Information Security Policy

The protection of information and information systems is of strategic importance to SOFMEDICA. It is essential for achieving both short- and long-term business objectives while ensuring the confidentiality, integrity, and availability of customer data and services.

Recognizing the critical role of information security in its business operations, SOFMEDICA has adopted this Information Security Policy with the following objectives:

- Ensuring the confidentiality, integrity, and availability of all managed information.
- Maintaining the reliable and secure operation of information systems.
- Responding promptly and effectively to incidents that may impact business operations.
- Complying with legislative and regulatory requirements.
- Continuously enhancing the level of information security through ongoing improvements.

Scope and Implementation:

To achieve these objectives, the following measures and controls have been established:

- Organizational Structure: Defining roles and responsibilities for monitoring and managing information security.
- Access Control: Implementing technical measures to regulate and restrict access to information and systems.
- Information Classification: Categorizing information based on its sensitivity and business value.
- Data Protection Measures: Safeguarding information during processing, storage, and handling.
- Employee Awareness & Training: Educating employees and partners on information security responsibilities.
- Incident Management: Establishing procedures for detecting, reporting, and responding to security incidents.
- Business Continuity & Disaster Recovery: Ensuring operational resilience in case of system failures or disasters.

SOFMEDICA conducts regular risk assessments to identify and mitigate potential security threats. A structured framework is in place to evaluate the effectiveness of information security processes, with clearly defined performance metrics and periodic management reviews to drive continuous improvement.

The Information Security Officer (ISO) is responsible for overseeing compliance with security policies and procedures, taking proactive measures to eliminate risks, and ensuring the protection of SOFMEDICA’s data assets. All employees and partners with access to SOFMEDICA’s information and systems are required to comply with this policy and uphold security best practices.

Commitment to Compliance and Continuous Improvement:

SOFMEDICA is fully committed to:

- Ongoing compliance with all relevant regulatory and legal requirements.
- The continuous enhancement of its Integrated Management System (IMS).
- Maintaining a security-conscious culture across the organization.

This policy is regularly reviewed and updated to align with evolving security threats, business needs, and industry standards.