



CYBERSECURITY AND CONFIDENTIALITY POLICY

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

São Paulo, March 5 of 2026

TABLE OF CONTENTS

1. Purpose	3
2. Concept of Confidential Information	3
3. Access Controls for Confidential Information	3
4. Information Barriers.....	3
5. Segregation of Activities.....	4
6. Cybersecurity	4
6.3. Officer Responsible for Cybersecurity Matters.....	5
6.4. Cybersecurity Procedures	5
6.5. Use of Artificial Intelligence	9

1. Purpose

- 1.1. The purpose of this Policy is to ensure the proper management of information temporarily held by or owned by DOMO.

2. Concept of Confidential Information

- 2.1. Confidential Information means any and all information protected against unauthorized public disclosure, i.e., electronic, written or oral information to which the Associate has access within the Company, including: data of DOMO, of the investee companies of the Funds managed by DOMO, and of their partners, officers, Investors and Associates, as well as reports from regulatory and self-regulatory bodies and public authorities, data from inspections and audits, marketing materials and other information owned by the Company.
- 2.2. The Associates' duty of confidentiality regarding the information to which they have access within the Company, or related to its Investors, shall survive their termination.

3. Access Controls for Confidential Information

- 3.1. All access to DOMO's information directories and systems must be controlled by the Compliance department. Only Associates previously authorized by the Chief Compliance Officer may access such information directories and systems.
- 3.2. Access control to DOMO's information systems shall take into account the following premises:
 - 3.2.1. Use of an Associate identifier (Associate ID);
 - 3.2.2. Assurance that the level of access granted to the Associate is appropriate to their profile;
 - 3.2.3. Immediate cancellation of the access granted to Associates who have been terminated, placed on leave or whose role within the Company has changed;
 - 3.2.4. Access log recording for the inclusion, modification and deletion of any and all information in the Company's technology environment; and
 - 3.2.5. Enabling audit trails.

4. Information Barriers

- 4.1. Associates holding Confidential or Privileged Information, by virtue of their positions or duties within the Company, must establish an information barrier with respect to the other Associates. On a non-exhaustive basis, the following conduct must be observed:

- 4.1.1. Associates should avoid circulating outside DOMO's premises with copies (physical or digital) of files containing Confidential Information, unless necessary for the development of the project and in the interest of the Investor, in which case such copies must be encrypted or password-protected;
- 4.1.2. Confidential Information in digital media must be disposed of in a manner that prevents its recovery, always under the guidance of the direct superior;
- 4.1.3. Information that allows the identification of an Investor of the Company must be limited to restricted-access files and may only be copied or printed if intended to serve the interests of DOMO or of the Investor itself;
- 4.1.4. Associates must be alert to external events that may compromise the confidentiality of the Company's information, such as computer viruses, fraud, etc.;
- 4.1.5. Confidential matters must not be discussed in public places or locations considered exposed;
- 4.1.6. The Associate's password for accessing DOMO's system is personal and non-transferable; and
- 4.1.7. The corporate e-mail must be used exclusively for matters related to the business conducted by the Company, and may be monitored by the Compliance department whenever necessary. Personal use of the corporate e-mail by Associates will be permitted provided that it does not impact the performance of their duties within the Company.

5. Segregation of Activities

- 5.1. Should DOMO come to engage in any other activity in the capital markets, in addition to third-party asset management, such new activity must be fully segregated from the activities currently carried out, except as expressly permitted by the legislation in force.
- 5.2. With regard to the segregation of the activities of the Chief Investment Officer, it is important to emphasize that their independence is an essential regulatory requirement and is intrinsically linked to the Company's culture. Accordingly, such Officer may not be responsible for any other activity in the capital markets, whether within or outside the institution.

6. Cybersecurity

- 6.1. The purpose of this section is to establish DOMO's cybersecurity rules, procedures and controls, in order to ensure the proper management of Confidential Information, as set forth in the ANBIMA Code of Regulation and Best Practices for Third-Party Asset Management, and in accordance with the recommendations and guidelines of the ANBIMA Cybersecurity Guide, dated June 2021.

6.2. In order to maintain the confidentiality of information, as well as to ensure its integrity and availability, DOMO takes into account three basic aspects, namely:

- Confidentiality: only persons duly authorized by the Company shall have access to the information;
- Integrity: only modifications, deletions and additions authorized by the Company shall be made to the information; and
- Availability: the information must be available to authorized persons whenever necessary.

