2023

BRAVOS GESTÃO DE RECURSOS LTDA.

Manual of Rules, Procedures and Description of Internal Controls

RULES, PROCEDURES AND DESCRIPTION OF INTERNAL CONTROLS

1. Purpose and Scope

This Manual of Rules, Procedures and Description of Internal Controls ("Manual") is in accordance with the terms of CVM (Securities Exchange Commission) Resolution No. 21, dated February 25, 2021 ("CVM Resolution No. 21"), and is applicable to all partners, Officers, employees, and interns who directly participate in daily activities and business, representing Bravos Gestão de Recursos Ltda. ("Co-Workers" and "Management", respectively), and shall be applied in conjunction with the Segregation of Activities and Information Security Manual and the other Manager's rules and policies.

Co-Workers must comply with the guidelines and procedures established herein, reporting any irregularity to the Compliance and Risks Board, so that the goals below are achieved and the operation is made possible according to the structure proposed in Item 2 hereof:

(i) establish a structure to enable Co-Workers to act impartially, having knowledge of the Code of Ethics, the applicable legislation and regulations, as well as the other Manager's internal policies;

(ii) monitor the adequacy of the Manager and its Co-Workers to this structure, to identify, manage, and eliminate any conflicts of interest that may affect the impartiality of Co-Workers linked to the Management Area; and

(iii) prevent, control and mitigate the risks involved in the activities carried out by the Manager.

2. Organizational Structure

The Manager shall be organized according to the assignments described in the sequence below:

The Manager shall be managed by a *Board*, composed of two (2) Officers, to be designated in the Articles of Association, to act for an indefinite term. The Management Board shall be responsible for managing securities portfolios, according to CVM Resolution No. 21, while the Compliance and Risks Board shall be responsible (a) for compliance with rules, policies, procedures, internal controls, and those of CVM Resolution No. 21, (b) for risk management, and (c) for compliance with the obligations set forth in CVM Resolution No. 50, dated August 31, 2021 ("CVM Resolution No. 50"), related to the prevention of money laundering and terrorist financing ("PLDFT - "prevenção da lavagem de dinheiro e ao financiamento ao terrorismo"").

The *Technical Department* shall be made up of Co-Workers, including the Management Board and one more senior Co-Worker who will replace them it in case of temporary absences. The Technical Department shall be responsible for making investment and disinvestment decisions - definition of strategies, investment origination and decision, ways of creating value in the investees - and for daily monitoring the operations of the investees of the investment funds under management, and shall also assist projects to integrate the most recent investments into the portfolio.

Investment and divestment decisions shall be taken by the Management Board and the documents and information that support them shall be filed electronically and subject to verification, and an investment committee may be formed with high know-how individuals, required for the best conduction or decision. When applicable, in addition to the deliberations and the decision taken, the minutes may mention the documents that helped and supported the decisions taken.

The *BackOffice* shall be composed of co-workers, some directly linked to the Compliance, Risk, PLDFT, and Controllership Areas, as shown below, and the others, to the support activities for both:

(i) *Compliance, Risk and PLDFT* shall be composed of at least two (2) Co-Workers, including the Compliance and Risk Board and a senior Co-Worker to support the duties of the Board and replace them in case of temporary absences. The Area shall be responsible for complying with rules, policies, procedures, internal controls, risk management and compliance with the obligations set forth in CVM Resolution No. 50, related to the prevention of money laundering and terrorist financing; and

(ii) *Controllership* shall be composed of at least one (1) Co-Worker and shall be responsible for (i) the organization's financial and administrative activities; (ii) for the supervision of service providers in charge of the Information Technology Area, Accounting, Legal Counseling, and other contractors on *ad hoc* basis; (iii) and financial analysis of investments, based on information made available by the Technical Department, for reporting to investors.

Information Technology service providers - subparagraph (ii), above - shall be responsible for supporting users, deploying and managing antivirus and applying user access control defined by the organization. File Server backups hosted on Sharepoint 365 are: Microsoft Standard integrated with Sharepoint 365 with retention of ninety (90) days and Wasabi Cloud Storage two (2) times a day with retention of ten (10) years.

