



| | | |
|-----------------------------------------------------------------------------------|-----------------------------------------------------------------|-----------------------------------------------------|
|  | PE05-1 INFORMATION SECURITY MANAGEMENT SYSTEM POLICY | |
| | Version: 1.0 | Date modified: 30/10/2022 Classification: Public |

INFORMATION SECURITY MANAGEMENT SYSTEM POLICY

| | |
|------------------|--------------------------|
| Carried out by | Reviewed and approved by |
| Head of Security | Address |

| REVISIONS | | | |
|-----------|------|----------|---------------------------|
| DATE | DONE | APPROVED | Description of the change |
| | | | |
| | | | |
| | | | |

| | | |
|-----------------------------------------------------------------------------------|---------------------------------------------------------|-----------------------------------------------------|
|  | PE05-1 INFORMATION SECURITY MANAGEMENT SYSTEM POLICY | |
| | Version: 1.0 | Date modified: 30/10/2022 Classification: Public |

Seabery is an international company pioneer and leader in the development of educational solutions applying Augmented Reality.

We design innovative solutions to transform traditional education and vocational training.

Our aim is to create a new methodology that defines the future of vocational training by applying RA.

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


For this reason, it has implemented an **Information Security Management System**, with the aim of protecting information resources against threats, internal or external, deliberate or accidental, in order to ensure compliance with the 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, in accordance with the ISO/IEC 27001:2013 reference standard, for which the Management establishes the following principles:

| | | |
|-----------------------------------------------------------------------------------|---------------------------------------------------------|-----------------------------------------------------|
|  | PE05-1 INFORMATION SECURITY MANAGEMENT SYSTEM POLICY | |
| | Version: 1.0 | Date modified: 30/10/2022 Classification: Public |

- Management competence and leadership as a commitment to develop the Information Security System.
- Determine the internal and external stakeholders involved in the Information Security System and meet their requirements.
- Understand the Seabery context and identify opportunities and risks in the Seabery, 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 to the information.
- To ensure the capacity to respond to emergency situations, re-establishing the functioning of critical services in the shortest possible time.
- Establish appropriate measures for the treatment of risks arising from the identification and assessment of assets.
- Promote information security awareness and training.
- Establish objectives and goals focused on the evaluation of information security performance, as well as the continuous improvement of our activities, regulated in the Management System that develops this policy.

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 set out and made public through this Information Security Policy.

Signed: The Directorate

Date: 14.12.2022