the investment portfolio of the Funds, without prejudice to consulting the Portfolio Management Director in order to better understand any specific investment strategy adopted. In this sense, in the event of non-compliance with the Fund, in accordance with the diversification rules contained in its bylaw, the Risk Management Director must inform the Portfolio Management Director in this Regard.

Lumina shall inform any non-compliance, by the Class, regarding portfolio composition, to the administrator so that it may report it to the CVM, observing the deadlines and details below:

a) **Active Non-Compliance:** Lumina shall immediately inform the administrator of the identification of an active Non-Compliance event, and the administrator shall inform the CVM if the portfolio of assets remains unbalanced for ten (10) consecutive business days, until the end of the business day following the end of the term, as well as inform its rebalance as soon as verified. If the non-compliance persists for the period above, Lumina shall submit to the CVM an action plan for the rebalance of the Class portfolio, within the same period of ten (10) consecutive business days, separately or jointly with the administrator's file.

b) **In case of Passive Non-Compliance:** If the passive Non-Compliance is prolonged for fifteen (15) consecutive business days, at the end of this period, Lumina must submit to the CVM its explanations for the Non-Compliance.

c) **Portfolio Rebalance:** Lumina must immediately inform the manager of the portfolio rebalance so that it can inform the CVM as soon as it occurs.

It is the administrator who will send such communications, as the agent operationally responsible for sending them to the CVM, even if they have been prepared or provided by Lumina, as the participant responsible for the production and preparation of the document in question.

C. Market Risk

Market risk is the risk of change in the value of the financial assets that compose an investment fund.

The value of financial assets may increase or decrease according to price fluctuations, market quotations, interest rates, and profit or loss of the issuing companies. When the value of the financial assets that compose an investment fund drops, the net worth of this investment fund can be negatively affected.

Lumina seeks to manage risks mainly through the use of a rigorous and integral analysis of each investment, incorporating unfavorable scenarios designed to take several exogenous variables into account, such as a slowing economy, sudden change in interest rates, or large movements in currencies. While Lumina acknowledges and makes use of risk management analysis, we believe that profitable investment decisions – including risk management – are based on solid judgement that can be developed over time and through varied experiences.

Lumina develops its own tools to control market risks. The main quantitative methods used to monitor risks include:

(a) *Value at Risk (VaR):* the concept of VaR allows the market risk to be represented by a single monetary value, indicating the maximum expected loss with a certain level of confidence for a given investment horizon. The statistical VaR (99%, 1 day) of the linear exposure of the Funds is calculated assuming a normal distribution of returns. Every instrument is mapped as a function of the risk factors and an idiosyncratic contribution. The risk contribution is then determined by the sum (statistically, assuming zero correlation) between the risk factor and the idiosyncratic risk of each Fund. The mapping of risk factors shall be reviewed when deemed appropriate by the Risk Management Officer; and the risk factors themselves will also be reviewed when appropriate.

(b) Stress test: it consists of simulating the worst return on the Fund's portfolio, according to its historical behavior, for a predefined time horizon. The stress test is an important tool to complement the risk management process, especially in situations of large market oscillations in which the usual volatility does not properly reflect the risk incurred. The stress test can be implemented by using historical, probabilistic, or hypothetical scenarios, as defined by the Risk

Management Officer.

Also, Lumina takes into account quantitative and market analyses of each investment, considering the impact of macroeconomic components and the specific risks contained in the different industry sectors.

.
The practice of hedging can be considered according to the business, strategy, and portfolio. At its discretion, Lumina may hedge its exposures, including to currencies, positions, and markets. Lumina's portfolios will always be exposed to certain risks that are not subject to or susceptible to hedging. Although market oscillations are a concern for Lumina, we do not specifically aim to control daily volatility, as we believe that a sound analysis should be able to offer a certain degree of protection against unfavorable situations.
Lumina actively seeks to measure hedge relations, beta exposures relative to global indexes, as well as derivative sensitivities. Risk management measurements may vary depending on the nature of different investment strategies.

D. Concentration Risk

Concentration risk is the risk incurred when a portfolio of investment funds is concentrated in securities issued by the same issuer, which makes the risks of these investments directly related to the performance of such issuer and its economic sector. Changes in the financial condition of a company or group of companies, in the expected performance/results of the companies, or in the competitive capacity of the invested sectors may, individually or cumulatively, adversely affect the price and/or yield of the financial assets in the portfolio.

Under the terms of this Policy, the Risk Management Officer shall be responsible for acting in a preventive and constant manner to alert and take action in case any adjustments to any assets or group of assets are necessary in accordance with the rules applicable to each Fund. .

E. Credit and Counterparty Risk

The credit/counterparty risk arises from issues in the settlement of transactions carried out through broker-dealers and distributors, as well as changes in the financial conditions of the issuers and/or counterparties, or in their perception by the market, which may compromise their ability to pay, thus impacting price and liquidity, among other factors.

Notwithstanding the possibility of making investments in companies undergoing

reorganization, distressed assets, and other such investments, for which one or more steps may not apply, as the case may be, the credit analysis shall take place in four steps, as described below:

(c) credit fundamentals: Lumina shall analyze the economic and financial situation of the company through its financial statements, taking into account, among others, its current economic and financial situation and projections, indebtedness, working capital, liquidity, fixed asset to equity capital ratio, financial capacity of the controller, asset quality, ability to generate results, cash flow, management and quality of controls, timeliness and delays in payments, contingencies, economic sector, and credit limit;
(d) operating risk level: Lumina shall analyze, among others, the nature and purpose of the transaction, guarantees offered, value and term;
(e) qualitative analysis: Lumina shall analyze, among others, the ability of the company and its management to compete in the market, its operational efficiency, market share, compliance with legal and contractual obligations, reputation, ethics, and professional stance;
(f) simulation of scenarios: Lumina shall perform stress analyses in an attempt to foresee scenarios that may impact the credit profile of the transaction.

Credit risk allocation is monitored and managed daily by Lumina. Lumina shall periodically review the quality of the guarantees and the fulfillment of the conditions in case of an eventual execution while the asset remains in the Fund's portfolio.

Also, in order to minimize risks when contracting counterparties, Lumina adopts a Third-Party Selection, Contracting and Monitoring Policy and performs internal due diligence on counterparties.

F. Operational Risk

Operational risk is the risk of losses arising from inappropriate processes or internal failures caused by system or human errors.

In order to avoid system errors, the operational controls implemented by the Manager shall include: (i) control of operations; (ii) comparative calculations of shares of investment funds under management; (iii) monitoring the value of the assets and liabilities that compose the portfolios; (iv) settlement of operations and their control; (v) training for Members to help them avoid failures and risks arising from lack of knowledge of internal rules and legislations; (vi) updated IT programs, including a Cyber Security Policy; among other activities and controls that may be adopted specifically to control and measure operational risks.

Lumina has implemented a Business Continuity Plan establishing procedures to prevent

operational discontinuity caused by technical problems in case of any contingencies.

G. Liquidity Risk

Liquidity risk consists in the possibility of the investment funds not having sufficient financial resources on a given date to honor their obligations, or the financial assets in the investment funds suffer a decrease in tradability due to market conditions.

The Risk Management Officer shall be responsible for managing liquidity risks. The liquidity of assets in the funds is managed daily, based on position sizes, sector exposure limits, and certain risk groups. The Funds, as applicable, shall operate with a minimum daily cash position or extremely liquid assets. These percentages shall be defined by the Risk Management Officer, after consulting the Portfolio Management Officer and the Compliance Officer.

Lumina does not manage any funds structured as open-ended investment fund. Therefore, the provisions relating to the measurement and monitoring of liquidity risk in open classes described below do not apply currently. However, if Lumina were to establish and manage open-ended funds in the future, these guidelines would be adopted as part of internal risk management procedures.

For funds registered as open-ended funds, liquidity risk is measured in each new investment decision and monitored periodically. The fund's liquidity analysis considers the potential volume of redemptions and obligations of the fund against the concentration and liquidity of the invested positions. We also consider redemption settlement periods and the investor profile. .

The management of the fund is done in such a way as to maintain a minimum availability of cash resources or extremely liquid assets, such as government bonds, intraday transaction backed by government bonds or shares of investment funds that invest in these assets.

In the event of market closure or in exceptional cases of illiquidity of the financial assets that make up the Class portfolio, including as a result of redemption requests incompatible with the existing liquidity, which may imply a change in the tax treatment of the Class or of all quotaholders, to the detriment of the latter, or insecurity in the correct pricing of the assets in the portfolio, Lumina, alone or jointly with the administrator, as established in the bylaw and in the agreements entered into between the parties, may declare the closing of the Class for redemptions, subject to all regulatory provisions applicable to such measure.

Any suspension of redemptions must be promptly reported to the CVM by Lumina, through the fund administrator, and shall be the subject of an immediate material fact

disclosure, both at the time of suspension and upon the reopening of the Class. Such material fact disclosure shall also be made available on Lumina's website.

In the event of the closing of a Class, Lumina shall take the necessary steps to define the action plan for managing the liquidity of the portfolio, which shall be prepared jointly by the Portfolio Management Officer and the Risk Management Officer. Lumina may use, including, but not limited to, the liquidity management mechanisms detailed below to formulate the plan for re-compliance of the liquidity management parameters.

Liquidity risk may be increased in special situations of illiquidity, related to systemic factors or events specific to each asset. In these situations, Lumina may define a specific process for each event or asset and may also maintain a greater share of the quotaholders' equity of each Class in assets with greater liquidity. In all cases, Lumina will control and manage the liquidity of each asset at an appropriate interval to avoid non-compliance with redemption rules and other obligations of the Classes.

As a result of the suspension of redemptions of the Classes, and as an alternative to convening a quotaholders' meeting to deliberate on matters expressly provided for in regulation, the Manager may also proceed with the implementation of a Side Pocket.

