

GENERAL PRINCIPLES OF INFORMATION SECURITY

For Ares Lusitani STC, S.A (“Ares Lusitani”), meeting the requirements, needs, and expectations of our stakeholders demands the highest levels of security and quality.

Ares Lusitani gives priority and full support to information protection due to its strategic nature and as way to ensure service improvement in its operations.

For this reason, Ares Lusitani, and consequently the entire organization, are committed to Information Security, based on the requirements of ISO/IEC 27001:2013.

Ares Lusitani pursues the adoption, implementation, and continuous operation of protocols and procedures that ensure the preservation of at least the basic components of information security:

- **Confidentiality:** Ensuring that only duly authorized individuals have access to data and systems.
- **Integrity:** Ensuring the accuracy of information and systems against alteration, loss, or destruction, whether accidental or intentional.
- **Availability:** Ensuring that information and systems can be used as and when required.

This policy shall be considered throughout all phase of the information lifecycle: generation, distribution, storage, processing, transport, consultation, and destruction, as well as the systems that process it (analysis, design, development, implementation, operation, and maintenance).

Information security is the responsibility of all personnel within the organization; therefore, this policy must be known, understood, and embraced at all organizational levels and communicated reliably across the organization, to its own staff and external partner companies, and made available to interested parties.

Relationships with third-party collaborators must always be covered by appropriate guarantees regarding the use and handling of information.

In summary, the core principles encompassed by this policy are as follows:

- Ensure that all information systems, networks, and business applications managed by Ares Lusitani are effectively and efficiently protected against threats and security risks, and that risks which cannot be directly mitigated are minimized.
- Ensure that all Ares Lusitani users are aware of their duty to comply with national and international legislation.
- Ensure that all Ares Lusitani users understand and acknowledge their personal responsibility to protect the confidentiality, integrity, and availability of accessed data.

- Assign necessary security roles and responsibilities and provide the required support.
- Ensure that all Ares Lusitani users are aware of compliance obligations, as well as all other applicable internal regulations.
- Safeguard the reputation and business of the Ares Lusitani brand, as well as legal compliance and protection.
- Consider information security requirements for suppliers and subcontractors.
- Establish and periodically review the security level (risk appetite) based on risk analysis.
- Demonstrate management leadership by ensuring that the Information Security Policy and security objectives are established and aligned with the organization's strategic direction.
- Meet the needs and expectations of stakeholders involved in information security, preserving the availability, integrity, and confidentiality of information.
- Ensure periodic review of policies and procedures to adequately address changes (legal, technical, or otherwise) and to promote the continuous improvement of security.

The Information Security Management System is based on the requirements of ISO/IEC 27001:2013 and is mandatory for all employees. The Board of Directors of Ares Lusitani is responsible for the development, implementation, updating, and oversight of compliance with the entire Management System and has appointed Hipoges as the entity responsible for its implementation.