The Compliance, Risk, PLDFT, and Controllership Areas shall also have outsourced service providers for the Legal, Accounting, Information Technology, Human Resources, Document Custody, Treasury, and General Services Areas.

Lastly, the *Compliance and Risk Committee* shall be a purely deliberative body and shall have decision-making powers only regarding the implementation of sanctions in view of the violation of the Manager's Policies and Manuals. It will be composed of at least two (2) members - by the Compliance and Risk Board or its backup, by the Management Board or its backup.

Said committee shall be responsible for keeping the performance of the Manager and its Co-Workers in accordance with the rules, procedures and internal controls, as well as those established by current regulations, regarding their investments, the activity of managing securities portfolios and ethical and professional standards. This Committee shall also be responsible for monitoring and making decisions regarding PLDFT matters.

Lastly, the Compliance and Risk Committee shall meet whenever required, but at least quarterly - in the months of January, April, July and October. The meetings shall focus on monitoring the activities inherent to the Manager, identifying points of attention and adopting measures aimed at monitoring or solving them, and discussions and decisions must be the subject of signed minutes (in person or electronic basis) and/or reports prepared later, filed for collection purposes and verification by the Compliance and Risk Board.

2.1. Description of Internal Controls

In order to ensure goals measurement and achievement hereof, the Manager shall implement internal controls, in accordance with or similar to the exemplary list below:

Information Security – the Manager shall act through routines developed by specialized service providers to ensure an environment protected from any type of risk to information and to the internal computer network, preventing the quality of management from being impaired by contingencies;

Email Monitoring - the Manager shall have up-to-date equipment and his e-mail server shall be hosted with Microsoft, through the Microsoft Office 365 Business Standard plan, from Exchange Online, which will guarantee high availability and security and will enable remote work and via spare computers, if and when necessary, notwithstanding the maintenance of records that will enable audits and inspections to be carried out;

Co-Workers Identity – administration shall take place centrally through AzureAD, where (i) users and their activities can be monitored; (ii) folder partitioning is enabled; and (iii) access profiles are configured according to the prerogatives and needs inherent to the positions of Co-Workers;

Compliance and Legal Counsel Software – Co-Workers and the Compliance, Risk, and PLDFT Areas shall rely on BTDocs, software whose purpose is to centralize, file, control, automate and provide more security to said activities through (i) control of document deadlines with due dates; (ii) controls related to compliance with regulatory requirements inherent to the Manager's activity; (iii) filing of all documents entered into by the Manager, the FIPs, and the investees companies by the FIPs; (iv) evidence custody and reporting; and (v) control of event dates provided for in the documents for the purchase and sale of assets of the investees by the FIPs.

Telephony - PABX with channels in the management room and corporate mobile lines as means of communication;

Contractual Aspects – the effective entering into any contracts and agreements by the Manager shall be preceded by (i) validation by the hired legal counsels; (ii) verification of powers of attorney; (ii) alignment of signature procedures – the digital ones, whenever possible; and (iii) filing of signed versions, with centralized control of deadlines; and

Hiring Service Providers - the effective hiring of new Co-Workers or service providers for the Manager (or for the FIPs, when applicable), as well as the approval of professionals to compose the management of the investees in the FIPs, shall be preceded by background checks and/or specific due diligence, aiming to identify the degree of risk shown by the potential contractor and the establishment of criteria for monitoring their assignments (whether contractual or otherwise).

We refer to the Money Laundering and Terrorism Financing Prevention Policy ("PLDFT Policy"), which includes, as an annex, the Know Your Client, Know Your Partner, and Know Your Employee ("KYC", "KYP" ", "KYE" and "ID Manual", respectively), from the Manager for additional information on Internal Controls.

3. Responsibilities and Reporting to Competent Authorities

Once approved at the Shareholders' Meeting, monitoring and responsibility for complying with the provisions hereof shall be the responsibility of the Compliance and Risk Board, which, in order to achieve the goals listed in subparagraph 1 above and ensure the existence of adequate internal controls, shall:

(i) develop and keep procedures to ensure that the Manager's activities comply with legal and regulatory requirements, assessing the adequacy, scope and effectiveness of Compliance systems and internal controls;

(ii) establish a continuity plan for data recovery or periodic interruptions of financial markets, as well as ensure that periodic security tests are carried out;

(iii) inspect the services provided by hired third parties through contractual control and quality assessment;

(iv) hire specific consultants to carry out "background checks" of partners, keeping the reports received filed;

(v) consolidate communications between the Manager and regulatory and self-regulatory bodies.

