# INFORMATION AND CYBERSECURITY POLICY

**ANGRA PARTNERS GESTÃO DE RECURSOS LTDA.**
**MATTERHORN INFRAESTRUTURA GESTÃO DE INVESTIMENTOS LTDA.**
**MANTIQ INVESTIMENTOS LTDA.**

**May/2024**

**INDEX**

## 1. INTRODUCTION AND OBJECTIVE

This Information and Cybersecurity Policy of Angra Group ("Policy") was developed in accordance with the Brazilian Securities Commission (CVM) Resolution No. 21 of February 25, 2021, as amended ("CVM Resolution 21"), and the codes of the Brazilian Association of Financial and Capital Market Entities (ANBIMA), especially the Code of Resource Administration and Management and the Rules and Procedures of Resource Administration and Management. The objectives are to:

I. Inform employees about the corporate guidelines for safeguarding the Group's Information Assets and data.
II. Establish standards of conduct related to Information and Cybersecurity aligned with the business needs and legal protections of Angra Group and all those who have access to its Information Assets and Information.
III. Prevent, detect, and mitigate vulnerabilities in incidents related to the cyber environment; and
IV. Guide the development of specific procedures for Information and Cybersecurity and the implementation of controls and processes to meet them in each area of Angra Group, always in compliance with the guidelines of Angra Group's Codes.

This Policy applies to all partners, administrators, employees, interns, trainees, and any others who hold a position, role, or trust relationship with any company belonging to Angra Group ("Employees" or "Employee").

This Policy also applies, as applicable, to any third-party or service provider that has access to Angra Group's Information and/or Information Assets.

This Policy must be interpreted together with the Code of Conduct (as defined below), of which it is an integral part, as well as with the other Angra Group Codes.

In case of questions or the need for guidance regarding this Policy and other Angra Group Codes, Employees must immediately seek assistance from Angra Group's Director of Risk, Compliance, and AML.

## 2. DEFINITIONS

| | |
|---|---|
| **"Information Asset":** | Refers to any means of storing, transmitting, or processing Information, including the equipment necessary for this, the systems used for it, the locations where these means are found, and the human resources that have access to them. |

| | |
|---|---|
| **"ANBIMA Codes":** | Refers to the codes of the Brazilian Association of Financial and Capital Market Entities (ANBIMA) that Angra Group follows, such as the Code of Regulation and Best Practices for Third-Party Asset Management. |
| **"Code of Conduct":** | Refers to Angra Group's Code of Conduct and Internal Policies. |
| **"Angra Group Codes":** | Refers collectively to the internal policies adopted by Angra Group as set forth in the Code of Conduct. |
| **"Employee":** | Refers to all partners, administrators, employees, interns, trainees, and any other individuals who hold a position, function, or professional, contractual, or trust relationship with any of Angra Group's companies, as applicable. |
| **"Personal Data":** | Refers to any information related to an identified or identifiable individual, including electronic identifiers. |
| **"Information Manager":** | Refers to the individual responsible for a particular Information Asset, corresponding to the manager of the area responsible for creating or controlling the Information or a person designated by them. |
| **"Information and Cybersecurity Incident" or "Incident":** | Refers to any occurrence that exploits or has the potential to exploit vulnerabilities in Angra Group’s systems and threatens or affects the confidentiality, integrity, or availability of any information system or Information Asset, or constitutes a violation or threat of violation of this Policy and other applicable rules and procedures. |

| | |
|---|---|
| **"Information":** | Refers to data, including Personal Data, processed or not, that can be used to produce and transmit knowledge, contained in any medium, support, or format (such as digital files, equipment, external media, printed documents, systems, mobile devices, databases, and conversations). It encompasses all information generated or developed for Angra Group's business, including but not limited to Employee data (personal or otherwise) and business strategic information. |
| **"Policy":** | Refers to this Information and Cybersecurity Policy. |
| **"Information and Cybersecurity":** | Refers to the set of concepts, techniques, and strategies aimed at protecting Information Assets and Angra Group's cybersecurity. |
| **"Confidentiality Agreement":** | Refers to the confidentiality agreement contained in "Annex II" of Angra Group's Code of Conduct. |
| **"Data Subject":** | Refers to the individual to whom the Personal Data being processed refers. |
| **"VPN" (Virtual Private Network):** | Refers to a private access module that allows secure remote access through public networks (such as the internet) to corporate networks. |

## 3. PRINCIPLES OF INFORMATION AND CYBERSECURITY

In line with the values stated in Angra Group's Codes, Angra Group's, clients', and the general public's information must be handled in accordance with the regulations in force and its internal classification. Under no circumstances should such information be handled by individuals who are not authorized by Angra Group.

