LUMINA CAPITAL MANAGEMENT LTDA.

COMPLIANCE MANUAL

March 2022

Version 1.0

Content

1. Definitions

The following terms shall have the meanings ascribed below:

"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.
"Anti-Corruption Law"	Law No. 12,846 of August 1st, 2013, as amended.
"COAF"	the Brazilian Council of Control of Financial Activities, Conselho de Controle de Atividades Financeiras.
"Compliance Officer"	the statutory Compliance Officer at Lumina. The Compliance Officer is the same person appointed as Legal Officer and AML/PTF Officer.
"Code of ART from ANBIMA"	Code of Administration of Third-Parties Resources of ANBIMA.
"CNPJ/ME"	National Registry of Legal Entities of the Brazilian Ministry of Economy, Cadastro Nacional da Pessoa Jurídica do Ministério da Economia.
"Confidential Information"	information deemed private, proprietary, or confidential or received by Members in relation to clients' activities or business, including personal data and sensible personal data, according to LGPD. Confidential Information may be in physical format (written on paper, email or recorded in disk) or not. Confidential Information includes information of Lumina or of its investors, which includes, but is not limited to: trade secrets, innovations, marketing plans, business plans, investor relations and information about investors 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, trading intentions and strategies, investment strategies, computer systems 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.
"Funds"	the investment funds under Lumina's management.
"General Personal Data Protection Law"	Law No. 13,709 of August 14th, 2018, as amended.
"Intellectual Property Law"	Law No. 9.279 of May 14, 1996, as amended.

"Internal Information"	information related to Lumina's business or operations that, although not necessarily confidential, implies certain kind of privacy. Examples include, but are not limited to, certain information regarding Lumina's internal controls or operational procedures, information regarding sellers, service providers, contractors and investments or other information which the discovery could be imposed by law or competent authority.
"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.
"Member(s)"	all partners, officers, and employees at Lumina.
"Person"	any individual, company, association or legal entity, or any other entity.
"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 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.
"IT"	Lumina's Information Technology department or group, including third-party services contracted for this purpose.

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 quotas of the Funds, provide securities advisory or manage managed portfolios ("carteiras administradas") or wealth portfolios ("gestão de patrimônio") and therefore is not subject to the rules applicable to these activities under Brazilian regulation.

Lumina and its Members abide by Brazilian law, applicable rules and regulations, and the Codes and Policies set forth in this Manual. The Codes and Policies herein were based on Brazilian law, applicable regulations (especially those of CVM and ANBIMA), and the best practices for governance and compliance.

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.

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 21 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 and Risk Management 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) 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;

(e) filing a complaint about acts of fraud, misconduct, corruption, AML/PTF, to the relevant authorities, as applicable;

(f) evaluating operations that may be suspected of money laundering and terrorist financing and filing them to COAF, as applicable;

(g) advising Members about the rules contained in this Manual and the compliance and AML/PTF rules applicable to their roles;

(h) developing and supervise training for Members according to the Training Policy contained herein;

(i) 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;

(j) supporting and encouraging compliance activities and programs;

(k) 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.

The Compliance Officer is the same person appointed as Legal Officer and AML/PTF 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.

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. 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 of Lumina's officers. Requirements such as their market reputation and profile are assessed, as well as their backgrounds.

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 guns 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) non-resident investors, especially those organized as trusts and companies with bearer bonds;

(b) high net worth investors whose funds are managed by areas of financial institutions focused on wealth management ("private banking"); and

(c) politically exposed persons, pursuant to the applicable law and regulations.

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 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 quotaholders 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.

Notwithstanding these provisions 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.

In the event Lumina decides to undertake distribution activities of its Funds and establishes relationships with its quotaholders, 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) 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.

Aiming to guarantee the efficacy and application of the herein above prohibitions, any contacts with public agents, by mailing, telephone, presential meetings or virtual meetings, may be supervised by the Compliance Officer.

8. Service Provider Selection, Contracting and Monitoring 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. 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, specially 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.

The monitoring shall comprise supervision based on risk, permitting to dispose more attention to the service providers that demonstrate more probability to present flaws in their action or represents a potential higher damage to the investors and to the integrity of the securities market, as classified below:

High risk: Service providers who are necessary to the functioning of the Funds, as determined by applicable law; service providers that have access to Confidential Information during the execution of the contracted service; and/or service providers that are not associated to ANBIMA or adheres to ANBIMA's Codes. Service providers classified in this category shall be monitored, at least, each 12 (twelve) months.

Medium risk: Service providers who are not essential to the functioning of the Funds, as determined by applicable law; and/or service providers that have access to Confidential Information during the execution the contracted service. Service providers classified in this category shall be monitored, at least, each 24 (twenty-four) months.

Low risk: other service providers that do not comply with the requirements of the classes herein above. Service providers classified in this category shall be monitored, at least, each 36 (thirty-six) months.

