



fama
re.capital

investing for change

Compliance Manual

Compliance Manual

1. GENERAL STANDARDS

1.1 Introduction

Transparency, seriousness and impartiality are affirmative in the conduct of the business of fama re.capital Ltda, hereinafter “fama” or “Manager”.

This fama Compliance Manual (“Manual” or “Policy”) is the basis for the necessary action and formalizes the compliance procedures required in the exercise of the activities carried out by fama and its Employees (as defined below), whether in internal or external relations.

This Manual is based on the legal, regulatory and administrative provisions in force and applicable to fama, mainly, but not limited to, those described below.

1.2 Legal basis

All Employees must ensure that they fully understand the laws and regulations applicable to Manager, as well as the entire contents of this Manual. The main rules applicable to Manager's activities are:

- (i) Securities and Exchange Commission (“CVM”) Resolution No. 21 of February 25, 2021, as amended (“CVM Resolution 21/21”);
- (ii) CVM Resolution No. 50, of August 31, 2021, as amended (“CVM Resolution 50/21”);
- (iii) CVM Resolution No. 175, of December 23, 2022, as amended (“CVM Resolution 175”) and its Normative Annexes;
- (iv) Code of Ethics of the Brazilian Association of Financial and Capital Market Entities (“Anbima”) (“Anbima Code of Ethics”);
- (v) Code of Administration and Management of Third Party Resources (“AGRT Code”);
- (vi) Rules and Procedures for the Administration and Management of Third Party Funds, especially its Supplementary Appendix III;
- (vii) Law No. 12.846, of August 1, 2013 and Decree No. 11.129, of July 11, 2022, as amended (“Anti-Corruption Rules”);
- (viii) Law 9.613, of March 3, 1998, as amended; and
- (ix) Other manifestations and guidance letters from regulatory and self-regulatory bodies applicable to Manager's activities.

1.3 Interpretation and Application

For the purposes of interpreting the provisions of this Policy, unless expressly provided otherwise: (a) the terms used in this Policy shall have the meaning assigned in CVM Resolution 175; (b) references to Funds shall include Classes and Subclasses, if any; (c) references to regulations shall include annexes and appendices, if the provisions of CVM Resolution 175 have

been complied with; and (d) references to Classes shall include Funds not yet adapted to CVM Resolution 175.

The provisions of the Policy are applicable, where appropriate, to Funds set up after CVM Resolution 175 comes into force (i.e. 02/10/2023) and to Funds set up prior to this date which have already been adapted to the rules of said Resolution. fama and the Funds must comply with the rules of CVM Instruction 555 of December 17, 2014, as amended (“CVM Instruction 555”), and other instructions applicable to the different categories of Funds under management, including regarding fama's responsibility and attributions as manager of the Funds' portfolio until the date on which such Funds adapt to the rules of CVM Resolution 175.

1.4. Objective

The purpose of this Manual is to disseminate fama's policies and procedures, so that the organization properly exercises the best practices governing the capital markets.

1.5. Applicability

The rules set out in this Manual are binding on all those directly¹ or indirectly² involved (“Employees”) in fama's activities and do not exempt Employees from complying with the other obligations imposed by law and the regulations applicable to the activities carried out by fama. In the event of conflict, legislation, regulation and self-regulation shall take precedence over this Manual.

Any infringement will be dealt with by applying the corresponding disciplinary and judicial measures, without prejudice to reporting it to the competent authorities, where applicable.

All Employees must, upon joining the company, sign the Statement of Acknowledgement and Agreement, in accordance with Annex I of this Manual, confirming, among other things, that they have received a digital copy and are aware of the contents of this Manual.

1.6. Responsible parties

Responsibility for drawing up, maintaining and regulating the rules described in this Manual lies with the officer responsible for implementing and complying with fama's rules, policies, procedures and internal controls and CVM Resolution 21/21 (“Compliance, Risk and Prevention of Money Laundering and Combating the Financing of Terrorism (PLDFT) Officer”), as indicated in the Articles of Association.

1.6.1 Compliance and Risk Officer

Pursuant to article 4, item IV of CVM Resolution 21/21, the Manager has appointed a Statutory Officer, as indicated in the Manager's Articles of Association, as the Officer responsible for implementing and complying with the rules, policies, procedures and internal controls established in said Resolution and in ANBIMA's self-regulation and for the Manager's Compliance area (“Compliance and Risk Officer”).

¹Partners, directors, administrators, employees and interns.

² Service providers (consultants, auditors, etc.) who work on the premises of the Fama or who are providing some service to the Management Company and represent it before third parties.

Reporting directly to the Compliance and Risk Committee and functionally to the Management Committee, he has full authority over the implementation of the Manager's Compliance Program and has experience with capital market legislation and regulations.

Pursuant to CVM Resolution 21/21, the duties of the Compliance and Risk Officer in relation to his activity within the scope of the matters addressed in this Manual and in the Code of Ethics and Corporate Conduct (together "Manuals") are:

- To define the ethical principles to be observed by all Employees, contained in the Manager's Compliance Program or other documents that may be produced for this purpose, preparing their periodic review;
- Promoting the wide dissemination and application of ethical precepts in the development of the activities of all Employees, including through the training provided for in the Manuals;
- Monitoring compliance with the Manager's policies, especially those described in the Manuals;
- Identify possible conduct contrary to the company's Compliance Program and the rules applicable to Manager;
- Analyzing all cases that come to its attention regarding potential non-compliance with the ethical and compliance precepts set forth in the Manual or in the other documents mentioned herein, as well as analyzing cases not provided for in this Manual and defining the actions to be taken;
- Treating all matters that come to its attention with the utmost confidentiality and preserving the interests and institutional and corporate image of the company, as well as those of the Employees involved;
- Guarantee the confidentiality of any whistleblowers, even when they do not request it, except in cases where judicial testimony is required;
- Evaluating situations of non-compliance with the Manual, applicable policies and standards and defining the actions to be taken, including any necessary sanctions;
- Answering questions from employees and managing the channel for questions and suggestions;
- Analyzing situations that come to their attention that could be characterized as personal and professional "conflicts of interest", including, but not limited to, situations involving:
 - Personal investments;
 - Financial transactions with clients outside the scope of the fame;
 - Receipt of gratuities, favors/gifts from managers and/or partners of investee companies, suppliers or clients;
 - Financial analysis or transactions with companies whose partners, directors or employees the Collaborator has a personal relationship with; or

- Financial analysis or operations with companies in which the Collaborator has his/her own investment.
- Bring any requests for authorization, guidance or clarification or cases of occurrence, suspicion or evidence of practice that is not in accordance with the provisions of the Manual and other policies and rules applicable to the company's activity to the attention of the Compliance and Risk Committee or the Board of Directors, as the case may be;
- Discuss existing compliance controls and policies, suggesting new controls if necessary, among other matters related to the area; and
- Submit to the fame's management bodies, by the last working day of April each year, a report for the calendar year immediately preceding the submission date, containing: (a) the conclusions of the examinations carried out; (b) the recommendations regarding any deficiencies, with the establishment of timetables for remediation, where appropriate; and (c) the statement of the director responsible for the management of securities portfolios or, where appropriate, the director responsible for risk management regarding the deficiencies found in previous verifications and the measures planned, in accordance with a specific timetable, or effectively adopted to remedy them; said report must remain available to the CVM at fama's head office;

In addition, it is the responsibility of the Compliance and Risk Officer to implement internal controls and processes for the processing of personal data, including digital data, by natural persons or by legal entities governed by public or private law, with the aim of protecting the fundamental rights of freedom and privacy and the free development of the personality of natural persons, in accordance with Law 13.709/18 (General Data Protection Law - LGPD).

Discussion of policies and monitoring of issues related to the Manual and other policies will be carried out by the Compliance and Risk Committee or, where appropriate, the Board Committee.

1.6.2 Compliance and Risk Committee

fama has a Compliance and Risk Committee, with autonomy over fama's compliance and risk issues, which is made up of the Compliance and Risk Director, who acts as Chairman of the Committee, and professionals from the operations area.

The Compliance and Risk Committee meets at least monthly. This Committee shall be set up with the presence of at least two (2) members, one of whom must be the Chairman or, in his absence, whoever he appoints.

Decisions will be taken by the vote of the majority of those present, observing the mechanism for preventing voting in the event of a conflict of interest in relation to the areas under its direct supervision or itself. The Chairman shall have the “casting” vote in the event of a tie in the Committee's deliberations. It is the responsibility of the Compliance and Risk Director to argue that any member linked to the investment area is prevented from voting, if they fail to do so, in order to avoid a conflict of interest. Minutes of the meetings must be drawn up, which may be in summary form and filed in the Manager's Compliance management system.

The Compliance and Risk Committee is responsible for:

- Define, disclose and review the procedures of the rules, procedures and description of internal controls and other Policies of the firm;
- Providing guidance to Employees in the event of doubts regarding the application of fama's Policies and Manuals, which cannot be clarified directly by the Compliance area;
- Investigate and make certain decisions and approvals regarding Risk, Compliance, Prevention of Money Laundering and Combating the Financing of Terrorism, Anti-Corruption and Contingency Plans;
- Investigating complaints or indications of conduct potentially contrary to internal Policies and legal or regulatory standards, assessing the need to report to regulatory bodies or COAF, and also assessing and discussing internal sanctions, and may submit to the Executive Committee when deemed necessary;
- Coordinating any regulatory inspections, whether conducted by the CVM or ANBIMA; and
- Approve the offer of new products and services, including new investment strategies and types of classes managed, as well as the modification of relevant conditions of the products offered; and
- Whenever he/she deems it necessary or convenient, the Compliance Officer may take any matter within his/her competence to the Compliance and Risk Committee or Board Committee for consideration or deliberation.

1.6.3 Compliance and Risk Area (Operations)

The Compliance area is primarily responsible for disseminating and supervising the company's internal rules, controls and procedures, with a view to mitigating the operational, regulatory, reputational and legal risks of its activity. To this end, the area is staffed by professionals with the technical qualifications and experience required for their role, and systems defined in this Policy.

The following activities are the primary responsibility of the Compliance area:

- Providing advice and consultative support to the business areas, internal Committees, and the Board of Directors regarding rules and standards issued by regulatory and self-regulatory bodies;
- Managing the Code of Ethics and Conduct, ensuring that the fiduciary duty towards Investors is maintained, providing for and implementing procedures to mitigate any conflicts of interest, as well as ensuring compliance with the regulatory prohibitions set out in art. 18 of CVM Resolution 21/21.
- Implement Employee Training Programs, including, but not limited to, those aimed at Employees who have access to Manager's confidential information;
- Identifying, documenting and evaluating the risks associated with the compliance of the company's activities with regulatory precepts, analyzing the impact of offering new products and services or relationships with certain Investors that involve a degree of risk;