The interpretation and implementation of this Policy are guided by the following principles:

I. **Confidentiality:** Ensures that Information is not available or disclosed to any person, body, or entity not duly authorized to access it.

II. **Availability:** Ensures that Information is accessible and usable upon demand and whenever necessary by duly authorized individuals, bodies, or entities.

III. **Integrity:** Ensures that Information has not been altered or destroyed in an unauthorized or accidental manner.

## 4. RISK IDENTIFICATION

Angra Group's Information Assets and Information are exposed to various cybersecurity risks and threats. To identify, prevent, and mitigate these risks, Angra Group has established the General and Specific Guidelines below.

## 5. GENERAL GUIDELINES

All Angra Group Employees must be aware of and understand this Policy to properly handle the Information Assets they have access to, avoiding unnecessary or excessive risks in the management of these Information Assets.

In addition, all Employees must, as stipulated by this Policy and within their professional responsibilities, ensure that all Information and Cybersecurity measures are routinely implemented to protect Information Assets from threats and crises.

Angra Group's Information and Cybersecurity objectives include:

I. Complying with applicable Brazilian legislation and the ANBIMA Codes followed by Angra Group.

II. Ensuring that Angra Group’s Information Assets are adequately protected and used solely for business purposes.

III. Appropriately classifying Information and ensuring the continuity of its processing according to the criteria and principles outlined in this Policy and other Angra Group Codes.

IV. Safeguarding Information from unauthorized access, modification, destruction, or disclosure.

V. Ensuring the integrity of Information Assets and the entire technological infrastructure where Information is stored, processed, or otherwise handled.

To meet these objectives, Angra Group:

I. Implements mechanisms to promote a culture of Information and Cybersecurity, including the dissemination of this Policy to all Employees and the provision of training on privacy, Personal Data protection, and Information and Cybersecurity.

II. Adopts procedures and controls to identify and reduce Angra Group's vulnerability to Incidents and meet cybersecurity objectives, including but not limited to Employee training, the implementation of the measures covered by this Policy in

Angra Group's daily operations, and the identification and mitigation of risks arising from Information and Cybersecurity gaps.

III. Controls, monitors, and restricts access to Information and Information Assets to the minimum necessary permissions and privileges, in accordance with Angra Group Codes.

IV. Records, classifies risks, analyzes causes, and impacts, and controls the effects of Information and Cybersecurity Incidents that affect Angra Group's activities.

## 6. SPECIFIC GUIDELINES

### 6.1. Classification and Use of Information

According to Angra Group's Confidentiality Agreement, the Group's information is classified as either "Confidential Information" or "Non-Confidential Information."

The Information Manager must classify the Information according to Angra Group's Confidentiality Agreement and based on its criticality. The Information may only be shared according to the following classification levels:

**Confidential Information:**

All types of information, whether written, verbal, or presented in tangible or intangible form, including but not limited to: know-how, techniques, copies, diagrams, models, samples, computer programs, technical or financial information, or information related to investment or commercial strategies. This includes client balances, statements, positions, and structured operations, as well as their respective values, plans of action, customer lists, business counterparts, suppliers, service providers, and any other strategic information related to Angra Group's activities and its partners or clients. This also includes information accessed by an Employee during their activities with Angra Group or strategic or market information obtained from Angra Group's partners, directors, employees, trainees, or interns, as well as from affiliates, consultants, advisors, clients, suppliers, and service providers.

**First Clause**: Confidential Information can only be shared with third parties through formalized agreements in contractual clauses or specific confidentiality documents.

**Second Clause**: Internally developed computerized systems, databases, analysis models, and evaluation files, as described in Law 9.609/98, are classified as "Protected Information" and merit greater protection.