If any new event occurs, of if there is significative change that, according to the Member responsible for the monitoring of the respective service provider, the monitoring shall be immediately performed.

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

A. Contracting Broker-Dealers

When contracting broker-dealers for its Funds, in addition to the rules described above, Lumina shall consider (i) strict observance of fiduciary duties; (ii) proven execution capacity; and (iii) minimum financial impact. 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.

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. *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.

9. 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/or personal data, which may be governed by privacy and other laws and/or may be viewed as proprietary, always processing personal data in accordance with this Confidentiality Policy and the General Personal Data Protection Law.

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 privacy 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.

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) do 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 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; and

(i) 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 his/her 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 that is clearly 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 (excluding the personal data and personal sensitive data that are not owned by Lumina and are only object of treatment), 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 owned by 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 ensure the due compliance of this Policy and the Cybersecurity Policy herein after.

10. 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.

Lumina has several data prevention and protection 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;

(f) Members shall not open messages of unknown origin and suspicious links, even if they come from a known source;

(g) procedures for the protection of Confidential Information and Internal Information, according to the Confidentiality 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;

(a) members shall avoid entering websites from unsafe sources or opening personal emails or emails from unknown sources whenever they communicate through Lumina's technology assets;

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

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

(i) the 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;

(j) 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;

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

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

(m) 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;

(n) annual contingency tests and security tests focusing on logical segregation, penetration tests, response to data leakage events, traceability of access logs to sensitive information, and data processing carried out by external auditors under supervision of the Compliance Officer and IT.

In accordance with best practices, Lumina has developed a response plan for evidence, substantiated suspicion, or leakage 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, (i) 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; (ii) elaborate communication to impacted clients, if applicable, as well as to the National Data Protection Authority (Autoridade Nacional de Proteção de Dados – ANPD), informing them about the leak of information;

(c) the Risk and Operating Officer shall, as applicable, analyze data 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.

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.

Furthermore, periodic security tests shall be carried out focusing on logical segregation, penetration tests, response to data leakage events, traceability of access logs to sensitive information, and data processing, among others, always aiming to safeguard the data held by the Manager, especially the confidential ones. 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.

11. 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 Tecno Qualify. The primary contact at Tecno Qualify is Clayton de Camargo Campos at the phone # +55 11 98244-7988 or by email: 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.

12. 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 quotas 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 and Internal Information;

(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 premises 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.

13. 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, primarly, 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.

Furthermore, all Members shall acknowledge and agree to send a report to the Compliance Officer every six months informing their personal investments in shares and other securities equivalent to shares, in order to verify their compliance with this Policy. The Compliance Officer shall be responsible for filing these documents and ensuring their confidentiality.

All Members shall seek approval from the Compliance Officer before acquiring or entering into any transactions with debt securities and stock exchanges within the securities market of Brazil or any other Latin America country (or other equivalent securities), as well we with quotas of investment funds in Brazil or any Latin American country (or other equivalent securities). The Compliance Officer shall approve or reject the transaction after consulting the Portfolio Management Officer and shall guide the Member, as applicable, regarding eventual periods of restriction/prohibition of trading, during the Member shall not trade the respective securities.

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) notification to the Compliance Officer of receipt of materials with potential Confidential Information and/or Internal Information;

(c) 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;

(d) 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).

14. Risk Management Policy

A. Procedures Related to Risk Identification

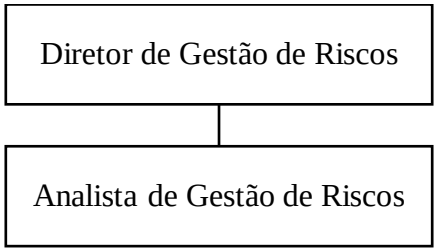
Lumina defines risk as the potential for permanent loss of invested capital. The goal of risk management is to obtain control and knowledge about the risks inherent to the asset management activity, aiming to adapt the strategies to the objectives of the investment funds and seeking to mitigate or reduce 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 evidences 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 Officer has the power to order the operation desk to adjust or reframe the positions in the Fund, without prejudice to consulting the Portfolio Management Officer, in order to better understand any specific investment strategies adopted. If an adjustment or reframe to the Fund is necessary, in accordance with the diversification rules contained in the Fund regulation, the Risk Management Officer shall inform the Portfolio Management Officer. In the event that such adjustment or reframe is not performed within a reasonable period of time, the Risk Management Officer shall (i) inform the trustee in order to obtain its support to adjust or reframe the Fund; (ii) determine that the purchase of any assets that exceed the Fund's risk limits be immediately ceased; (iii) elaborate a gradual divestment plan, deliberate on an action plan in conjunction with the Portfolio Management Officer and the Compliance Officer, and monitor its execution.