- Maintaining the regulatory forms, especially the Reference Form, taking responsibility for updating and reviewing these documents on a regular basis, including keeping the information updated on the fama and CVM websites;
- Monitor the main rules, guidelines and warnings issued by regulatory and self-regulatory bodies and keep an up-to-date regulatory agenda containing all the deadlines issued by such bodies, using electronic systems for this purpose;
- Carrying out periodic tests in order to monitor and evaluate the effectiveness of the Manager's Policies, procedures and the company's systems and controls, suggesting and following up on improvement actions resulting from such tests, and may use its own electronic system for this purpose and always keep evidence of the tests carried out;
- Carrying out access control tests on computer resources (internal directories and systems), as well as other tests to verify the functionality of the electronic systems used by fama and making effective backups of documents and systems available;
- Develop an internal controls report in accordance with article 25 of CVM Resolution 21/21, which must be drawn up annually and made available to the Compliance and Risk Committee for approval by the Compliance and Risk Director, who will send it to the Directors by the last working day of April for the calendar year immediately preceding the delivery date (based on the adherence tests referred to in the item above);
- Keeping the policies set out in Article 16 of CVM Resolution 21/21 up to date and available on the company's website, as well as those required to be publicized by ANBIMA;
- Providing for inspections and supervision by regulatory and self-regulatory bodies, third-party audits and due diligence, interfacing between their requests and fama's internal areas;
- Manage Money Laundering Prevention and Combating the Financing of Terrorism activities, implementing its own policy and procedures in order to prevent the occurrence of atypical situations and enabling their immediate identification in the event of occurrence and eventual communication to COAF, as provided for in CVM Resolution 50/21;
- Establishing the standard and approving communication and marketing materials, in accordance with the procedure established in the respective Manager's policy, based on the ANBIMA Code and other applicable ANBIMA Guidelines;
- Cross border issues: assessing regulatory issues applicable in the foreign jurisdictions with which the company carries out operations or is registered;
- Managing the policies for external activities and personal investments of Employees, including the granting of approvals when applicable, and periodic monitoring;
- Informing the CVM whenever it finds, in the course of carrying out its duties, the occurrence or evidence of a violation of the legislation that the CVM is responsible for monitoring, within a maximum of 10 (ten) working days of the occurrence or identification;

- Monitor Employees' corporate e-mails whenever it deems necessary;
- Verify, at least annually, whether the “Key Employees”, in particular the controlling partners and Managing Partners, are involved in administrative proceedings by regulatory and self-regulatory bodies, criminal proceedings of any nature, or other proceedings that may result in contingencies for the Manager and that, therefore, their public disclosure may be necessary, under the terms of CVM Resolution 21/21 and ANBIMA's self-regulation;
- Verify that the appropriate professionals in the Management area have their certification or exemption in force, keep the ANBIMA Database up to date, as well as verifying that all the procedures in the Policies for the Continued Certification of Employees and for the Selection and Hiring of Employees are being complied with;
- Confirm, through CVMWEB, by March 31st of each year, that the information contained in the fame registration form provided for in CVM Resolution 51/21 is still valid, as well as updating said registration form whenever any of the data contained therein is altered, within 7 (seven) business days of the fact that caused the alteration; and
- Carry out any other activities, monitoring, tests or internal controls expressly assigned to it by this Policy or other policies of Manager.

1.7 Sanctions

Failure to comply with the rules of this Manual, legislation, regulation or self-regulation, or the exercise of inappropriate conduct, will result in internal sanctions for the offending Employee, which may range from a simple warning to dismissal from the company.

Inappropriate conduct includes, but is not limited to:

- Insubordination;
- Theft of company property;
- Misuse or destruction of fame property;
- Violation of any rule set forth in the fame policy;
- Unauthorized use or exposure of confidential information;
- Forgery or alteration of records and documents;
- Being under the influence of, possessing, using or offering narcotic substances on fama premises;
- Carrying a firearm or similar on fama premises;
- Engaging in a competing activity; and
- Carrying out another activity which competes with the Collaborator's duties at fama or which, although not competing, impairs the performance of their duties at fama.

Any Employee who becomes aware of information or situations in progress that could affect fama's interests, generate conflicts or even prove to be contrary to the terms set out in this

Manual, must inform the Compliance, Risk and PLDFT Director, or any member of the compliance area, or any member of the Management Committee, in person or electronically, so that the appropriate measures can be taken.

Employees who commit or omit any unlawful act (criminal or administrative) as defined by law will be subject to investigation and legal proceedings, without prejudice to the right to claim compensation for losses and damages that they may incur.

The possible application of sanctions resulting from non-compliance with the principles established in this Manual is the responsibility of the Management Committee, at its sole discretion, guaranteeing the Collaborator, however, a broad right of defense. Penalties may include a warning, suspension, dismissal or exclusion for just cause, in the case of Employees who are partners of fama, or dismissal for just cause, in the case of Employees who are employees of fama, in the latter case, under the terms of article 482 of the Consolidation of Labor Laws - CLT, without prejudice to fama's right to claim compensation for any losses incurred, damages and/or lost profits, through the appropriate legal measures.

fama does not assume responsibility for Employees who break the law or commit infractions in the performance of their duties. If fama is held liable or suffers damage of any kind as a result of the actions of its Employees, it may exercise its right of recourse against those responsible.

1.8. Training Policy

1.8.1 Training and retraining process

fama has an initial training process for all its Employees, especially those who have access to confidential information or participate in investment decision-making processes.

As soon as each Employee is hired, he/she takes part in a training process in which he/she will acquire knowledge about fama's activities, its internal rules, especially this Manual, and will have the opportunity to clarify doubts related to such principles and rules, as well as about the main laws and rules governing fama's activities.

Nevertheless, fama believes that it is essential that all employees, especially those who have access to confidential information or participate in investment decision-making processes, always have up-to-date knowledge of its ethical principles, laws and regulations.