**Third Clause**: For Protected Information, it is strictly prohibited to reproduce, translate, adapt, rearrange, distribute, or publicly communicate it, even after the termination of a contract with Angra Group. Violation of these provisions will result in penalties, as outlined in Law 9.609/98.

**Non-Confidential Information**: Information that:

I. Is or becomes public without any violation of Angra Group's Codes.

II. Is known to the recipient without violating any law or Angra Group's internal regulations.

III. Must be disclosed by law, judicial, or administrative order.

IV. Is intended for public disclosure or is authorized by Angra Group for disclosure (e.g., institutional materials).

**First Clause**: Public Non-Confidential Information can be made available to anyone within or outside Angra Group without compromising the Group's interests.

**Second Clause**: Disclosure of other Non-Confidential Information must be done on a case-by-case basis, based on the Information Manager's assessment of the necessity and relevance of the disclosure.

**Third Clause**: "Internal Non-Confidential Information" refers to internal information that, while Angra Group does not intend to disclose, would not cause significant damage if accessed by external individuals (e.g., internal policies and guidelines).

### 6.2. Logical Access Control

The IT Department must assign access privileges to individuals only to the extent necessary for them to perform their professional activities, following the principle of least privilege.

It is prohibited to share access credentials for use by others, or for an Employee to open a system session for another user.

Employees are responsible for changing their password: (i) upon their first access to Angra Group systems; (ii) periodically, as defined in section 7.14; and/or (iii) in case of suspected incidents.

The access credentials of employees who leave Angra Group must be revoked upon termination of their employment relationship, definitively terminating access to the Group's data network and systems.

### 6.3. Remote Access

In addition to the provisions on access control, the IT Department must implement specific Information and Cybersecurity mechanisms for remote access to Angra Group's Information Assets, including encryption tools and multi-factor authentication, wherever feasible.

As a general rule, access to Angra Group's Information Assets and Information must only occur through corporate devices. Remote access to these assets via personal devices is not permitted.

### 6.4. Use of Equipment

All employees are individually responsible for the equipment they use or manage and are committed to using and safeguarding such equipment appropriately, as outlined in the "Equipment Custody and Use Responsibility Agreement". Employees must sign this agreement when receiving any equipment from Angra Group.

Only equipment approved by the IT Department may access Angra Group's corporate network, and the installation of unauthorized software is prohibited.

All mobile devices provided by Angra Group must have screen lock passwords.

The use of removable storage devices is prohibited, and any equipment taken for maintenance or external use must have prior approval from the IT Department.

### 6.5. Software

Any installation, update, or removal of software on any Angra Group equipment must be pre-authorized by the IT Department. Installing unauthorized software is strictly forbidden.

If an Employee requires software access to perform their professional duties, they must request it from the IT Department, which will evaluate the request's feasibility.

### 6.6. File Storage, Clean Desk, and Clean Screen Policy

Angra Group employees must safeguard physical documents, electronic files, and any Confidential Information they have access to. To ensure this, Employees must store Confidential Information in locked cabinets, always lock screens when leaving their desks, store electronic files on Angra Group's corporate network, and adhere to the Information classification guidelines in this Policy, limiting access only to authorized Employees.

### 6.7. Handling of Information

Confidential Information must not be shared with third parties unless a contractual agreement exists to authorize access and usage by those parties.

Additionally, and in accordance with Angra Group's Codes, Employees should refrain from discussing or handling Confidential Information in public places or with unauthorized individuals, including other Employees. When transporting such information, Employees must ensure that no documents are visible, that storage devices are password-protected, and that printed copies are not left available for third parties.

### 6.8. Handling of Personal Data

Esta This Policy applies to all Personal Data processed in Angra Group's environments or under its control. This includes, but is not limited to, Personal Data of clients, suppliers, and Employees. The use of Personal Data for purposes other than those for which it was

collected, stored, or otherwise processed is strictly prohibited, as outlined in this Policy and the Privacy Policy available on Angra Group's website.

Every Angra Group Employee must comply with applicable privacy and data protection legislation, particularly the General Data Protection Law (Law 13.709/2018 or "LGPD"), and must observe the following principles when handling Personal Data in the course of their duties and their relationship with Angra Group:

I. **Purpose, Adequacy, and Necessity:**
The Personal Data processed must be only that which is necessary for the intended, legitimate purpose, and must be clearly communicated to the Data Subject.