The Side Pocket is an emergency measure that allows Lumina to separate certain assets that have exceptionally low liquidity or in special or critical situations ("Stressed Assets") from the rest of the healthy portfolio of the Class, until the situation of stress or illiquidity is resolved.

Thus, Side Pocket can be used by Lumina in extreme and unpredictable situations related, for example, to the lack of liquidity of the Classes and derived from uncertainties related to the pricing of assets, without prejudice to the other liquidity controls adopted by Lumina in the course of its management activities. Notwithstanding this, Side Pocket cannot be activated exclusively in the event that there are excessive redemption requests.

According to the evaluation of the liquidity of the Class's portfolio, and provided that there is a provision in its regulatory documents, as an alternative to the call for the meeting to deal with cases arising from the closure of the Class for redemptions, Lumina may split from the equity of a given Class the exceptionally illiquid assets, for use in the payment of quotas of a new closed class or closed subclass

If it chooses to use Side Pocket, Lumina must inform (i) the administrator so that it can take the necessary measures to constitute a new class, together with Lumina; (ii) the Class quotaholders who will be impacted by the formation of the Side Pocket.

Prior to the creation of the Side Pocket, Lumina must ensure that the assets that will be

the subject of the spin-off will be transferred at fair value, according to the manuals and criteria adopted by the administrator.

In addition to the Stressed Assets, the establishment of the Side Pocket must also consider the spin-off of a net portion of the portfolio intended for the payment of expenses and maintenance charges of the spun-off class or subclass. Lumina must establish, according to the specific case and the expectation of treatment of the assets subject to the Side Pocket, the criterion used to calculate the net portion spun off and inform the administrator so that it can disclose a relevant fact on the subject.

If Lumina chooses to create the Side Pocket, it may request that the administrator cancels any redemption requests that have already been requested and not converted, provided that the Class annex or Subclass appendix, as the case may be, sets forth the procedures that must be adopted in this scenario.

Lumina must prepare the detailed description of the event that caused the spin-off, as well as identify the assets involved at the time of its creation, which must be included in the annex of the spun-off Class.

The spun-off Class must maintain its original name, adding to it the suffix "Special Purpose Vehicle" and the name of the event that generated the spin-off, as well as will not be subject to the limits provided for in the regulation, for example, those related to the minimum net equity that must be maintained by the Classes and classification by type of assets and issuer.

The collection of a performance fee within the scope of the Side Pocket will only be allowed if the original Class or Subclass has such a provision, noting that the establishment of a performance fee must consider the loss resulting from the Stressed Assets, in order not to burden the quotaholders.

After the creation of the Side Pocket, Lumina should make efforts to promote the disposal of Stressed Assets in a primary or secondary market.

Alternatively, Lumina may also propose the delivery of such Stressed Assets to the quotaholders of the Class (i.e., redemption in kind), subject to the conditions applicable to each Class.

The gross portion of Stressed Assets may be reincorporated into the original Class provided that the following conditions are met:

(i) that the same quotaholders and proportion of quotas as when the spin-off that originated the Side Pocket was carried out remain in the original Class or subclass;

(ii) that the asset returns to liquidity and mark-to-market; and
(iii)that a special meeting of quotaholders be held in the original class or subclass approving the reinstatement.

Notwithstanding that the reintegration of the Side Pocket is permitted, Lumina will also endeavor to ensure that, as the Illiquid Class receives any proceeds arising from the liquidation of the Distressed Assets, such proceeds are returned to the unitholders.

The use of the Side Pocket is a prerogative of the Manager, and such decision must be made in a collegiate manner, by the Portfolio Management Director and the Compliance Officer and must consider: (i) that the use of the Side Pocket does not result in an increase in the charges assigned to the Class; and (ii) the best interest of the quotaholders, including with regard to the political and economic rights of the quotaholders of the Class.

The records of such decision, as well as the evidence of compliance with the regulatory and self-regulatory requirements for the establishment of the Side Pocket must be filed at Lumina's headquarters.

In addition, the applicable regulation allows Lumina to use redemption gates ("Gates") as one of the available tools for optimizing Class liquidity. Gates partially limit investors' ability to redeem their units in a given Class, in accordance with the conditions set forth in the Appendix of such Class – operating differently from a full redemption suspension, which entirely, indiscriminately, and temporarily prevents Class unitholders from making redemptions.

Through the Gates, Lumina, in its sole discretion and in accordance with the conditions described in the Class annexes, in this policy, as well as established by the Risk Management Director, may limit the execution of redemption requests to a fraction of the Class's stockholders' equity, canceling or postponing the remainder of the requests.

When establishing the Gates, the Manager must consider the following principles:

a. Promote a level playing field for investors who have requested redemption and for other investors;
b. Not creating incentives for investors to submit redemption requests early or in larger amounts (i.e., avoiding a redemption rush); and
c. Promote and preserve the stability of each Class's portfolio.

The following liquidity parameters authorize the Manager to adopt the Gates:

a. in Classes intended for the general public: the request for redemptions that represent, at least, a specific percentage of the Class's net equity, provided that it is proportionally applied to all Class quotaholders. In addition, Lumina may also

consider for the establishment of the Gate whether the quarterly liquidity of the assets presents a decrease below a certain percentage of the quotaholders' equity of the Class established by Lumina for the activation of the Gate. In the Classes intended for investors in general, the criterion used for the reduction of redemption requests will be adopted in the same proportion for all investors or must observe the chronological order of redemption requests up to the limit established for triggering the Gate.

b. In the other Classes, regardless of the target audience: the implementation of the Gates may, at Lumina's discretion, observe the parameters adopted for the Classes intended for the general public, as well as the Class annex or Appendix of the Subclass may freely provide for the method to be adopted, so that Lumina may establish differentiated parameters based on the representativeness of redemption requests from certain investors or on the liquidity of certain assets contained in the Class card.

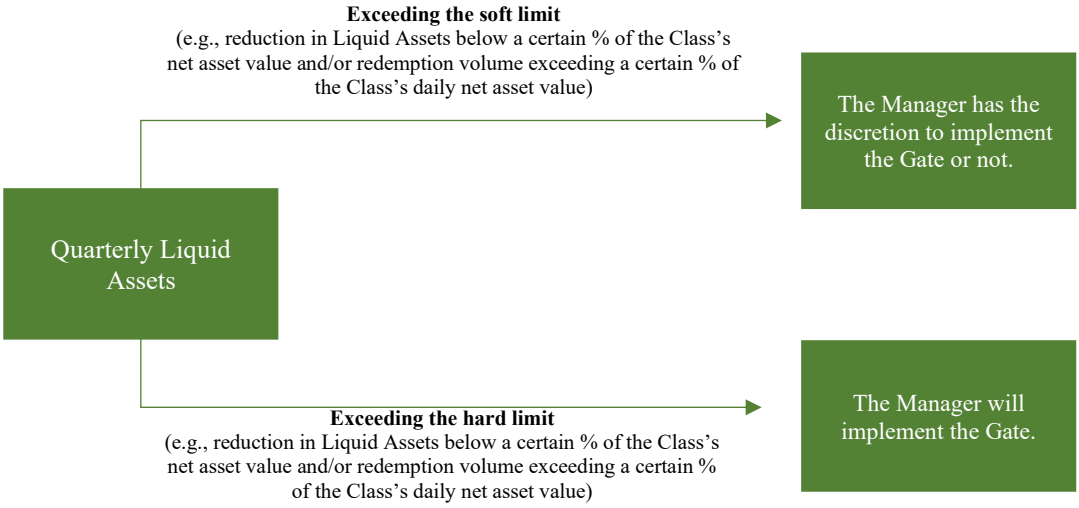
c. Master – Feeder Structures: At Lumina's discretion, provided that the target audience of the Classes and Subclasses is observed, Gates may be established at the Master Class level that will be reflected for the subclasses or for the other investing Classes (as the case may be), except in the case where the investments are made directly by the Classes in the final assets, in which case the Class documents must establish the Gates applicable to such structures.

At the time of the constitution of each Class or Subclass, Lumina may establish the percentage limit that will trigger the Gate, which must be provided for in the Class Annex.

Lumina shall periodically monitor the liquidity of the portfolio and its compatibility with the volume of redemption requests, as well as internally evaluate the establishment of the Gates and, in the event of exceeding the liquidity soft limits, the Risk and the Portfolio Management Director shall meet to evaluate the implementation of the Gates.

The annexes and appendices, as appropriate, shall also set forth the treatment that will be given to redemptions that exceed the limits of the applicable redemption barriers, which may be cancelled or postponed, as the case may be.

In addition, the imposition of the Gates will become mandatory in the event of exceeding the hard limits established by Lumina, and it will also be a collegiate decision-making process that will observe the following procedure:



The Gates may be activated by the Manager (a) on the date of receipt of redemption requests that exceed the limits established for each Class or Subclass, as the case may be; or (b) until the date of payment of such orders, as expressly provided for in the Class or Subclass documents, as the case may be.

Subject to the specific provisions provided for each Class or Subclass, the Gates will be terminated after the reestablishment of liquidity limits, at the discretion of the Manager and observing the operationalization procedures and the decision-making process described below.

The conditions of use of the Gates shall be established at the time of incorporation of the Class, after the Manager's initial assessment of the potential liquidity risk of said Class.

The decision to use the Gates provided for in the regulatory documents, as well as to close the Gates, will be made jointly by the Portfolio Management Director and the Risk Management Director, jointly, and the records of such decision and the reasons that led to the use of the Gate must be filed at the Manager's headquarters.

Immediately after making the decision regarding the imposition and removal of the Gates, Lumina must inform the administrator, so that he can immediately disclose a relevant fact to the Quotaholders.

