2023

# BRAVOS GESTÃO DE RECURSOS LTDA.

Segregation of Activities and Information Security Manual

## SEGREGATION OF ACTIVITIES AND INFORMATION SECURITY MANUAL

**1.** Purpose and Activities of the Manager

This Segregation of Activities and Information Security Manual ("Manual") of Bravos Gestão de Recursos Ltda. ("Manager") was prepared pursuant to Articles 27 and 28 from CVM (Securities Exchange Commission) Resolution No. 21, dated February 25, 2021 ("CVM Resolution No. 21") and aims to: (i) ensure the physical segregation of facilities between the Technical Department (also referred to as "Management") and the areas responsible for Compliance, Risks and PLDFT, and Controllership (together, the "BackOffice") of the Manager; (ii) ensure good use of common facilities, equipment and information; (iii) preserve confidential information and allow the identification of persons who have access to it; and (iv) restrict access to files and allow identification of persons who have access to confidential information.

Additionally, the Manual also covers issues related to Information Security, which will rely on specialized service providers to ensure efficiency and security compatible with the needs of the Manager, its Co-Workers, investors and other stakeholders, as well as the accountability of those involved in case of breach (leaks).

Non-exercise of the Distribution and Brokerage Activities:

The Manager operates in the Private Equity Sector, adopting equity investment funds ("FIPs" "fundo de investimentos em participações") as vehicles for investments by its clients/investors. Considering that distribution of shares of investment funds under management will not be carried out, nor brokerage, this Manual will have reduced relevance in relation to the others and in relation to the other players in the capital market. Notwithstanding, its provisions shall apply to all partners , employees, Directors, and interns of the Manager ("Co-Workers").

Absence of Conflict between Management and BackOffice:

The definition of the Manager's Investment Policy is contained in the agreements signed between the Manager and each of its investors, as well as in the regulations of the FIPs under management. In this sense, the Manager did not identify potential conflicts of interest between the Technical Department and the BackOffice, (which performs activities of the same nature also for foreign investment vehicles), and/or in relation to the management of the Manager's own financial resources (which are invested only in third-party investment funds or in Bank Deposit Certificates issued by financial institutions).

**2.** Structure

Considering Manager's structure, rules were developed, applicable to (i) physical segregation between the Technical Department and the BackOffice; (ii) Chinese Wall; and (iii) the Manager's information security.

With regard to item (iii) above, information technology service providers are hired by the BackOffice and are responsible for implementing and streamlining processes, maintaining computer systems, information security with user access control and data backup.

**3.** Physical Segregation

Access to the area used by the team specialized in securities portfolios management shall be allowed to authorized Co-Workers. Said area occupies a completely separate room, communicating only with ancillary services to the securities portfolios management, in order to

remain physically segregated from any Areas of the Manager that may be responsible for other activities related to the capital market.

Access to the physical facilities of the Securities Portfolio Management Area is limited to persons who are not Co-Workers involved in the securities portfolios management.

***4.*** *Chinese Wall*

Aims to establish a communication barrier between different individuals or sectors of the same entity, aiming to ensure compliance with the rules that require the segregation between the activity of managing securities portfolios and other activities related to the capital market, as well as the segregation between the Manager's own financial assets and the financial assets of third-party ownership.

As a rule, access restrictions to information and documents contained in the Manager's computer network and systems respect the functional organization chart. However, exceptions may be evaluated by the Compliance and Risk Board, according to a substantiated request and assessment of need.

**5.** Confidentiality, Secrecy and Information Security

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/investors, so that requests, attempts or actions aimed 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.

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 are under the responsibility of the information technology services - outsourced for quality assurance and under the responsibility of the Controllership, as described in the next subparagraphs hereof - 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.

More information can be found in the Annex I hereto, which contains some rules regarding the Management and Security of Confidential Information.

