Internal Controls Policy

MAR Asset Management Gestora de Recursos Ltda.

Purpose of Policy

Establish a set of internal rules and principles to be adopted by MAR Asset Management Gestora de Recursos Ltda. (“MAR”) and its Employees (as defined below) to outline appropriate responsibilities and practices to ensure compliance with applicable regulatory rules and standards.

To whom does it apply?

MAR partners, as well as MAR executives, employees, service providers, consultants, interns and temporary staff (hereinafter referred to as “Employee(s)”).

Summary

I. Introduction

MAR's Internal Controls Policy ("Policy") reaffirms the commitment to comply with the legislation and regulations in force, combined with behavior based on the best market practices and the highest standards of ethics, integrity, honesty, and professionalism, and must be analyzed in conjunction with MAR's Code of Ethics and Conduct (“Code”) and the principles listed therein.

This Policy was adopted to assist Employees in the decision-making process with the description of the best practices expected by MAR, as well as guidance on a variety of subjects. However, it is not possible to exhaust all topics, and the Employee must contact the Chief Compliance Officer directly to resolve any doubts.

II. Confidentiality

The information obtained by Employees about clients/shareholders cannot, under any circumstances, be disclosed internally, unless another Employee must have access to the same information or if the disclosure is necessary considering MAR's internal policies.

Thus, the use of confidential information outside the work environment is also prohibited.

In the execution of their duties, the Employees must sign, together with the other documents of the “Know your Employee” Form, a declaration that they will observe such confidentiality rules, under penalty of fair dismissal.

Given the current dimensions of MAR and the fact that the company does not carry out the activity of distributing its investment funds, Employees will not have access to a few numbers of customer information. Thus, the barrier to information will be extended to all Employees who will sign such commitment through the referred Form "Know Your Employee".

Privileged information regarding investments and investment strategies will be held exclusively by the management team and the Chief Compliance Officer, and employees or service providers from unrelated areas should not have access to this type of information.

III. Privacy

To establish a safe and reliable environment for its customers, MAR has a privacy barrier that designates the responsibilities and information that are essential for each of the Collaborators involved to control the risk in conducting business and confidential information to its customers.

Considering that, currently, MAR does not carry out the activity of distributing the quotas of the investment funds and performs only the management, confidential information of clients is all maintained by the company that carries out the distribution of our quotas, being responsible for the custody and maintenance of such information.

Thus, the segregation of information security is focused on the control of internal information, such as spreadsheets, documents and risk reports, minutes, and corporate documents, mainly from the Ethics and Compliance Committee, "Know Your Employee" forms, among others (together, such internal information will be designated and referred to as "Confidential Information"). Such control is given by the following principles:

- Segregation of attributions: each Employee will be responsible for the information of the area to which he/she is linked, with the other Employees not having access to information from other areas, only if strictly necessary, and the Chief Compliance Officer must control access to folders through the internal storage system Google Drive. More details on such segregation can be found in chapter V. Segregation of Activities in this Policy.

- Security Measures: Information security measures must be selected based on business requirements, through risk assessments, economic efficiency, and legal restrictions.

- Avoiding Incidents: Employees responsible for maintaining the information must monitor their respective computers to detect any breaches or abnormalities in security and immediately report any internal information leakage to the Chief Compliance Officer.

- Shared Systems: The access of Employees to the specific systems of their areas will only be authorized by the Board of Directors of each area that is responsible for such system. Thus, each user will be responsible for keeping their password and other access information.

- Owners of information assets: all Confidential Information assets must have an explicit owner, who will be responsible for the appropriate classification and definition of requirements for the protection of all information assets entrusted thereto.

- Information Technology Training: the Compliance area may provide specific training on MAR's data storage and security measures, being allowed to also invite IT specialists or contracted outsourcers to assist in such specific training.

More detail on measures that help to follow MAR principles about information security will be given in chapter V. Segregation of Activities.

Any non-compliance with the guidelines of this Chapter will be analyzed directly by the Ethics and Compliance Committee.

III.1. Employees' Responsibilities

Employees have the following responsibilities with this Policy:

- Ensure that MAR's technological resources and information are used in accordance with this Policy.

- Confidential Information when printed by Employees must be immediately removed from the printer and torn up when not needed.

- Employees must not leave papers containing Confidential Information without proper storage when away from the workplace (clean desk policy), and they must also always lock their computers when they leave their workstation.

- Only use MAR's Google Drive to save Confidential Information, not being allowed to store such information in systems or programs other than those authorized directly by this Policy or expressly by the Chief Compliance Officer.