20. Asset Selection and Allocation Policy.

Lumina shall allocate assets in compliance with each Fund's regulations and investment policies, while also observing its availability of cash in the Funds. Lumina shall be responsible for managing a portfolio of multiple funds.

In addition, in accordance with the regulations applicable to the Funds, Lumina is

responsible for the investment and divestment decisions of the Classes, for monitoring the funds invested, as well as for complying with the limits of portfolio composition and concentration and concentration in risk factors, as established in the regulations, self-regulation and in the respective regulatory documents of the Classes. Detailed information on how portfolios risk management and portfolio composition compliance are managed can be found in the Manager's Risk Management Policy.

The investment management and analysis team, supervised by the Portfolio Management Officer and assisted by the Risk Management Officer, shall adopt the following procedures for the selection and allocation of assets for the Funds:

(a) Research: the investment management and analysis team carries out a series of studies on the investment and develops projection models to predict the asset value considering different scenarios.

(b) Approval from the Portfolio Management Officer: the studies carried out in the previous step are sent to the Portfolio Management Officer, who will then define the investment thesis and strategies to be implemented.

(c) Implementation: once the investment thesis and strategies are defined by the Portfolio Management Officer, the size of the investment will be calculated. The Portfolio Management Officer, assisted by the Legal Officer, will also decide on the legal and financial instruments that will be used to achieve the expected scenario. Simultaneously, adherence of each selected asset to the Fund's regulations and investment policies shall be verified, as well as its adequacy to the portfolio, while also observing applicable risk and liquidity rules.

(d) Monitoring: Lumina updates the portfolio of each Fund under management by registering transactions and monitoring cash inflows and outflows. Lumina also updates the prices of all assets in the portfolio; and

(e) Performance analysis (by fund and consolidated): Lumina measures the performance of the total portfolio as well as of each asset in the portfolio, analyzes their risk exposure, and generates expense and cost reports.

Adherence, risk, and liquidity controls, as well as monitoring are carried out in conjunction with the manager of each Fund.

The same procedure shall be applied to private credit investments. In such cases, private credit acquisition procedures shall be considered according to the paragraphs below.

As a basic principle, the Manager manages its investment funds with the highest standards of diligence, while observing the risks to which investors are exposed and in

accordance with the rules governing the allocation of resources to this type of assets (private credit) issued by competent bodies.

The following procedures shall be adopted prior to making an investment – pre-trade: (i) the management area will search for opportunities available in the market; (ii) definition of limits and owners, considering the characteristics of the assets and their issuers; (iii) indication of investment opportunities and their allocation limits as defined in the Fund's regulations; (iv) in case of operations involving companies of the same economic conglomerate or group as the Manager and/or the trustee, observe the same criteria adopted in operations with third parties, keeping documentation to prove that the operations were carried out on an equitable basis and free of conflicts of interest; (v) evaluate the ability to pay of the debtor and/or its controlling companies, as well as the quality of the guarantees involved, if any; and (vi) analyze the need to contract third parties to assist in the evaluation or monitoring of the private credit, in which case a thorough analysis and selection shall be made of the contracted parties, pursuant to the Third-Party Selection, Contracting and Monitoring Policy.

The following procedures shall be adopted after the investment – post trade: (i) monitor compliance with the obligations assumed in each investment (guarantees, information disclosure etc.); (ii) report to the compliance area any extraordinary and relevant events relative to the asset, its issuer or sector which may somehow affect the credit quality or the ability to pay of the issuer, as well as the actions to be taken by the management area; (iii) every six months, update the opinions/reports relative to the assets in the portfolios, evaluating any events that occurred in this period; and (iv) annually, the management area shall prepare a report containing the following information and documents, if any: rating reports; audit reports; trustee reports; certificates from the registry of commerce for each of the players and, if applicable, relevant corporate changes; updated registrations and appraisal reports of collateral properties; updated documentation of ownership and appraisal reports of other collateral assets; reports regarding other assets/rights given as fiduciary security.

In the case of Funds of Investment in Receivables (***Fundos de Investimento em Direitos Creditórios – FIDCs***), each Fund has a regulation that determines the general characteristics of credit claims that may or may not be acquired by the respective FIDC. Based on the analysis and selection of eligible Credit Rights, as opposed to the regulations of the FIDCs under Lumina's management and their regulations, Lumina shall require the following documents and information from the creditor: (i) updated article of incorporation; (ii) CPF/ME of legal representatives; and (iii) personal document of legal representatives.

The credit and the debtor shall be approved by the Manager according to criteria such as: (i) creditor risk; (ii) transaction risk; (iii) issuer risk; and (iv) objective criteria.
Finally, the control areas shall also verify the main credit and counterparty risk performance indicators of FIDCs looking for possible deviations from expected values.

21. Insider Trading Policy

U.S. federal and state securities laws prohibit both Lumina and its Members from trading securities based on material, nonpublic information ("MNPI"). These laws also prohibit the improper dissemination of MNPI to others who trade securities (so-called "tipping", as described below).

Section 204A of the Advisers Act requires that are established, maintained, and enforced written policies and procedures, taking into consideration the nature of the business, to prevent the misuse of MNPI.

We impose a variety of limitations and restrictions on personal trading, including mandating the disclosure of accounts and positions, pre-approval of many transactions and prohibitions on certain personal investments. See Lumina's Personal Investment Policy.

A. Policy Statement on Insider Trading

Lumina forbids any Member from trading, either personally or on behalf of others, on material non-public information or communicating material non-public information to others in violation of the law.

The requirements contained in these procedures apply to securities trading and information handling by all Members. No Member to whom these procedures apply may trade, either personally or on behalf of others (such as Funds managed by Lumina), on the basis of material, non-public information, nor may any Member communicate material, non-public information to others in violation of the law.

If any Member learns of information that they believe may be considered MNPI, contact the Compliance Officer.

B. Elements of Insider Trading

The elements of insider trading and the penalties for such unlawful conduct are discussed below. If, after reviewing this policy statement, any Member has any questions, they should consult the Compliance Officer.

1. What is "Material" Information?

Information is "material" where there is "a substantial likelihood that a reasonable investor would consider that information important in making his or her investment

decisions". Generally, this includes any information that – if disclosed – would have a substantial effect on the price of a company's securities. Although the following is by no means a comprehensive list, information on a company's financial results and operations, such as the following, is generally deemed "material":

- dividend changes,
- earnings results,
- changes in previously released earnings estimates,
- significant merger or acquisition proposals or agreements,
- major developments in litigation,
- liquidity problems, and
- extraordinary management developments.

Note that the test for materiality does not require that the information would have changed a trader's (or a prospective trader's) mind – it merely requires a "substantial likelihood" that the actual or prospective trader would consider it "important".

"Material" information also may relate to the market for a company's securities; for example: information about a significant order to purchase or sell securities or the portfolio holdings, pre-publication information regarding reports to be published in the financial press, and advance notice of analyst upgrades and downgrades could all, in certain contexts, be material.

2. What is "Nonpublic" Information?

Information is considered to be nonpublic if it has not been disseminated broadly to investors in the marketplace. In addition, once disclosed, a sufficient period of time must pass for the information to permeate through the public channels to be considered "public". This can sometimes be a difficult determination to make, particularly when a company is actively followed by only a small number of analysts.

3. When is a "Duty" Violated?

U.S. law generally requires that a duty be violated in order to have an insider trading violation. This also can be a difficult determination to make, as one needs to examine not just the information itself, but the source of the information and what duties are owed (and these duties do not necessarily have to be owed to the source of the MNPI). For example, an officer can o we a variety of duties to a company by virtue of its position or an independent contractor can assume a duty of confidentiality by contract. It is also important to be aware that an affirmative misrepresentation may be considered the equivalent of a breach of duty for insider trading purposes.

With respect to so-called "tipper-tippee" liability, a person (the "tippee") who receives

MNPI from another (the “tipper”) will be deemed to have breached a duty when the tipper has disclosed the information in question in exchange for a personal benefit. Whether a personal benefit has been received is a fact-specific inquiry. In 2016, the United States Supreme Court reiterated that a personal benefit may be inferred where MNPI is communicated to a close friend or relative.

However, Members should be aware that no breach of duty needs to be shown to prove insider trading in the context of tender offers. Tender offers represent a particular concern under the laws governing insider trading for two reasons: First, tender offer activity often produces extraordinary gyrations in the price of the target company's securities. Trading during this time period is more likely to attract regulatory attention (and produces a disproportionate percentage of insider trading cases). Second, the SEC has adopted a specific rule that expressly forbids trading and “tipping” while aware of MNPI regarding a tender offer received from the tender offeror, the target company or anyone acting on behalf of either.

4. Disclosure of Relevant Facts

Although it is the responsibility of the administrator of the fund to make the disclosure of any relevant fact that occurred or related to the operation of the fund, the class or the assets that are part of the portfolio, as soon as it becomes aware of it, it is the responsibility of the other service providers, including Lumina, to immediately inform the administrator of the relevant facts of which they become aware, for proper dissemination.

In this sense, any facts that may have a significant influence on the value of the quotas or on the investors' decision to acquire, redeem, dispose of or maintain quotas are considered relevant, under the terms of article 64, paragraph 1 of the General Part of RCVM 175/22.

The following list is not exhaustive and provides examples of potentially relevant facts:

- change in the tax treatment given to the fund, class or quotaholders;
- hiring a market maker and the termination of the provision of this service; hiring of a risk rating agency, if not established in the fund's bylaw or in the class annex;
- change in the risk classification assigned to the fund, class or subclass of quotas;
- change of essential service provider; merger, incorporation, spin-off or transformation of the fund or class of quotas;
- change in the organized market in which the trading of the fund's quotas is admitted; cancellation of the admission of the fund or class quotas to trading in the organized market; and
- issuance of closed-end fund quotas.