**6.** Reporting, Penalties and Responsibility

Every Co-Worker shall inform the Compliance and Risk Board about violations or possible or suspected violations of the provisions regarding Physical Segregation contained herein, being assured that the non-compliance with any rule established herein shall imply, at the discretion of the Compliance and Risk Board, 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 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.

With regard to Information Security, the responsibility for hiring and supervising the services provided shall be a responsibility of the Controllership, which shall assess third parties with potential for hiring under the terms of the Compliance Manual and other internal rules and shall monitor and qualitatively assess of the services provided.

Monitoring:

In the event of occurrence, suspicion, or indication of non-compliance with any of the rules established herein, the Compliance and Risk Board may use the available electronic records to verify Co-Workers' conduct.

The Compliance and Risk Board shall have access to all content that is on the Manager's internal computer network and shall be able to access such content, if necessary. Information confidentiality shall be respected and its content shall be made available only for legal purposes[1], thus ensuring check of those responsible for any leakages.

[1] Likewise, professional e-mail messages from Co-Workers may be intercepted and opened to have the regularity of their content verified, computers may be audited and telephone conversations may be recorded and listened, and this will not represent an invasion of the privacy of Co-Workers, since they are work tools

## 7. Officer in Charge

Please find below the registration information of the Compliance and Risk Officer in charge of Manager's Compliance, Risks, 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 Officer is not subordinated to other fields of expertise, including resource management or commercial department.

## 8. Update

This Manual shall be subject to annual review or in shorter periods, whenever the Compliance and Risk Officer deems it 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 |
| **4** | May 2023 | Emir Josafaf Calvo Correia |

made available by the Manager, which may occur at any time that the Compliance and Risk Officer deems necessary.

## ANNEX I - INFORMATION MANAGEMENT AND SECURITY SYSTEM

The Manager considers information management a matter of strategic scope, since the decisions that serve as guide to the management of its assets depend on the reliability, security and accessibility of the information management system.

In order to reach these goals, the Manager established rules for Compliance and IT Security Management.

Confidential Information Management

As for the Compliance parameters, the Manager, when systemically permitted, defines the access profiles of each user of the internal computer network so that Confidential Information is accessible only by certain people of the Manager, authorized by the Compliance and Risk Board. Customer information is preserved and, at the same time, problems related to conflicts of interest or misuse of Confidential Information are avoided.

In addition, data traffic control between Co-Workers is carried out through firewall systems and access control to the computer network, which are responsible for the protection of Confidential Information. For this reason, there is control over who has actually accessed certain data and/or systems and unauthorized access is prevented.

Thus, access levels were defined for the members of the Compliance and Risk Committee, the Technical Department and the BackOffice.

With regard to the management of risks related to information security, Bravos 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.

Structure of Information Technology and Hardware:

In addition to the information contained in the subparagraph above, the Manager shall have an integrated network of computers reviewed for capacity, security, and level of updating of its components, with the technical support of a hired outsourced company. In addition, continuous procedures related to antivirus software shall be adopted, responsible for protecting, twenty-four (24) hours a day, without interruption, the internal computer network of Bravos and the computer of each co-worker.

Also, regarding emails, the Manager shall have up-to-date equipment and its e-mail server shall be hosted with Microsoft, through Exchange Online, which will guarantee high availability and security and will enable remote work and via spare computers, if necessary, when necessary, notwithstanding the maintenance of records that will enable audits and inspections to be carried out according to Manager's Manuals and Policies;

With regard to the ids of Co-Workers and computers, their management shall take place centrally through server, 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;

Additionally, regarding the telephony structure, the Manager shall have a PABX with channels in the management room, an exclusive line for the use of facsimile and corporate mobile lines (for use by Co-Workers, whenever necessary) as means of communication.

Lastly, all Co-Workers of the Manager shall have access to assistance related to information technology systems through different channels, being able to opt for assistance via the central telephone, via the Co-Workers' cell phones and, also, through periodic and/or emergency visits.