INFORMATION SECURITY POLICY

AltamarCAM group

INFORMATION SECURITY POLICY

Version number:	2
Approval date:	28/03/2025
Made by:	IT Department
Approved by:	Board of Directors of Altamar CAM Partners, S.L.
Status:	Approved

Control Version

Date	Changes implemented	Version
February 2025	Original Policy	1
March 2025	Wording and grammatical adaptation based on audits recommendations	2

INDEX

1. Introduction

This document contains the Information Security Policy of Altamar CAM Partners, S.L., its subsidiaries and investee companies (hereinafter "AltamarCAM"), defining the organization's principles for information security. It aligns with ISO27001 and establishes the foundation for protecting information and systems across all organizational levels.

The Information Security Policy or "The Policy" hereinafter, is designed to address the evolving cybersecurity landscape and protect against threats such as errors, sabotage, terrorism, extortion, espionage, and service disruptions. These measures ensure the confidentiality, integrity, and availability (CIA) of AltamarCAM's information assets.

2. Scope

This Information Security Policy applies to the information systems that are part of AltamarCAM. It is designed to align with ISO27001 requirements for managing changes to information systems.

3. Objective

The purpose of this Policy is to establish a regulatory framework to:

- Identify and implement technical and organizational measures to secure information and privacy.
- Protect the systems supporting AltamarCAM's activities.
- Comply with applicable legal, regulatory, and contractual requirements

4. Diffusion

This document will be published on AltamarCAM's internal website and communicated to all interested parties, especially internal personnel who handle AltamarCAM's information assets.

5. Compromise of Management

The information, especially the personal data of employees, customers and suppliers, as well as the systems that support it, are strategic assets for AltamarCAM, which wishes to protect them against threats such as errors, sabotage, terrorism, extortion, industrial espionage, privacy violations, service interruptions and natural disasters, in order to ensure the efficient and effective achievement of the defined business objectives.

Management is committed to lead and promote safety at all levels, in accordance with the Safety Policy and the objectives defined therein.

6. Politics

6.1 Scope

AltamarCAM protects the resources involved in the management of information related to the normal development of its functions, complying with current legislation, preserving the confidentiality and privacy of information and ensuring the availability, integrity and conservation. These objectives are also transferred to the information systems used for the development of its activity.

AltamarCAM is willing to establish conditions of confidence in the use of electronic media and the continued provision of its services, taking the necessary measures to protect the information systems of the organization of those threats to which they are exposed, in order to ensure the

security of information systems, minimize risks and thus consolidate the basis for preventing, detecting, reacting and recovering from possible incidents that may occur.

This Information Security Policy applies to the entire scope of AltamarCAM, i.e.:

- All resources, services and business processes that make up AltamarCAM. In this way it will apply to all information systems involved in the provision of services and all those systems that support the different functions and responsibilities of AltamarCAM. Specifically, the following core services of the business:
  - **Business Services**: Investor Relations Services
  - **Fund Management Services**: Investment Management, Administration (Accounting, Operational Management, Legislative, Transfer Agents and Portfolio Monitoring) on the funds
  - **Reporting Services**: Legal, tax and regulatory compliance services to group companies and funds
  - **Transactional Services**: Payments, Collections and Accounting in the part of group companies
- To all users, whether internal or external, directly or indirectly linked to AltamarCAM that use the systems described in the previous point.

6.2 Information Security Objectives

The objectives to be achieved are:

- Guarantee, ensure and implement adequate and necessary security measures on all resources, processes, functions and services related directly and indirectly with internal and external users, and with customers, suppliers, *partners* or other third parties, in order to ensure the availability, confidentiality, integrity, of information, and compliance with applicable legislation.
- To guarantee the continuity, security and quality of the services offered.
- Implement and maintain continuous improvement processes to promote the efficiency and effectiveness of information security measures.
- To reduce as much as possible the possibilities of security incidents and minimize the impact of such incidents should they occur.
- Have the means by which the different users of AltamarCAM services and processes make good use of information, information systems and resources used in the development of their functions, duties and responsibilities, as well as those that do not compromise the security of AltamarCAM information.
- Align with international best practices and standards in the field of information security and/or cybersecurity in force at any given time.
- Implement appropriate security measures on information and personal data processed by electronic means and on paper support that AltamarCAM manages within the scope of its competences. This information will be regulated by Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and, as well as by the Organic Law 3/2018 of 5 December on the Protection of Personal Data and guarantee of digital rights (LOPDGDD).

In accordance with the aforementioned objectives, this Information Security Policy seeks the adoption of the following security principles, guaranteeing:

- **Authenticity:** the property that the entity/person is who he/she claims to be, or the source of the data is guaranteed.
- **Availability**: the information and information systems can be used at the required time and in the required form.

