COMPLIANCE MANUAL

IG4 CAPITAL INVESTIMENTOS LTDA.

("Manager")

Current version: June/2022
Previous version: July/2021

Document No.:	Review No.:	Effectiveness:
1	6 (June 2022)	11/30/2016, and, when applicable, as from obtainment of CVM consent to operate as fund manager

Approved by: DocuSigned by: 206EC3047D064CD... _____

Flávia Andraus Troyano

Compliance Officer

CHAPTER I
INTRODUCTION

1.1. Compliance is an activity adopted by international financial market that, with ethical precepts, and always in conformity with all the laws wherever it develops its activities, intends to prevent any exposure to risk.

1.2. Compliance aims at guaranteeing the reputation of an institution, which is its most valuable asset, conducting business with transparency and correctness, granting a strategic competitive differential to the Manager.

1.3. In that sense, the Manager adopts this Manual aiming at defining internal routines that ensure faithful enforcement, by the Workers of the Manager, of legal and

regulatory standards it is subject to, therefore guiding the compliance activities of the Manager.

1.4. “Workers”, in line with the concept defined by the Code of Ethics and Conduct of the Manager, are understood as: (i) partners and associates; (ii) employees; (iii) officers; (iv) interns; or (v) any people who, due to their jobs, functions or positions at the Manager, have access to confidential information about the Manager, its business or investors or, moreover, those who participate in the investment decision process.

CHAPTER II
GOVERNANCE

2.1. The area of Compliance is coordinated by its own Officer in charge, who is completely independent to carry out the duties and decision-making in her scope of operation, without any subordination to the other areas of the Manager.

2.2. The Compliance Officer shall report directly to the Executive Board, especially to report the outcome of the activities related to internal controls, including potential irregularities and failures identified.

2.3. The responsibility of Compliance consists in the preparation, implementation and maintenance of internal controls and procedures intended to permanently enforce the standards that govern the activities of the Manager and the best practices adopted by the market.

2.4. For this purpose, Compliance must be granted full access to information and documents related to the activities of the Manager, so that it may check conformity with legislation and rules established internally.

2.5. The area of Compliance of the Manager must make all workers aware of the internal rules of conduct and procedures adopted, aiming at enforcing regulation and self-regulation, as well as maintaining the strict fiduciary relationship between the Manager and the other members of the market, investors, regulating agents, market inspectors and other authorities.

2.6. The Compliance area is completely independent of the risk area of the Manager, so that the activities performed by each of these teams happen in an autonomous and independent manner, coordinated by the respective officers in charge for each one of them.

CHAPTER III
COMPLIANCE ROUTINES

3.1. Compliance is responsible for adopting the following routines regarding the matters listed below:

I. Internal Manuals and Policies:

(a) review of internal manuals and policies, keeping in mind the best practices of the market and the demands from regulatory and self-regulatory bodies; and

(b) presenting to workers the manuals and policies adopted by the Manager, which is the opportunity when the Terms of Adhesion, Commitment and Confidentiality. Such rite must be carried out whenever new workers start working at the Manager, and the referred Term shall be collected until the last day of the month subsequent to the start of the working relationship.

II. Information Security:

(a) monitoring the effective lock up of work stations and backup of informations archived at the Manager;

(b) constant check of occasional documents forgotten on the desks and/or printers, instructing the workers about the need to preserve the information;

(c) coordination of periodic security tests for information systems, especially those in electronic media and, also, for the purpose of the business continuity policy and information security policy adopted by the Manager;

(d) checking information security incidents, coordinating the investigation of the facts, mitigation of risks, implementation of corrective procedures and assigning accountability of the parties involved;

(e) notification of interested parties in the event of confidential information leakage, preparing a report about the damage, percentage of activities affected, financial impact, suggesting, in addition, measures to be taken in order to enable the activities to be normally resumed;

(f) checking the compliance with the principles and routines inherent to data protection, including providing information to their holders, upon request, answering requests from governmental bodies, as well as reviewing contracts and terms of

confidentiality with partners and service providers aiming at complying with the Data Protection General Law (*LGPD*).