- Protect personal Information against unauthorized access, modification, destruction, or disclosure by MAR, being responsible for the proper use of the information it has access to, which includes, in addition to Confidential Information, passwords to access Google

Drive, corporate email, wi-fi, etc., and sharing of such information by outside parties is not permitted.

- In relation to passwords and access information, Employees: (i) cannot share the password, write it down or save it on easily accessible files; (ii) cannot use simple codes such as their name, date of birth, names of relatives, telephone numbers, words in the dictionary or sequential numbers; (iii) should preferably use different passwords for corporate use and personal use; and (iv) shall change passwords periodically and whenever they suspect something.

- When using corporate email, Employees: (i) must always use corporate email to communicate with MAR's counterparties or to deal with any matters related to MAR's day-to-day activities, the use of personal accounts to that end; (ii) when receiving emails with links, verify that it corresponds to the address that appears on the screen; and (iii) do not open, under any circumstances, if they are not sure of the origin of the sending and the legitimacy of the email.

- Regarding the use of the shared internet network in the work environment, Employees: (i) may not upload or download illegal software or data; (ii) are not allowed to download or send music, videos, or any other files that may compromise the proper functioning of the local infrastructure or that violate copyright laws; and (iii) shall not download software from unknown sources or that may contain viruses or other types of malware and should contact the Chief Compliance Officer if in doubt, who will contact IT support to verify the issue.

- Immediately contact the Chief Compliance Officer if you have any suspicion of a security incident if you deem it necessary, or have questions about how to proceed, and the Employee is not allowed to take any action related to the leak or attempt to access the Confidential Information, without obtaining authorization from the Chief Compliance Officer.

- Provide the password to access Google Drive and MAR email to the Chief Compliance Officer so that he/she has access to all account information, as well as so that he/she can verify how Confidential Information is being saved and if the restrictions of the system, as will be listed below in item III.2. File Storage is being strictly followed by each of the Employees.

III.2. File Storage

Regarding the use of MAR's storage network, i.e., Google Drive (GSuite), use will follow the following guidelines:

- The internal storage folders will be segregated, each user having an access profile to each folder with two levels of security - reading and editing, being defined by the Area Director who will have each type of attribution, and any change must be approved by the Chief Compliance Officer.

- It is forbidden to store any files that are not of interest to MAR, as well as files that are not owned by the company, such as music, videos, and photos.

- The copying of files contained in MAR's Google Drive is strictly prohibited by Employees and is only permitted if authorized by the Chief Compliance Officer.

Additionally, Google Drive allows shared files to be blocked, both for editing and downloading. Thus, when an Employee saves a file containing Confidential Information, the restriction for editing must be included, which makes it impossible to download the document by people who do not own the information.

Likewise, such blocking allows that, in the event of a leak of Confidential Information, those responsible are immediately identified and held accountable, both internally and from a civil and criminal point of view, if necessary.

Regarding the maintenance of MAR registration, all information and documents must be filed for a minimum period of 05 (five) years, as provided in CVM Resolution No. 21, dated February 25, 2021.

III.3. Periodic Safety Tests

Periodic security tests must be carried out on the computer of all Employees, to previously detect security flaws and vulnerabilities. The test will be carried out monthly by the Chief Compliance Officer or by an outsourced company through the central antivirus management system hired by MAR.

The Chief Compliance Officer shall monitor the performance of such tests and maintain internal records in case of failures and violations hereof.

Additionally, the Compliance department must ensure the existence of periodic security tests for information systems, especially for those kept electronically.

It should be noted that certain systems, such as Google Drive, do not require periodic security tests given the various internal protocols of such a system.

III.4. Outsourced Company

MAR uses an outsourced company's services to maintain and control computers, firewalls, and internet, as well as security systems. The structure, operation, and internal control systems are detailed in Annex 1 hereto.

III.5. Remote Work

Remote work is allowed for all employees, and the work computer must be used, in cases where it is possible to take it or use a computer that has an antivirus system and protection at the same level as Mar's internal systems.

If an employee is using a personal computer, all files related to Mar Asset must be saved solely and exclusively on Google Drive, and must not be stored on the personal computer under any circumstances.

IV. Training

MAR's training strategy aims to improve the performance of its Employees in relation to internal rules and regulations related to the activity of managing third-party resources. In addition, the legislation in force and the current situation make it necessary for all Employees to be aware of and learn about all applicable rules and laws, requirements, controls, methods, and internal conduct so that everyone adopts the best practices for prevention against insider trading, money laundering and combating the financing of terrorism.

Additionally, it is also extremely important that Employees are aware of MAR's policies, in addition to some relevant information, such as risk and liquidity rules, among others.