To this end, fama offers a retraining program for its Employees, which is offered at least every 24 months or as the rules and concepts contained in this Manual or relevant policies of the Manager are updated, with the aim of ensuring that they are always up to date.

1.8.2 Implementation and Content

The implementation of the initial training process and the ongoing retraining program is the responsibility of the compliance area and requires the commitment of Employees to the subject, who must dedicate themselves to understanding it, including all being obliged to certify that they have understood the standards and rules transmitted when there is no certification of completion issued by the retraining program.

Both the initial training process and the refresher program must cover the company's activities, its ethical principles and conduct, compliance rules, segregation policies, where applicable, and the other policies described in this Manual and separate policies of the Manager (especially

those relating to confidentiality, information security, cyber security and personal investments), as well as the penalties applicable to Employees arising from non-compliance with such rules, in addition to the main laws and regulations applicable to said activities.

Employees who work in the distribution of quotas of the classes of investment funds under FAMA's management and those who are directly linked to the operational routines will take part in specific training, in which they will receive instructions on commercial materials, the main applicable rules and other topics related to the distribution of quotas, under the terms of the item "Initial and Periodic Training" contained in FAMA's Distribution Manual.

The compliance area may hire specialized professionals to conduct initial training and refresher programs, depending on the subjects to be covered.

1.9 Communication Channel

In addition to direct contact with the Compliance, Risk and PLDFT Director, questions and suggestions can be sent to the e-mail etica@famarecapital.com.

2. COMPLIANCE RULES

2.1 Anti-corruption policy

2.1.1 Introduction

fama is subject to anti-corruption laws and regulations, including, but not limited to, Law No. 12.846/13 and Decree No. 8.420/15 ("Anti-Corruption Regulations").

Any violation of this Anti-Corruption Policy and the Anti-Corruption Rules may result in severe civil and administrative penalties for fama and/or its Employees, as well as reputational impacts, without prejudice to the possible criminal liability of the individuals involved.

2.1.2 Scope of Anti-Corruption Standards

The Anti-Corruption Rules establish that legal entities will be held objectively responsible, in the administrative and civil spheres, for harmful acts committed by their partners and collaborators against the national or foreign public administration, without prejudice to the individual responsibility of the author, co-author or participant in the illegal act, to the extent of their culpability.

The following are considered public officials and therefore subject to the Anti-Corruption Rules, without limitation: (i) any individual who, even temporarily and without compensation, is in the service of, employed by or holds a public position in a government entity, an entity controlled by the government, or an entity owned by the government; (ii) any individual who is a candidate for or is holding public office; and (iii) any political party or representative of a political party.

Foreign public administration is considered to state bodies and entities or diplomatic representations of a foreign country, at any level or sphere of government, as well as legal entities controlled, directly or indirectly, by the public authorities of a foreign country and public international organizations.

The same requirements and restrictions also apply to family members of civil servants up to the second degree (spouses, children and stepchildren, parents, grandparents, siblings, uncles and nephews).

Representatives of public pension funds, notaries and advisors to public officials should also be considered “public officials” for the purposes of this Anti-Corruption Policy and the Anti-Corruption Rules.

2.1.3 Definition

Under the terms of the Anti-Corruption Rules, harmful acts against the public administration, whether national or foreign, are all those that violate national or foreign public assets, public administration principles or international commitments made by Brazil, as defined below:

- Promising, offering or giving, directly or indirectly, an undue advantage to a public official, or to a third party related to them;
- Proven financing, funding, sponsoring or in any way subsidizing the practice of illicit acts provided for in the Anti-Corruption Rules;
- Proven use of an individual or legal entity to hide or conceal their real interests or the identity of the beneficiaries of the acts committed;
- Regarding tenders and contracts:
 - frustrating or defrauding, by means of an arrangement, combination or any other expedient, the competitive nature of a public bidding procedure;
 - preventing, disturbing or defrauding the performance of any act of a public bidding procedure;
 - removing or seeking to remove a bidder, by means of fraud or offering an advantage of any kind;
 - defrauding a public tender or contract arising from it;
 - fraudulently or irregularly creating a legal entity in order to participate in a public bidding process or enter into an administrative contract;
 - fraudulently obtaining an undue advantage or benefit from modifications or extensions to contracts entered into with the public administration, without authorization by law, in the public bid invitation or in the respective contractual instruments; or
 - manipulating or defrauding the economic and financial balance of contracts entered into with the public administration.
- Hindering the investigation or inspection activities of public bodies, entities or agents, or interfering in their activities, including within the scope of regulatory agencies and national financial system inspection bodies.

2.2 Confidentiality and secrecy of information

In order to safeguard the privacy of clients' personal or financial information, the confidential nature of data, information, communications, balances, positions and any other type of information relating to clients that is not known to the public shall prevail, as a rule and in any doubtful situation. Employees must preserve the confidentiality of any information relating to clients obtained in the course of their activities related to fama, whether of a personal or professional nature, even after their relationship with fama has ended. Failure to observe confidentiality will be subject to liability in the civil and criminal spheres.

It is forbidden to reveal the portfolios and strategies of all products analyzed or managed by fama to any non-Collaborator, whether from the press, personal circle, immediate family connection or marital status. Failure to comply with this item will be subject to liability in the civil and criminal spheres.

Furthermore, considering fama's role as an asset manager, insider information is any relevant information regarding any security that has not been publicly disclosed and that is obtained in a privileged manner (as a result of the professional or personal relationship maintained with a client, with people linked to analyzed or invested companies or with third parties).