II. **Free Access and Quality:**
The Data Subject must have the ability to exercise their rights. In addition, all Employees must ensure that Personal Data remains accurate and up to date while respecting Angra Group's trade secrets and business confidentiality.

III. **Transparency:**
Data Subjects must receive clear and accessible information regarding the processing of their Personal Data, whether through privacy policies embedded in products or through privacy notices provided at the point of data collection.

IV. **Non-Discrimination:**
Personal Data may not be processed for discriminatory, illegal, or abusive purposes, ensuring that practices do not unjustly violate Data Subjects' rights.

V. **Security and Prevention:**
The processing of Personal Data must be protected by technical and administrative measures to ensure its security, preventing unauthorized access and incidents.

If Personal Data is shared with third parties, contractual agreements must be established to ensure technical and organizational measures are in place to properly handle Personal Data in compliance with applicable legislation.

### 6.9. Vulnerability Management

The procedures and controls adopted to reduce vulnerabilities that may lead to Information and Cybersecurity Incidents must cover:

I. Authentication, prevention, and detection of intrusions in Angra Group's logical environments.
II. Prevention of Information leaks.
III. Periodic testing and scanning to detect vulnerabilities.
IV. The establishment of traceability mechanisms, whether expressly stated in this Policy or not.

Collectively, the Specific Guidelines presented in this Policy are considered control measures adopted to reduce vulnerabilities and risks.

Additionally, Angra Group's IT Department maintains updated protection mechanisms against malware on its devices and antivirus software designed to detect, prevent, and, when possible, eliminate malicious programs (such as viruses, worms, spyware).

Periodic scans, external penetration tests, and phishing detection exercises are conducted, along with vulnerability assessments of the technological infrastructure and log monitoring routines to detect and mitigate threats to Angra Group's Information Assets. Backup routines for Information are also maintained.

### 6.10. Third Parties and Service Providers

When it is necessary to hire third parties or service providers, the contracting department is responsible for determining the necessary level of access to Information and IT resources for the service provider or third party to perform their activities. This includes specifying the controls to monitor such access.

The process of hiring third parties to provide processing and storage services or cloud computing for Angra Group must include a prior risk and criticality assessment, which must be approved by the IT Department. Without prejudice to the obligations stipulated in the Third-Party Contracting Policy, this assessment should consider, at a minimum:

I. Angra Group's access to Information that will be processed or stored by the service provider.
II. Confidentiality, integrity, availability, and recovery of the Information processed or stored by the service provider.
III. Compliance with certifications required by Angra Group or regulatory bodies, as applicable, for the service being contracted.
IV. Adequate provision of information and management resources to monitor the services provided.
V. Physical or logical controls for identifying and segregating client, Employee, or third-party Information from Angra Group.
VI. The quality of access controls aimed at protecting client, Employee, and third-party Information belonging to Angra Group.

This Policy applies, as applicable, to all third parties and service providers that have access to Angra Group's Information and/or Information Assets.

### 6.11. Monitoring

The use of Angra Group's logical environment, equipment, and other corporate tools provided to Employees may be monitored by any legal means available to verify compliance with the provisions of this Policy and other Angra Group Codes, as well as with

Brazilian law. Thus, the use of technology tools provided by Angra Group to Employees for personal, non-work-related purposes is prohibited.

### 6.12. Use of Email and Instant Messaging

Confidential Information and Angra Group's Internal Non-Confidential Information must circulate exclusively through corporate communication tools provided by Angra Group, such as corporate email, proprietary applications, and corporate instant messaging platforms like Microsoft Teams and Zoom.

The use of professional email accounts for signing up on shopping websites, promotions, or any other matters unrelated to the Employee's activities at Angra Group is prohibited.

### 6.13. Internet Use

Internet access is provided for activities related to Angra Group's professional interests and matters. Its use for personal purposes or activities unrelated to professional duties is prohibited.

Access to inappropriate websites or the sharing of inappropriate content (such as pornography, illegal or unethical activities, or content of a racist nature) is prohibited and subject to administrative and criminal sanctions.

