Policy

Rev. 4 dated 7 August 2026

INTEGRATED MANAGEMENT SYSTEM POLICY

Quality · Environment · Information Security · Gender Equality · Artificial Intelligence

1. Mission, context and scope

The mission of Parsec 3.26 S.r.l. is to provide ICT solutions and services that help public and private sector customers innovate their processes and become more competitive, drawing on its extensive experience in the IT sector, its broad range of services, its wide geographical coverage and its ongoing focus on customer needs and satisfaction. Its core business is the management of resources, applications and data, including the development and provision of generative artificial intelligence (AI) systems, machine learning models and intelligent automation components.

To fulfil this mission, Management has adopted an Integrated Management System compliant with **UNI EN ISO 9001 (quality), UNI EN ISO 14001 (environment), UNI CEI EN ISO/IEC 27001 (information security)**, supplemented by the controls set out in the **ISO/IEC 27017 and 27018** guidelines for cloud services, **UNI CEI EN ISO/IEC 42001 (artificial intelligence)**, and the **UNI/PdR 125:2022** reference practice (gender equality).

The IMS applies to the activities, processes and roles within the approved scopes, as described in the Scope of Application (DdA) and the AI Scope of Application (DdA IA). This policy takes into account the analysis of the organisation's context, the needs of interested parties and the assessment of risks and opportunities, and is consistent with the company's strategic direction.

The company's activities are guided by a people-centred approach and respect for individuals, transparency and integrity, social responsibility, teamwork, awareness of the collective interest and respect for the environment, in line with its Sustainability Plan and the goals of the UN 2030 Agenda. Management promotes a culture of quality and ethical conduct at all levels and regards dialogue with personnel and interested parties as an essential means of fulfilling the company's mission.

2. Management commitments

Top Management takes responsibility for the effectiveness of the IMS and undertakes to:

- Meet applicable requirements, including customer and contractual requirements, compliance obligations, and statutory and regulatory requirements relating to quality, the environment, information security, personal data protection (Regulation (EU) 2016/679), cybersecurity (Italian Legislative Decree No. 138/2024), artificial intelligence (Regulation (EU) 2024/1689 and Italian Law No. 132/2025), occupational health and safety, and gender equality;
- Protect the environment, including the prevention of pollution, while also taking into account the effects of climate change on its activities;
- Preserve the confidentiality, integrity and availability of its own information and that of its customers;
- Ensure equal opportunities and prevent all forms of discrimination;
- Develop and use AI systems responsibly, reliably and in compliance with applicable requirements;
- Set objectives for each area of the IMS, ensure the resources needed to achieve them and periodically review their achievement;
- Continually improve the IMS, customer satisfaction, environmental performance, information security performance and AI management performance.

3. Guiding principles

Customers and service quality. Customers are at the heart of the company's processes, which are identified and organised from a customer perspective. The company continually measures customer and interested party satisfaction, monitors processes and services through performance indicators, and explores new technologies and market opportunities to offer innovative services with high added value.

Environment. Parsec 3.26 controls the significant environmental aspects of its activities from a life cycle perspective, including energy consumption associated with offices, infrastructure and cloud services; waste generation, particularly waste electrical and electronic equipment; resource use; and supplier selection criteria. It promotes environmental awareness through information and training activities for personnel.

Information security and cybersecurity. Information is a strategic asset. The company classifies and protects information, both on-premises and in the cloud, using measures proportionate to the risks to prevent unauthorised access and processing. It implements the cybersecurity risk management measures required under NIS legislation, manages incidents and vulnerabilities in a structured manner through preventive and reactive activities, ensures service continuity, requires suppliers to meet appropriate security requirements, and protects personal data by design and by default.

Gender equality and inclusion. In accordance with Articles 3, 37 and 51 of the Italian Constitution, the company undertakes to:

- Adopt transparent, non-discriminatory criteria for recruitment, hiring and career development, promoting women's employment and representation in positions of responsibility;
- Ensure pay equity between women and men, monitoring it periodically, and equal access to training and professional development opportunities;
- Protect parenthood, promote the full use of maternity and paternity leave, and support work–life balance and employee welfare policies;
- Prevent and combat all forms of physical, verbal or digital abuse and harassment in the workplace, providing confidential reporting channels and protection against retaliation;
- Promote an inclusive culture, including through language and communication that respect differences.

Responsible artificial intelligence. The design, development and use of each AI system are subject to the definition of its purposes, context of use, intended users and recipients, limitations of use and responsibilities, and to an assessment of its risks and impacts on individuals, groups and society. In particular, the company:

- Prohibits uses that are incompatible with applicable legislation and reassesses the use case whenever its purposes, data, model, intended users or recipients, or level of automation change;
- Designs systems in accordance with proportionate criteria for reliability, security, data quality, robustness, transparency and accessibility, ensuring human oversight; outputs are not, in themselves, regarded as confirmation of truth, legal compliance or technical correctness;
- Uses AI in services for public administrations to support preparatory and assessment activities, within the limits of authorised purposes: legal and administrative assessments and the adoption of administrative decisions remain the responsibility of the competent persons or bodies;
- Applies data minimisation and selects protective measures—pseudonymisation, encryption, segregation of knowledge bases and access control—verifying their effectiveness against actual processing activities;

- Manages dependence on external models, platforms and suppliers through qualification requirements, contractual agreements, verification of terms of use and continuity measures.

Commercial needs or project deadlines do not justify departures from legal requirements or the deployment of a system without the required authorisations. Any exceptions to this policy must be authorised by Management, justified and documented.

4. Objectives, responsibilities and resources

This policy provides the framework for setting objectives across all areas of the IMS. Objectives are relevant and, where possible, measurable; for each objective, responsibility, resources, deadlines, indicators and verification methods are defined and recorded in the Improvement Programme. Management assigns roles, responsibilities and authorities and makes available adequate expertise, tools, infrastructure and financial resources. Process owners implement the policy within their areas of responsibility and report to Management any obstacles to achieving objectives, resource shortages and risks that cannot be managed within the established criteria.

5. Awareness, communication and reporting

The policy is communicated to all personnel and external personnel working under the company's control, who must be familiar with it and understand their contribution to the effectiveness of the IMS and the consequences of failing to meet requirements. The company delivers training and awareness programmes proportionate to each role, including AI literacy, and retains evidence of these activities. Personnel are required to suspend and report activities involving clear violations or uncontrolled risks; reports made in good faith are handled confidentially and without retaliation. The policy is available to interested parties through the company's communication channels; the confidentiality of procedures and technical controls does not restrict access to the commitments set out herein.

6. Policy review

Management reviews this policy at planned intervals, at least as part of the Management Review, and whenever significant changes occur in the regulatory context, strategy, scope of the systems or impacts on interested parties, to ensure its continuing suitability, adequacy and effectiveness. Changes are approved and communicated in accordance with document control rules.

This document is public and available to anyone who wishes to consult it.

Cavallino, 21/10/2026 The Management