Examples of inside information are: verbal or documented information about a company's operating results, corporate changes (mergers, spin-offs and takeovers), information about the purchase and sale of companies, securities, including initial public offerings (IPOs), and any other fact that is the subject of a confidentiality agreement signed by a company with the public or a third party.

Inside information must be kept confidential by anyone who has access to it, whether as a result of professional activity or personal relationship.

Anyone who has access to inside information must immediately disclose it to the Compliance, Risk and PLDFT Officer, and must not disclose it to anyone, not even to other Employees, market professionals, friends and relatives, or use it for their own benefit, for the benefit of Fame and its investment fund classes, or for the benefit of third parties. If there is any doubt about the privileged nature of the information, the person who has access to it must immediately report it to the Compliance, Risk and PLDFT Officer. Anyone who has access to inside information must also completely restrict the circulation of documents and files containing this information.

The use, including as front running³, and preferential disclosure, to anyone, of confidential, secret or privileged information is prohibited.

Requests for information from bodies such as the Central Bank, CVM, Internal Revenue Service, Public Prosecutor's Office or judicial, arbitration or administrative proceedings must be forwarded to the Compliance, Risk and PLDFT Officer for appropriate action.

³ illegal practice of obtaining advance information about the execution of operations on the stock exchange or over-the-counter markets and which will influence the formation of prices of certain investment products.

2.3 Trading in shares with Relevant Information

All Employees must handle, disseminate and use Material Information in accordance with specific regulations and the general principles set out in this Manual and in the Personal Investment Policy.

The term “Relevant Information” will have the same definition in this Manual as in Brazilian corporate law and CVM instructions, notably CVM Resolution 44/23.

Employees are prohibited from trading, advising or assisting investments in securities with knowledge of any Material Information that has not been properly disclosed to the market.

Should any Employee receive or become aware of any Material Information from any issuer, such Employee must immediately inform the Compliance, Risk and PLDFT Officer of the possession of the material information.

- In the event of the above paragraph, it shall be strictly forbidden for the Employee and fama to trade any securities of said issuer, whether for their own benefit, for the benefit of third parties or for the benefit of any classes of funds or portfolios managed by fama, until the relevant information has been properly disclosed to the market;
- The Compliance, Risk and PLDFT Officer shall, whenever he receives a communication under the terms of the paragraph above, block any and all trading in securities of the issuer involved until the relevant information is properly disclosed to the market;
- The Employee may not transmit any Material Information to any person, unless the provision of such Material Information is necessary to comply with the provisions of this Manual or is strictly necessary for the performance of the duties or position held by the Employee (in this case, the Employee must alert the recipient to the fact that this is Material Information, which may not be disclosed or used for trading in the issuer's securities).

If the Employee has any doubts about the appropriate treatment of any information, he/she should request a meeting with the Compliance, Risk and PLDFT Officer to assess the materiality of the information and the need to comply with the rules set out herein.

Even after its disclosure to the public, fama and its Employees shall continue to treat Material Information as not having been disclosed until a reasonable time has elapsed for market participants to have received and processed the Material Information.

The rules stipulated in this section apply to any Relevant Information, regardless of the way such Relevant Information was obtained.

2.4 Intellectual Property

All documents developed while carrying out fama's activities or directly related thereto are the intellectual property of the Manager. These include files, models, methodologies, formulas, projections, analyses, manuals and reports.

The use and disclosure of any item subject to fama's intellectual property may only be carried out with the express written authorization of the Compliance, Risk and PLDFT Officer.

All Employees must sign the Responsibility and Confidentiality Agreement set out in Annex II hereto upon their admission.

In the event that an Employee, upon being admitted, makes available to Manager documents, spreadsheets, files, formulas, evaluation, analysis and management models or similar tools for the purpose of carrying out his/her professional activity with Manager, the Employee shall sign a statement pursuant to Annex III hereto, confirming that: (i) the use or availability of such documents and files does not infringe any contracts, agreements or confidentiality commitments, nor does it violate any intellectual property rights of third parties; and (ii) any alterations, adaptations, updates or modifications, of any form or kind, to such documents and files shall be the exclusive property of Manager, and the Employee may not appropriate or make use of such altered, adapted, updated or modified documents and files after his/her termination from Manager, unless expressly approved by Manager.

Once the employment or partnership relationship has been severed, the former employee of the company remains obliged to comply with the restrictions set out in the previous item, subject to liability through the courts.

2.5 Controls on access to Confidential Information

All access to Management's directories and information systems must be controlled. Only Employees previously authorized by the Compliance and Risk Officer may access these directories and information systems.

Control of access to Manager's information systems shall take into account the following premises:

- Ensuring that the level of access granted to the Employee is appropriate to his/her profile; and
- Immediate cancellation of access granted to Employees who have been dismissed, removed or whose role in Manager has changed.

2.6 Information control barriers

Employees holding Confidential or Privileged Information, as a result of their positions or duties at Manager, must establish an information barrier for other Employees. In a non-exhaustive manner, the following conduct must be observed:

- Employees must avoid circulating in environments outside Manager with copies (physical or digital) of files containing Confidential Information, and these copies must be encrypted or kept by means of an access password;
- Information that enables the identification of a Manager's client should be limited to files with restricted access and should only be copied or printed if it is in the interests of Manager or the client itself;
- Employees must be alert to external events that may jeopardize the confidentiality of Manager's information, such as computer viruses, fraud, etc;
- Confidential matters should not be discussed in public environments or places considered exposed; and
- The disposal of Confidential Information in digital or physical form must be done in such a way as to make it impossible to recover.

In this regard, all Employees must carefully read and understand the provisions of this Manual, as well as sign the confidentiality agreement contained in Annex II to this Manual.