### 6.14. Passwords

All passwords within Angra Group's technological environment must adhere to the following security standards:

I. At least 8 characters.

II. A mix of uppercase and lowercase letters.

III. Inclusion of numbers and special characters.

IV. Periodic changes, every 60 days for the quotaholder portal and every 180 days for the network and email.

The primary corporate communication tools of Angra Group, such as email and Microsoft Teams, use two-factor authentication. In addition, any mobile device attempting to access corporate email for the first time will be quarantined until released by IT administrators.

Passwords are non-transferable, and Employees are prohibited from sharing their access credentials with third parties, even other Angra Group Employees.

### 6.15. Disposal of Information

The disposal of any Information, whether in physical or digital form, must be carried out using secure and appropriate tools. All disposals must be properly documented to ensure auditability.

In the case of Information involving Personal Data, disposal should only occur when:

I. It has been verified that the purpose for which the Personal Data was processed has been fulfilled, or the Personal Data is no longer necessary or relevant for Angra Group, whether to comply with a legal obligation or to defend Angra Group's legitimate rights.
II. The Data Subject has communicated that they no longer wish Angra Group to process their Personal Data, and it is not possible to justify retaining the involved Personal Data.
III. There is a specific order for disposal due to a judicial or administrative decision.

## 7. INFORMATION AND CYBERSECURITY INCIDENTS

**Angra Group's IT Department will act to:**

I. Detect and correct any incidents.
II. Alert, communicate, and advise Angra Group Employees about emerging incidents.
III. Educate and raise awareness among Angra Group Employees on incident detection and response.
IV. Adopt necessary measures to prevent incidents and minimize the impact of their effects.

Any incidents that affect Angra Group must be communicated to the IT Department, recorded, and have their cause and impact analyzed. The criticality factors must be defined in accordance with the following guidelines:

| Severty | Criteria |
|---|---|
| **Very High** | • Angra Group is unable to provide its services.<br>• The recovery time is unpredictable or impossible without the provision of high-cost resources.<br>• The class of Information affected is Confidential. |
| **High** | • Angra Group is unable to provide its services to a specific group of users or clients.<br>• The recovery time is unpredictable and will require some resources.<br>• The class of Information affected is Confidential or Internal Non-Confidential. |
| **Medium** | • Angra Group can still provide its services, but efficiency is minimally compromised.<br>• The recovery time is predictable, though some resources will be required.<br>• The class of Information affected is Internal Non-Confidential. |

| | |
|---|---|
| **Low** | • There is no impact on Angra Group's ability to provide services.<br>• The recovery time is predictable and can be met with existing resources.<br>• The class of Information affected is either Internal Non-Confidential or Non-Confidential. |

If any Employee identifies or suspects an incident, they must immediately report it to their manager, who is responsible for informing the IT Department, which will conduct the initial investigation and assessment of the incident.

The IT Department will be responsible for engaging other departments of Angra Group if necessary, during incident response and containment, including legal, financial, and public relations teams, among others. These departments will make every effort proportional to the urgency and severity of the incident to resolve the issue presented to them.

After containment, response, and damage minimization, every incident will be documented and recorded by the IT Department in a report containing lessons learned and appropriate internal controls or technical and administrative measures to prevent similar incidents in the future.

Incidents involving Personal Data must be classified by the Data Protection Officer (DPO) in terms of severity, considering the relevant risks or harm to the Data Subject. If the incident is materially significant, the DPO will follow the required procedures to notify the Data Subjects and relevant public authorities, including the National Data Protection Authority.

## 8. RESPONSIBILITIES AND DUTIES RELATED TO INFORMATION AND CYBERSECURITY

Information and Cybersecurity is a collective responsibility within Angra Group. The following responsibilities apply to specific departments and roles:

### 8.1. Risk, Compliance, and AML Committee

I. Serve as the body responsible for the direct coordination of activities related to the Information and Cybersecurity Policy, including promoting training, dissemination, and responding to regulatory and supervisory bodies, as per applicable ANBIMA Codes.
II. Commit to the continuous improvement of Information and Cybersecurity procedures.
III. Ensure compliance with the provisions of this Policy.