Additionally, pursuant to Article 25 from CVM Resolution No. 21, the Compliance and Risk Board shall forward to the Management bodies of the Manager, by the last working day of April of each year, a report for the calendar year immediately preceding the delivery date, containing: (a) the conclusions of examinations carried out as above described; (b) recommendations for any deficiencies, with the establishment of sanitation schedules, when applicable; and (c) the opinion of the Officer in charge of the management of securities portfolios or, when applicable, of the Officer regarding the deficiencies found in previous checks and the measures planned, in accordance with specific schedule, or effectively adopted in order to remedy them ("Annual Compliance Report").

Lastly, together with the Annual Compliance Report, the Compliance and Risk Board shall prepare a report on the PLDFT internal assessment, to be forwarded to the senior management bodies specified in the PLDFT Policy[1].

4. Segregation of Management Activity

We refer to the Segregation of Activities and Information Security Manual for more information on this matter.

5. Confidentiality and Secrecy

Confidential Information:

In the exercise of their activities, Co-Workers may have access to information from the Manager's clients, as well as from third parties, which are not known to the general public and which, therefore, may be considered confidential ("Confidential Information"). The disclosure of any Confidential Information to third parties, for his/her own benefit or that of a third party (tipping), or even if there is no intention to benefit anyone, is strictly prohibited. The obligation of confidentiality applies even after the Co-Worker is dismissed.

The Manager and the Co-Workers have a legal and professional duty to keep confidentiality regarding the Confidential Information of their clients, so that requests, attempts or actions aimed

[1] Containing (a) a list of all products offered, services provided, respective distribution channels and trading and registration environments in which the Manager operates, classified according to the Internal Risk Assessment ("AIR" - Avaliação Interna de Risco); (b) the classification of the Manager's clients under the AIR; (c) identification and analysis of LD/FTP risk situations, considering the respective threats, vulnerabilities, and consequences; (d) if applicable, analysis of the performance of agents or relevant service providers hired, as well as a description of the governance and duties associated with maintenance of the simplified register provided for in CVM Resolution No. 50; (e) table relative to the previous year, containing: the consolidated number of operations and atypical situations detected, separated by each hypothesis; the number of analyses carried out; the number of communications of suspicious transactions reported to the Financial Activities Control Council – COAF ("Conselho de Controle de Atividades Financeiras") or the date of reporting of the negative statement; the measures adopted to deal with and mitigate the identified risks (including the presentation of effectiveness indicators under the terms defined in the PLDFT policy), including the timeliness of detection activities, analysis, and communication of operations or atypical situations; and the presentation, if applicable, of recommendations aimed at mitigating the risks identified from the previous year that have not yet been properly addressed.

at breaching confidentiality shall be immediately communicated to the Compliance and Risk Board, so they may decide on their regularity and necessity.

Sensitive Information:

Sensitive Information, in addition to Confidential Information, are those that, if they come to light, may result in loss of the Manager's security level.

Loss, misuse, modification or unauthorized access to Confidential Information may adversely affect an individual's privacy, disrupt business, tarnish the Manager's image and the continuity of its business.

The Manager is legally responsible for keeping the confidentiality of its clients and, therefore, information relating to clients and investees by investment funds managed by the Manager may never be sent to third parties, with the exception of requests from public bodies, regulatory bodies and the Judiciary and, even in these hypotheses, within the strict limits of the orders received.

The disclosure and access to Confidential Information and Sensitive Information shall only be made to Co-Workers who come to assist and join in the development of activities related to the securities portfolios management and only in the exact extent in which it is required to be aware of such Confidential Information.

All Co-Workers receive a confidentiality agreement upon joining the Manager, whose reading and signature is mandatory.

We refer to the Manager's Segregation of Activities and Information Security Manual for more information on information security and on the rules of secrecy and conduct.