Relevant facts may, exceptionally, not be disclosed, if it is understood by the Manager and the administrator of the fund that their disclosure jeopardizes the legitimate interest of the funds or their quotaholders. In this case, such information will be treated as confidential until the Manager deems the time for its disclosure to be opportune.

On the other hand, the administrator is obliged to immediately disclose a relevant fact in the event that the information escapes control or if there is an atypical fluctuation in the quotation, price or quantity traded of quotas, in the event of trading in a regulated market. The Manager shall notify the administrator if it becomes aware of any situation in this regard.

As a rule, the Manager must make available to the administrator the relevant facts related to the funds under its management immediately, so that the latter can publish them on its website and communicate them to the CVM.

5. Penalties for Insider Trading

Any violation of this policy can be expected to result in serious sanctions by Lumina, including dismissal of the Members involved.

Penalties for trading on or communicating material non-public information are severe, both for individuals involved in such unlawful conduct and their employers. A person can be subject to some or all of the penalties below even if he or she does not personally benefit from the violation. Penalties include

- civil injunctions;
- treble damages;
- disgorgement of profits;
- jail sentences;
- fines for the person who committed the violation of up to three times the profit gain or loss avoided, whether or not the person actually benefited; and
- fines for the employer or other controlling person of up to the greater of $1,000,000 or three times the amount of the profit gained or loss avoided.

C. Handling Material, Nonpublic Information

Before executing any trade, whether for personal investment or not, Members must determine whether they are aware of MNPI. If a Member believes he/she might be aware of MNPI, they are required to take the following steps:

- Do not execute any trades in any related securities.

- Do not communicate the information to anyone inside or outside Lumina, other than the Compliance Officer.
- Report the information and proposed trade to the Compliance Officer as soon as possible.
- The Compliance Office will determine whether Lumina is in possession of material and nonpublic information and, if so, what action should be taken.
    - Restricted List

Lumina will maintain a "Restricted List" of securities about which a determination has been made that it is prudent to restrict trading activity. This might include, for example, a company about which investment personnel may have acquired MNPI or a position where the Firm may have a securities filing obligation.

The Compliance Officer is responsible for maintaining the Restricted List. When adding a name to the Restricted List because of MNPI, the Compliance Officer will determine whether there are any other issuers whose securities would also be materially impacted by the MNPI that should also be added to the Restricted List.

As a general rule, trades will not be allowed in the securities appearing on the Restricted List, except with the approval of the Compliance Officer. Similarly, any determination to remove a company from the Restricted List must be approved and documented by the Compliance Officer. Restrictions with regard to securities on the Restricted List are also considered to extend to options, rights, or warrants relating to those securities and any securities convertible into those securities.

22. Abroad Investment Policy

Investments made by Lumina in assets located abroad will follow the provisions and limits of the fund regulations and all policies described in this manual.

The selection and allocation process of those assets follows the same process and due diligence used for local asset acquisitions, except in situations that require additional checks. The manager will select abroad assets that are overseen by recognized local authorities and are in a regular supervisory situation.

23. Allocation Orders Policy

It is the responsibility of Lumina's management team to select and allocate orders according to this Policy. It is the responsibility of all Lumina Members to report any non-compliances they become aware of in relation to the terms of this Policy. The Compliance Officer shall monitor compliance with this Policy and evaluate and resolve

any deviations.

Lumina exclusively and independently manages structured investments, whose objective is to invest primarily in illiquid assets. Invested assets are generally shares of structured funds, convertible and nonconvertible debentures, real estate, shares issued by privately held or publicly held companies, limited liability companies, credit, and special situations.

As a result, buy and sell orders issued with broker-dealers, when they occur, are individual and always carried out with the precise identification of the Fund in whose name they must be executed.

If Lumina needs to allocate grouped buy and sell orders in exceptional situations, the criterion adopted shall consider the equity of Funds with same strategy, weighting the allocations through formalized orders, which shall be subject to supervision. No advantages shall be allowed to one portfolio over another.

In the case of structured transactions, opportunities in the same investment shall be weighted among Funds with appropriate investment policies. In the event of opportunities offered to investors, such offers shall be made to all investors simultaneously, according to their investment strategies and interest.

For each Fund, Lumina will document how the fund will be managed, considering: (i) the period that the asset will remain in the portfolio; (ii) the duration or expected duration of the Fund and the expected timeframe of investments; (iii) committed capital of each Fund at the time of purchase/selling of the asset; (iv) the Fund's risk profile; (v) the Fund's investment policy and mandate; and (vii) existence of restrictions/requirements in regulations and contracts with investors.

Therefore, when determining the allocation of investment opportunities among co investors, and observing the Fund's regulations and contracts entered with investors, Lumina shall consider especially the following:

(a) the time required for the co-investor to decide on the investment;
(b) the co-investor's relationship with certain industries;
(c) the sophistication of the investment structures used by the co-investor;
(d) the preferences expressed by the co-investor in other opportunities;
(e) legal, regulatory and tax considerations of the co-investor's portfolio;
(f) co-investor's service relationships and track record with certain investment opportunities; and
(g) any perceived opportunity to strengthen relationships and enhance the long-term potential of the co-investment in view of the specific contributions of the co-investor to the development of the project..

In case of operations between Funds and/or between a Fund and a counterparty or intermediary under common control, the rules provided for in the regulations and contracts signed with investors regarding conflicts of interest shall be followed.

When necessary, Lumina shall address known conflicts of interests in its allocation practices by disclosure to clients and/or investors via the Fund's offering documents. If any Member of the management team becomes aware of any potential conflict of interest, he/she must immediately notify the Compliance Officer so that applicable measures can be taken.

The Compliance Officer will periodically examine the allocations across client accounts to determine fairness and compliance with this Policy.

24. Voting Rights Exercise Policy

The purpose of this Voting Rights Exercise Policy is to regulate the exercise of voting rights at general meetings or at Lumina's shareholders' meetings as a representative of the Funds ("Voting").

Lumina's management team shall be responsible for ensuring and controlling the execution of this Policy. All Members shall be responsible for reporting any non-compliances they become aware of Lumina's Voting. The Compliance Officer shall monitor compliance with this Policy and evaluate and resolve any deviations from the rules provided for in this Policy.

When exercising its voting rights, Lumina shall seek the best interests of its investors. Lumina shall vote for resolutions that, in Lumina's view, will appreciate the assets in its portfolios. On the other hand, Lumina shall vote against resolutions that could otherwise negatively impact the assets in its portfolios.

In the event of situations of conflicts of interest, Lumina shall abstain from voting, unless permitted by applicable law and regulation. When in doubt as to whether a given situation constitutes a conflict of interest, Members shall seek advice from the Compliance Officer and vote accordingly.

A. Compulsory Matters

The following matters require to exercise its voting rights:

I. Shares, their rights and splits:

a. election of representatives of minority shareholders on the board of directors, if applicable;

b. approval of options plans for the compensation of company executives, if the plan includes “in the money” purchase options (the exercise price is lower than that of the underlying share at the date of notice of the meeting);

c. acquisition, merger, incorporation, spin-off, changes in control, corporate reorganizations, changes or conversions of stocks and other changes to the article of incorporation, which may, in Lumina's understanding, significantly impact the value of the asset held by the Fund; and

d. other matters that require differentiated treatment.

II. Other assets and securities allowed in the Funds:

a. changes in payment terms or conditions, guarantees, early maturity, early redemption, repurchase and/or compensation originally agreed upon for the transaction

III. Specifically for the classes of Financial Investment Funds ("FIF"):

a. changes in the investment policy that change the category, type or class classification ANBIMA of the Fund and/or class, as the case may be
b. change of any of the Essential Service Providers, as long as they are not members of the same conglomerate or economic group;
c. increase in the administration fee, management fee, performance fee, minimum distribution fee or creation of entry and/or exit fees contained in the fund's bylaw, as applicable;
d. changes in redemption conditions that result in an increase in the exit period;
e. a plan for the resolution of the negative quotaholders' equity of a class whose liability of the quotaholders is limited to the amounts subscribed by them;
f. merger, incorporation, or spin-off that may change the conditions set forth in the previous items;
g. liquidation of the Fund and/or its classes, as applicable; and
h. investors' meeting, as provided for in the CVM regulations.

IV. Real Estate Funds (Fundos de Investimento Imobiliário – FIIs):

a. changes in the investment policy and/or in the object described in its regulation;
b. change of the essential services providers or real estate consultant, as long as they are not members of the same conglomerate or economic group;
c. increase in management fees, creation of entry fees, or creation or increase in advisory fees;

d. appraisal reports of goods and rights used when paying FII shares;
e. election of investors' representatives;
f. merger, incorporation, or spin-off that may change the conditions set forth in the previous items; and
g. liquidation of the Fund.

V. Properties that compose the FII:

a. approval of extraordinary expenses;
b. budget approval;
c. election of trustee and/or advisers; and
d. amendments to the co-ownership agreement that may have an impact on the property's liquidity, at the discretion of the Portfolio Management Officer.

In each case above, matters that in Lumina's view have a relevant impact on the value of the assets held by the Fund and/or are necessary to ensure the best interest of its investors are also compulsory.

B. Optional Matters

Lumina shall exercise its voting rights, at its sole discretion, in the following situations:

I. if the meeting takes place in any city that is not the capital of the State and it is not possible to vote remotely and/or participate by electronic means;
II. cost related to the exercise of the vote is not compatible with the participation of the financial asset in the portfolio of the Fund's class; and
III. the total participation of the Classes of Funds managed by Lumina subject to the vote, in the voting fraction of the matter on the agenda at the general meeting or special quotaholders' meeting, is less than 5% (five percent) and no Fund individually owns more than 10% (ten percent) of its equity invested in the asset in question.