6.3. **Officer Responsible for Cybersecurity Matters**

6.3.1. The Chief Compliance Officer, assisted by Mr. William Silva, DOMO's technology advisor, is DOMO's officer directly responsible for handling cybersecurity-related matters within the Company.

6.4. **Cybersecurity Procedures**

6.4.1. DOMO is responsible for acting against cyber threats through, at a minimum, the following functions: *(i)* identifying/assessing risks (risk assessment); *(ii)* prevention and protection; *(iii)* monitoring; *(iv)* preparing a response plan for potential incidents; and *(v)* governance.

6.4.2. **Risk Identification and Assessment (Risk Assessment)**

6.4.2.1. The main cyber risks to which the Company is exposed include, but are not limited to:

- Malware (viruses, trojan horses, spyware and ransomware);
- Unauthorized access to investor data;
- Unauthorized access to investee company data;
- Unauthorized copying of documents and/or confidential information;
- Personal access;
- DDoS attacks and botnets; and
- Intrusions (advanced persistent threats).

6.4.2.2. DOMO must also continuously identify all of the Company's relevant assets (whether equipment, systems, processes or data) used for the proper functioning of its activities. The vulnerabilities of the identified assets must be assessed, identifying possible threats and the degree of exposure of the assets to them, and different scenarios must be considered in such assessment.

6.4.2.3. Potential financial, operational and reputational impacts in the event of a security incident will also be considered, as well as the likelihood of such event occurring. The risk assessment process will therefore cover the activities carried out by outsourced service providers, including, but not limited to, cloud services.

6.4.2.4. Based on the identification of vulnerabilities, confidential information must be classified, thereby allowing the implementation of processes for the proper handling, storage, transportation and disposal of such information.

6.4.2.5. In this context, DOMO's relevant assets include, but are not limited to:

- Equipment: computers, flash drives and hard drives;
- Systems: proprietary systems, website, accounting systems, e-mail and Google Workspace;
- Processes: research and assessment of potential investee companies;
- Data: Confidential Information.

6.4.3. Prevention and Protection

6.4.3.1. DOMO has rules to control access to the Company's equipment, systems, processes and data, as well as rules for granting access passwords to the different devices, systems and network.

6.4.3.2. In this context, login and password change events are auditable and traceable, and remote access to internal files and systems is inventoried, with the entire process taking place within Google Workspace. All access to DOMO's information directories and systems must be controlled by means of login and password. Only Associates who need such information to perform their activities may access such information directories and systems, subject to the proper segregation of duties and upon prior authorization from the Chief Compliance Officer.

6.4.3.3. The password provided for access to the institutional data network shall under no circumstances be disclosed to any other person, and the Associate may be held liable if they make such passwords available to third parties for any purpose.

6.4.3.4. DOMO's Associates change their passwords periodically, in accordance with the Google Workspace password policy.

6.4.3.5. The password rules may be modified at any time, as a result of technological advances or an internal decision by DOMO's Compliance department, always aiming to improve procedures, systems and information security.

6.4.3.6. All content on the network may be accessed by the Compliance department, if necessary. In addition, any personal files that may be saved on DOMO's official computers may be accessed if the Chief Compliance Officer deems it necessary, whether in random or specific verification processes and/or in the event of audits or regulatory requests. The other Associates have predefined access.

6.4.3.7. DOMO backs up all of its files and systems on cloud servers, which comply with the regulatory cybersecurity recommendations, including for cloud services.

The adequacy of legal matters will also be assessed, including, but not limited to, confidentiality clauses and the requirement of security controls within the third parties' own structure.

6.4.4. Monitoring

- 6.4.4.1. Automatic monitoring is performed by Google Workspace systems.
- 6.4.4.2. There is also online monitoring of any attempted intrusions into DOMO's file system, and tests are performed using Google Workspace systems. Monitoring of security controls will follow a risk-based approach, being intensified as the level of risk increases.
- 6.4.4.3. The reports generated from such monitoring are used as the basis for updating our preventive measures and response plan.

