DISASTER RECOVERY PLAN

VELT PARTNERS

1. Introduction

1.1. Purpose

VELT Partners Investimentos Ltda. ("**Firm**" or "**VELT Partners**") has prepared this disaster recovery and contingency plan (the "**Disaster Recovery Plan**") in order to set forth the appropriate procedures to manage contingency situations, incident, disaster or failure scenarios that have an effect on the operational routines of the firm as a whole ("**Contingency or Disaster Events**") to ensure full continuity of the activities of the firm for VELT Partners and its employees at all times and under any circumstances.

The following are examples of Contingency or Disaster Events: full suspension or temporary interruption in the provision of services by providers of electricity, internet access, telephone communication services etc., natural catastrophes that prevent access to the building, prevented access to the building where the headquarters of VELT Partners are located for any reason, including in strike scenarios, failure in systems and software used by the Employees of the Firm, losses of files for any reasons, among other things.

Among VELT Partner's critical functionalities that this Disaster Recovery Plan seeks to cover the following are included (i) continuous execution of trades (with the respective maintenance of the applicable compliance rules), (ii) performance of operational rules, (iii) possibility to receive and regularly exchange emails (both internal emails and emails with external counterparties) and to answer the telephone through the switchboard in addition to (iv) uninterrupted access to, and use of, systems, functionalities and files used by the Firm, as specified in item 1.2 below ("**Covered Systems**"), including in case of complete impossibility to access the physical offices of the Firm.

1.2. Covered Functionalities and Systems

The following are covered functionalities and systems for purposes of this Disaster Recovery Plan:

(i) Emails & Intranet;

(ii) Files;

(iii) Controls system, trade and compliance system, order management system, portfolio systems – AlphaTools/INOA*;* and

(iv) *Bloomberg*.

2. Preventive Measures

VELT Partners adopts the following preventive measures seeking to mitigate any risks of occurrence of Contingency or Disaster Events:

A. **Escape route, emergency signs and fire drills:** the escape route signs and the emergency signs are placed at strategic places at the offices of the Firm and are easily identifiable. Employees are also instructed to behave appropriately in case of incidents involving fire. In this case, employees are under an obligation to participate in fire drills conducted from time to time by the building to become familiar with the minimum procedures needed in case of an occurrence that requires the building to be evacuated.

B. **Identification of visitors / Circulation of third parties:** to ensure a minimum level of security at its premises, visitors are identified by building staff and only allowed to go up to VELT Partner's office after the prior approval of an employee. In this sense, visitors and contractors are instructed to comply with the standard procedure to circulate within the offices and their entry in the main room is not allowed, unless they are accompanied by an employee. In addition, entry by employees at the offices is controlled by a biometric system implemented at the only entrance available to the offices, preventing entry by third parties who may gain possession of employee security passes (which only allow entry into the building, but not into the offices of the Firm).

C. **Monitoring the Corporate Environment:** the corporate environment is monitored by cameras placed at strategic points throughout the offices allowing the identification of who circulates in the common areas thereof at all times and retaining the recordings.

D. **Periodic Assessment of the Electric Circuits and Hydraulic Systems:** by means of outsourced personnel the Firm reassesses every year the electric circuits and hydraulic systems of its offices to mitigate short circuit and rupture risks and/or defects in the hydraulic systems (meters, valves, infiltration points).

E. **Employee Telephones:** on its intranet, the Firms provides its employees with access to a list of personal cell phones of each employee, also for use in case of emergency, facilitating communications in distress or emergency situations.

3. Technology Infrastructure

VELT Partners has a strong technology infrastructure. The Firm operates with 3 cloud-based datacenters - Microsoft Azure, AWS and Google Cloud. Microsoft Azure has geo-redundancy services in another continent and is where AlphaTools, File Server and the backup files are kept. Whereas AWS is responsible for the intranet and Google Cloud for the Data Science filings.

Systems and Data Base: The server in charge of the production system (Alpha Tools) and database service are located at an external datacenter (Microsoft Azure Cloud, hereinafter referred to as "Cloud") under an agreement that includes 99.99% of uptime and geo-redundancy – i.e., the systems and mirrored online on another system of the supplier located in another continent. VELT Partners connects with Microsoft Azure through an encrypted VPN and IP redundant.

Files: VELT Partner's servers in charge of the file system (File Server) are located at Microsoft Azure with daily back-ups and a 5-year retention policy.

Email: The email system is also located outside the offices (Microsoft Office 365) and automatically retains/stores all emails for 5 years. Therefore, in case of a Contingency or Disaster Event the whole history of emails will be available via webmail, which is also subject to a two-factor authentication mechanism, and the email entrance and exit flows will not be affected.

Access to the network: All network/login/password permissions are controlled by a domain controller within the Microsoft Azure, thus allowing remote access to the network with the same login and password details as used in the physical office. Remote access to the systems and files is available through a VPN with Two Factor Authentication to ensure no password leakage.

