INTEGER CONSULTING

Integrated Management Policy

Code:	PS.01
Version:	04
Version Date:	20/06/2024
Author:	IMS
Approved by:	Luís Setúbal
Classification:	Public

* ISO 9001:2015, ISO/IEC 27001:2022 and ISO/IEC 27701:2019

Change History

Date	Version	Author	Change Description
20/06/2024	03	IMS	ISO/IEC27001:2022 review and transition and update to the new Integer template
10/01/2025	04	IMS	Included item 10: associated documents and in Item 11 updated the description of the Standards

Index

1. Introduction

Integer Consulting, S.A. (hereinafter INTEGER), is committed to excellence in all its operations, ensuring compliance with the international standards ISO/IEC 27001:2022 (Information Security Management System), ISO/IEC 27701:2019 (Information Privacy Management System) and ISO 9001:2015 (Quality Management System). This Integrated Management Policy establishes the guidelines to ensure that our activities are conducted securely, efficiently and in compliance with applicable legal and regulatory requirements, meeting the expectations of all stakeholders.

This policy aims to guarantee information security, the protection of personal data and the quality of the services and products offered by the organisation.

2. Goals

The goal of this policy is to establish guidelines and principles to guide our integrated management practices, ensuring compliance with the aforementioned standards and promoting a culture of ongoing improvement, safety and quality in our outsourcing services.

3. Scope

This policy applies to all business units, operations, employees, service providers, customers, suppliers and other stakeholders involved with INTEGER. It covers all processes, information, information assets and systems under the company's management, whether internal or external, among other outsourcing services.

4. Recipient

This policy applies to all INTEGER processes, employees, internal and external, and stakeholders, covering all areas of operation and services provided, including infrastructure, technical support, software development, and other outsourcing services.

5. Principles of the Integrated Management Policy (Goal)

5.1 Commitment to Information Security (ISO/IEC 27001:2022)

- Protect the confidentiality, integrity and availability of our customers' and our company's information;
- Implement effective security controls to mitigate risks identified in outsourcing services;
- Carry out periodic risk assessments and implement ongoing improvements;
- Ensure that all employees understand and fulfil their responsibilities in relation to information security.

5.2 Commitment to Personal Data Protection (ISO/IEC 27701:2019)

- Respect the privacy and protect the personal data of customers, employees and other stakeholders, in accordance with the European Union's General Data Protection Regulation (GDPR);
- Implement and maintain privacy controls in accordance with applicable regulations and best practices;
- Ensure transparency in the processing of personal data, obtaining appropriate consent when necessary;
- Respond promptly to privacy incidents and ensure the ongoing protection of personal data;
- Responsibility and Compliance: Ensure that all employees and stakeholders understand their responsibilities in relation to data protection and are empowered to fulfil these responsibilities.

5.3 Commitment to Quality (ISO 9001:2015)

- Meet and exceed customer expectations by delivering high quality outsourcing services;
- Implement a quality management system that promotes ongoing improvement and process efficiency;
- Establish clear and measurable quality goals, regularly monitoring performance against these goals;
- Involve all employees in the process of ongoing improvement and compliance with quality requirements;
- Ongoing Improvement: Promote a culture of ongoing improvement in all processes, services and products, using the PDCA (Plan-Do-Check-Act) cycle as an approach;
- Leadership**:** INTEGER's leadership is committed to promoting a culture of quality and to providing the necessary resources for quality goals to be achieved.

6. Implementation Guidelines

6.1 Planning and Risk Assessment

- Carry out regular and detailed risk assessments to identify threats and vulnerabilities in outsourcing services;
- Develop action plans to mitigate risks and implement appropriate controls.

6.2 Training and Awareness

- Promote ongoing training for all employees on information security, data protection and quality;
- Carry out awareness campaigns to reinforce the importance of compliance with this policy;
- Adequate Resources: Provide the necessary resources to implement, maintain and continuously improve the Integrated Management System;
- Effective Communication: Ensure that all employees, partners and stakeholders are aware of this policy, understand its requirements and contribute to its implementation.

6.3 Monitoring and Measurement

- Establish performance indicators to monitor the effectiveness of IMS in outsourcing services;
- Carry out regular internal audits to check compliance with standards, ensuring full compliance with the requirements of the ISO/IEC27001:2022, ISO/IEC27701:2019 and ISO9001:2015 standards, as well as all applicable legal, regulatory and contractual requirements.

6.4 Ongoing Improvement

- Implement an ongoing improvement cycle (PDCA - Plan, Do, Check, Act) for all areas covered by IMS;
- Periodically analyse and review the effectiveness of the IMS and identify opportunities for improvement.

7. Responsibilities

7.1 Senior Management

- Show leadership and commitment to the implementation and maintenance of the IMS;
- Ensure that the necessary resources are made available for the effective implementation of the IMS.

7.2 Managers

- Managers are responsible for ensuring that their teams are aware of and comply with this policy, as well as facilitating the implementation of regulatory requirements in their areas;
- Implement policies and procedures in their areas of responsibility;
- Promote a culture of security, privacy and quality among its teams.

7.3 Employees

- All INTEGER employees are responsible for applying this policy in their daily activities and reporting any incidents or non-conformities;
- Comply with the policies and procedures established at IMS;
- Actively participate in training and report any incidents or non-conformities.

7.4 Internal Auditing

- Internal auditing is responsible for monitoring compliance with this policy and regulatory requirements, reporting the results to senior management.

8. Ongoing Improvement

INTEGER is committed to the ongoing improvement of its Integrated Management System. This policy will be reviewed periodically to ensure its relevance and effectiveness, and any updates will be communicated to all interested parties.

9. Review and Update of the Policy

This policy is approved by Senior Management and will be reviewed annually or as necessary, based on changes in regulatory requirements, organisational goals or stakeholder feedback. Reviews will be carried out by the IMS management team.

10. Associated Documents

PS.00.02 Information Security Policy

11. Reference Documents

ISO/IEC 27001:2022 (Information Security Management) - Information security, cybersecurity and privacy protection Information security management systems
ISO 9001:2015 (Quality Management) - Quality management systems—Requirements
ISO/IEC 27701:2019 (Information Privacy Management) – Security techniques

12. Definitions and Acronyms

IMS - Integrated Management System
PDCA - PLAN-DO-CHECK-ACT, or also PLAN-DO-CHECK-ADJUST.

13. Conclusion

INTEGER is committed to maintaining an Integrated Management System that guarantees information security, the protection of personal data and the quality of the outsourcing services offered. This commitment reflects our dedication to excellence and to satisfying the needs of our customers and other stakeholders.