



CONTINGENCY POLICY

This material has been prepared by ("Domo Venture Capital Gestora De Ativos Financeiros e Valores Mobiliários Ltda. DOMO" or "Manager") and may not be copied, reproduced or distributed without the prior and express agreement of the latter. The terms and expressions used herein in capital letters have the meanings attributed to them in item 1 of DOMO's Code of Ethics and Conduct.

São Paulo, March 5 of 2026

SUMMARY

1	Objective	3
2	Predicted Events/Threats	3
3	Classification of Events/Incidents	3
4	Internal Procedure (Key Persons)	3
5	Alternative Workplace	3
6	Data and Document Protection and Recovery	4
7	Public Communication	4
8	Periodic Evaluation and Testing	4

CONTINGENCY POLICY

1 Objective

1.1. The purpose of the Contingency Policy is to define the Contingency and Disaster Recovery Plan ("Contingency Plan") to be followed by DOMO, in order to prevent the operational discontinuity of the Manager, considering the occurrence of the Events/Threats Foreseen in item 2 below, determining the procedures that must be followed in order to protect the interests of the Investors and the continuity of activities.

2 Predicted Events/Threats

2.1. DOMO's Contingency Plan includes as main events/threats to the Manager's business, including, but not limited to:

- Low connectivity or loss of internet connectivity;
- Systemic intrusion that harms internal data;
- Failure in telephone lines;
- Temporary inaccessibility of the office;
- Permanent inaccessibility of the office;
- Inaccessibility of the Directors responsible for decision-making for more than 24 (twenty-four) hours; e
- Any other situation that threatens, physically, structurally or virtually, the Manager's environment, even if not described above.

3 Classification of Events/Incidents

3.1. Contingency events may be classified according to their severity and potential impact (low, medium, high or critical), considering unavailability of systems, impact on the Funds, regulatory exposure and reputational risk, and it is up to the Key Persons to prioritize response and communication actions according to the level identified.

4 Internal Procedure (Key Persons)

4.1. In case of effective need to implement the Contingency Plan, the "Key Persons", previously identified in this way by the Compliance area, must be referred to the Alternative Location.

4.2. Key Persons will assess the event or threat and determine the duties and responsibilities of the other Employees.

4.3. Key Persons should be responsible for the priority functions:

- *Alternate Site Use Trigger*: Managing Director
- *Contact with Employees*: Compliance Director
- *Contact with Investors and Counterparties*: Compliance Officer / Risk Officer / AML/CFT Officer / Managing Director
- *Reliability of Stored/Retrieved Data*: Chief Risk Officer

5 Alternative Workplace

5.1. In cases of temporary or permanent inaccessibility, the Contingency Plan contemplates the use of an alternative workplace, and may authorize DOMO Employees to work from their homes or to go to a specific location that will be defined by the Compliance area.

5.2. In case of emergency, DOMO has the installation of an "Emergency Room" in Rio de Janeiro, in a specialized company, which can be used as an alternative work office in case of unavailability of the headquarters in São Paulo. The alternative site in Rio de Janeiro is available to receive up to 07 (seven) Employees considered Key Persons.

5.3. Both offices have computers with internet access, and it is possible to access the entire database and systems, saved "in the cloud", through the service contracted with Google (Google Drive; Vault), as well as landlines and notebooks for use by Employees. DOMO's office has redundancy of internet access (broadband). The residential address of the 03 (three) Partner-Directors is also prepared to receive up to 04 (four) Key Persons, if necessary.

6 Data and Document Protection and Recovery

6.1. DOMO's electronic data is kept "in the cloud", on Google servers, and daily *backups* of the Manager's information are performed.

6.2. In addition to the daily *backup* procedure, a physical copy of the files is made by each of the 03 (three) Partners, and, alternatively, the use of additional backup (Dropbox) is also contracted.

6.3. The Compliance area will supervise access to the information contained in the *backups* and will only use this information for internal purposes or under the terms provided for by law.

6.4. Included in the Contingency Plan are information technology and cybersecurity incidents, such as cyber attacks, data leakage, unavailability of systems, backup failures, improper access and corruption of databases. Such events must be immediately communicated to the Risk and Compliance areas for assessment, mitigation and, when applicable, communication to the authorities and affected parties, in compliance with the applicable legislation, including the Law No. 13,709/2018 (LGPD).

7 Public Communication

7.1. In the event of an event or threat resulting in the temporary or permanent inaccessibility of the firm, the Compliance area is responsible for preparing a formal communication to Investors, contracted third parties and the market in general.

7.2. If it is impossible for the Compliance area to act, only the Executive Board is authorized to perform this function, and the other Employees are absolutely forbidden to publicly communicate about what happened.

7.3. When applicable, the Compliance area will assess the need to communicate the contingency event to the CVM, ANBIMA and other relevant regulatory parties, under the terms of the regulations in force.

8 Periodic Evaluation and Testing

8.1. The Contingency Plan must be evaluated and tested periodically, at the discretion of the Compliance area, due to the natural changes that occur in the Manager, such as entry and exit of Employees, change of systems, change of protection strategy, etc. It is established that the execution of this test is the responsibility of the Compliance area.