IV.1. Types of Training

MAR's internal training may be prepared by the Compliance area, which must use the available legislation on the matters to be dealt with, as well as MAR's internal policies and other available sources of knowledge that the Chief Compliance Officer understands to be beneficial and can contribute to such training.

Additionally, the Compliance department may outsource the activity of preparing the courses or make the Employees take courses available on the internet, provided that they comply with all legal requirements, such as support and study material containing practical examples, explanations, and a summary of all the applicable legislation, proof with guarantee and monitoring of the hits, issuance of a certificate, the legislation in force, practical examples, among other needs that the Chief Compliance Officer deems relevant.

This possibility of hiring specialized companies may also be used for lectures or courses, in general, to be given to Employees.

The training may be of 3 (three) types:

- Training to prevent insider trading, money laundering, and terrorism financing: This training will be based on the typical methodology of financial market training related to the prevention of insider trading, money laundering, and terrorism financing, always seeking to bring knowledge, improve MAR's internal controls in the various areas of the institution. The purpose of such training is also to analyze the type of conduct appropriate for, mainly equity analysts, but also all members of the front, on how to organize questions and doubts to avoid that they can be framed as attempts to obtain privileged information, in addition to what to do if they obtain any such information. This training will always be carried out annually and mandatory for all Employees, being carried out electronically (with the material to be consulted by the computer of each Employee and the tests electronically as well) or in person, in which the date will be chosen so that all employees can attend, and the training must be reapplied if any of the Employees cannot be present. The AML and CFT training may be accompanied by evidence of knowledge so that the Employees can test their knowledge and the Compliance area is aware of the level of training of the Employees, and the evidence or certificates must be filed, provided that the Employees' notes will be confidential and cannot be shared by the Compliance area with the other internal areas of MAR, with the exception of the Ethics Committee in exceptional cases evaluated by the Chief Compliance Officer. In the event of any new regulations or relevant legislation, the Compliance area may provide extra training or course to Employees outside the mandatory annual frequency described in this item.

- Compliance Training: will be conducted as provided in MAR's Internal Controls Policy. MAR's Compliance area will organize, annually, training to pass on the main rules of the fund to Employees, such as risk and liquidity rules, in addition to other topics such as physical trading restrictions, continuity, contingency plan, and information security. The aim is to introduce the main rules practically to

complement the mandatory reading of all policies that are carried out at the beginning of each year. It can also be carried out online in the same way as training on preventing insider trading, money laundering, and terrorism financing.

- Miscellaneous Training: Additionally, MAR may offer Miscellaneous Training to the Employees, which are internal courses or lectures to address various subjects, such as courses on topics related to the financial market, lectures on MAR's culture and values, presentations on the current situation of MAR and perspectives for the company's future using the principle of transparency as a basis. The purpose of these trainings is to enable the training of employees and the internal dissemination of MAR's culture and principles and may be given by any of the Employees or external guests, depending on the topic to be addressed.

It should be noted that AML, CFT, and Compliance training can be carried out on the same date if an agenda is available, and the Chief Compliance Officer understands that it is possible.

Attendance at AML, CFT, and Compliance training will be mandatory for all Employees, giving rise to sanctions under the Ethics Committee's Internal Regulations if any Employee does not voluntarily participate in the training.

In the case of training carried out online, Employees will be required to carry out such training, giving rise to the same sanctions as above apply in the case of face-to-face training, if they do not carry out it as stipulated by the Chief Compliance Officer.

V. Segregation of Activities

Considering the volume of activities currently carried out by MAR and the very small number of employees at the moment, MAR's organizational structure contemplates the total segregation of files referring to all Employees, especially those who perform activities related to resource management, to a: (i) maintain the segregation of activities required by CVM Resolution No. 21, dated February 25, 2021; (ii) avoid the inappropriate and improper use of confidential information and privileged information; and (iii) avoid potential conflicts of interest.

The segregation of files takes place through the use of the paid Google Drive cloud storage service, which offers all the necessary security, compliance, and data privacy requirements, with access to certain files only given by the Officer responsible for the area.

Storage through Google Drive also allows for contingency security in case of problems, given the possibility of accessing it from any computer remotely.

In addition to the controls stipulated above, access to MAR's physical facilities is controlled, and only third parties are allowed to stay in the meeting room or the living room, only while accompanied by at least one Employee. In this way, third parties will not have any access to the systems or computers used by the Employees.

VI. Compliance

The Compliance area will have the autonomy to act in its functions in order to ensure the compliance of MAR's operations with the provisions of the regulation in force, apply, monitor, and supervise with independence and efficiency the compliance with internal policies and implement procedures to comply with the provisions in internal policies.

