Version 2024.01 October 21, 2024

# CYBERSECURITY POLICY

# OF

# MIRADOURO ASSET MANAGEMENT LTDA.

In compliance with current regulations and in accordance with the ANBIMA Code, MIRADOURO ASSET MANAGEMENT LTDA. ('Miradouro') maintains this Cybersecurity Policy, with the aim of defining cybersecurity rules, procedures, and controls that are compatible with its size, risk profile, business model, and complexity of activities carried out.

This Policy must always be interpreted in conjunction with Miradouro's other internal policies and rules, particularly with regard to the confidentiality, integrity, and availability of data and information systems used.

## 1. Risk Assessment

Miradouro estimates that the main cybersecurity risks to be considered are:

**Miradouro Headquarters:**

- Absence or instability of electrical power in the area;
- Absence or instability of internet provider in the area;
- Unauthorized access to Miradouro's facilities;
- Unauthorized access to Miradouro's restricted areas;
- Unauthorized access to Miradouro's physical documents.

**Physical Assets (notebooks, desktops, and/or mobile phones):**

- Loss or theft of Miradouro's technological assets;
- Improper access to data stored on Miradouro's technological assets;
- Malfunction or misuse of Miradouro's technological assets.

**Systems (all Miradouro systems will be hosted in the cloud, PaaS or SaaS models):**

Operations:

- – Unavailability of services and systems contracted by Miradouro;
- – Data loss of services and systems contracted by Miradouro;
- – Unprotected data in systems contracted by Miradouro.

Access:

- – Data capture between Miradouro's communication and the systems;
- – Unauthorized access to systems contracted by Miradouro;
- – Improper access to functions and features in the systems.

Changes:

- – Unauthorized changes in software used by Miradouro;
- – Improper changes in software used by Miradouro.

## 2. Protection and Prevention Actions

The protection and prevention actions adopted by Miradouro are:

**Miradouro Headquarters:**

- Use of UPS (Uninterruptible Power Supplies) to sustain the infrastructure;

• Use of new machines with batteries capable of sustaining hours without charging;

• Redundancy of internet providers at Miradouro's headquarters;

• Access door to Miradouro's facilities with key and/or digital lock;

• Door and biometric verification for access to Miradouro's restricted areas;

• Use of a safe to safeguard Miradouro's documents.

**Physical Assets (notebooks and/or mobile phones):**

• Signing of a responsibility agreement (proper use) by all Miradouro employees;

• Maintenance contract with suppliers in the event of a problem with any physical asset;

• Use of encryption on all physical assets to prevent unauthorized access in the event of loss or theft.

**Systems (all Miradouro systems will be hosted in the cloud, PaaS or SaaS models):**

Operations:

– Vendors contracted by Miradouro offer 99.9% service availability through redundancy and tier I or higher data centers;

– Data from systems contracted by Miradouro will be stored in the vendors' clouds, with online backup guaranteed across different drives;

– Data stored in systems contracted by Miradouro is encrypted at rest.

Access:

– Miradouro will use a VPN service to prevent data leakage in communications and to safeguard them;

– Systems contracted by Miradouro have authentication systems requiring the use of complex usernames and passwords for access. Additionally, some systems will also feature multi-factor authentication (MFA);

– Access to systems will be segregated according to the area and function of each professional, and only these professionals will have knowledge of authentication credentials or specific profiles.

Changes:

– SaaS: Software contracted under the SaaS model will follow the development process of the manufacturers, as these are off-the-shelf software, with the responsibility for mitigating the risk of improper changes lying with them.

– PaaS: Miradouro's proprietary software will be hosted in the cloud, where only the respective Miradouro directors will have modification access.

– PaaS: Any modifications to Miradouro's software will be developed in a segregated environment and migrated to production only after being tested and approved by the respective area directors.

## 3. Description of Supervision Mechanisms

For the purposes of supervising the risks mentioned above, Miradouro carries out the following activities:

**Miradouro Headquarters:**

• Annually, UPS systems are reviewed to assess proper functioning;

• Annually, physical access control systems at Miradouro's facilities are reviewed;

• Annually, the safe containing Miradouro's physical information is reviewed to ensure its integrity and the safekeeping of stored documents.

**Physical Assets (notebooks and/or mobile phones):**

• Annually, notebooks, desktops, and/or mobile phones undergo inspection covering: battery, encryption, installed software, and applied configurations;

• Annually, responsibility agreements are updated with the respective users.

**Systems (all Miradouro systems will be hosted in the cloud, PaaS or SaaS models):**

Operations:

– Annually, Miradouro's vendors are reviewed to ensure: 1. Data is being properly encrypted at the source; 2. Backups are being carried out adequately; 3. Service availability has been delivered in accordance with the established contracts.

Access:

– Annually, access to all Miradouro systems is reviewed, considering: 1. Professional x Function x Access (Segregation of Duties); 2. VPN usage; 3. Password change (minimum annual and use of complex standard); 4. MFA enabled for access whenever possible.

Changes:

– SaaS: Annually, Miradouro will request evidence from vendors of their internal governance processes to be confident that changes are made following established controls and do not impact the contracted software.

– PaaS: For each new change, Miradouro will: 1. Specify the change; 2. Test the new package before applying it in production; 3. Approve the new package before applying it in production.

## 4. Incident Response Plan

**Miradouro Headquarters:**

• Power outage: contact the regional power provider (CEMIG) and register a service request for normalization. Additionally, in cases where the UPS is not sufficient, Miradouro professionals must go to their homes and work remotely until the situation is normalized. Finally, an email describing the problem (and possibly screenshots) must be sent to: compliance@miradouro.co;

• Internet outage: if both internet providers are unavailable in the area, the professional must contact Miradouro's Directors and contact the providers to register a service request. Additionally, Miradouro professionals must go to their homes and work remotely until the situation is normalized. An email describing the problem must be sent to: compliance@miradouro.co;

• Physical access restriction: if there is any restriction on physical access to Miradouro's facilities, the professional must contact Miradouro's Directors and go to their homes and work remotely until the situation is normalized. An email describing the problem must be sent to: compliance@miradouro.co.

**Physical Assets (notebooks and/or mobile phones):**

- In the event of loss or theft of any physical asset, the professional must file a police report with local authorities and notify Miradouro's Directors. Additionally, a copy of the police report must be sent to: compliance@miradouro.co;
- In the event of malfunction of any physical asset, the professional must contact Miradouro's Directors to register a support request with the manufacturer. Additionally, an email describing the problem must be sent to: compliance@miradouro.co.

**Access:**

- In the event of a breach or unavailability of access to any Miradouro system, the professional must immediately contact Miradouro's Directors and send an email to compliance@miradouro.co.

## 5. Designated Responsible for Cybersecurity

The Risk and Compliance Department is responsible for cybersecurity matters and is assisted by outsourced IT professionals for risk assessment and remediation, as set forth in this Policy.

## 6. Review of Cybersecurity Policy

This Policy is reviewed at least annually, or at shorter intervals when there are changes in cybersecurity regulations, in order to keep its provisions always up to date.

*** * ***