### 8.2. Data Protection Officer (DPO)

I. Coordinate internal and external awareness campaigns related to Personal Data protection practices.

II. Monitor compliance with Personal Data protection obligations established in this Policy, manage responses to Information and Cybersecurity incidents involving

Personal Data, and maintain a process for recording Personal Data processing activities.

III. Respond to complaints, queries, and requests for rights from Data Subjects, as well as respond to requests from regulatory bodies such as the National Data Protection Authority and other organizations.

### 8.3. Human Resources Department

I. Assist in disseminating the culture of Information and Cybersecurity across Angra Group by publicizing this Policy, Angra Group's Codes, and other relevant materials to Employees.
II. Support the organization and delivery of training for Employees on Information and Cybersecurity-related topics.
III. Inform all Employees joining Angra Group about this Policy.
IV. Request the IT Department to create, block, or delete Employee and ex-Employee accounts.

### 8.4. IT Department

I. Support the development and updating of regulations and the design and implementation of IT controls in accordance with this Policy.
II. Raise awareness among Employees about best Information and Cybersecurity practices for Angra Group's business.
III. Select and implement appropriate technical measures to protect each Information Asset based on the classification of Information.
IV. Select and implement tools to be used in Angra Group's logical environment to ensure the security of Information in accordance with its classification.
V. Verify and validate the standards, guidelines, and operational procedures necessary to ensure Information and Cybersecurity in all areas that use Angra Group's Information Assets.
VI. Periodically conduct vulnerability checks and scans in Angra Group's logical systems.
VII. Periodically back up Information.
VIII. Restrict and control access and privileges of Employees to the corporate network, VPN, and Information Assets.
IX. Detect, identify, record, and investigate any Information and Cybersecurity failures or unauthorized attempts to access Angra Group's Information Assets.
X. Provide support and advice on Information and Cybersecurity matters to Employees.
XI. Create, delete, and/or block Employee accounts when necessary.
XII. Manage the response to Information and Cybersecurity incidents.
XIII. Support the process of contracting third-party services for processing and storing Information and cloud computing.

### 8.5. Managers of Angra Group Departments

I. Ensure compliance with the rules and guidelines set forth in this Policy in their respective areas of responsibility.
II. Immediately notify the IT Department via email in case of an incident or suspicion of an incident.

### 8.6. All Angra Group Employees

I. Understand and comply with the rules and guidelines set forth in this Policy and Angra Group's Codes.
II. Ensure the prohibition of sharing or negotiating credentials (e.g., ID, passwords, access cards, etc.) is understood and followed.
III. Report any suspicious or confirmed situations that may compromise Angra Group's Information and Cybersecurity to their Managers.

IV. Protect Information and Information Assets while performing their duties.

## 9. COMPLIANCE

**9.1.** Angra Group reserves the right to verify compliance with the guidelines established in this Policy at any time and without prior notice.

**9.2.** Compliance with the guidelines outlined in this Policy must be verified at least annually and documented in writing, including the following:

I. A description of the processes and controls adopted during the verification process.
II. The definition of methodologies, metrics, criteria, and indicators used.
III. Identification and correction of any deficiencies found.

Exceptions to the provisions of this Policy must be formally analyzed and approved by Angra Group's IT Department in conjunction with the Group's senior management, as applicable.

## 10. SANCTIONS

Failure to comply with any aspect of this Policy, as well as failure to comply with the Information and Cybersecurity and confidentiality guidelines provided in Angra Group's other Codes, constitutes a serious violation. This may result in the application of appropriate penalties, including those provided for under applicable Brazilian civil, criminal, and labor laws, as well as warnings under Angra Group's Codes and relevant contractual provisions.

## 11. CONTACT

Any matters related to this Policy, including but not limited to questions, comments, and suggestions, or other concerns related to Angra Group's Information and Cybersecurity, should be addressed via email to the Risk, Compliance, and AML Committee.

## 12. VALIDITY AND UPDATES

This Policy is effective as of the date of its release and must be reviewed within a period not exceeding twenty-four months or sooner, if necessary, due to legal, regulatory, or self-regulatory changes or additions. This Policy must remain updated on Angra Group's website.

| Version | Date | Responsible Approver |
|---|---|---|
| 2 | 01/05/2024 | Director of Asset Management and Director of Risk, Compliance, and AML |