These are attributions of the Compliance area, in addition to the provisions of CVM Resolution 21 dated February 25, 2021, in its articles 22 et seq.:

- Implement and maintain Employee training programs, ensuring the presence of Employees.

- Ensuring, through adequate internal controls, permanent compliance with the rules, policies, and regulations in force, referring to the different types of investment, to the activity of managing securities portfolios, and to ethical and professional standards.

- Forward complaints to regulatory bodies or suspicions raised by Employees in relation to the prevention of money laundering and terrorism financing.

- Prepare and review all internal policies and ensure their alignment with the regulations in force and with the reality of MAR.

- Ensure the confidentiality of issues raised by Employees, both in relation to internal and personal matters.

- Define the evaluation and monitoring methods of MAR's internal control processes, being also the only MAR area responsible for attending/responding to regulatory and self-regulatory bodies.

Given the size of the number of Employees, MAR will not have a Compliance Committee for the moment, with all day-to-day topics being dealt with by the Chief Compliance Officer and the most sensitive ones must be taken by the Chief Compliance Officer to the Ethics Committee as provided in the Code.

Annually, according to the guidance on the maintenance of the internal controls department provided in CVM Resolution No. 21, dated February 25, 2021, MAR's

Compliance area will issue internal controls report with the conclusion of the examinations carried out, which will be available to the CVM at MAR's headquarters.

VI.1. Conflicts of Interest

In relation to possible conflicts of interest at MAR, the Compliance area must analyze the situations that have been brought to its attention in relation to conflicts involving personal investments of Employees, financial transactions of Employees with customers outside the MAR environment, participation of Employees in the administration of other companies, receiving gifts or favors from clients, analysis of companies in which they are partners or have direct or indirect personal relationships. To analyze conflicts of interest, other MAR policies should be consulted, such as the Code and the Policy for Trading Securities by MAR Employees.

Employees will not be able to take part in management positions in companies that work in activities related to MAR in the financial and capital markets, both in Brazil and abroad, such as securities consultants, third-party asset managers, Family Offices, brokers securities, investment banks, etc., except in the case of advisory positions without any inference in the day-to-day of the company, for which the restrictions below shall apply.

Concerning the participation of Employees in the management of other service providers, mainly whose activity involves business consulting, Employees are obliged to:

- If there are companies that are clients of the company in which the Collaborator holds a management position and sells securities, both in Brazil and abroad:
  - If the Employee does not participate, due to his/her position at MAR, in the Investment Committee, he/she must inform the Compliance area so that the existence or not of a conflict of interest can be evaluated;
  - If the Employee participates in the Investment Committee, if any discussion arises about the securities issued by such client, the existence of a conflict must be raised immediately by such Collaborator at the time the Committee is held, for which the Chief Compliance Officer and who shall resolve on such a conflict situation.

- Inform the Compliance area of all situations of conflict of interest that may arise given privileged information that they have access to during the provision of services, and the Compliance area must decide in which category of restriction the asset will be classified,

considering the Policy on Prevention of Insider Trading and MAR's Unfair Market Practices.

- Ensure the segregation of all MAR activities from the activities performed in the administration of other companies, not being allowed to share information, use MAR corporate tools, use of email or other MAR systems (especially storage), to perform the other functions that the Employee may perform in that company.

Regarding the position as an advisory member of public companies, such as the Board of Directors, the only member of Mar Asset whose participation is allowed is Mr. Luis Moura, who already performed such functions before joining Mar Asset. In addition to the above measures to prevent conflicts of interest above, they shall follow the following specific guidelines for such cases:

- In case Mr. Luis Moura will perform the administrative function in a company whose securities are traded, both in Brazil and abroad, all MAR employees, and all the measures that will be taken for the rules of paper commercialization must be fully described to the Employees by MAR funds, considering the Policy of Prevention of Insider Trading and Inequitable Market Practices of MAR and the provisions below.

- The management area, if the investee company is publicly traded, must be immediately informed about such restriction so that the quiet period rules are respected in the negotiations of the securities of such companies (or their subsidiaries and affiliates), both in relation to the financial statements (CVM Resolution 44/21), both with the concept of restriction for public offerings, according to the concept created by Article 48, subsection IV of CVM Instruction No. 400/03. The quiet period treatment should be followed even taking into account that Mr. Luis Moura is not part of Mar's portfolio management department and has no decisive power.

- In the composition of the equity portfolio, the maximum exposure to companies in which Mr. Luis Moura participates in the Board of Directors is 5% (individually or in a combined form) of the fund at cost.

VI.2. Selection, Hiring, and Supervision of Service Providers

Regarding the hiring of service providers, both for MAR and for the investment funds under its management, the Compliance area established certain procedures and minimum criteria to guide the selection, hiring, and maintenance processes (with due monitoring) of such contracted service providers.

