# INFORMATION SECURITY POLICY
# - UNI EN ISO 27001 -

Sesa S.p.A. (hereinafter “Sesa” or the “Company”) is committed to protecting the Confidentiality, Integrity and Availability of the Company’s information assets and of the data managed through its highly reliable infrastructure, as a necessary condition for the Company’s competitiveness and reputation. Information represents corporate assets that are valuable to the Company and must be adequately protected. This document sets out the Information Security Policy (hereinafter “Policy”), in accordance with the guidelines of the ISO 27001 standard, adopted by Sesa on a voluntary basis. It constitutes the highest-level reference for the Information Security Management System (hereinafter “ISMS”) defined and implemented at Sesa in order to ensure adequate protection of information in line with the expectations of the several stakeholders.

The issue of information security has become increasingly important at both national and international levels. The relevant regulatory framework includes, in addition to the above-mentioned ISO standard, the applicable European legislation, in particular the NIS2 Directive, transposed into Italian law by Legislative Decree 138/2024, and the European DORA (Digital Operational Resilience Act) Regulation 2022/2554, concerning digital operational resilience, as relevant to Sesa's activities.

This Policy applies to all employees and partners of the Company (hereinafter “Recipients”) and will also apply to stakeholders involved in the treatment of information who are required to implement specific policies set out in this document. All Recipients are responsible for implementing this Policy, with the aim of protecting the Company’s information assets from all threats, whether internal or external, intentional or accidental.

Information security is responsible for protecting information from a wide range of threats in order to ensure business continuity, minimise damage and maximise return on investment and commercial opportunities. According to the ISO 27000 standard, it is based on the protection of three fundamental principles: confidentiality, integrity and availability of information.

Ensuring an adequate level of protection for a system means:

- reduce the likelihood of IT security parameters being breached to an acceptable level;
- promptly identify when and where in the system this breach occurs;
- minimise damage and restore any breached requirements as quickly as possible.

In accordance with the requirements of the ISO 27001 standard, protection is provided through an ISMS, which refers to the set of technical and organisational measures designed to ensure the protection of the confidentiality, integrity and availability of information.

The principles the company follows and applies to ensure the protection and security of information are:

- ICT risk management in accordance with solid Frameworks that ensure governance and control;
- management of all types of incidents, particularly ICT incidents, with structured and well-defined processes and reporting that is as standardised as possible, in order to reduce response times;
- continuous security monitoring and the detection and management of incidents;
- Business Continuity Management and planning of operational resilience tests tailored to the company's specific context, carried out periodically and supported by test plans of several levels of complexity linked to the assessments formalised in the Business Impact Analysis (BIA) and supported by recovery procedures;
- alignment of security measures with the company's business requirements, in compliance with current regulations and contractual obligations;
- risk management of ICT service providers and external collaborators, in order to establish strong contractual relationships of commitment and accountability with third parties operating within the supply chain of the ICT service provided;
- identification of the security measures (controls) to be adopted following the risk assessment process, based on agreed acceptance criteria, in order to maintain an appropriate balance between the cost of the controls and the associated risk;
- training and awareness-raising for all company staff, as a fundamental part of the safety process, aimed at increasing individual awareness and promoting the responsible use of resources, thereby contributing to the achievement of the set targets;
- definition of clear and easily understandable security measures, in order to facilitate their correct and widespread application;
- integration of security into the services provided, to be planned and applied at all stages, starting from the initial design and development phases;
- definition of access authorisations to information according to the need-to-know principle, in line with the company's operational and business requirements;
- promoting the exchange of information and cyber threat analyses among Group companies, in line with guidance from the competent authorities, as a means of strengthening the collective ability to respond to such threats.

Information security, defined as the protection of the principles of confidentiality, integrity and availability (service continuity), is a critical success factor to which the company attributes the highest importance, given both the nature of the services it provides and its market position. To this end, Sesa has implemented an ISMS which, in accordance with the principles listed above and with the aim of containing such risks to acceptable levels and remaining cost-competitive, sets out to achieve the following targets:

- comply with legal regulations (including, but not limited to, Legislative Decree 196/03, EU Regulation 2016/679, Legislative Decree 231/01 and subsequent amendments and additions, the NIS2 Decree and EU Regulation DORA), industry standards and regulations, and clients' contractual requirements;
- maintain a corporate security system aligned with best practices and International Standards, demonstrating this to stakeholders;

- verify, through a risk assessment and management process, the ongoing strategic alignment of security targets with the company's business;
- foster a culture of information security within the Company;
- consider continuous improvement as a way to keep safety standards high.

The Company is committed to promote knowledge and awareness of the Information Security Policy amongst all stakeholders.

Sesa is committed to constantly monitoring and assessing the level of Information Security achieved and the effectiveness of its Management System with a view to continuous improvement, including through the attainment and maintenance of Certifications required by the most advanced International industry Standards, in order to consolidate its efficiency, quality and reliability in the provision of services and the secure protection of public administration data.

The Policy is continuously updated and reviewed, through an annual review and whenever necessary, to ensure its ongoing improvement; it is shared with the organisation and made available to customers, stakeholders, and third parties.

Empoli (FI) - April 30, 2025

Sesa S.p.A.