Telephony: Our telephone system (PBX and trunks) is also located in Microsoft Azure. All extensions connect to this PBX by means of a redundant VPN IP. In case of a contingency, calls made to the original extensions will be forwarded to each person's personal phone. Therefore, there is certainty of complete and unrestricted telephone access in Disaster Recovery situations. In addition, it is important to emphasize that all calls are recorded and are retained for 5 years.

Offices: VELT Partner's offices enjoy redundancy for internet access (3 links), electricity backup (2 no-break power systems with 3-hour autonomy and 4 generators in the building and firewall redundancy. In addition, there are backup Notebooks available in case of fault in the existing equipment. This Disaster Recovery Plan has been structured to guarantee the longest time of activity possible for our offices.

Disaster Recovery: The external Disaster Recovery structure (please see below "Disaster Recovery Structure and Plan") is automatically synchronized and can be accessed in Contingency or Disaster Events, subject to the criteria and procedures determined below.

4. Disaster Recovery Structure and Plan

VELT Partners has a strategy for disaster scenarios comprising (i) backups of its systems and (ii) remote access workstation, with daily synchronicity. These are fully available for use in case of a physical disaster involving its offices.

(i) System Backup: in relation to the systems, all production systems of the Firm are in a Microsoft external datacenter in São Paulo, with online backup to another datacenter of the same supplier in another continent (geo-redundancy). Therefore, in case of a physical disaster in the main datacenter, employees will be immediately able to access the production systems from the backup datacenter.

(ii) Remote access: in relation to remote access by employees of the Firm to their computers, the Firm has a virtual workstation at the Cloud for contingency scenarios. The purpose of the virtual workstation is to satisfy the needs of the most critical areas of the Firm whose functions are time sensitive and cannot stop ("**Virtual Workstation**"). The Covered Systems are updated in the Virtual Workstation always making a Disaster Recovery ("**DR**") environment. Whenever a new system is installed or a version of a system is updated in the production environment, the same procedure is replicated in the DR environment. Accordingly, everyday use laptops and the Virtual Workstations are simultaneously synchronized. Remote access to such workstations is available through a VPN with Two Factor Authentication to ensure no password leakage. Similarly, the webmail access is also available through a two-factor authentication mechanism. The entire DR environment is protected by a firewall.

Access to the DR environment takes place by using the same username and password adopted for regular access in the Firm, but with the additional closing of the VPN with the Two Factor Authentication in the environment, similarly to what is already currently done for remote access.

5. Procedures

5.1. Procedures during a Contingency or Disaster Event

- **System Failure:**

In case of a Contingency or Disaster Event resulting in the discontinuity of the provision of a service related to operating systems deemed critical – Covered Systems, and/or its servers and network, the CTO will act to restore access to such services on an emergency basis in addition to immediately activating and providing a redundant mode on the network. Should such failure result from a Contingency or Disaster Event that prevents access to the physical offices of VELT Partners, employees are instructed to work from home, using their laptops which can be connected to the Cloud via VPN or accessing the Virtual Workstation.

- **Infrastructure Failure:**

(a) Electricity: should there be a failure in the supply of electricity, VELT Partners relies on the following resources: (i) 2 secondary electricity feeding systems (no-break power systems) with 3 hours battery autonomy; and (ii) 4 generators in the building, automatically triggered upon the occurrence of a power failure and have more than 36-hour autonomy.

- ✓ Key Actions and Persons in Charge: In case the above-mentioned electricity backups do not work or are insufficient, the CTO will instruct the Key Users to go home and operationally continue their work by accessing their laptops which are connected via VPN to the VELT infrastructure located in the Cloud.

(b) Communications: VELT Partners has 3 internet access links (redundancy) for the possibility of failure in the provision of this service by the internet provider and/or the data link. All line extensions are linked to a switchboard that is connected to a redundant VPN IP, allowing uninterrupted voice link supply.

- ✓ Key Actions and Persons in Charge: IT team is responsible for setting up Employees personal cellular telephones so that employees are forwarded and have full access to calls made to their original extensions.

(c) DPC Environmental Control: the DPC environment located at the offices of VELT Partners is regularly monitored to ensure that it works correctly and maintains the temperature (approximately 21º C).

- ✓ Key Actions and Persons in Charge: The CTO is responsible for monitoring the minimum operation conditions of the DPC every day, including by means of remote access. Should there be any intercurrence in the DPC environment resulting in failure in the control mechanisms and/or changes in such conditions, the CTO will act to mitigate such failures and reestablish the functionalities thereof and will also inform VELT Partner's Compliance and Risk Management Officer (appointed under its by-laws) if the CTO notes that a problem with the DPC may cause ancillary systemic failures. In this sense, the CTO and the Compliance and Risk Management Officer will act together to develop an immediate action plan. Depending on the level of complexity of the failure and as a security measure, the Compliance and Risk Management Officer may instruct the other employees to evacuate the offices and continue to work from home using their laptops which can be connected to the Cloud via VPN. Should this happen, the CTO will ask the office manager to immediately inform the facts to the building.

(d) Disasters (Fire, flood, theft etc.): Contingency or Disaster Events resulting in the evacuation of, and/or no access to, the physical offices in which the headquarters of the Firm are located, preventing access to the operating systems of the firm.