Such criteria use the best market practices, as well as the guidelines contained in ANBIMA's Manuals and Codes, including, but not limited to, the Regulation and Best Practices Code.

The analysis of such service providers must also undergo an analysis based on the Conflicts of Interest criteria listed in the previous item of this Chapter in relation to Employees, and conflict issues and the level of the relationship existing in the Ethics Committee must be discussed, if the Chief Compliance Officer, after an initial analysis, concludes that such a relationship is possible based on the principles determined in this Policy and current legislation.

It should be noted that the procedures described in this chapter must be monitored and carried out in accordance with the Know Your Customer, Registration, AML and CFT Practices Policy in relation to feeding information in the counterparty control table, both monitorings being carried out together by the Compliance area.

A. Specific Exceptions

The Compliance area may, by its exclusive deliberation, exempt the application of certain procedures established in this item in relation to monitoring if the contracted third party has: (i) an unblemished reputation; (ii) technical and economic-financial capacity for the performance of activities; (iii) is associated with ANBIMA or adheres to the ANBIMA's Regulation and Best Practices Code for the Management of Third Party Assets.

B. Prior Procedure for Selection of Providers

As provided above, the selection process of counterparties will be carried out directly by the Compliance area, and various information about the third party must be obtained in the pre-selection phase, including: (i) brief history of the company; (ii) corporate documents; (iii) information about the service provider's management and partners; (iv) authorizations to act in the activity, if applicable; (v) brief history of the service provider; (vi) reports and

general information about the partners, officers and the company itself, which can be publicly found on the internet; (vii) ANBIMA's due diligence questionnaire, when applicable.

In addition to the criteria listed above, the Compliance area may determine specific criteria for research considering the specific performance of a certain counterparty or its history and may request additional documents and information.

C. Hiring of Service Providers

After the prior hiring procedures, the Compliance area must approve, or not, the service provider. If approved, the service agreement will be signed in line with the minimum required by the Code, containing:

(i) The obligations and duties of the parties involved;
(ii) The description of the activities that will be contracted and performed by each of the parties;
(iii) The obligation to carry out activities per the provisions of the Code, if applicable;
(iv) Term of service provision, remuneration to be paid, confidentiality; and
(v) Service provider's obligation to make available to the trustee all documents and information required by the regulations in force for the preparation of mandatory periodic reports, except for those considered confidential.

D. Hiring Brokers

In addition to the procedures described above for hiring service providers, specifically for brokers hired by MAR, the Compliance area must request the completed ANBIMA questionnaire, in addition to

E. Classification of Service Providers

To define and highlight the third parties with the greatest risk to MAR or to the funds managed thereby that are the contracting parties, as the case may be, the Compliance area may create a classification system to be used and included in the control table of counterparties.

The classification system will be established at low, medium, or high-risk levels using the following classification criteria: (i) counterparty history; (ii) negative news and reports in the media involving scandals or suspicions of corruption; (iii) management members involved in corruption-related news and information; (iv) existence of PEP or links with PEP; (v) transparency in the corporate structure; (vi) be a publicly-held company; (vii) the fact that the counterparty is not associated with ANBIMA or adherent to the ANBIMA Codes; and (viii) other factors specific to certain counterparties.

F. Securities Brokers

Specifically regarding securities brokerages, in addition to the hiring criteria being more easily verified by the Compliance area thanks to the possibility of obtaining reputational and regulatory information from the regulatory and self-regulatory body, a monthly monitoring should be carried out on the allocations of orders and the number of orders given at each broker, in line with the quality of the service offered, speed of service and similar services offered such as research, events with publicly traded companies, etc.

G. Monitoring of Service Providers

During the term of the contracts entered into, MAR's Compliance area may carry out periodic maintenance of the contract and control of the counterparties, updating the database, as well as new research on the information obtained during the pre-contracting period described in item A above.

Additionally, the areas that benefit from the services provided by the service providers must also carry out a qualitative analysis of the services provided, immediately reporting to the Legal and Compliance Director if any service is being provided correctly and adequately, who must take the appropriate actions of the contractual and legal point of view, and the decision may be taken to the Ethics Committee if it deems necessary.

Regarding the risk classification established in item D above, the Compliance area must review the registration and criteria, respecting the following deadlines:

(i) Every 12 (twelve) months for counterparties classified as “High Risk”;
(ii) Every 24 (twenty-four) months for counterparties classified as “Medium Risk”; and
(iii) Every 36 (thirty-six) months for counterparties classified as “Low Risk”.