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:

(a) 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;

(b) operating risk level: Lumina shall analyze, among others, the nature and purpose of the transaction, guarantees offered, value and term;

(c) 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;

(d) 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 quotas 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 tradeability 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 only manages Funds established in the form of closed-end fund, without the possibility of redemption by quotaholders. If this scenario changes, Lumina shall adopt the rules described in this Policy for open-end funds, making the necessary changes and adaptations. In such case, the ANBIMA Liquidity Management Guidelines will be used

for liquidity matters. The Risk Management Officer shall be responsible for implementing the Liquidity Policy when applicable.

15. 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.

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.

16. 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 quotas in 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 into 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. 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.

17. Voting Rights Exercise Policy

Under the terms of ANBIMA's Rules and Procedures for Exercising Voting Rights at Meetings No. 02 of May 23rd, 2019, 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 with regard to 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 Lumina 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. 555 Funds:

a. changes in the investment policy that change the CVM class or the ANBIMA classification of the Fund, pursuant to ANBIMA's Rules and Procedures for Classification of 555 Funds;

b. changes of trustees or portfolio managers, as long as they are not members of the same conglomerate or economic group;

c. increase in the administration fee or creation of entry and/or exit fees;

d. changes in redemption conditions that result in an extension of the exit term;

e. merger, incorporation, or spin-off that may change the conditions set forth in the previous items;

f. liquidation of the Fund; and

g. quotaholders' 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. changes of trustees, portfolio managers, or real estate advisors, 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 quotas;

e. election of quotaholders’ 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 a state capital and remote voting is not possible;

II. the cost related to the exercise of Lumina's voting rights is not compatible with the share of the financial asset in the portfolio; and

III. the total share of the Funds managed by Lumina subject to voting, according to the fraction agreed upon at the general meeting or special shareholders' meeting, is less than 5% (five percent) and no Fund has individually more than 10% (ten percent) of the assets invested in the asset.

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 applicable regulations, the manager of the Funds under Lumina's management shall grant Lumina adequate powers and access to information for full exercise of voting rights. The manager of the Funds shall be responsible for sharing with Lumina meetings notices and agendas.

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 quotaholders, with the exception of 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 quotaholders.

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 Quotaholders

The results of the meetings in which Lumina exercises its voting rights shall be made available to quotaholders by the Fund manager. Likewise, the manager shall be responsible for the elaboration of a summary of the voting with due reasoning to CVM, according to applicable regulations.

Without prejudice to the obligations of the fund manager, Lumina shall disclose reports regarding its exercise of voting rights 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.

18. 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 Multimarket Funds and other Funds regulated by CVM Instruction No. 555;

(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.

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, provided that 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.

19. 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 the aforementioned 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.

20. 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), 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.

21. 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

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 among Members

2.1. Individual rights shall be respected in order to promote the workplace wellbeing. At every level of the organization, Members shall act in a careful, transparent, and responsible manner in relation to any commitments undertaken internally. The work environment should be permeated by courtesy, respect, team spirit, trust, and assiduity.

2.2. No Member is allowed to practice acts that represent disrespect, abuse of power, violence, retaliation, offense, physical or moral discomfort, harassment, and racial, sexual, religious, or disability discrimination.

2.3. As a principle, Lumina treats all Members in an impartial and fair manner and does not practice any kind of discrimination or favoritism.

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 quotaholders 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 quotaholders of the Funds; (iii) quotaholders 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; and (iv) Members shall inform any actual or potential conflicts of interest to the Compliance Officer.

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. Any gifts or benefits received by Members that total more than BRL 1,000.00 (one thousand reais) shall be previously approved by the Compliance Officer. Members shall not offer or accept gifts or economic advantages of any nature, which could be understood as improper attempts to influence the Member or any other person or company that has contracted or is seeking to contract with Lumina or on behalf of Lumina.

9.3. 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 intellectual property law clearly states that every invention and utility model is the sole property of the employer (in this case, Lumina), if they result from any work performed in connection with Lumina and while the agreement between the Member and Lumina is valid.

11.2. Every material that is in Lumina’s corporate network or in the personal computers used for work by its Members is the company’s property. Any information contained in such materials shall be solely used for performing the works of the Member and shall not be disclosed or retransmitted in any manner whatsoever.

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. 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 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.

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 aforementioned 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 termination 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 (i) 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 and (ii) acknowledge that to earn the benefits offered by Lumina to me and my dependents it will be necessary the sending and treatment of personal data and sensible data, according to LGPD.

In this sense, I declare my express agreement in relation to the treatment of my personal data and sensible data, according to Art. 7, I, of LGPD and, if applicable, in relation to the personal data and sensible data of my dependents, including minors, as requested by Art. 14, §1º of LGPD. In this context, I am aware that service providers of benefits or intermediates could have access to the following personal data and sensible data, as exemplified: CPF/ME, name, birthdate, banking data, health plan identification, information regarding the use of health plan, etc.

Full Name: _____

CPF/ME:_____

Date: ____/_____/_____

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.

With this in mind, the following are taken 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.
- 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.
- 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.

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