



Management Policy

Information Security Policy

Digital & PPlatform

MARCO, an organization dedicated to generating marketing and sales strategies for different brands, to promote information security management, intends to implement and communicate the following Policy and related objectives at all levels of the organization.

STATEMENT OF MANAGEMENT INTENT

This Information Security Policy establishes guidelines for protecting information and personal data throughout their entire life cycle, including creation, use, disclosure, modification, storage, retention, and deletion. It also applies to the media supporting such information and to the people who access or manage it.

MARCO Management's intention is to preserve the confidentiality, integrity, and availability of information, as well as to protect the personal data processed by the organization, ensuring compliance with applicable legal, regulatory, and contractual requirements.

MARCO is committed to ensuring that personal data under its responsibility is processed appropriately, lawfully, transparently, and securely, in accordance with policy **PG-04 Global Personal Data Protection and Transfer Policy**.

INFORMATION SECURITY PRINCIPLES

- Promote information security culture, personal data protection at all levels of the organization, and continuous improvement.
- Promote, through MARCO's leadership, the dissemination of compliance with the policy.
- Establish and apply the defined security measures, identifying the necessary resources to carry them out.
- Keep the policies and other management system guidelines updated to ensure their validity and effectiveness.
- Ensure the continuity of operations and functions established in the organization within the framework of information security.
- Implement preventive, predictive, and corrective measures to protect information assets and personal data.
- Comply with legal, regulatory, contractual, and other applicable requirements related to information security and personal data protection.

INFORMATION SECURITY MANAGEMENT OBJECTIVES

Specific Objectives

The organization establishes the following information security objectives:

- Identify and manage information assets and personal data by classifying them according to criticality and sensitivity criteria, ensuring the proper protection of their confidentiality, integrity, and availability.
- Manage information security risks, including those associated with the processing of information and personal data, considering emerging threats, applicable requirements, and stakeholder expectations, to maintain them at acceptable levels according to the criteria established by the organization.
- Manage the technological infrastructure to provide appropriate service delivery, implementing contingency plans, and ensuring operational continuity.
- Implement and periodically review the controls established in the Statement of Applicability.
- Establish and maintain ISMS policies, thereby ensuring compliance with them.
- Communicate and keep personnel informed about these objectives.

SCOPE OF THE INFORMATION SECURITY POLICY

General Scope

PREPARED	REVIEWED	APPROVED
ISMS Manager	CDPO	CEO

This policy applies to the ENTIRE organization, its processes, information, technological assets, and personal data processed in the course of its activities, as well as to employees and third parties who, through contracts, agreements, or other relationships, access, process, store, or safeguard the organization's information.

Everyone is responsible for complying with the requirements established in this policy and actively collaborating in the protection of our information assets and the continuity of our operations.

DEFINITION OF INFORMATION ASSETS

They are all relevant elements involved in the generation, issuance, storage, disclosure, visualization, and retrieval of valuable information for MARCO, distinguished across three levels:

- Information itself, in its multiple formats (**paper, digital, text, image, audio, video, etc.**).
- The equipment/systems/infrastructure that support this information.
- The personnel who use the information and have knowledge of institutional processes.

DEFINITION OF INFORMATION SECURITY

MARCO understands information security as the set of preventive, predictive, and corrective measures intended to protect information through systems that safeguard and protect its information assets, seeking to maintain their confidentiality, availability, and integrity and to ensure business continuity. In other words, it refers to the protection of information assets, which are fundamental to the success of our organization.

GENERAL FRAMEWORK OF MARCO SECURITY POLICIES

General Aspects

Senior Management is committed to taking all actions within its reach to enable operational continuity, address interruptions to the organization's activities, protect critical processes from the effects of major failures or disasters in information systems, and ensure their timely resumption.

Policy Approval

This Information Security Policy shall be approved by Senior Management, thereby demonstrating its commitment, support, and interest in promoting and developing an information security culture at MARCO.

Policy Review

The Information Security Policy shall be reviewed annually to verify its suitability and appropriateness. If necessary, changes will be made that may affect its definition, such as technological changes, the impact of security incidents, structural and business changes at MARCO, changes in legal conditions and/or requirements, or at the request of Management.

Related Policies and Guidelines

This Information Security Policy is complemented by the other policies and guidelines established by the organization to guide the management, protection, and proper use of information, data, and associated resources. In this regard, the organization has, among others, the following related policies:

- Acceptable Use of Devices and Good Practices Policy
- BYOD Device Use Policy
- Global Personal Data Protection and Transfer Policy
- Password Management Policy
- Cryptography Policy
- Clean Desk and Clear Screen Policy
- Information Transfer Policy
- Information Backup and Retention Policy
- ISMS Supplier Relationship Policy
- Artificial Intelligence Use Policy

PREPARED	REVIEWED	APPROVED
ISMS Manager	CDPO	CEO

- Information Security Control and Disciplinary Regime Policy

Version History

Version	Description of Change	Position of the Person Making the Change	Approval Date
00	Initial issuance	ISMS Manager	12/04/2021
01	The policy is reviewed and adjusted to better align with the organization.	IT Analyst	08/02/2022
02	The logo format and the organization's name are updated.	ISMS Manager	25/11/2025
03	The content is reviewed to highlight the commitment to information privacy. Related policies are included.	ISMS Manager	11/09/2026

Lisandro Zapararte
CEO MARCO

PREPARED	REVIEWED	APPROVED
ISMS Manager	CDPO	CEO