In addition, Lumina shall attend a meeting and exercise its voting rights when, at its discretion, there is a matter that is of interest to the Fund and/or its investors.

C. Exceptions to the Exercise of Voting Rights

As an exception, the voting rights may not be exercised, at Lumina's discretion, in the situations listed below:

I. if there are situations of conflict of interests or the information provided by the company is not sufficient, even after request by the Portfolio Management Officer for additional information and clarification for decision making;

II. for exclusive and/or restricted funds with clauses that do not oblige the Portfolio Management Officer to exercise his/her voting rights in meetings;
III. for financial assets of issuers with head offices outside Brazil; and
IV. for certificates of deposit of securities.

D. Decision Making Process and Procedure for Exercising Voting Rights

The management area, under responsibility of the Portfolio Management Officer, shall implement this Policy and coordinate the process of decision-making, registration, and formalization of voting rights.

Under the terms of the applicable regulations, the administrator of the Funds under Lumina's management must, if necessary, access to information for the full exercise of the right to vote. As a result, the administrator is responsible for sharing with Lumina the call for participation in the meeting, as well as the content on the agenda and the date of occurrence of such meetings.

Upon receipt of notice by the management area, the following steps must be taken:

(a) the notice shall be analyzed and filed internally;
(b) the information shall be submitted for evaluation by the responsible managers;
(c) a voting recommendation shall be made in advance of the meeting; and
(d) a Member or a person who is not part of the staff shall be appointed as representative to participate in the voting, when applicable.

The exercise of voting rights shall not require prior consultation with investors, except for any provisions to the contrary in the regulations of the Funds. Voting decisions shall be made based on research, evaluations, and beliefs of Lumina, in a reasoned manner and consistent with the best interests of its investors.

The decision to participate in the meetings and the vote itself shall be defined and formalized in the minutes or by email from the Lumina portfolio management area. Lumina's decision not to participate in each meeting shall imply that Lumina will not exercise its voting rights and shall be registered together with the reasoning for its decision.

Lumina shall send to the Fund manager a summary of the content and the reasoning for its vote or the reasons for any abstention from exercising its voting rights within 5 (five) days after the meeting.

The files with the minutes of the meetings and Lumina’s eventual votes shall be kept for 5 (five) years according to Lumina's retention policy.

E. Communication of Votes to Investors

The Manager shall communicate to the administrator of the Funds the votes cast at the meetings of the assets invested by it, as they occur, or, alternatively, by means of a report containing: (a) the summary of the content of the votes cast; and (b) the summary justification for the vote or, when applicable, the reasons for any abstention or non-exercise of the right to vote. The communication may occur on a one-off or periodic basis, according to the Manager's decision, observing, in all cases, what is described in the operating agreements signed with the respective managers:

Based on the report mentioned above, the administrator will perform., as applicable:

(a) the completion of the monthly profile, if the Fund Class adopts a policy that provides for the exercise of voting rights arising from the ownership of financial assets; and
(b) communication to the quotaholders by means of a note contained in the statement of the month following the holding of the meetings

It shall be incumbent upon the administrator to make available to the quotaholders and to the supervisory bodies the information provided to it by the Manager regarding the exercise of this policy, and such provision may be made by letter, e-mail and/or extract accessible through the world wide web.

Without prejudice to the obligations of the fund manager, Lumina shall make available the votes to the quotaholders on its website. Communications to investors and summaries of exercise of voting rights will be filed and maintained by Lumina and made available to ANBIMA.

25. Continuous Certification Policy

The Continuing Certification Policy aims to establish rules and procedures to ensure adequate certification and qualification of Members, considering the rules established by CVM and ANBIMA.
All Members shall be responsible for obtaining the necessary certifications for the performance of their functions, when applicable, and to report any non-conformities they become aware of to the Compliance Officer. The Compliance Officer shall monitor compliance with this Policy, assess and resolve any deviations, and resolve any requests for exceptions, where applicable.
Considering Lumina's business, which consist of exclusively and independently managing investment funds, the following certifications and/or exemptions from certifications are required:

(a) Certified ANBIMA Manager – professionals who have discretionary

power to invest in Financial Investment Funds;

(b) Certified ANBIMA Manager of Structured Funds – professionals with discretionary power to invest in Debt Funds, Private Equity, and Real Estate Funds.

This Policy shall be amended if Lumina decides to act in other activities that require certification.

When hiring new Members, the hiring area shall provide the Compliance Officer with information as to whether certification will be required, according to the roles and competencies to be performed by the new Member. If it is decided that the certification will be required, the new Member shall provide proof of certification before signing the employment contract.

The ANBIMA Certification Rules and Procedures determine that assets managers must maintain in their structure a professional primarily responsible for the investments and, at least, one deputy with discretionary power to invest in the activity of Asset Management in case of temporary unavailability of the professional primarily responsible for the investments.

Therefore, as of January 2, 2026, both professionals must be part of the Manager's permanent staff and act directly and regularly in the activity of managing third-party resources, and the appointment of external service providers is prohibited, except in certain specific cases.

CGA and CGE certifications, including those obtained before January 2, 2026, are valid for 5 (five) years. Therefore, prior to the expiration of the certifications, eligible professionals must participate in the update procedure established by ANBIMA, so that the certification obtained is duly updated within the established deadlines.

Every year or on an as-needed basis, the Compliance Officer shall check if all positions, functions, and competencies that require certification are being held by Members with proper certification and/or exemption, and if certifications are duly updated.
The Compliance Officer shall be informed immediately of any promotions, at which time he/she will determine whether the new position will require certifications. If this is the case, the Compliance Officer shall require the Member to prove certification and/or exemption before being promoted.
Members who do not have proper certification and/or exemption shall not be allowed to make individual decisions in the context of asset purchase or selling or portfolio management. The continuation of activities by a Member with investment discretionary power without the proper certification and/or exemption constitutes serious misconduct, which may lead to his/her termination by decision of the Compliance Officer and/or the Portfolio Management Officer. In such case, the Compliance Officer

shall be responsible for investigating potential irregularities or failures and elaborate a plan to remedy the situation.

Exceptions to this Policy shall be requested from and be granted exclusively by the Compliance Officer, if they are provided for in the applicable law and regulations and that they are granted in conjunction with an appropriate action plan to include any necessary regulations.

26. Training Policy

Lumina encourages its Members to grow professionally by attending courses related to the area of interest in the company as well as other related courses.

In order to be hired as a new Member, the individual shall take a special training organized by the Compliance Officer, when the procedures contemplated by this Manual (including all its Policies) shall be presented and explained.

Training shall be taken on a business day to be determined by the Compliance Officer. Training must be provided to all new Members. The Compliance Officer shall send notification to all new Members informing the date, time, and room in which the training is going to be held. Attendance of all Members notified by the Compliance Officer is mandatory.

Still according to RCVM 21/21 article 24, III, which deals with the need to implement and maintain a training program, the Manager understands that it is essential that all Members are aware of the ethical principles applicable to their activities, always maintaining them up to date.

Thus, in compliance with this rule and Lumina's values, Lumina shall offer an annual recycling program to all Members, updating them on the terms and responsibilities described herein.

The Compliance Officer shall monitor the Members attendance in the training as well as their periodic renewal of the training.

27. Political Contributions Policy

The SEC, along with a growing number of states, localities and foreign jurisdictions, has implemented laws and regulations designed to monitor and regulate political contributions to government officials and candidates for office who are (or, if victorious, will be) in a position to directly or indirectly influence the allocation of investment mandates for investment funds. The most visible of these is Rule 206(4)-5

under the Advisers Act, the so-called "pay-to-play rule," which prohibits a number of practices relating to political contributions and the violation of which imposes a two year "time out" from receiving advisory-related compensation from the applicable public entity.
Because these rules are numerous, and are sometimes inconsistent with each other, Lumina has adopted a simple pre-communication policy, which requires that any contributions (i.e., any gift, subscription, loan, advance, deposit, service, or anything else of value) to:

- State or local government officials or candidates for office;
- state and local branches of political parties; or
- any non-US office holders, candidates or any non-US political parties

by a Member be pre-communicated to the Compliance Officer in writing.

The pay-to-play rule also includes a "look-back" provision that may cover contributions made by Members prior to joining Lumina, which period can be as long as two years. Therefore, all candidates for employment are required to disclose what political contributions, if any, they or any of their immediate family members made in the two years preceding the date on which they joined Lumina. The disclosure shall be submitted in the manner designated by the Compliance Officer.

Lumina and its Members are prohibited from doing anything indirectly which, if done directly, would violate the rule. Therefore, Lumina and its Members are prohibited from using third-party solicitors, attorneys, family members or companies affiliated with Lumina to make contributions that would violate the pay to play rule or these policies.

If Lumina has any client who is a member of any governmental entity, all necessary records will be kept in order to avoid any conflicts of interest.

28. Penalties

As described in the Code of Ethics, failure to comply with the requirements of this Manual and all laws, rules, and regulations applicable to Lumina's business may subject its Members to disciplinary action by Lumina, which may comprises, among others, written or verbal advertency, suspension up to 30 days and termination of the agreement, depending on the gravity of the violation. Lumina may also take disciplinary action against a Member that engages in conduct deemed to be unethical or illegal, whether or not such conduct constitutes a violation of this Manual. Non-compliance that violates law may result in civil and criminal penalties.

Members shall report to the Compliance Officer concerns that the policies and

procedures contained in this Manual may be or have been violated. Members shall also report concerns about violations of any other laws, rules, or regulations applicable to Lumina's business. Examples of concerns that shall be reported include but are not limited to suspected money laundering according to the Anti-Money Laundering Policy, suspected fraud, accounting, or auditing irregularities, bribery, kickbacks, theft or misuse of clients' assets or the Lumina's assets, misuse of Confidential Information (whether Lumina's information or that of third parties, such as insider trading (see Lumina's Insider Trading Policy)), or other regulatory, compliance, or ethics-related violations. If you are unsure whether a violation has occurred or could occur, you should discuss the matter with the Compliance Officer.

