

POL Management system policy

Version history

Version	Date	Author	Approved by
1	02/10/2025	Riccardo Chiaverini	Silvio Di Crosta

Table of contents

- Field of Application
- Regulatory References
- Terms and Definitions
- Roles and Responsibilities
- Management System Commitment and Objectives
- Archiving and Updates
- Reference Documents

Field of Application

This policy formalizes the commitment of Onerian S.r.l. to quality and information security in the design, development, and operation of its SaaS platforms. It establishes the framework for the Integrated Management System, in compliance with ISO 9001 and ISO/IEC 27001, and applies to all company processes, personnel, and assets.

Regulatory References

- ISO 9001
- ISO/IEC 27001
- General Data Protection Regulation (GDPR)

Terms and Definitions

- **Availability** : The property of being accessible and usable on demand by an authorised entity.
- **Confidentiality** : The property that information is not made available or disclosed to unauthorized individuals, entities, or processes.
- **Continual Improvement** : A recurring activity to enhance performance.
- **Documented Information** : Information that must be controlled and maintained by an organization.
- **Integrity** : The property of accuracy and completeness.
- **Interested Party** : A person or organization that can affect, be affected by, or perceive itself to be affected by a decision or activity.
- **Top Management** : A person or group of persons who directs and controls an organization at the highest level.

Roles and Responsibilities

- **CEO** : As the representative of Top Management, the CEO is responsible for establishing, endorsing, and ensuring that this policy is aligned with the company's strategic direction and objectives.
- **Integrated Management System Manager** : Responsible for the implementation, maintenance, and communication of this policy, ensuring the Integrated Management System conforms to the established requirements.

Management System Commitment and Objectives

Onerian S.r.l. establishes this Management System Policy to formalize its commitment to quality, information security, and the satisfaction of its clients. The CEO, representing Top Management, ensures this policy is appropriate to the company's purpose and strategic direction, which is to design, develop, and operate SaaS platforms based on Artificial Intelligence for business process automation. This policy is foundational to our operations and reflects the principles defined in our "Context analysis".

Onerian is committed to achieving excellence and fostering trust by integrating the following core principles into its Integrated Management System, which complies with the requirements of ISO 9001 and ISO/IEC 27001:

- **Customer Satisfaction** : We shall systematically identify and meet the needs and expectations of our B2B clients by delivering innovative, reliable, and effective AI-powered solutions and providing timely technical support.
- **Quality of Products and Services** : We are committed to the design, development, and maintenance of high-quality SaaS platforms. Our focus is on ensuring our AI assistants and automation solutions are scalable, secure, and performant, delivering tangible value to our clients' business processes.
- **Information Security** : We shall protect the confidentiality, integrity, and availability of all information assets, including our intellectual property and the data entrusted to us by our clients. Security is a fundamental component of our product design, development, and service delivery processes.
- **Compliance** : We shall comply with all applicable legal, statutory, regulatory, and contractual requirements relevant to our products, services, and operations, with a particular focus on data protection regulations such as the GDPR.
- **Continual Improvement** : We are committed to the continual improvement of our Integrated Management System. We shall regularly review our performance, processes, and this policy to enhance effectiveness and adapt to new challenges and opportunities.

This policy provides the framework for setting and reviewing quality and information security objectives. The process for defining, planning, and monitoring these objectives is detailed in the "PRO Objectives and planning for their achievement" procedure.

The CEO shall ensure this policy is established and fully endorsed. The Integrated Management System Manager is responsible for its implementation and maintenance, ensuring it is available as documented information in accordance with the "PRO Documented information management procedure".

The policy shall be communicated to and understood by all personnel, whose responsibilities are defined in the "PRO Roles and responsibilities procedure". All employees and collaborators are required to apply these principles in their daily activities.

This policy shall be made available to relevant interested parties as deemed appropriate. Its continued suitability, adequacy, and effectiveness will be reviewed periodically as part of the "PRO Management Review Process".

Archiving and Updates

This document is managed as controlled documented information. It is subject to periodic review, at least annually, during the management review process to ensure its continued suitability, adequacy, and effectiveness. Updates are managed in accordance with the procedure for the management of documented information.

Reference Documents

- Context analysis
- PRO Objectives and planning for their achievement
- PRO Documented information management procedure
- PRO Roles and responsibilities procedure
- PRO Management Review Process