If any extraordinary news arises or the Compliance area deems it necessary, it may review the information in a shorter period than the above.

Additionally, this area may also make changes to include new criteria for analysis as they emerge.

VI.3. Internal File:

In addition to the Google Drive cloud file policy as provided above, MAR's Compliance area will be responsible for keeping the documents, both physical and electronic, for 05 (five) years following the applicable legislation.

The established period of 05 (five) years refers to the best practices of document files and also to comply with current regulations, mainly about tax document files, as well as labor and corporate documents and proof of payments.

The physical file must also respect this deadline and will be maintained and organized by the Compliance area.

VI.4. CompliAsset System:

We have the CompliAsset system (specific Compliance software that helps in the control of new legislation, regulatory obligations, registration of internal events, acceptance of policies, and training, among many other features and today it is widely used by the financial market, being present in more than 200 companies).

This system has several features related to Compliance, such as a calendar of regulatory obligations, tools to assist in the preparation of regulatory documents, information on new applicable legislation, a document filing system, and acceptance, among several other features that add even more control to the Compliance area.

VII. Insider Trading Prevention

Considering the rules and concepts applicable concerning the trading of securities in the capital market, it is necessary to establish in this Policy the procedures and restrictions to ensure that investment decision-making is based on information obtained through lawful means and sources.

The purpose of this chapter is to establish all applicable rules and procedures to ensure that the Funds' decision-making process is under the regulations in force, and their rules and conduct must be analyzed in conjunction with all other MAR's internal policies.

It should be noted that the purpose of this chapter is different from the chapter on Segregation of Activities contained in this Policy, whose purpose is to establish, mainly, security and measures for non-disclosure of information about the investment strategies of the Funds with third parties.

VII.1. Applicable legislation:

Brazilian legislation directly establishes the concept and punishment for the practice of insider trading, characterized as an administrative offense, as well as a criminal offense.

Several restrictions and penalties applicable to such illicit acts are established in Law 6.404/1976, Law 6.385/1976, as well as in CVM Resolution 44/21 (Disclosure of Information by Issuers), Instruction 400/2003 (Public Distribution of Securities), CVM Resolution 20/21 (Investment Analysts) and CVM Resolution 21/21.

The restrictions established in current legislation, mainly the CVM Instructions/Resolutions listed above and the Criminal Code will be presented by the Chief Compliance Officer at the Annual Insider Trading, PLD, and CFT Training and, therefore, must be known to all Employees. All doubts about legislation and framework must be taken directly with the Chief Compliance Officer, whether in the theoretical field or relation to any day-to-day situation, and no other MAR employee is suitable for this doubt to be resolved.

It should be noted that the practice of insider trading can occur regardless of profit, only due to strong suspicion considering the operations carried out and the exchange/obtention and misuse of certain privileged information, both in the administrative and criminal scope, according to the understanding already established by the Brazilian courts

In relation to possible conflicts of interest at MAR, the Compliance department should analyze the situations that have been brought to its attention concerning conflicts involving personal investments.

VII.2. Concept of Insider Trading:

First, it is necessary to establish a concept for “insider”, which is, in relation to a given company, any person who, due to circumstantial facts, has access to “relevant information” relating to the business and situation of the company in which it operates.

Concerning “material information”, Brazilian doctrine and case law have established as a concept, by the provisions of Law No. 6.404/76 affect investors' decision to buy or sell a particular security, such as information about the company's operating results; corporate operations; changes in company management positions; information on capital market operations; new designs, patents or discoveries; and situations of insolvency, bankruptcy or judicial reorganization.

It should be noted that “material information” may also involve privileged information about affiliates, subsidiaries, parent companies, or even counterparts of companies whose securities are traded on the stock exchange.

Additionally, although Law No. 6.404/76 has not defined a legal concept for such a specific position of "insider", from the consultation of certain articles of such provision, the concept defined by the legislation can be implicitly verified, i.e., that of any person who, by the position he/she occupies in the company, by the relationship he/she has with people who occupy a relevant position in the company or even outsourced employees who provide services for the company have access to information capable of influencing the price of the company's securities.

Thus, the practice of insider trading is characterized as carrying out transactions in the financial market with the use of relevant non-public information disclosed by insiders to obtain a financial advantage for itself or third parties, with the exchange, or not, of a financial advantage or payment to the insider for privileged information.

Regarding “non-public information”, this concept encompasses any information that has not yet been officially disclosed by the public media, either by the publicly traded company to which the information is considered relevant or through a communication or social networks that are available for unrestricted access by the entire public.