2.7 Identification of information holders, maintenance of records and logs

The Compliance and Risk Officer shall keep a record of the Employees who hold Inside Information, indicating the type of information held, and shall inform the Compliance and Risk Committee or the Board of Directors Committee of any Inside Information held by Employees which may restrict Manager's operations.

Each account or access device to computers, systems, databases and any other information asset will be assigned to a person identifiable as a natural person, with the individual login users of internal Employees being their responsibility and the login users of third parties being the responsibility of the manager of the contracting area. In this way, it is possible to identify the owners of the information so that they can be held responsible, if necessary.

With regard to monitoring and auditing the environment, Management has monitoring systems in place for workstations, servers, email, internet connections, mobile or wireless devices and other network components. The information generated by these systems can be used to identify users and their respective accesses, as well as the material handled.

The Manager also informs that it may take the following measures:

- make public the information obtained by the monitoring and auditing systems, in the event of a judicial requirement or by order of the Compliance and Risk Officer;
- carry out, at any time, a physical inspection of the machines it owns; or
- install preventive and detectable protection systems to guarantee the security of information and access perimeters.

Failure to comply with the requirements set forth in this Policy will result in a violation of Manager's internal rules and will subject the user to the applicable administrative and legal sanctions, subject to the provisions of the item on Sanctions in Manager's Manual.

For purposes of illustration, the following is a non-exhaustive list of possible examples that may result in sanctions: illegal use of software; introduction (intentional or not) of computer viruses; attempts at unauthorized access to data and systems; or disclosure of Manager's sensitive information.

2.8. Database Protection

Manager's computer resources must be: (i) protected against tampering; and (ii) allow audits and inspections to be carried out.

All electronic records held by the Manager must be kept and available to meet the legal and regulatory deadlines set by local regulatory bodies and jurisdictions in which the Manager operates in a regulated market.

Information kept in electronic media must be saved in replicated databases (backups) and must remain intact and accessible for a period of no less than five (5) years. Access to these databases must be limited to persons authorized by the Compliance department.

Access as a desktop “administrator” is limited to users approved by the Compliance Officer and, with this, appropriate privileges/credentials and user access levels will be determined for Employees.

The Manager maintains different levels of access to electronic folders and files according to the functions and seniority of the Employees. Login and password combinations are used to authenticate authorized persons and grant access to the part of the Manager's network necessary for the performance of its activities.

2.9 Leakage of Confidential Information

Employees must report to the Compliance area any cases of violations of information security rules of which they become aware. Any violation or deviation is investigated in order to determine the necessary measures to correct the failure or restructure processes. In the event of a leak of confidential information by electronic means, the Compliance and Risk Officer will discuss with the Cyber Security Officer the best effective recovery plan and measures to minimize and prevent damage.

2.10. Information Security Testing and Training

The Manager will carry out periodic security tests on information systems (not limited to, but electronic media), at least annually, in order to reduce the risk of loss of confidentiality, integrity and availability of information assets.

Training on information security will be part of the Manager's initial and periodic training, as provided for in the Manual's Training Policy, which should consider, among other things, ensuring that all Employees are aware of the procedures and obligations provided for herein, as well as minimizing the occurrence of security incidents due to problems in the use, misappropriation of information, fraud and interpretation of the rules and procedures.

2.11. Disclosure of Material Facts

Although it is the responsibility of the fund's fiduciary administrator to operationalize the disclosure of any material fact occurring or related to the operation of the funds, the class or the assets in the portfolio, as soon as they become aware of it, it is the responsibility of the other service providers, including the Manager, to immediately inform the fiduciary administrator of any material facts of which they become aware, so that they can be duly disclosed.

In this sense, under the terms of article 64, paragraph 1 of the General Part of CVM Resolution 175, any facts that may have a significant influence on the value of the shares or on the decision of investors to acquire, redeem, sell or hold shares are considered material.

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

- change in the tax treatment of the fund, class or shareholders;
- the hiring of a market maker and the termination of this service;
- hiring a risk rating agency, if not established in the fund's regulations or in the class annex;
- change in the risk rating attributed to the funds, class or sub-class of quotas;
- change of essential service provider;

- merger, incorporation, spin-off or transformation of the funds or class of shares;
- alteration of the organized market where the trading of fund quotas is admitted;
- cancellation of the admission of fund or class shares to trading on an organized market; and
- issuance of shares in closed-end funds.

Material facts may, exceptionally, not be disclosed if it is understood by the Manager and the funds' fiduciary administrator that their disclosure jeopardizes the legitimate interests of the funds or their shareholders. In this case, such information will be treated as confidential until the Manager deems it appropriate to disclose it.

On the other hand, the trustee is obliged to immediately disclose material facts in the event that the information is beyond its control or if there is an atypical fluctuation in the quotation, price or quantity of shares traded, in the event of trading on a regulated market. The Manager shall notify the trustee if it becomes aware of any such situation.

The Manager shall make the relevant facts relating to the funds under its management available on its website.

