IG4 CAPITAL

BUSINESS CONTINUITY PLAN
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: 205EC3047D054CD...

Flávia Andraus Troyano

Compliance Officer

CHAPTER I
PURPOSE

1.1. The purpose of the Business Continuity Plan of the Manager is to ensure continuity of operations in the event of a long unavailability of essential resources (people, data, information systems, equipment and facilities).

CHAPTER II
OPERATIONAL CONTINUITY PLAN

2.1. The Operational Continuity Plan of the Manager is comprised of the following phases, which are coordinated by the area of Compliance:

a) Identification of activities essential to carry out the activity of professional management of third party resources:

Essential activities for the corporate purpose of the Manager are all of those which comprise the investment and divestment process and follow up of invested companies by managed investment funds.

b) Identification and analysis of risk in potential:

The most common incidents that may result in operational discontinuity are fires, floods, blackouts, robbery, strikes, attacks from hackers, computer virus, sabotage and human errors, blockage or impossibility to access the building, severe failure of the Internet link and its redundancy, hardware or software, as well as issues related to public health.

c) Identification of interruption of resources:

As any interruption of any essential resources to the activities of the Manager is identified, the Compliance Officer must be immediately communicated, in order to take suitable measures in the terms of this Business Continuity Plan.

In order to characterize an emergency situation, the impediment to carrying out the essential activity must be for a long or indefinite time. Time is considered to be long whenever the time elapsed since the interruption of the activity reaches 24 (twenty-four) hours, the time expected for solving the interruption is longer than 24 (twenty-four) hours, when the remaining time for the conclusion of the activity is insufficient for it to be carried out in the same day or if failing to immediately carry out the activity may cause losses for the managed portfolios.

d) Communication to the Workers of the Manager:

It is a responsibility of the Compliance Officer or of the Worker assigned by her, communicating the contingency to the Workers of the Manager, guiding them about the suitable attitude and measures, according to the nature and severity of the contingency, being responsible for the implementation of the activation and operationalization of the Plan below, presented in a maximum period of 24 (twenty-four) hours after identification of the interruption of the normal flow of resources, according to the item above.

e) Activation of the Plan and access to the information for continuity of critical operations:

Activation of the Continuity Plan consists in the access, by the Workers, to the data and information required to carry out their respective activities, at a different location from the corporate headquarters.

All systems hired to help in the process of analysis and management of portfolios may be accessed from any location, only requiring a connection to the World Wide Web. Such systems have their own redundancy and security mechanisms.

The area of Compliance shall contact service providers critical for the business of the Manager, according to a list held internally and updated quarterly, informing alternative communication channels and the form of business continuity.

f) Periodic Tests:

Tests of the activation of the Plan are carried out annually by the Department of Compliance, jointly with the IT Team. In that opportunity, a professional assigned by the Compliance Officer must work at least for one day with the laptops intended for that purpose.

In addition to checking distance working, the area of Compliance shall validate with the IT Team the correct maintenance of the file backup and recovery process, in line with the routines indicated in the Information Security Policy present in the Code of Ethics and Conduct.

CHAPTER III
RECOVERY PLAN

3.1. This Plan has the purpose of defining a guide to recover and restore the functionalities affected that support the investment decision-making process, in order to reestablish the environment and the original operating conditions in the shortest time possible.

3.2. Thus, the area of Compliance is responsible for developing reports 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; Such reports must be submitted to the Board of the Manager in order to promote suitable initiatives to return to normality as soon as possible.

3.3. After returning to normality, in the attempt to prevent similar incidents, the Manager shall study preventive procedures to be implemented and included in this Business Continuity Plan.