29. Periodic Updates and Reviews

To ensure continuous adequacy and effectiveness of this Manual, the Codes and Policies contained in this Manual will be reviewed at least every 12 (twelve) months after its publication or (i) whenever there is a modification in the applicable law and regulations that require its due review, or (ii) whenever any activities provided for in this Manual change and require its respective update and/or review.

VERSION CONTROL	DATE	MODIFIED BY	DESCRIPTION OF CHANGE
1.0	Mar/2022	Ana Luiza Tesser Arguello	First version
1.1	Jun/2022	Ana Luiza Tesser Arguello	Adjustments related to the Personal Investment Policy
2.0.	Jun/2023	Inez Costa de Barros Lisboa	Adjustments related to the LGPD (Brazilian General Data Protection Law), ANBIMA AML/CFT Guidelines, inclusion of exclusive open-ended investment funds in Lumina's portfolio of managed vehicles, remote work, foreign investments, and amendments to comply with U.S.

			legislation applicable to the manager's investments.
3.0.	Julho/2025	Catarina Rosa Rodrigues	Adjustments related to the policies in accordance with the provisions of CVM Resolution 175/22 and the new ANBIMA certification rules.

Appendix I – Code of Ethics

Your performance as well as your attitudes are essential to maintain and improve the reputation and success of Lumina.

The strength of Lumina's reputation depends on a range of factors, from integrity to quality to investor relations.

The standards of professional conduct were developed to guide you both in routine activities and in those unexpected situations that may arise in everyday life.

Please read this Code of Ethics very carefully and, whenever required, ask the Compliance Officer for clarification. Please note that Lumina's Policies, as well as the general policies and principles contained in this Manual, must be complied with in its entirety.

The defined terms not defined in this Code of Ethics shall have the same meaning of Lumina's Compliance Manual.

1. Responsibility

1.1. *Compliance* is an activity adopted by the international financial market which, based on ethical principles and always pursuant to the law, whenever the activities are carried out, intends to minimize any and all exposure to risks, whether they are financial, litigation, or reputational risks. Compliance aims at protecting the reputation of an institution as its most valuable asset.

1.2. Each Member is responsible for his or her behaviors and actions and shall ask for guidance in relation to the interpretation or applicability of the rules contained in this Manual. For that purpose, the Compliance Officer is fully available for clarifications.

1.3. Each and every communication with the Compliance Officer is confidential and shall be made by phone or via email: compliance@luminacm.com.

1.4. All Members are expected to be familiar with the Code and to formalize that by signing the Statement of Compliance (Appendix II).

2. Relationship between Members and Anti-Harassment Policy

2.1. Lumina is committed to promoting an ethical, safe and respectful work environment, based on respect for the human rights of its Members and related parties. The company adopts a zero-tolerance policy for any form of harassment, including sexual

harassment, moral harassment (power harassment), and discriminatory conduct related to pregnancy, childbirth, parental leave or family care. These practices are prohibited both in the work environment and in external interactions linked to professional activities.

2.2. The work environment must be permeated by behaviors based on courtesy, respect, team spirit, trust and assiduity. It is not allowed for any Member to practice acts that constitute disrespect, abuse of power, violence, harassment, discrimination, retaliation, offenses, physical or moral discomfort, including any form of racial, sexual, religious or disability-related harassment and discrimination.

2.3. Lumina adopts a zero-tolerance policy for any form of harassment, including sexual harassment, moral harassment, and discriminatory conduct related to pregnancy, childbirth, parental leave, or family care. These practices are prohibited both in the internal environment and in external interactions linked to professional activities.

2.4. Sexual harassment is defined as any behavior of a sexual nature, unwanted, that harms the work environment or causes embarrassment to Members or third parties, regardless of gender or sexual orientation.

2.5. Moral harassment, on the other hand, refers to abuses of authority that exceed what is reasonable in the professional context, causing physical or psychological suffering or violating the dignity of the individual.

2.6. Also considered forms of harassment or discrimination are conducts that hinder or impair the exercise of legal rights related to maternity, paternity or family care, as well as any action based on race, origin, belief, occupation or personal condition.

Thus, Lumina's principle is to treat its Members impartially and fairly, without practicing any type of discrimination or personal favoritism.

2.7. To ensure the effectiveness of this Code, Lumina provides formal reporting channels, as provided for in item 16 below. The Manager ensures that there will be no retaliation or any form of unfavorable treatment to whistleblowers or people involved in the investigation, ensuring the protection of the privacy of all involved.

2.8. Complaints will be investigated quickly and impartially, and may result in penalties, according to item 17 of this Code. In cases involving external parties, the Manager will adopt measures to protect its Members and will request measures from the party involved.

3. Relationship with the Team, Managers, and Colleagues

3.1. Members are expected to share knowledge and information required to perform Lumina’s business, always according to the Lumina’s Confidentiality and Security of Information Policy.

3.2. Members are expected to voluntarily co-operate in situations such as: emergency replacement to cover the absence of another colleague or to perform works outside the normal routine.

4. Relationship with Clients, the Market and Competitors

4.1. Under the terms of RCVM 21/21 article 18, I, II, and III, respect for the rights of clients must be translated into concrete attitudes and actions that seek the permanent satisfaction of their expectations in relation to the products and services provided by the Manager. All Members must be aware that maximum client satisfaction is the primary objective of the Manager, having a direct impact on its corporate and institutional image, and therefore they should always seek to serve the interests of the Manager's clients.

4.2. All Members should seek to protect the interests of the investors of Manager.

4.3. All Members should seek to protect Lumina's reputation.

4.4. Under the terms of this Code of Ethics and the Manual, all information provided shall always be based on legal, regulatory, and ethical aspects, and shall not be disrespectful to other players in the financial and capital markets.

4.5. Members who possess relevant, strategic, privileged, and/or non-public information shall not act or cause other individuals to act based on such information and must maintain absolute secrecy about such information, pursuant to the terms of the Confidentiality Policy herein.

4.6. Members shall not engage in activities that focus on deliberate attempts to interfere with the behavior of the financial markets, change prices, or artificially increase trading volumes with the intention of creating artificial conditions for market participants.

4.7. Members shall be transparent and responsible in their negotiations with the market and shall not engage in unfair competition or acts that create unfair market conditions.

4.8. The Manager shall respect all its competitors and seek to promote a fair and loyal competition based on ethical principles and following the applicable rules and legislations.

4.9. Comments or rumors that may harm the business or the image of competing companies shall not be disclosed by the Manager or its Members, and the Manager shall demand and expect reciprocal and cordial treatment from its competitors as well.

4.10. It is absolutely forbidden to disclose to competitors any relevant information or information that may be of interest to the Manager, except in exceptional cases, and with prior and express authorization of the Compliance Officer.

5. Relationship with Affiliate Companies

5.1. The Manager, always taking into consideration ethical standards, best practices in the market, as well as respect to its clients, competitors, and the market, shall discourage any kind of relationship with institutions in which any Member has interests.

5.2. In the case of affiliate asset managers, if Lumina concludes that an investment in an affiliate company is the best opportunity for its investors, Lumina shall carry out a detailed analysis of the potential investment fund, as well as of the respective asset manager. Once the due diligence is approved, Lumina shall communicate to the investors of the investment fund about its relationship with the respective asset manager.

5.3. No advantage shall be granted to induce Lumina to invest in asset managers with which their Members may have any kind of relationship.

5.4. If any potential conflicts of interest are identified between Lumina and an affiliated asset manager or an asset manager in which any Member has interests, the Compliance Officer shall resolve the potential conflicts of interest.

6. Relationship with Vendors and Service Providers

6.1. Guided by the highest standards of conduct, the Manager shall honor its commitments with vendors and service providers, always seeking to establish objective, efficient, and adequate contracts for the good conduct of its business, which, as far as possible, shall not leave room for multiple interpretations, material omissions, or ambiguities.

6.2. In the best interest of the Manager, technical, professional, marketing, logistical, and ethical criteria shall always prevail when selecting vendors and service providers. The Manager shall carry out a detailed analysis prior to contracting new professionals, respecting the best practices, and contributing to the fight against money laundering, terrorist financing, and corruption, in accordance with the specific Policies applicable to the matters.

7. Relationship with Supervisory and Oversight Bodies

7.1. Under RCVM 21/21 article 18, VIII, should the Manager be aware of any occurrence or indication of violation of any regulation issued by CVM, the Manager shall inform such occurrence or indication of violation within 10 (ten) business days..

8. Conflicts of Interest

8.1. Lumina shall adopt certain corporate governance frameworks in order to avoid conflicts of interest and, when they exist, ensure that any conflicts are resolved in accordance with applicable law and regulations, as well as best market practices and ethical standards.

8.2. Conflicts of interest may arise between (i) Members and Lumina; (ii) interests of two or more investors of the Funds; (iii) investors of the Funds and Lumina; and (iv) between Members.

8.3. In addition to the specific rules contained in this Code of Ethics and the Manual that aim to prevent and resolve conflicts of interest, the following guidelines are also implemented in case of conflicts of interest: (i) when managing Funds, transactions with companies in which a Member has interests or personal relationships are forbidden, unless authorized by the Compliance Officer and in accordance with the Personal Investment Policy herein; (ii) receipt of gifts or benefits is forbidden, except within the limits authorized in the item below; (iii) Members shall not perform any activities that conflict with the interests of Lumina and with their professional performance at Lumina; (iv) Members shall inform any actual or potential conflicts of interest to the Compliance Officer; and (v) Lumina shall maintain record of conflict of interest events, including the individuals related thereto.