- **Confidentiality**: data and information systems will only be accessed by duly authorized persons.
- **Integrity**: accuracy of information and information systems against alteration, loss or destruction, whether accidental or fraudulent.
- **Traceability:** property consisting of tracking the movement of any user that is part of the management system.
- **Legality**: the information is processed in accordance with the regulatory framework.
- **Training**: in accordance with the principle of comprehensive security, ensure an adequate level of information security awareness and training for all the organization's personnel.
- **Incident management**: the analysis and management of risks as an essential part of the organization's security process, keeping the environment under control and minimizing risks, in accordance with prevention, detection, reaction and recovery measures, and establishing protocols for the exchange of information related to incidents.

6.3 Regulatory Compliance

This Information Security Policy and other associated documentation are aligned with the current legal scope of laws, rules and regulations that apply to AltamarCAM, with respect to any material or territorial scope.

6.4 Application of Resources

AltamarCAM's Management declares its commitment to ensure, within its scope of functions and responsibilities, the provision of the necessary resources to implement and maintain the processes related to AltamarCAM's information security and the continuous improvement of these. All this in order to achieve the strategic objectives, dissemination, consolidation and compliance with this Information Security Policy, as well as implement the appropriate distribution and publication mechanisms in order that it can be known by the different users it affects.

6.5 Roles and responsibilities

Any user affected by this Policy shall have the obligation to:

- Comply at all times with the Organization's Information Security Policy, rules, procedures and instructions on Information Security.
- Take an active role in the cybersecurity of any assets that are subject to protection within the scope of this Policy.
- Maintain professional secrecy and confidentiality with respect to the Organization's information.
- Report, in accordance with the corresponding procedure, suspicious situations or anomalies, security incidents, and non-conformities or security breaches of the organization's information systems and/or assets.

Overall responsibility for Information Security rests with the person assigned the duties of the ISMS Responsible.

Regarding the breach of the Information Security Policy of AltamarCAM and the rest of the documents related to information security, by anyone to whom they apply and that jeopardizes the security of information in any of its dimensions, AltamarCAM Management reserves the right to initiate appropriate action according to the codes and internal rules of behavior and the legal framework in force.

6.6 Compliance Control

The degree of implementation of this Policy will be measured periodically (at least annually) through self-assessments coordinated by the ISMS Responsible and through internal or external audits (at least annually), and whenever there are substantial changes in AltamarCAM's information systems. The approval of this Policy is made in the Management Review, indicated in the ISMS.

6.7 Information Security Regulations

This Information Security Policy will be supported and complemented by a set of specific documents. These documents are called Information Security Regulations and will be based on best market practices and aligned with the specific needs of AltamarCAM.

6.8 Information Classification

All information shall be classified according to its importance to the organization and shall be treated according to such classification, in accordance with the provisions of the "Altamar Information Classification Procedure Structure".

6.9 Audit

The information systems shall be periodically subjected to internal or external audits in order to verify the correct functioning of the security implemented in them, determining degrees of compliance and recommending corrective measures.

6.10 Suppliers and third parties

All relevant acquisitions of goods or services or that have an impact on AltamarCAM's services or systems will be subject to a risk analysis process.

Information security requirements for the mitigation of risks associated with the supplier should be agreed with the supplier and documented and should follow the dictates of established security regulations that complement this Policy.

6.11 Liabilities for noncompliance

Failure to comply with this Policy and the Regulations derived from it will be considered a serious offense, giving rise to the application of the Disciplinary Regime regulations without prejudice to any other responsibilities that may arise.

Similarly, any collaborating member, subcontractor or consultant who fails to comply with this Policy shall be subject to removal from AltamarCAM's facilities and termination of employment.

6.12 Climate Change

AltamarCAM has conducted an analysis of the services provided by the organization, as well as its usual operations for the provision of the same, finding no aspects that could influence climate change on the planet beyond those generated by air conditioning systems and vehicle emissions that serve the organization, in both cases within the established legal requirements.

Stakeholder requirements have been analyzed without finding any specifically related to climate change. Based on both analyses, it is concluded that there is no need to apply measures beyond the standard legal requirements.

Al information related to climate change inside the ESG Policy are available in the intranet for all employees and on our public web.

6.13 Exception management

Any exception to this Information Security Policy must be registered and reported to the person in charge of AltamarCAM's ISMS. These exceptions will be analyzed to assess the risk that they could introduce to the company and, based on the classification of these risks, these must be assumed by the petitioner of the exception along with those responsible for the business.

7. Approval and review

The Information Security Policy is formally approved by the Security Committee and will be reflected in the corresponding minutes and will be in force until it is replaced by a new version. Likewise, it will be reviewed annually and whenever significant changes occur that require it, in order to adapt it to new circumstances, technical and/or organizational, preventing it from becoming obsolete.

For these purposes, their suitability, timeliness and accuracy shall be regularly reviewed. The modifications that may result will be proposed by the Information ISMS Responsible for validation.