O3 enterprise
ZUCCHETTI

Policy for the Information Security

Version	2
Language	EN
Date	10 ott 2025

INDEX

1. POLICY

O3 Enterprise is a company specialized in the development of software in the medical field. The company recognizes the importance of information security in ensuring customer trust, compliance with industry regulations, and the protection of sensitive data.

This policy outlines our commitment to safeguarding the confidentiality, integrity, and availability of information in accordance with the ISO/IEC 27001:2022, ISO/IEC 27017:2021 and ISO/IEC 27018:2025 standards and applicable regulations.

This policy applies to all processes managed by the company and all employees and third parties who access or handle company information.

Top Management obligations:

- Implement and maintain an Information Security Management System (ISMS) in compliance with ISO/IEC 27001:2022, ISO/IEC 27017:2021 and ISO/IEC 27018:2025 standards and in accordance with the requirements of Regulation EU 2016/679;
- Adopt a PDCA (Plan-Do-Check-Act) approach to continuously improve the ISMS;
- Identify, assess, and mitigate risks associated with information security and the protection of *personal identifiable information* (PII);
- Ensure that all software development processes comply with regulatory requirement;
- Establish, implement and maintain security controls to protect sensitive data (e.g. access control, activity monitoring, etc.);
- Promote and support continuous training and awareness programs for all personnel on information security and the protection of sensitive data.

Employees obligations:

Each employee of the company is required to actively contribute to the protection of information and sensitive data processed in the course of their activities. In particular, each employee must:

- Comply with all policies, procedures, and operational instructions related to information security and the protection of processed data;
- Regularly participate in training and awareness programs promoted by the company, in order to maintain an adequate level of awareness of the risks associated with information security and personal data protection;
- Promptly report any incidents, anomalies, or suspected information security breaches;
- Comply with all applicable laws, internal policies, and contractual requirements.

O3 Enterprise adopts a proactive approach to managing security incidents, with processes to:

- Detect and report breaches and vulnerabilities;
- Investigate each incident and implement corrective actions;
- Maintain an incident log for analysis and continuous improvement.

This policy will be reviewed periodically to ensure compliance with applicable regulations and company requirements.

2. MANAGEMENT COMMITMENT

As we are entrusted with treating sensitive (patients) information as well as sensitive company assets, the Top Management at O3 Enterprise feel strongly that our reputation and success depend on safeguarding our own and our Customer information.

Unauthorized disclosure of confidential information could have negative consequences for our organization, exposing us to legal risks. Similarly, any harm to the data we rely on for business decision-making and production processes or any delays in accessing critical information would be unacceptable.

We affirm our intention to treat information security as an integral part of our culture.

We show our commitment to strong security in the following ways:

- By establishing a way to allow employees to suggest new security policy or measures;
- By identifying in the CEO the security manager position;
- By establishing and communicating clear security policies, standards, and processes that are aligned with the strategic direction of the organization;
- By ensuring that ISMS requirements and controls are integrated into the organization's processes;
- By serving as models of compliance with security policies;
- By swiftly detecting and dealing with violations of security policies;
- By directing and supporting persons directly involved with information security and the ISMS;
- By regularly reviewing and continuously improving our information security program;
- By providing adequate resources — human, technical and financial — for the implementation, maintenance and continual improvement of the ISMS and the systems for the protection of personal and sensitive data.