6. Information Security

Information security measures are intended to protect against threats, in order to guarantee business continuity, minimize risks and maximize returns to investors. Such measures, as well as carrying out annual intrusion tests and vulnerability scans, shall be implemented by information technology service providers - outsourced for quality assurance and under the responsibility of the Controllership, as described in the next paragraphs hereof - based on the guidelines of the Compliance and Risk Board, and shall be observed by all Co-Workers.

The following actions bring situations of risk to Information Security:

(i) Accessing websites unrelated to the Manager's activities;
(ii) Using media ("pen-drives", CDs, among others) to store digital files, with the exception of those made available by the Manager;
(iii) Accessing or save Sensitive Information and Confidential Information in publicly accessible virtual folders;
(iv) Saving personal files on the institutional computer network;
(v) Using media to transport unencrypted information;
(vi) Sharing passwords.

Access restrictions to Privileged Information - as well as to documents contained in the Manager's computer network and systems - respect the division of positions in the functional organization chart, being separated by means of the *Chinese Wall*[2] and systems that allow the identification of information holders, for liability in the event of a leakage.

[2] *Chinese Wall* is the term used to refer to the communication barrier between different individuals or sectors of the same entity, aiming to ensure (i) compliance with the rules that require the segregation

Exceptions to the above rules may be evaluated by the Compliance and Risk Board, according to a formal and duly substantiated request, and assessment of convenience and opportunity. Evidence of the analysis of said requests shall be filed electronically in the Manager's Directory, and the Compliance and Risk Board is responsible for ensuring such a procedure, even if by delegating this assignment to another Co-Worker.

More information can be found in the Segregation of Activities and Information Security Manual, which contains some rules regarding the Management and Security of Confidential Information.

7. Prevention of Money Laundering and Terrorism Financing

According to Law No. 9613, dated March 3, 1998, as well as CVM Resolution No. 50, preventing the use of the Manager's assets and systems for illicit purposes, such as crimes of money laundering and terrorism financing, concealment of assets, rights and values, is a duty of all Co-Workers.

The Manager complies with all applicable laws and regulations in conducting its business and activities executed by it. Any Co-Worker who violates a law or regulation applicable to the prevention and fight against money laundering shall be subject to the applicable disciplinary sanctions. Should any Co-Worker intentionally violate one of these laws or regulations, the Compliance and Risk Board shall immediately notify the competent authorities.

Should any Co-Worker suspect financial operations that may involve corruption or money laundering activity, he/she shall immediately notify the Compliance and Risk Board so that appropriate actions can be taken.

It is mandatory that all Co-Workers keep all and any information filed, such as documents and extracts that may be required for the monitoring or investigation of possible clients suspected of corruption or money laundering, provided that within the limits provided for by Law 13.709, dated August 14, 2018 (General Data Protection Regulation).

For more information, we refer to the PLDFT Policy and the Manager ID Manual, which also include provisions regarding the Anti-Corruption Rules and KYC, KYP, and KYE policies.

8. Trainings

All Manager's Co-Workers shall receive copies of the Code of Ethics, this Manual and other internal regulations, and shall analyze the provisions contained therein and, in case of doubt, access the Compliance and Risk Board for clarification and guidance.

Additionally, Co-Workers who may be hired to work in the Technical Department shall be trained and supervised directly by a Senior Co-Worker and/or by the Management Board, being under the direct responsibility of said Board during the training period of at least 90 days.

There shall also be an incentive on the part of the Manager for the Co-Worker to seek permanent technical and professional training, for which he may provide educational subsidies.

9. Contingency Plan

---

between the activity of managing securities portfolios and other activities related or not to the capital market, (ii) the identification of the holders of information (privileged or not, as defined below) for eventual liability in case of leakage, as well as (iii) the segregation between the Manager's own financial assets and the financial assets of third-party ownership.

The Manager acts through routines designed to ensure an environment protected from any type of risk to information and internal computer network.

Ongoing procedures related to Information Technology ("IT") security are related to antivirus software. They protect twenty-four (24) hours a day, without interruption, the internal network of computers of the Manager and the computer of each Co-Worker.