6.4.5. Response Plan

- 6.4.5.1. Associates must report to the Compliance department any violations of the cybersecurity rules of which they become aware. Every violation or deviation must be investigated to determine the necessary measures to be adopted, aiming to correct the failure or restructure processes.
- 6.4.5.2. In cases of violation of this Policy or of the Information Security rules by Associates, administrative and/or legal sanctions may be applied, which may culminate in termination and potential criminal, civil and administrative proceedings, as applicable.
- 6.4.5.3. In the event of a cybersecurity incident, DOMO shall initiate the response plan, as described below:

6.4.5.4. Assessment and Measures

- 6.4.5.4.1. Once a cybersecurity event has been identified, the Chief Compliance Officer will call a meeting of DOMO's Executive Committee and the IT representative. The purpose of the meeting will be to analyze the facts, their causes and immediate consequences, based on the previously performed risk assessment, thereby identifying the severity of the situation, the necessary measures to be adopted and the DOMO departments to be engaged.
- 6.4.5.4.2. The Chief Compliance Officer will be responsible for coordinating the implementation of the measures decided jointly with the Executive Committee and the IT representative. Among the immediate measures, depending on the incident, the fact must also be disclosed to the competent authorities, such as CVM, ANBIMA, COAF, ANPD, etc., and, if applicable, reported to the police by means of a police report or criminal complaint.

6.4.5.4.3. Furthermore, each DOMO department must take the following actions when engaged by the Chief Compliance Officer:

IT Department or Outsourced IT Company under the Supervision of the Compliance Department:

- Verification and audit of logs;
- Preparation of a forensic report containing the information potentially leaked;
- Running applications externally or on affected systems to remove unwanted applications;
- Uninstalling software;
- Running offline scans to detect any additional threats;
- Formatting and rebuilding the operating system;
- Physical replacement of storage devices;
- Rebuilding systems and networks;
- Restoring data from the daily backup;
- Assessing whether DOMO's operations need to continue remotely, considering the level of compromise of the office facilities/systems;
- Among others.

Compliance Department

- Preparation of a report based on the forensic report prepared by the IT department, including any reputational and legal consequences arising from the damage caused by the security incident;
- In the event the security incident and any leakage of Confidential Information are confirmed, preparation of a notification to the affected clients and competent authorities informing them of the occurrence.

Back Office

- Analysis of lost data and its impact on accounting planning and on DOMO's assets;
- Planning the containment of liquidity risk in view of possible redemptions of investments resulting from the security incident.

6.4.5.4.4. If necessary, a company specialized in combating the identified event, as well as in responding to any damage, may be engaged.

6.4.5.4.5. Every incident must be duly classified by severity level (low, medium or high), considering the degree of impact on the Company's activities, and will be filed and documented by the Compliance department, and further formalized in DOMO's Internal Controls Report.

6.4.5.4.6. In addition, DOMO shall define the steps to be taken with the IT department in order to prevent the incident from recurring.

6.4.5.5. Day After

- 6.4.5.5.1. Once the problem has been identified and the necessary actions have been taken, new measures will be defined, including, but not limited to, (i) the return to use of the attacked equipment and network, where applicable; and (ii) the implementation of contingencies, physical or cloud-based, where applicable.
- 6.4.5.5.2. The entire history related to the incident must be filed as evidence for any future clarifications.

6.4.6. Governance

- 6.4.6.1. DOMO will carry out periodic security tests of its information systems (without being limited to them, but in particular electronic means), at least annually, in order to reduce the risks of loss of confidentiality, integrity and availability of information assets.
- 6.4.6.2. Information security training will form part of DOMO's initial and periodic training, in accordance with the annual training program, which shall, among other things, ensure that all Associates are aware of the procedures and obligations set forth herein, as well as minimize the occurrence of security incidents due to problems in use, misappropriation of information, fraud and misinterpretation of rules and procedures.
- 6.4.6.3. The Chief Compliance Officer, responsible for cybersecurity, will review this Policy annually or whenever deemed necessary.
- 6.4.6.4. Any communications and questions should be sent to the Compliance department via e-mail at dir_compliance@domo.vc.

6.5. Use of Artificial Intelligence

- 6.5.1. DOMO's Associates must mandatorily use Google's artificial intelligence ("A.I.") called "Gemini", as it is the official platform of Google Workspace.
- 6.5.2. The use of any A.I. (e.g., ChatGPT, DeepSeek and Perplexity) in its basic and/or free and/or freemium versions is expressly prohibited for the analysis / review / comments / adjustments, among others, of documents and/or text, image and/or video files, given that such unpaid versions of A.I. use information outside the DOMO domain in their analyses, constituting a risk of data leakage.

(*****)