- ✓ Key Actions and Persons in Charge: In addition to the standard evacuation procedures of the building and active participation of the members of the fire brigade to safeguard the lives of VELT Partner's employees, VELT Partner's CTO, and in his/her absence, VELT Partner's Compliance and Risk Management Officer will be in charge of activating the contingency site, allowing the main critical areas and the employees for whom access shall have been designated, as provided above, to have safe and full access to the network, the Covered Systems, their emails and other minimum required resources for the operational resumption of the activities without further disruptions.

  For such purpose, the guidance to employees is to return to their homes or a safe place in which they can, with the use of any computer, access the virtual workstations available at the Cloud, following the procedures set forth in item 4.2 below.

- ✓ Action Time: Immediate - the sooner the action on the part of the Firm and its employees the smallest the losses. VELT Partner's CTO will be fully available to the Key-Users to allow access to the Covered Systems in Contingency or Disaster Events.

5.2. Access to the DR Environment

As all Covered Systems are on the cloud, Contingency or Disaster Events and events causing unavailable access to the physical offices do not cause a direct impact on business continuity. To this end, we rely on preconfigured Virtual Workstations that allow immediate continuity of the most critical functions, as discussed in more detail below.

In this scenario, employees continue to have full access to their emails (including cellular telephones) and redirected calls originally made to extensions. The databases, systems and files are in the precise state as they were immediately before the Contingency or Disaster Event and all that is necessary is to access the Virtual Workstation. The procedures for access to the Virtual Workstations are detailed below:

- ➢ Access to the DR using Windows 11 / 10
- ➢ Access to the DR using Mac

The Firm provides access to the DR environment to two separate groups of employees, namely:

(I) Key Users – In a Contingency or Disaster Event, the Virtual Workstation is available primarily to the 4 critical areas for business continuity purposes: Trading, Operations, Compliance and Investor Relations.

(II) Other Employees: Subsidiarily, additional Virtual Workstations will be available to the IT area and other employees who will be able to access the network files and for such purpose just need to use the VPN.

Service priority is for the Key Users, followed by restoration of the production environment and next service to, and access by, other users. In case of problems in relation to access during a Contingency or Disaster Event, employees are instructed to call or contact one of the IT members of the Firm.

5.3. Procedures after a Contingency or Disaster Event

In the occurrence of a Contingency or Disaster Event, a crisis management committee ("**Crisis Management Committee**") will be established, comprising essentially the CTO, the Compliance and Risk Management Officer and one employee designed together by both and they will be responsible for:

(i) assessing actual direct and indirect impacts;

(ii) preparing and implementing an action plan to recover all impacted services, to reestablish the 4 critical functions of the Firm as soon as possible;

(iii) informing the other employees about the action plan and if necessary calling them for a face to face meeting to clarify doubts and discuss the steps that will have been taken and will still be taken in such scenario; and

(iv) acting to repair the affected structure, including, without limitation reestablishing the environment, the network and operating systems, and establishing methodologies to prevent the occurrence of further contingency or disaster events with similar characteristics (if and where possible) thus mitigating the risk of recurrence.

The Crisis Management Committee will be put in place and will continue to act until all problems resulting from the Contingency or Disaster Event are remedied and the functions and activities of the Firm are fully resumed.

6. Logs, Training, Tests and Periodic Reviews

6.1. Logbook

The Crisis Management Committee shall record in a logbook all events that result in triggering the contingency procedures described in this plan. Any entry shall contain at least:

- Description of the facts;
- Date and time (where applicable) of the occurrence;
- Description of the steps taken;
- Date and time (where applicable) of the resumption of normal work conditions;
- Additional information (incidents, damages and similar items); and
- Signatures of the Compliance and Risk Management Officer and the CTO.

The logbook shall be stored by the Compliance and Risk Management Officer for five years.

6.2. Periodic Training

All employees shall attend an annual training about this Disaster Recovery Plan (and where necessary, additional meetings on the topic), which can be delivered through internal communications drafted for the consciousness of all Employees. If training, it shall be prepared and delivered by the CTO under the supervision of the Compliance and Risk Management Officer.

6.3. Periodic Reviews and Testing

This Disaster Recovery Plan shall be reviewed by the CTO on an annual basis or whenever required upon the occurrence of changes in the processes or the structure adopted by VELT Partners (as a matter of optimization, adaptation or introduction of new technologies) and is subject to validation by VELT Partner's Compliance and Risk Management Officer.

Once per year (or at a shorter period if necessary), the Key Users will be subject to a test by means of a simulation of a disaster event as per described herewith. Key Users will be required to access the DR environment to ensure the remote access reliability, security, consistency of its database in accordance with files previously saved, and that it can be easily and timely accessed to ensure the business continuity. Attendance sheet will be filed in the Firm´s offices.

All Employees can access the most updated version of this Disaster Recovery Plan at any time by accessing the internal HUB platform which is also linked to the Teams Group dedicated to Compliance and Risk.