

SP Ventures

Code of Ethics and Conduct

2022



SP VENTURES GESTORA DE RECURSOS LTDA

("Company")

CNPJ: 09.594.756/0001-80

Rua Pais de Araújo, 29, 14th floor, suite 141

Itaim Bibi, São Paulo, SP – CEP 04531-940

Phone: +55 11 2594-
8774

CODE OF CONDUCT AND ETHICS

Valid from 01/01/2023

CHAPTER I

OBJECTIVE

1.1. The main objective of this instrument is to define the rules and principles that guide the conduct of the Company's employees, understood as (i) partners; (ii) employees; or (iii) any persons who, by virtue of their jobs, functions or positions in the Company, have access to relevant information about the Company or its investment strategies.

1.2. Such principles must be observed by the Company's employees, starting that they are aware of all the rules and policies set forth herein, which were previously presented to them by the Company's Compliance Officer and in relation to which there is no doubt, undertaking to observe them at all times while performing their activities.

CHAPTER II

GUIDING PRINCIPLES OF CONDUCT

2.1. All employees of the Company must guide their conduct in accordance with the values of good faith, loyalty and truthfulness.

2.2. All efforts towards efficiency in the management of funds and portfolios should aim at obtaining a better return for investors, based on the analysis and interpretation of information disclosed to the market, and never based on access to insider information.

2.3. The Company's employees must be aware that transparent, accurate and timely information is the main instrument available to the investing public to ensure the necessary equitable treatment.

2.4. The relationship of the Company's employees with market participants and opinion makers must take place in an ethical and transparent manner.

2.5. All employees of the Company must act in an ethical and respectful manner, and no discriminatory action or any type of harassment between them or with other stakeholders is tolerated.

2.6. Any cases of discrimination or harassment, suffered or witnessed, must be directed to the SP Ventures reporting channel.

CHAPTER III

TREATMENT OF CONFIDENTIAL INFORMATION

3.1. The employees of the Company shall:

- a) refrain from using insider information to obtain, for their own benefit or that of others, an advantage through trading of securities and/or bonds;
- b) refrain from recommending or in any way suggesting that any person buy, sell or retain securities and/or bonds if the information to which they have privileged access could, in theory, influence any decision making process;
- c) clearly warn those to whom there is a need to disclose insider information about the responsibility for complying with the duty of confidentiality and the legal prohibition from using such information to obtain, for their own benefit or that of others, advantage through negotiation with such securities and/or bonds; and
- d) maintain secrecy on any information to which they have access and which has not yet been disclosed to the general public, except for the disclosure of the information when necessary for the Company to effectively conduct its business and, also, only if there are no reasons or evidence to assume that the recipient of the information will misuse it.

3.2. The Company's employees must keep absolute secrecy about any and all confidential information to which they may have access or knowledge while performing their duties, including through the systems and files made available by the Company for this purpose. Such determination applies equally to information obtained/transmitted verbally or informally, as well as to written or printed information.

3.3. The disclosure of confidential information to persons outside the Company will be carried out only when strictly necessary to comply with the rules related to the activity carried out by the Company, to ensure protection against fraud or any other suspected illegal activity, through confidentiality agreements, when applicable.

3.4. Under no circumstances may the Company's employees use confidential information to obtain personal advantages, nor may they provide it to third parties, including family members, relatives and friends, or even to other employees of the Company who do not need such information to perform their tasks.

3.5. Confidential information means all information to which the Company's employees may have access while performing their duties in the Company, including through the systems and files made available by the Company for this purpose, which are not known and proven to be in the public domain.

3.6. In case of doubts about the confidentiality of any information, the employee must, prior to its disclosure, seek the person responsible for Compliance to obtain adequate guidance, which must attribute extensive interpretation to the concept of confidential information as defined above.

3.7. The disclosure of such information to governmental authorities or by virtue of judicial, arbitral or administrative decisions must be previously and timely communicated to the officer in charge of the Company, who will decide on the most appropriate form for such disclosure.

3.8. Annually, the Company's employees will undergo a training program, in order to clarify, among other matters, their obligations regarding the maintenance of the confidentiality of information.

3.9. Control of access to confidential files on physical media is ensured through the physical segregation of the third-party resource management team.

3.10. The virtual segregation of confidential information is ensured by the use of personal and non-transferable password keys, allowing the identification of its user. Backup is made for all documents filed on the Company's computers with control of changes made to the files, ensuring the security of their contents and liability.

3.11. The electronic database used by the Company is segregated so that confidential information is filed in restricted folders, accessed through the use of a password, to persons previously authorized by the Company's Compliance department.