The disclosure of non-public information is not limited to conversations and the private transfer of information, but also concerns, mainly, information disclosed in meetings, presentations, lunches with executives, text messages, messages on Bloomberg, telephone conversations, etc., being also considered within this definition information shared in informal conversations in the scenario of the Employees' private life, and all such information must have the same treatment as will be described herein.

VII.3. Responsibilities:

The risk and compliance areas are closely linked to the prevention of the practice of insider trading, and must jointly create the appropriate mechanisms to avoid such practices and mitigate the risks, whose rules must be followed by all Employees.

Regarding privileged information that may be received by third parties, such as counterparties in operations, investment advisors, and service providers, among others, risk mitigation takes place, mainly, through the establishment of policies that establish the rules for relationships with third parties, whose contracting must be approved by the Compliance area, and Employees who deal directly with such third parties must consult this Policy concerning the exchange of information, consulting the Chief
Compliance Officer whenever you have any questions.

Additionally, since Employees are allowed to occupy management positions in other companies or have technical and advisory functions in other companies, if they have access to privileged information, as defined herein, they must follow all the procedures hereof, in addition to immediately informing the Chief Compliance Officer.

In addition to the responsibility of MAR's internal bodies, Employees will have the obligation to immediately inform the Chief Compliance Officer if they have access, even if occasionally, to privileged information, when they start negotiations to enter into contracts that establish a flow of potentially relevant information and confidential information of a particular securities issuer, on the existence of commercial, professional or trust relationships from which privileged information may arise.

If in doubt about the classification of privileged information, the Employee must immediately contact the Chief Compliance Officer so that he/she can analyze the information and verify the potential classification.

After receiving the information, the Chief Compliance Officer must process and proceed as described herein in relation to the restriction of the sale of assets.

VII.4. Preventive Measures:

In addition to all trading restriction measures that will be taken, as provided below, upon knowledge by the Chief Compliance Officer of the situation of conflict or insider trading, MAR shall determine additional measures to be taken before the occurrence of insider trading and/or to restrict the role immediately after the fact that has originated the knowledge of such information by the MAR management team.

Concerning closed meetings that Employees intend to hold with analysts or members of the management of publicly-held companies, PEPs, or people who may potentially hold privileged information, Employees should always try to follow certain procedures, such as:

• Have the presence of at least 02 (two) representatives of MAR; and

• Send a meeting report to the Chief Compliance Officer, who must file such report internally, containing a description of those present, matters dealt with, and date, among other information that the Employee deems relevant. Alternatively, the Chief Compliance Officer may prepare such a report with the help of the Employee who was present at the meeting.

Such procedures are not necessary in the case of public events, lectures, or if, after contacting the Chief Compliance Officer, there is an understanding that such a report is not necessary. The relevance of the content of the meeting must also be taken into account by the Employee to assess the need to make such a report. Case of the debate on the relevance can be held with the manager of the area and responsible for the investment decision.

VII.5. Trading Restrictions:

After the Compliance area is aware of the inside information combined with the confirmation of the materiality or expectation of future materiality of the information and its non-public character, the Chief Compliance Officer must classify the asset as restricted in whole or in part, and the resource management area is not allowed to negotiate (including rental operations, options, etc.) this type of asset (and any securities related to it) in Brazil or abroad.

After analyzing the materiality and the information itself, the asset (and any securities related thereto) will fall into the following restriction categories:

• ***Watch List*:**

Framework considering that the relevant information is not relevant for the moment or does not have elements that confirm its relevance, being only a suspicion, requiring monitoring by the Compliance area and partial restriction of operations.

In the partial restriction of the asset, the negotiation thereof is only allowed in the same directional that MAR had been positioned/operating in the last 30 (thirty), 60 (sixty), or 90 (ninety) days, and a formal opinion must be issued by the Chief Compliance Officer describing the reasons for the restriction, the information obtained, materiality and impact analysis and detailing the history of trades so that the directional of the restriction can be determined, the content of which must be shared with all Employees.

• ***Restricted List*:**

When material non-public information is considered relevant and material at the time of its knowledge, the asset should be considered fully restricted.

In such a situation, the Chief Compliance Officer must fully restrict operations with such asset by all Employees, not being allowed to trade the articles in question, and a formal opinion is also issued describing the reasons for the restriction, the information obtained, materiality analysis and impact, that is, containing all relevant information and whose content must be shared with all Collaborators.

VII.6. Unfair Market Practices:

Inequitable market practices and the creation of artificial conditions of supply and demand are characterized as the actions or omissions of market participants that intentionally aim to manipulate the capital market and the purchase and sale of securities, characterized in the ways set out in Law 6.385/1976.