III. Training Program:

(a) implementation and maintenance of the Training Program described in the Code of Ethics and Conduct, which all workers are subject to, according to the definition approved by item 1.4. of this Manual, with the purpose of guiding them on internal rules of conduct, operating procedures defined by the Manager and current regulations that govern the activities of the Manager. Such training may be delivered by the Compliance Officer or a third party outsourced for that purpose;

(b) promotion of extraordinary training upon changes in the rules that govern the activities of the Manager, aiming at dealing with concrete cases that may happen inside or outside the institution; and

(c) incentive to attend lectures, seminars, congresses and discussion groups, collaborating with the update of the practices adopted by the market.

IV. Personal Investments:

(a) checking whether the personal investments of the workers are adequate according to the Personal Investment Policy defined by the Manager, which is carried out upon collection of investment receipts from brokers and distributors to workers selected by sampling, as well as annual collection of the conformity statement, where the workers confirm their compliance with the parameters defined by the Manager.

V. Correct Treatment of Confidential Information:

a) guidance to workers regarding the Confidentiality Policy of the Manager and collection of the Term of Adhesion, Commitment and Confidentiality of the workers, by which they pledge to follow the guidelines defined in the manuals and internal policies;

(b) collection of the Term of Confidentiality from service providers of the Manager who have access to confidential information, in case there is no clause with that purpose in the signed Contract;

(c) reviewing and monitoring the electronic system of the Manager, at any time, without warning or permission, in order to detect any irregularities in information transfers, either internally or externally;

(d) checking, without previous notice, by sampling, e-mails sent/received by workers, internally and externally, in order to guarantee proper use of that tool and check proper treatment of confidential or privileged information;

(e) checking the backup of messages received/sent by workers through the applications used to communicate with external agents, and the records of meetings held in any virtual conferencing platform used by workers to communicate with external agents, as well as checking, by sampling, their content for any transgressions regarding the correct treatment of confidential information;

(f) analysis and, if necessary, implementation of corrective and accountability procedures regarding the individuals involved in case an information security incident is identified, including due to inadequate use or information leakage. The workers' accountability must follow the Enforcement Policy contained in the Code of Ethics and Conduct.

VI. Money Laundry and Terrorism Financing Prevention:

(a) checking the framework of operations carried out by the Manager in the scope of the financial and capital market, regarding the rules that govern such market, assessing the operations from the perspective of the Money Laundry and Terrorism Financing Prevention Policy adopted by the Manager;

(b) adoption of control measures designed to confirm and review registration information of clients, in case the Manager has a direct relationship with the investors, and counterparts in the operations, whenever their identification is possible and according to the nature of the operation;

(c) recording and reporting to the Board in case of suspected economic/financial activity developed by the client;

(d) maintenance of proper updating of registration information and those inherent to the knowledge process, in the form and periodicity defined in the Money Laundry and Terrorism Financing Prevention Policy, as well as risk rating of clients whom the Manager has a direct relationship with, identifiable counterparts and service providers and relevant partners for the activity of professional management of third party resources;

(e) guidance to the team for the purpose of recording all operations carried out by the Manager for a minimum period of 05 (five) years after their date of conclusion, as

well as the documentation that proves the adoption of the procedures provided for in ICVM 617;

(f) identification and thorough supervision of the operations and relations held by people rated high risk, in the form of the Policy adopted by the Manager, and ensure their registration is updated;

(g) reporting to COAF (Brazilian Financial Activities Control Council) upon identification of serious evidence of "laundry" crimes or concealment of assets, rights and securities deriving from criminal infraction, in the operations coordinated by the Manager, archiving for a minimum period of 05 (five) years, the foundation that led to the reporting or to the decision of not reporting, as the case may be; and

(h) preparing the report related to the internal risk assessment for the purposes of the Money Laundry and Terrorism Financing Prevention Policy, until the last working day of April, every year.