9. Gifts (*Soft Dollar*)

9.1. Any gifts or benefits received by Members shall comply with the provisions set forth in the Third-Party Selection, Contracting and Monitoring Policy herein, that is:

9.2. Gifts or benefits received by Members that add up to more than R$ 1,000.00 (one thousand reais) must be previously approved by the Compliance Officer. Gifts or benefits offered by Members to third parties that have or may potentially have a direct or indirect relationship with Lumina's activities (counterparties, service providers, authorities, among others) and that amount to more than R$ 500.00 (five hundred reais) must be previously approved by the Compliance Officer. When prior approval is not feasible due to the circumstances involved, there must be immediate communication by the Member to the Compliance Officer about the receipt or offer of gifts or benefits.

9.3. Members must not, directly or indirectly, neither for themselves nor for third parties, request, accept or admit money, benefits, favors, gifts, promises or any other advantages that may influence the performance of their duties or as a reward for an act or omission arising from their work.

9.4. All gifts, gifts, hospitality or benefits received or offered that are subject to prior approval or mandatory communication must be registered by the compliance area. This record must contain the following information:

- Estimated value of the gift or benefit;
- Origin (name of the individual or legal entity that offered or received the item);
- Declared purpose (e.g. institutional courtesy, partnership celebration, corporate event); and
- Context of the transaction (e.g. existing business relationship, specific occasion, contractual relationship).

9.5. The compliance area may carry out periodic audits to verify adherence to the Code and identify any deviations.

9.6. Finally, according to RCVM 21/21 article 18, VI, the Manager shall transfer to the investment fund any benefits or advantages it receives as a result of its position as manager of the investment fund.

10. Understanding and Accepting Changes

10.1. Members should be able to understand and accept changes implemented in the work environment by the company.

11. Intellectual Property

11.1. The Member, in duty of his/her professional activities at Lumina, may receive, access, use, create, conceive and contribute to the development of intangible assets, such as innovations, technologies, business information, customer lists, spreadsheets, memoranda, opinions, reports, presentations, training, strategies, forecasts, advice, consultancies, know-how and business secrets. Such assets constitute the exclusive intellectual property of Lumina ("IP Lumina"), even if stored and/or used on the Member's personal devices.

11.2. The Member shall keep IP Lumina under the strictest confidentiality and, except with the prior written authorization of Lumina, may not disclose it to any third party, nor copy it, use it, reproduce it, share it or modify it, except as necessary to perform its functions and obligations to and for the benefit of Lumina.

12. Press Communication

12.1. For the purpose of protecting the interests of Lumina and in view of the highly sensitive information related to financial and capital markets and to the activities of Lumina that are received by the Members, only the Compliance Officer and the Portfolio Management Officer, or any other person authorized by them, may have any kind of communication, on behalf of Lumina, with journalists, reporters, interviewers or agents of the broadcast media and the press (the “Press”).

12.2. For the purposes of the prohibition set forth in the section above, communication means the disclosure of any Confidential Information or any other item subject to the intellectual property of Lumina to the Press, as well as any and all information, especially information relating to investors, obtained while carrying out the activities of Lumina.

12.3. Any Members previously authorized to take part in interviews and similar disclosures shall limit themselves to make strictly technical comments, avoiding the use of any unnecessary judgment, and any statements shall be based on careful disclosure of sensitive information. Any Member taking part in interviews is expected to always use discernment and politeness when he or she is publicly representing Lumina.

13. Charity and Political Contributions and Donations

13.1. Lumina does not donate to or participate in any charity or make any political contributions or donations but shall respect the rights of its Members to join or contribute to political parties or donate to or participate in any charity, subject to Lumina's Political Contributions Policy. As such, all Members shall inform the Compliance Officer prior to engaging in any form of political affiliation, political contribution, or charity donation or work.

14. Impartiality in Business

14.1. A basic principle of Lumina is treating its Members and clients in an impartial and fair manner, not taking into account any aspect that may represent discrimination or violation of the law.

14.2. In every relationship, decisions shall include considerations based on facts, thus avoiding the influence of personal opinions, interests, or feelings, in addition to minimizing partiality.

15. Organization

15.1. The Members shall organize and keep their workplace, as well as their daily work, organized and clean, establishing priorities and sequencing of tasks.

16. Hot Line

16.1. Lumina values integrity in all its operations and, therefore, maintains a secure and confidential channel so that its members can report suspected irregularities or risks related to their activities.

16.2. For the purposes of this Code, communication of improper conduct is understood to be any report regarding suspected legal, regulatory or ethical infractions, including, but

not limited to, improper conduct, fraud, criminal offenses, judicial failures, health and safety risks, negative environmental impacts, violations of accounting or auditing standards, discrimination, harassment, violence, unethical conduct or any other situation provided for in Lumina's internal guidelines. Any suspicion should be reported as soon as possible.

16.3. Members may file a complaint through any of the following channels: (a) their direct supervisor, (b) Lumina's human resources area, (c) compliance area, and (d) whistleblowing channel.

16.4. Lumina provides its Members, clients, counterparties, and the public with a hot line for reports and complaints, available in the e-mail compliance@luminacm.com and Lumina´s website www.luminacm.com. The hot line is a safe and anonymous tool. It also allows Members to ask questions about institutional policies and suggest improvements to operational processes.

16.5. The Member may freely choose the channel he considers most appropriate and safe.

16.6. Upon receipt of the communication, Lumina will confirm the entry protocol and, when applicable, may schedule a meeting with the complainant, provided that the latter has not chosen anonymity. The responsible area will conduct a preliminary analysis and, if necessary, initiate an investigation process, which may involve evidence collection, interviews and, eventually, the designation of external professionals to conduct the investigation.

16.7. The identity of the complainant and the content of the communication will be treated with the highest degree of confidentiality, observing the legal limits and the need for proper conduct of the investigation. Protection against retaliation will be ensured, including in cases of anonymous complaints. During the six months following the complaint, the whistleblower can only be dismissed with the prior approval of the Compliance Officer. For the two cycles of evaluation and promotion following the complaint, the Compliance Officer must monitor the treatment attributed to the whistleblower in order to ensure that there is no direct or indirect retaliation.

16.8. This Code does not restrict, under any circumstances, the right of Members to communicate directly with public authorities, either voluntarily or in response to official requests, as provided for in current legislation.

17. Penalties

17.1. Any violation to the Code of Ethics due to negligence, recklessness and/or omission is deemed an act of indiscipline and shall subject the defaulter to punishment.

17.2. If any irregularity performed by a Member or misconduct in relation to the established standards is found, the Member shall be requested to provide clarifications and present his or her defense. The Compliance Officer may archive away the proceeding, warn the Member, enter into an Instrument of Commitment with the Member, or begin an Internal Administrative Inquiry Proceeding.

17.3. If the act performed by the Member is shown to be serious, but despite of indicating an unsatisfactory behavior, is not an indication of incompatibility with the performance of his or her duties, then the Compliance Officer may choose to enter into an Instrument of Commitment with the Member.

17.4. By means of the Instrument of Commitment, the Member shall acknowledge the inappropriateness of his or her behavior in relation to the rules established in this Code and acknowledge the need for adjustment of his or her conduct to said rules. Given that the purpose of the mentioned instrument is the functional recovery of the person involved, there shall always be a term established for verification of the adjustment of conduct, which shall not exceed 90 (ninety) days.

17.5. The document shall be signed by the Member and the Compliance Officer. The immediate manager is liable for overseeing and ensuring the conditions required for full compliance with the Instrument of Commitment.

17.6. The implementation of an Internal Administrative Inquiry Proceeding shall occur when: (i) the violation incurred by the Member is serious; (ii) the violation is classifiable under article 482 of the Consolidated Labor Laws (Consolidação das Leis Trabalhistas – CLT), which provides for the events of dismissal of an employee for cause; or (iii) the violation may result in damage to Lumina. Broad defense and right to adversary proceeding are ensured in such proceeding.

17.7. After conclusion of the Administrative Inquiry Proceeding, weighting the severity of the occurrence, the Member may be held liable and subject to disciplinary actions; the Compliance Officer shall have authority to define the application, as provided for by law, of the following penalties (without prejudice of applying other penalties permitted by applicable law, as applicable):

- Written or oral warning;
- Suspension for up to 30 (thirty) days;
- Termination.

17.8. The Compliance Officer may use electronic and telephone monitoring records and systems to verify the conduct of any Members involved in actual or potential violations of this Code of Ethics, this Manual, and/or other applicable rules.

18. Violations to the Code

18.1. Any concerns that a Member may have in relation to any violation to this Code of Ethics or any facts and actions that may lead to such occurrence shall be communicated immediately to the Compliance Officer.

Appendix II - Statement of Compliance

I hereby declare that I have received, read, understood and adhere the Compliance Manual of Lumina Capital Management Ltda. ("Lumina"), which includes all policies from Lumina, including Lumina's Code of Ethics. I also declare that I have participated in the onboarding process and in the initial training offered by the Manager.

I hereby undertake to fully comply therewith, subject to penalty of any internal punishment measures (enforcement) of Lumina and to termination as provided for by my employment contract and the applicable law.

Full Nome : _____

CPF/ME:_____

Datw:____/_____/_____

Signature: _____

(This instrument is composed of two counterparts, being one for the Member and the other to be filed as hard copy at Lumina's principal office and stored electronically in Lumina's cloud.)

Appendix III - Risk Assessment Methodology and AML/PTF Monitoring

With the purpose of adhering to the provisions of RCVM 50/21 and other rules regarding the AML/PTF, the Manager shall classify the risk of money laundering and financing of terrorism and the proliferation of weapons of destruction of its transactions according to the risk assessment methodology outlined in this Appendix.