The Manager has access to IT-related assistance through different channels, being able to opt for assistance via the central phone, via the Co-Workers' cell phones and also through periodic and/or emergency visits.

Therefore, through the combination of the above elements, the Manager ensures an efficient, reliable and safe information system environment even in possible contingency situations.

10. Reporting and Penalties

The violation hereof shall subject the Co-Worker to the measures provided for in the Manager's Code of Ethics. All Co-Workers must inform the Compliance and Risk Board about violations or possible violations of the provisions set forth herein, in order to guarantee fair and equitable treatment of investors by the Manager, thus safeguarding its reputation.

Failure to comply with any rule established herein shall, at the discretion of the Compliance and Risk Board, result in the following penalties, depending on the severity of the non-compliance and possible recurrence: (i) written warning; or (ii) dismissal.

Any Co-Worker who believes he or she has violated this Manual or is aware of a violation and/or suspected any violation must report the fact directly and immediately to the Compliance and Risk Board, and any disciplinary action shall take the report into account. Disciplinary actions may also be taken against the Co-Worker who (i) authorizes, coordinates or participates in violations hereof; (ii) having information or suspected violations, fails to report them; (iii) fails to report violations that, due to his/her official duty, he/she should have known or suspected; and/or (iv) promotes retaliation, whether directly or indirectly, or encourages others to do so.

11. Officer in Charge

Please find below the registration information of the Board in charge of Manager's Compliance, Risk Management, and PLDFT:

Name	Emir Josafaf Calvo Correia
Email	*compliance@bravosgestao.com.br*
Phone	(21) 3235-0770 or (11) 3074-0920

Lastly, the Manager attests that the Compliance and Risk Board is not subordinated to other fields of expertise, including resource management.

12. Update

This Policy shall be subject to annual review or in shorter periods, whenever the Compliance and Risk Board deems necessary, in order to preserve the security conditions for the Manager.

Version	Date	Responsible
1	December 2020	Suelen Marinho de Souza
2	May 2021	Márcia Regina Brambilla
3	June 2022	Emir Josafaf Calvo Correia

ANNEX I - SCOPE OF ACTIVITY OF THE BOARD OF COMPLIANCE, RISK MANAGEMENT AND PLDFT

Normative Topics

- ✓ Controlling adherence to new laws, regulations, practices and self-regulation guidelines applicable to the Manager, and periodically deliver the result of its checks to the Compliance and Risk Committee;
- ✓ Controlling and monitoring the required legal licenses, registrations and certifications (registrations with CVM, ANBIMA and other applicable ones), as well as their renewal/maintenance with the authorities;
- ✓ Assisting the Manager's senior management in the relationship with regulatory bodies and ensure that the required information is provided in the required time frame and quality;
- ✓ Carrying out mandatory reviews and reports at the frequencies defined in the legislation in force.

Good Practices

- ✓ Appointing the person responsible for promoting and providing access to the information required for compliance with legal, infra-legal and self-regulation internal rules, as well as for collecting the acknowledgment and adherence agreements signed by all Co-Workers;
- ✓ Establishing controls so that all Co-Workers of the Manager act independently and comply with the due fiduciary duty towards their clients, avoiding conflicts of interest;
- ✓ Ensuring that internal controls are compatible with the Manager's risks in its activities, as well as effective and consistent with the nature, complexity, and risk of operations carried out for the professional activity of managing securities portfolios;
- ✓ Analyze information, evidence, or identify, manage and, if required, take the matter to the Compliance and Risk Committee for analysis and deliberation, in case of any conflicts of interest or regulatory non-compliance with policies and standards; and
- ✓ Communicating to the competent bodies, within the regulatory deadlines, regarding any regulatory non-compliance.

Governance

- ✓ Approving new procedures and submitting new policies and manuals for approval by the Manager's partners, based on the opinion of the Compliance and Risk Committee;
- ✓ Submitting the result of their controls and checks to the Compliance and Risk Committee;
- ✓ Monitoring and seeking the effective application of Compliance and Internal Controls documents;
- ✓ Act as a channel for communicating regulatory non-compliance and/or issues related to the Manager's Code of Ethics; and
- ✓ Preparing the minutes of the Compliance and Risk Committee, ensuring that they are duly filed digitally.