
	PE05-1 INFORMATION SECURITY MANAGEMENT SYSTEM POLICY	
	Version: 2.0	Modification date: 4/11/2024 Clasification: Public

INFORMATION SECURITY MANAGEMENT SYSTEM POLICY

Made by	Reviewed and approved by
Security Manager	Address

REVIEWS			
DATE	DONE	APPROVED	Description of change
4/11/2024	R. Security	Address	Update

	PE05-1 INFORMATION SECURITY MANAGEMENT SYSTEM POLICY	
	Version: 2.0	Modification date: 4/11/2024 Clasification: Public

Seabery, as a leader in Augmented Reality educational solutions for welding training, recognizes the criticality of information security in all its development, production and customer service processes.

The scope of our ISMS covers all processes related to the development, production and support of our welding simulation solutions, including our core facilities and critical information systems.

We are committed to conducting periodic risk assessments and implementing commensurate security controls to protect our critical information assets.

Seabery, aware of the corporate social responsibility involved in the development of its economic activity, has established a form of management that implies a transparent and moral behavior with its stakeholders. Among its objectives, in addition to economic competitiveness and obtaining profits, it establishes objectives aimed at favoring its social and environmental surroundings, for which it adopts policies to improve working conditions, respect for human rights, ethical behavior with all stakeholders (employees, customers, suppliers, etc.).

For this reason, it has implemented an **Information Security Management System**, with the objective of protecting information resources against threats, internal or external, deliberate or accidental, in order to ensure compliance with confidentiality, integrity and availability of information.


The effectiveness and application of the **Information Security Management System** is the direct responsibility of the **Information Security Committee**, which is responsible for the approval, dissemination and compliance with this Security Policy. In its name and on its behalf, an Information Security Management System Manager has been appointed, who has sufficient authority to play an active role in the Information Security Management System, supervising its implementation, development and maintenance.

The Information Security **Committee** shall develop and approve the risk analysis methodology used in the Information Security Management System.

Any person whose activity may, directly or indirectly, be affected by the requirements of the Information Security Management System is obliged to strictly comply with the Security Policy.

For all these reasons, we assume our commitment to information security, according to the ISO/IEC 27001 reference standard, for which the Management establishes the following principles:

- Management competence and leadership as a commitment to develop the Information Security System.

	PE05-1 INFORMATION SECURITY MANAGEMENT SYSTEM POLICY	
	Version: 2.0	Modification date: 4/11/2024 Clasification: Public

- Determine the internal and external stakeholders involved in the Information Security System and comply with their requirements.
- Understand Seabery's context and identify opportunities and risks as a basis for action planning to address, assume or deal with them.
- Comply with current legislation on information security.
- To ensure the confidentiality of the data managed by Seabery and the availability of the information systems, both in the services offered to customers and in internal management, avoiding undue alterations in the information.
- Ensure the capacity to respond to emergency situations, restoring the operation of critical services in the shortest possible time.
- Establish the appropriate measures for the treatment of risks derived from the identification and evaluation of assets.
- Promote information security awareness and training.
- Establish objectives and goals focused on the evaluation of information security performance, as well as continuous improvement in our activities, regulated in the Management System that develops this policy.
- Ensure the protection of the privacy of personal information, complying with applicable regulations and stakeholder expectations.
- Continually strengthen our cybersecurity capabilities to address emerging threats in the digital environment.
- Extend information security principles to our supply chain, ensuring that our suppliers and business partners comply with appropriate standards.
- Develop and maintain the resilience of our information systems to ensure the continuity of critical operations in the face of security incidents.

These principles are assumed by the Management, which has the necessary means and provides its employees with sufficient resources to comply with them, and they are expressed and made public through this Information Security Policy.

Each Seabery employee is responsible for adhering to this policy and actively contributing to information security in their daily activities.

Signed: The

Management

Date: 4.11.2024