2.12. Manager's website

The Manager's website must make available the Policies required by CVM Resolution 21, as well as the following documents and information relating to the investment funds under management, as required by the regulations in force:

Document or Information ⁴	Legal Basis
Updated Regulation, Annexes and Appendices	Art. 47, General Part, CVM Resolution 175
Description of the taxation applicable to the investment fund and/or Class	Art. 47, General Part, CVM Resolution 175
Voting Policy	Art. 47, General Part, CVM Resolution 175
Periodic and occasional information on each investment fund and/or Class	Art. 61, General Part, CVM Resolution 175
Material Facts	Art. 64, §2, General Part, CVM Resolution 175
Call to the general shareholders' meeting of the investment fund and the special shareholders' meeting of the classes and subclasses	Art. 72, General Part of CVM Resolution 175
Identification of contracted Service Providers	Art. 48, item I, CVM Resolution 175
Statement of performance of financial investment funds	Art. 13 of Annex I (FIFs), CVM Resolution 175
Financial investment funds sheet (if any)	Art. 13 of Annex I (FIFs), CVM Resolution 175

⁴ The following documents may, alternatively, be made available exclusively on the fiduciary administrator's website, as agreed between the Essential Service Providers: performance statement, sheet, regulations, annexes and appendices, description of the taxation applicable to the Fund or class.

2.13. Maintenance of the Reference Form and other Forms

In order to comply with CVM Resolution 21/21, the Compliance area must send the Reference Form through the CVM's electronic system by March 31st of each year.

When preparing and reviewing the Reference Form, the Compliance area must ensure that the information contained therein is true, complete and does not mislead the investor, as well as being in simple, clear, objective and concise language.

The Compliance area is responsible for keeping the Reference Form updated on the company's website and making the most up-to-date version available to the CVM, reviewing it in full at least annually and whenever there are significant changes to the company, its structure and activities.

The Compliance area will also be responsible for preparing, maintaining and updating other regulatory forms, including but not limited to those requested by ANBIMA, in accordance with the internal system maintained by the Compliance area, and under the terms of the regulations applicable to fama's operations.

2.14. Annual Compliance Review

At least once a year, the Compliance area must conduct a complete review of the entire Compliance Program, which includes this Policy, the regulatory agenda, the controls and systems used to manage Compliance, the training program, including that of the Compliance area itself, reviews of forms and adherence tests, detailed in an internal system.

As a result of the annual review, the Compliance area must draw up a report on the conclusions of internal controls, as referred to in article 25 of CVM Resolution 21/21, which must follow the terms of the company's own model.

Version Control	
Jun-2010	version 0
Mar-2013	version 1
Jun-2016	version 2
Apr-2017	version 3
Jan-2019	version 4
Jun-2021	version 5
Nov-2022	version 6
Oct-2024	version 7

ANNEX I

Statement of Acknowledgement and Agreement for Fame Members

I, _____ registered with the Brazilian Individual Taxpayer Registration (“CPF/MF”) _____, hereby declare that:

(i) have received, read and understood fama's Compliance Manual and am aware of the guidelines established and their relevance to me and the company; and

(ii) I have participated in fama's integration and initial training process, where I was made aware of the principles and rules applicable to my activities and those of fama and had the opportunity to clarify any doubts related to these principles and rules, so that I have understood them and undertake to comply with them fully in the performance of my activities, under penalty of being subject to the punitive and termination measures provided for in the employment contract and current legislation, as well as participating in the ongoing training program.

Date: _____

Employee's signature: _____

ANNEX II

Term of Responsibility and Confidentiality

I, _____, registered with the CPF/MF under no. _____, hereinafter referred to as Employee, and fama re.capital Ltda., registered with the National Register of Legal Entities (“CNPJ/MF”) under no. 00.156.956/0001-87 (“MANAGER”) hereby resolve, for the purpose of preserving the personal and professional information of clients and the MANAGER, to enter into this Responsibility and Confidentiality Agreement (“Agreement”), which shall be governed in accordance with the following clauses:

1. The following are considered confidential information (“Confidential Information”) for the purposes of this Agreement:

a. Any type of information written, verbal or presented in tangible or intangible form, which may include: know-how, techniques, copies, diagrams, models, samples, computer programs, technical, financial information or information related to investment or commercial strategies, including balances, statements and positions of clients and of the classes managed by the MANAGER, structured operations, other operations and their respective values, analyzed or carried out for the class of the investment fund managed by the MANAGER, structures, action plans, client relationships, commercial counterparties, suppliers and service providers, as well as strategic, marketing or other information of any nature relating to the activities of the MANAGER and its partners or clients, regardless of whether this information is contained on pen drives, hard drives, other types of media, cell phones or physical documents.

b. Information accessed by the Employee as a result of the performance of his/her activities at the MANAGER, as well as strategic or market information and other information of any nature obtained from partners, managing partners, employees, trainees or interns of the MANAGER and/or subsidiaries or affiliated companies, affiliated or controlled by the MANAGER, or from its representatives, consultants, advisors, clients, suppliers and service providers in general.

1.1. Any information which: (i) is already in the public domain at the time it was obtained by the Employee; (ii) becomes in the public domain after the Employee becomes aware of it, without the disclosure being made in violation of the provisions of these Terms; (iii) is already legally known to the Employee before it has been disclosed to him/her and he/she has not received such information in confidence; (iv) are legally disclosed to the Employee by third parties who have not received them under an obligation of confidentiality; (v) are or are disclosed or requested by judicial order, by the Public Power and/or by the competent authority, in which case the Employee must immediately inform the Compliance and Risk Officer of the MANAGER so that the appropriate legal measures may be taken, subject to the provisions of item 5 of these Terms.

2. The Employee undertakes to use the Confidential Information to which he/she may have access strictly and exclusively for the performance of his/her activities at the MANAGER, and therefore undertakes, subject to the provisions of the MANAGER's Policies, not to disclose such Confidential Information for any purpose or to any person outside the MANAGER, including, in the latter case, the Employee's spouse, partner, ascendant, descendant, any person of close relationship or financial dependent.