This methodology consists in exclusive activity of administration of portfolio by Lumina's funds, considering that Lumina does not perform activities in the quality of distributor of such funds. This methodology is based on the experience of the Manager, as well as the instructions, opinions, and guidelines issued by the Brazilian regulators and self-regulators, taking into account the limits of its attributions as an asset manager, while prizing for its efficiency in identifying, analyzing, understanding, and mitigating the risks of AML/PTF.

For the purposes of the ANBIMA AML/FTP Guide (Edition IV, 2022), regarding Lumina's relationship with the investors of the funds under its management, Lumina plays the role of "investment fund manager with multiple quotaholders" and "exclusive fund manager". Specifically in relation to the exclusive funds under its management, Lumina shall (i) collect the onboarding information of the ultimate beneficial owner of these vehicles from the respective distributors and/or administrators, and (ii) monitor such information, in line with the AML/FTP Policy.

The AML/PTF risk assessment and monitoring methodology will take into account: (a) the negotiation environment; (b) the pricing of the traded asset; and (c) the counterparty, for which all products and services offered by the Manager shall be identified, in addition to the mandates granted by the investment funds under its management, in order to classify the operations into (i) Low Risk; (ii) Medium Risk; or (iii) High Risk, as follows:

Methodology and Assessment

Low Risk

Operations classified as Low Risk are:

(a) initial and secondary public offerings of securities, registered in accordance with the CVM rules;
(b) public offerings with restricted efforts, exempted from registration according to the CVM rules;
(c) assets issued or traded by a financial institution or equivalent;
(d) assets issued by issuers of securities registered with the CVM;
(e) assets of the same economic nature as those listed above, when traded abroad, provided that they are allowed to trade on stock, commodities, and futures exchanges, or registered in a registration, custody, or financial settlement system, duly authorized in their country of origin and supervised by a local authority recognized by CVM, or whose existence has been ensured by third parties duly authorized to exercise the activity of custody in

countries that are signatories to the Treaty of Asunción or in other jurisdictions, or supervised by a local authority recognized by CVM.

Examples of operations classified as Low Risk are: shares traded on the stock exchange; government bonds and private bonds of companies with investment grade and traded in organized markets, among others.

Medium Risk

Medium Risk operations are those occurring in less regulated trading environments, may involve complex pricing assets with little trading history, so that the price cannot be measured with certainty against the historical price, in addition to involving a counterparty that is not a Politically Exposed Person or that has some significant risk of money laundering, according to RCVM 50/21.

Examples of operations classified as Medium Risk are: private securities of companies with a risk rating below investment grade traded in organized markets; complex assets traded in non-organized over-the-counter markets; among others.

High Risk

Operations classified as High Risk take place in trading environments with low or no regulation, involve assets that are difficult or extremely complex to price, in addition to all operations involving counterparties classified as Politically Exposed Persons or any others that may represent a higher degree of money laundering risk, as per RCVM 50/21.

Examples of operations classified as High Risk are any dealings involving Politically Exposed Persons as counterparties, as well as their relatives, close members and entities in which they participate, non-profit organizations, or any other high risk of money laundering, as per RCVM 50/21; private credit assets outside the organized trading environment; private equity; among others.

Evidence of Suspicious Activities

Notwithstanding the risk classification carried out by the Manager as described above, it should be noted that the Manager shall also consider the following evidence of money laundering when monitoring its operations:

- a transaction carried out between the same parties or for the benefit of the same parties, in which continuous gains or losses are verified in relation to any of the parties involved;
- a transaction that shows a significant oscillation in relation to the volume and/or frequency of deals of any of the parties involved;
- a transaction with consequences that include characteristics that may represent a mechanism to disguise the identification of the actual beneficial owners and parties

involved;

- a transaction whose characteristics and developments show evidence of acting in a contumacious way on behalf of third parties;
- a transaction showing sudden changes, objectively unjustified in view of the operational modalities typically used by the parties involved;
- a transaction with a degree of complexity and risk incompatible with:

    - ✓ the trading profile and history of the counterparty or its representative; and
    - ✓ the size and purpose of the client;

- a transaction performed for the perceived purpose of generating loss or gain which objectively lacks economic basis;

- a private transfer, for no apparent reason, of funds and securities, such as::

    - ✓ transfer between investors' current accounts vis-à-vis the intermediary;
    - ✓ transfer of ownership of securities without financial movement; and
    - ✓ transfer of securities outside of the organized market environment;

- a deposit or transfer made by third parties for settlement of transactions of clients or guarantee of transactions in future settlement markets;
- a payment to third parties, in any manner whatsoever, by way of settlement of transactions or redemption of amounts deposited in guarantee, recorded on behalf of the client;
- transactions not performed at market prices.
- Operations and situations related to persons suspected of involvement in terrorist acts, the financing of terrorism, or the financing of the proliferation of weapons of mass destruction, such as those involving:

    - ✓ assets obtained from sanctions imposed by UNSC resolutions referred to Law No. 13,810 of March 8th, 2019;
    - ✓ assets obtained through a foreign authority's request for unavailability measure that comes to Lumina’s knowledge;
    - ✓ the conduct of business, regardless of its value, by persons who have committed or attempted to commit terrorist acts, or participated in or facilitated those acts, in accordance with Law No. 13,260 of March 16th, 2016;

    - ✓ securities owned or controlled, directly or indirectly, by persons who have committed or attempted to commit terrorist acts, or participated in or facilitated those acts, in accordance with Law No. 13,260 of 2016; and
    - ✓ movements that may be associated with terrorist financing, according to the provisions of Law No. 13,260 of 2016.

- Operations with the participation of natural persons, legal entities or other entities residing, headquartered or incorporated in countries, jurisdictions, dependencies or locations:

    - ✓ which do not implement or insufficiently implement the recommendations of the FATF; and

    - ✓ with favored taxation and subject to privileged tax regimes, as per norms issued by the Brazilian Internal Revenue Service.

All transactions involving any of the above evidence, whether classified as Low Risk, Medium Risk or High Risk, shall be reported to the Compliance Officer. Lumina understands that dealing with the evidence described above is the best way to mitigate the risks of money laundering in its activities.

Monitoring

Transactions shall be monitored according to their risk classification. The metrics to classify Lumina's investors, products or services in the risk classification will be defined by the Compliance Officer.

However, even in cases in which the monitoring is considered low risk, any kind of suspicious activity that is identifies shall be reported to the competent authority.

In relation to the monitoring of investors that Lumina does not have direct relationship due to not exercising distribution activity, in the limits of its attributions, Lumina shall:

(a) consider, for the purpose of the monitoring according to risk classification, the AML/PTF Policy and the respective rules, procedures and internal controls of other institutions responsible to the investors' registration;

(b) perform the exchange of the information with the internal controlling areas of the entities mentioned in item (a) herein above that have direct relationship with the investor, taking into account the privacy regimes and restrictions to access information provided by law;

(c) continuously monitor the operations performed on behalf of such investors considering the operations and situations that neither depend on the possession of register data, not the identification of the ultimate beneficial owner, as well as, if applicable, adopt the measures described in this Appendix and the AML/PTF Policy;

(d) evaluate the adequacy and the opportunity of requesting additional information to the entities mentioned in the item (a) herein above that have direct relationship with the investors, using the exchange mechanisms referred in item (b) herein above, if applicable, in accordance with the rules set forth in this Appendix and in the AML/PTF Policy.

The Manager shall monitor the transactions based on the methodology approved by the Compliance Officer, checking all evidence of money laundering described above, as well as the price range of the traded assets and the risk of the counterparties. The results of the monitoring shall be documented and filed.

Lumina understands that the indicators referred to above are able to mitigate money laundering risks consistent with the activities performed by the company.

Appendix IV – Statement for Contracting Third Parties

In my capacity as legal representative of the company [include company name and qualification], I declare that the company, its direct and indirect controlling shareholders, and its subsidiaries, if any, adopt a zero-tolerance policy with regard to acts of corruption, fraud, money laundering, and terrorist financing, and any other acts that may be harmful to the national or foreign public administration and to the economic order.

In addition, to the extent legally and contractually permitted, in this act I undertake to report any violation that may be known to [society] or myself.

[Place and date]

Signature

Appendix V – Holding Report

Name: _____

CPF/ME : _____

I declare for the proper purposes:

1. I have fully observed the Personal Investment Policy, so that all investments held by me are in accordance with said policy, not characterizing infringement or conflict of interest.

2. I am aware of and in accordance with the content of the Personal Investment Policy, which becomes part of my obligations as an Member.

3. I am aware that non-compliance with the Personal Investment Policy, as of this date, implies serious misconduct, liable to the application of the appropriate sanctions, including dismissal for cause.

4. I acknowledge that the following table sets forth all my investments in Brazil and abroad, held by me in [month]of [year], except for assets exempt from reporting according to the Personal Investment Policy:

Issuer Name / Fund Name	Issuer's CNPJ / Fund	Asset Type	Asset Quantity	Ticket / CUSIP (if applicable)	Manager (if Fund)

OR

____ I do not hold assets that must be reported.

I declare that I have sent this form together with the consultation of the brokerage statement(s) provided to the Compliance Officer, containing information related to the assets that are to be reported, as requested above.

I certify that I have not been involved in any transaction involving securities that violates

the Personal Investment Policy.

5. To acknowledge, also, that the table below includes all the equity interests held by me in Brazil and abroad, in [MONTH] of [YEAR], as well as any positions held by me on boards, creditors' committees or other relevant professional activities that may result in potential conflicts of interest :

Company Name	Shareholding (%)	Voting Rights	Functions Performed

[CITY], [DAY] of [MONTH] of [YEAR].

_____

[MEMBER]