The classified cases involve the dissemination of rumors and the “front running” in the market if the Compliance area becomes aware of such practices, the Chief Compliance Officer will communicate such irregularity or evidence of regularity to the Securities and

Exchange Commission, being the Employee subject to possible civil, criminal and regulatory sanctions.

VII.7. Conflict of Interests:

About situations that may configure or resemble conflicts of interest, Employees must carry out all measures as provided in the Internal Controls Policy, immediately contacting the Compliance area.

To verify examples of occurrences that may be characterized as a conflict of interest and to avoid situations of risk of exchanging privileged information for MAR, Employees must verify the Internal Controls Policy.

VIII. Final Considerations:

The update of this Policy will be carried out by the Chief Compliance Officer within a reasonable period, following changes in applicable regulations or when it deems it appropriate. The updated version will be disclosed to all employees and will be available on MAR's website: marinvestimentos.com.br.

Upon contracting/initiating the relationship and annually, all Employees must adhere to this Policy by completing and signing the “Meet Your Employee” Form, which will be made available by Compliance.

ANNEX 1 – MAR report prepared by the outsourced company Luckyb Informática Eireli

Rio de Janeiro, October 22, 2019.

Re.: Resilience and Business Continuity Policies and Procedures - Version: 1.0

1. **Use license.**
   1.1. This document was created by **Luckyb TI** for **MAR Asset Management Gestora de Recursos Ltda (MAR)** which it may use and publish in whole or in part.
   1.2. No use hereof will be allowed for anyone other than MAR Asset Management.

2. **Equipment, operating systems, and applications.**
   2.1. MAR has complete management of all its equipment. The entry of a new equipment requires approval from the compliance department.
   2.2. Each piece of equipment is periodically monitored by Luckyb TI, which allows identifying potential risks to the security of data owned by MAR.
   2.3. The updates proposed by the manufacturers of the respective equipment are applied monthly. In this same routine, the updating of applications, if applicable, and the recommendations of their manufacturers are also verified.

3. **Backup systems.**
   3.1. Shared files are stored and managed on the Google GSuite platform. This platform ensures backup and versioning of files.
   3.2. Most important computers that have trading, news, and risk systems have their local backup system to increase the recoverability of the systems as a whole.

4. **Cyber Security Systems**
   4.1. A state-of-the-art firewall controls access between equipment operated by employees and services used on the internet. Each service has a security policy managed by the firewall.
   4.2. In addition to internet services, applications that can be used to access said services are also controlled.
   4.3. The employees and their equipment will not have access to services not registered in the firewall.

4.4. All traffic is monitored, logged, checked for viruses, and detected intrusion attempts or denial of service.
4.5. Firewall automatically blocks the originating connection if any non-compliance with rules and policies is detected. In addition to detecting and blocking the firewall, it alerts by email and records each occurrence.
4.6. In the internal network of the MAR office there is no service published on the internet.
4.7. A state-of-the-art antivirus system protects employee workstations. This system detects and blocks threats in real time on computers. It has intrusion detection, alerts, and reports increasing control and security against cyber-attacks. Management is done through a personalized and centralized internet console and alerts are sent to Luckyb TI and the compliance department.

5. Power management.

5.1. A centralized UPS ensures 1-hour autonomy for all computers and network equipment.
5.2. A computer records the events and manages the UPS.

6. Business Continuity Plan.

6.1. MAR's business continuity plan is managed by the compliance department.
6.2. The plan is initiated if employees cannot access the computers in MAR's office, either due to lack of electricity, cyber-attack, or unavailability of access to the building, among other events.
6.3. The basic premise is to guarantee employees access to a computer or mobile device with internet access. MAR has three notebooks outside the office that can be used to access files and systems.
6.4. The data is on the Gsuite Google Drive platform and available to employees via computer or mobile device, facilitating access to file-based systems, without the need to be physically inside the MAR office. Employees already use files and systems daily both inside and outside the office,
6.5. Bloomberg anywhere, an important system for MAR's activities, has the characteristic of containing the profile of each employee in the cloud. It is used daily both inside and outside the office.
6.6. MAR manages to operate with relative normality even though the employees are not concentrated in the same place. All you need is internet access, mobile or landline, and a standard computer. Employees are constantly instructed to use the flexibility and mobility of Google Drive and Bloomberg Anywhere, keeping the company always ready to exercise its social commitment.

7. Summary.

7.1. The set of MAR's computer system has modern protection against cyber-attacks composed of a state-of-the-art firewall and antivirus, updated operating systems, and the latest version. All equipment is controlled, monitored, and evaluated for the risks inherent therein.

7.2. Great resiliency with systems that work anywhere or on any device and data recovery capability.

7.3. Monitoring and alerts make the response time to system downtimes immediate, triggering IT teams for proper mitigation.