- 2.1. The Employee undertakes, during the term of this Agreement and for an indefinite period after its termination, to maintain absolute personal and professional confidentiality of the Confidential Information to which he/she had access during his/her period at GESTORA.
 - 2.2. The obligations assumed herein shall continue to apply in the event that the Employee is transferred to any subsidiary or company related to, affiliated with or controlled by the MANAGER.
 - 2.3. Non-compliance with confidentiality and secrecy, even after the term of this Agreement has expired, shall be subject to liability in the civil and criminal spheres.
3. The Employee understands that the unauthorized disclosure of any Confidential Information may cause irreparable damage and no legal remedy for the MANAGER and third parties, and the Employee is hereby obliged to indemnify the MANAGER, its partners and third parties who have suffered damage, under the terms set forth below.
 - 3.1. Failure to comply with the terms set forth above shall be considered a civil and criminal offense, including classification as just cause for the purposes of termination of the employment contract, when applicable, pursuant to article 482 of the Consolidation of Labor Laws, and termination or exclusion for just cause of the Employee if he/she is a partner of the MANAGER, without prejudice to the MANAGER's right to claim compensation for any losses incurred, damages and/or lost profits, by means of the appropriate legal measures.
 - 3.2. The obligation to indemnify the Employee in the event of disclosure of Confidential Information shall subsist for the period during which the Employee is obliged to keep the Confidential Information referred to in items 2 and 2.1 above.
 - 3.3. The Employee is aware that he/she will be responsible for proving that the information improperly disclosed is not Confidential Information.
4. The Employee acknowledges and is aware that:
 - a. All documents related directly or indirectly to Confidential Information, including contracts, draft contracts, letters, presentations to clients, e-mails and all types of electronic correspondence, computerized files and systems, applications on mobile devices, spreadsheets, action plans, evaluation, analysis and management models and memoranda prepared by the Employee or obtained as a result of the performance of his/her activities at the MANAGER are and shall remain the exclusive property of the MANAGER and its partners, for which reason he undertakes not to use such documents, now or in the future, for any purpose other than the performance of his activities at the MANAGER, and all documents shall remain in the possession and custody of the MANAGER, unless, due to the MANAGER's interests, it is necessary for the Employee to keep such documents or copies thereof outside the MANAGER's premises;
 - b. In the event of termination of the Employee's individual employment contract, dismissal or exclusion, the Employee shall immediately return to the MANAGER all documents and copies containing Confidential Information in his/her possession;

c. Pursuant to Law 9. 609/98, the database, computerized systems developed internally, computerized analysis, evaluation and management models of any nature, as well as electronic files, are the exclusive property of the MANAGER, and their total or partial reproduction, by any means or process; their translation, adaptation, rearrangement or any other modification is strictly prohibited; the distribution of the original or copies of the database or its communication to the public; the reproduction, distribution or communication to the public of partial information, the results of operations related to the database or, furthermore, the dissemination of rumors, being subject, in the event of infringement, to the penalties provided for in said law.

d. It is expressly forbidden for Employees to install software not approved by the MANAGER on their equipment.

e. The password provided for access to the institutional data network is personal and non-transferable and must not, under any circumstances, be disclosed to another person.

5. In the event that the Employee is requested by Brazilian or foreign authorities (in oral questions, interrogations, requests for information or documents, notifications, summonses or subpoenas, and investigations of any nature) to disclose any Confidential Information to which he/she has had access, the Employee must immediately notify the MANAGER, allowing the MANAGER to seek the appropriate judicial measure to comply with or prevent the disclosure.

5.1 If the MANAGER is unable to obtain a court order to prevent the disclosure of the information in due time, the Employee may provide the Confidential Information requested by the authority. In this case, the provision of the Confidential Information requested shall be restricted exclusively to that which the Employee is obliged to disclose.

5.2 The obligation to notify the MANAGER subsists even after the termination of the individual employment contract, the dismissal or exclusion of the Employee for an indefinite period.

6. This Agreement is an integral part of the rules governing the Employee's employment and/or corporate relationship with the MANAGER, who by signing it is expressly accepting the terms and conditions set forth herein.

6.1 Any breach of any of the rules described in this Agreement, without prejudice to the provisions of item 3 et seq. above, shall be considered a breach of contract, subjecting the Employee to the sanctions attributed to him/her as described in the Manager's Manual or policies.

Therefore, agreeing with the aforementioned conditions, they sign this Agreement in 02 counterparts of equal form and content, to produce a single effect.

Date: _____

Signature of Employee: _____

Signature of the Compliance Officer: _____

ANNEX III**Intellectual Property Agreement**

I, _____, registered with the CPF/MF under no. _____, hereinafter referred to as the Collaborator, hereby declare for all due purposes:

(i) that Employee has made available to fama (“MANAGER”), on this date, the documents contained [on the __ brand pen drive, serial number __/ in the virtual storage system (cloud) of the provider _____ associated with the account with the same provider, with the e-mail address _____ / in the electronic correspondence forwarded by the e-mail address _____] (“Documents”), as well as its future use by Manager, does not infringe any confidentiality contracts, agreements or commitments that the Employee has entered into or is aware of, nor does it violate any intellectual property rights of third parties;

(ii) acknowledging and agreeing that any changes, adaptations, updates or modifications, in any form or kind, to the Documents shall be the exclusive property of Manager, and Employee may not appropriate or make use of such changed, adapted, updated or modified documents and files after his/her termination from Manager, unless expressly approved by Manager.

For all due purposes, the Employee certifies that the Documents have been duplicated by the Manager and that their content is identical to that made available by the Employee.

The [pen drives] form an integral part of these terms and conditions for all legal purposes. The list of files made available can be found in the Appendix to this agreement.

Date: _____

Employee's signature: _____

Appendix

List of files made available by the Collaborator