CONTINGENCY PLAN

KIRON CAPITAL GESTÃO DE RECURSOS LTDA

Version 1.2
August 2021

Contingency Plan

1 INTRODUCTION

1.1 Purpose

The purpose of this Contingency and Disaster Recovery Plan ("Contingency Plan") is to organize the procedures related to the management of contingency situations, incidents, disasters or failures that may impact the operating routines of KIRON and its Investment Vehicles ("Contingency Events").

Contingency Events are described in detail in the KIRON manuals and policies, where applicable, such as: temporary interruption in the provision of infrastructure services (electricity, internet access, telephone service), occurrence of impediments to access to KIRON headquarters (fire, temporary ban on entry, and other catastrophes in the building where the company operates), operational risks and organizational risks that may affect the continuity of KIRON's activities and of the Investment Vehicles.

Among the activities critical to KIRON, this Contingency Plan proposes to cover the following:

(i) The continuous execution of trades by the Investment Vehicles, with proper fulfillment of the pertinent compliance rules;
(ii) The continuous execution of the operational routines of the Investment Vehicles and the management firm;
(iii) Regular communication between Collaborators, clients and partners, either by email or telephone;
(iv) Uninterrupted access to systems, information and files licensed or owned by KIRON.

2 PREVENTIVE MEASURES

KIRON adopts the following preventive measures for the possible Contingency Events:

A. Emergencies and fire drills: The Collaborators are obliged to participate in the periodic fire drills carried out by the office complex in order to familiarize themselves with the minimum procedures required in the event of an occurrence that requires evacuation of the building.

B. Circulation of third parties: visitors are identified by the office complex management, and only allowed to go to the KIRON office with previous approval of one of the employees. Moreover, the entry of Collaborators into the office is controlled by a system of personal passwords, installed at the only entrance way available in its office, thereby avoiding access by third parties who may have taken possession of the Collaborators' personal ID badges (which only allow entry into the building, but do not guarantee actual access to the Company's offices).

C. Monitoring of the Corporate Environment: the corporate environment is monitored by cameras installed in strategic locations throughout the office, allowing the identification of those who circulate in its common areas at all times, with the respective retention of the recordings.

D. Periodic Infrastructure Evaluation: on an annual basis, KIRON – with the aid of third-party service providers, re-evaluates its servers, internet access links, redundancy of services, as well as electrical circuits and other services of the office complex relevant to the company, aimed at mitigating risks to the continuity of activities due to failure of support infrastructure.

3 IT INFRASTRUCTURE AND DISASTER RECOVERY

The company's infrastructure (installations, hardware and software) are all first-rate and aimed at meeting the most demanding investors. In this regard, KIRON operates with a dual redundancy policy, with servers, storage and firewall replicated internally and also replicated in the cloud (Microsoft Azure and Amazon AWS). Thus, there are always three complete sets of infrastructure (two physical sites and one cloud site) available 24/7 and in parallel operation, so that any failure at any point in the infrastructure is immediately replaced in real time in a seamless structure integration that keeps all services running.

All this operational structure is aimed at ensuring that activity can be maintained for the longest time possible at KIRON's office. Additionally, the company has a service agreement with an IT infrastructure provider and an information security provider, both available 24/7. These vendors are able to work remotely on almost all problems and, if necessary, are committed to sending a technician to the office for support.

The email system is located in the cloud (Microsoft Office 365), with a local contingency domain. The office has redundancy in internet access (2 links) and electricity backup (1 UPS with 1 hour of autonomy, plus a generator in the building, which comes into service on average 8 seconds after a power outage). Additionally, there are always backup PCs in the event of failure of existing equipment.

It is also worth mentioning that all network/login/password permissions are synchronized online with the Private Cloud environment, in view of the existence of a network domain controller. In other words, a password change in the production environment is replicated in the Private Cloud environment in a matter of seconds, thus enabling remote access to the network with the same login and password used in the physical office. Remote access to systems and files by employees is done via a VPN with Two Factor Authentication, to make sure that a password leak does not allow someone outside the company to access the systems and files.

Furthermore, the Disaster Recovery framework mirrors all internal services (files saved once a day, databases once a day, and accesses and permissions of online users), and are fully available through virtual computers. Thus, key processes (Trading, Compliance, Back Office and IR) do not suffer any shutdown, even in the event of a disaster.

KIRON's entire technology environment is protected by firewall operating in redundancy and 24/7 monitoring, in order to ensure maximum availability and immediate handling of occurrences.

Infrastructure summary:

Systems and Databases	Located on local servers at KIRON headquarters, as well as redundancies in the cloud, distributed between Microsoft (Azure) and Amazon Web Services.
Files	Located at the company's office, at Rua Tabapuã, with scanned copies available on the local server in a real-time mirroring system between two servers ("bridge") and in the Microsoft datacenter, in a daily back-up regime, with a history and versioning control.
E-mails	Stored and streamed through a Microsoft cloud solution (Office365), with retention for the last five years.
PABX/Telephony	Available via Amazon Web Services and also in the database of the PABX provider (Option Telefonia). VoIP is programmed to allow transfers of calls made to the extensions of the Company to the corresponding personal cellphones of Collaborators.