3.12. The electronic system used by the Company is subject to review, monitoring and recording at any time without notice or permission, in order to detect any irregularity in the transfer of information, whether internally or externally.

3.13. Failure to comply with confidentiality policies will be subject to civil and criminal liability, without prejudice to the subjection to the penalties provided for in this Guide.

CHAPTER IV

TRAINING

4.1. The Company has a training program divided into 02 (two) distinct stages. In the first stage, the person in charge of the Compliance department shall present the internal regulations to the employee when joining the Company, and shall be available to provide any clarification that may be needed.

4.2. In the second stage of the training, which occurs annually, the person in charge of the Compliance department, in addition to ratifying the content of internal regulations and collecting signatures of employees stating their adhesion to the Code of Conduct, shall address the following issues:

- Image risk and legal risk (Non-compliance with legislation/regulation).
- Enforcement - Implications of non-compliance with standards of conduct and ethics.

- Good practices for handling information.
- Information careers and segregation of activities in order to avoid any conflicts of interest.
- Information security and preservation policy, “need to know” concept.
- Record of operations and decision-making.
- Identification and communication of atypical/suspicious operations.
- Misuse of insider information.
- Parameters for internal analysis reports.
- Segregation between management of own and third-party resources – own investment policy.
- Compliance Rules.
- Obligations and responsibilities of other related service providers: trustee / distributors / custodian /independent auditor.
- Operational and risk limits and ranking for investment policies of portfolios under management.
- Methodology adopted for the accounting of assets.
- Rules for the application, redemption, grace period and conversion of quotas. Liquidity of assets X movement rules provided for in the regulation.
- Risk Management Policy

CHAPTER V

CONFLICT OF INTEREST

5.1. The employees of the Company must avoid performing other functions outside the Company that may generate conflicts of interest, or even that may appear to generate such conflicts. They must also avoid defending the interests of third parties that may generate conflicts of interest at the time of decision-making and imply some type of damage to the Company or its investors.

5.2. Transactions on behalf of the Company with individuals or legal entities with which any of the Company's employees or person related to it has a financial interest are strictly prohibited.

5.3. Conflicts of interest are generally and not limited to any personal interests of employees, for their own benefit or that of third parties, contrary or potentially contrary to the interests of the Company, the investors of the funds and other investment vehicles managed by the Company and the other clients of the Company.

5.4. If the employee decides to carry out other activities, whether or not for profit, in addition to those practiced with the Company, he/she must previously notify the Compliance Officer for proper approval in order to avoid potential conflicts of interest.

CHAPTER VI

PERSONAL INVESTMENTS

6.1 Any operations in the financial and capital markets on behalf of the Company's employees are expressly prohibited, except in the case of financial investments in open investment funds whose quotas are available to the general public, public securities traded through the Direct Treasury and shares, provided that there is no conflict of interest with the investment policy applied for the purpose of managing third party resources.

6.2 Exceptionally, certain operations may be carried out on behalf of employees, provided that they are previously and expressly approved by the person in charge of Compliance and do not constitute a situation of conflict with the portfolios managed by the Company.

6.3. For the purpose of authorizing the operations referred to in item 6.2. above, Compliance shall analyze the following aspects:

(i) whether the intended transaction may entail any loss to the Company or its investors;

(ii) whether the intended transaction may in any way limit the discretion of the Company's employees in the analysis of securities and in making investment decisions. If this operation limits the power of analysis and decision of the Company's employees, the Compliance department may not authorize it; and

(iii) the actual objectives of the intended operation, in order to ensure the good faith of the Company's employee and maintain the strict fiduciary relationship between the Company and its investors.

CHAPTER VII

INFORMATION SECURITY SYSTEMS

7.1. The employees of the Company who have access to the information systems will be responsible for taking the necessary precautions in order to prevent unauthorized access to the systems, and must safeguard the passwords and other means of access to them, respecting the rules of Business Continuity and Information Security Plan.

CHAPTER VIII

BUSINESS CONTINUITY PLAN

8.1. The Company maintains copies of the files in an alternative environment capable of processing and carrying out operations in contingency situations. With this, the officer in charge is able to access the data and information stored, through a location other than the Company's headquarters, allowing the activation and continuity of the activities. Every 6 (six) months, activation tests of said plan are carried out.

CHAPTER IX

GENERAL PROVISIONS AND ENFORCEMENT

9.1 This instrument prevails over any previous oral or written understandings, binding the Company's employees to its terms and conditions.

9.2. By way of *enforcement*, it is worth noting that non-compliance with the provisions of this Code will result in warning, suspension or just cause termination, according to the severity and recurrence of the violation, without prejudice to civil and criminal penalties.