VII. Conduct of Workers:

(a) analysis of any infractions of the rules contained in the manuals and internal policies and of the current legislation, suggesting to the Board suitable administrative sanctions; and

(b) assessment of occurrence or indications of violation of the legislation CVM is competent to inspect, aligning with the Board the reporting to CVM, in a maximum term of 10 (ten) working days from the occurrence or identification, as well as archiving the documentation related to the assessment that has founded the decision to report or not to CVM.

VIII. Conflict of Interest:

(a) investigation, whenever it happens, of potential situations of conflict or incompatibility of interests between workers, clients and the Manager itself, guiding the parties involved and taking the suitable measures;

(b) guidance to the Board regarding the internal organization chart and regarding the controlling company, in order to prevent the adoption of conflicting positions by workers while performing their duties at the Manager; and

(c) previously assess the external activities carried out by the workers, either profit-seeking or non-profit, in order to identify potential risks to the reputation and

image of the Manager, as well as any influence on the discretion of the workers while carrying out their duties at the Manager.

IX. Hiring employees, service providers and other partners:

(a) preparation and maintenance of internal controls aiming at the knowledge of employees and partners of the Manager, with the purpose of ensuring high standards of its personnel, avoiding hiring people without an unblemished reputation or that may, in any manner, damage the image and the reputation of the institution, according to the parameters defined in the specific Service Provider Selection, Hiring and Monitoring Policy; and

(b) certification of all workers who have the required qualifications to carry out their respective functions at the Manager and follow the rules of conduct and restrictions established in the legislation that regulates the activities.

X. Provision of Information:

(a) send periodic and occasional information demanded by CVM and ANBIMA;

(b) keep registration data of the Manager with regulating and self-regulating bodies duly updated, as well as those made available at the website of the Manager in the Internet, especially regarding the manuals and policies adopted by the Manager, and those related to the team;

(c) preparation of annual report on the internal control activities, pointing to the conclusions of the assessments made, recommendations about identified deficiencies or failures in internal controls, setting a reorganization schedule, which must be submitted to the Board and archived at the headquarters of the Manager;

(d) considering the intention of the Manager of managing equity funds, one he duties of the area of Compliance is assuring that the ABVCAP/ANBIMA Database remains properly updated, under the terms of the Database Guidelines of the ABVCAP/ANBIMA Code of Regulation and Best Practices for the Market of Equity Funds (FIP) and Investment Funds in Emerging Companies (FIEE).

XI. Business Continuity:

(a) structuring the business continuity plan;

(b) activating the Business Continuity Plan annually in order to ensure its effectiveness in the event of contingency with efficiency and agility, preventing the stoppage of social activities;

(c) in case of contingency, preparing reports containing the reasons that have caused the situation, as well as suggesting measures to the Board in order to prevent new incidents.

XII. Risk Management:

(a) checking compliance with the internal controls and confirming the actions taken in order to follow the Risk Management Policy, including checking proper archiving of information and documents, especially the monthly Risk Report;

(b) analysis of occasional non-conformities reported by the Risk Officer and assessment of appropriateness of adjusting the internal procedures or, furthermore, the need of applying the rules of enforcement, always considering the severity of the infraction and recurrence;

(c) checking the procedures inherent to legal, image and systemic risk monitoring.

CHAPTER IV
GENERAL PROVISIONS

4.1. The area of Compliance shall keep a spreadsheet with the deadlines of all periodic and occasional obligations related to the activities carried out by the Manager, in line with the regulation and self-regulation which the Manager and its activities are bound by. The spreadsheet may be prepared with MS Excel or with an outsourced system.

4.2. Control of the routines of the area of Compliance shall be made with an internal spreadsheet.