Virtual Desktops	Four Virtual Desktops available at the KIRON IT infrastructure service provider's datacenter, which are always up-to-date and fully compatible with the operating systems used in the Company's daily routines. Access to Virtual Desktops is also available via VPN with Two Factor Authentication, allowing the full continuity of the critical functions inherent to the business in case of a Contingency or Disaster Event. For access to such Virtual Desktops, suffice it for the collaborator to have a computer (Windows or Mac) with internet access.

4 PROCEDURES

4.1 Procedures during a Contingency or Disaster Event

System failure:
In the case of a Contingency Event that involves discontinuity in the provision of service linked to the operating systems considered critical (Covered Systems) and/or in its servers and network, the Information Security Committee, in partnership with the IT service providers, will act to re-establish access to such systems on an emergency basis. If such failure is due to a Contingency Event in which access to the physical office of KIRON is unfeasible, the Collaborators must be instructed for systems to be accessed remotely and according to the guide of remote access via VPN.

Infrastructure failure:
(a) Electric Power: if there is a power failure, KIRON has a battery-operated UPS with autonomy up to 1 hour, in addition to the building's generator, which automatically starts within 8 seconds of the power outage.

- Main Actions and Persons Responsible: In the event that the electricity back-up devices listed above do not work or are insufficient, the Information Security Committee will instruct Key Users to go to their respective homes and to continue working through access to Virtual Desktops.

(b) Communications: KIRON has two internet access links (redundancy) in the event of a service outage by the internet provider and/or data link, and two firewalls operating simultaneously, in redundancy ("bridge"). Likewise, telephone services are provisioned in the cloud of Amazon Web Services, in addition to all extensions being connected by PABX, configured through an IP VPN, thus allowing the provision of uninterrupted voice link.

- Main Actions and Persons Responsible: The Information Security Committee will be responsible for activating the call forwarding script so that Collaborators have full access to calls made to their original extensions on their personal mobile phones.

(c) Disasters (Fire, flood, robbery, etc.): Contingency events that involve the evacuation and/or inaccessibility of the physical office where KIRON's headquarters are located, making it impossible to access the company's operating systems.

- Main Actions and Persons Responsible: In addition to standard building evacuation procedures and active response by fire brigade members to safeguard KIRON's collaborators, the Information Security Committee and the Chief Compliance and Risk Management Officer will be responsible for enabling the activation of the contingency site, allowing critical areas and collaborators to have secure and full access to the network, the Covered Systems, their emails, and other minimum resources necessary for operational restoration, with no major disruptions.

- In order to do this, collaborators are advised to proceed to their homes or to a safe place where, using any computer, they can access the virtual computers that are available 24/7.

4.2 Procedures after Contingency or Disaster Event

In the event of a Contingency or Disaster Event, a Crisis Management Committee will be formed, essentially consisting of the Information Security Committee, the Compliance and Risk Management Officer, and a collaborator appointed jointly by both. The Crisis Management Committee shall be responsible for:

(i) assessing the direct and indirect impacts;
(ii) developing and implementing a plan of action for the recovery of services impacted, especially aimed at re-establishing KIRON's critical functions, as soon as possible;
(iii) communicating to the other collaborators about the aforementioned action plan and, if necessary, call them to a face-to-face meeting to clarify doubts and to go over the measures that have been and will be adopted in such scenario; and
(iv) repairing the affected structure, including, but not limited to, re-establishing the environment, network and operational systems, as well as establishing methodologies to prevent the occurrence of new contingency or disaster events with similar characteristics (if and when possible), thereby mitigating the risk of recurrences.

The Crisis Management Committee shall be instated and remain operative until all problems resulting from the Contingency or Disaster Event have been remedied and the functions and activities of KIRON have been fully re-established.

4.2.1 Records of events

The Crisis Management Committee will be responsible for recording any and all incidents involving the activation of the contingency procedures described in this plan. Such record shall consist of at least the following:

- Description of facts;
- Date and time (where applicable) of the occurrence;
- Description of the measures adopted;
- Date and time (where applicable) of re-establishment of normal working conditions;
- Additional information (eventual outcomes, damage, etc.); and
- Signatures of the Chief Compliance and Risk Management Officer and a member of the Information Security Committee.

These records will be stored with the Director of Risk Management for a period of five years.

4.3 Periodic Reviews

This Contingency Plan will be reviewed annually by the Chief Compliance and Risk Management Officer, or whenever there are changes in the processes or structure adopted by KIRON (whether by optimization, adjustments or introduction of new technologies), as needed.

Contingency Plan

All collaborators will receive a copy of this Contingency Plan, together with the Compliance Manual, Code of Ethics and Cybersecurity Policy. Collaborators can also access it at any time, in its most current version, on the company's website.