Information Security Policy

1. Purpose and Scope

Intecs Engineering S.p.A. recognises information and the systems used to process it as strategic assets for achieving its business objectives and safeguarding the interests of the organisation, its customers and other interested parties.
To this end, the Company has implemented an Information Security Management System (ISMS) in accordance with ISO/IEC 27001, with the aim of protecting information and managing risks that could compromise its confidentiality, integrity and availability.
The Management System applies to the activities, processes, services and locations included within the following scope:

> *Development of integrated hardware and software products and systems based on advanced technologies with a high R&D content. Acquisition and management of orders for the design, development, verification and validation, installation, maintenance, and after-sales support of HW/SW products and systems.*

This Policy establishes the general principles and guidelines for information security and provides the framework for defining security objectives and implementing the Management System.

2. Organisational Commitments

Intecs Engineering S.p.A. is committed to:

- protecting the confidentiality, integrity and availability of information processed in the course of its business activities;
- identifying, assessing and managing information security risks through a systematic approach proportionate to the Company's business context;
- establishing information security objectives consistent with the Company's business objectives and this Policy, and periodically monitoring their achievement;
- meeting applicable information security requirements, including legal, statutory, regulatory and contractual obligations, as well as commitments made to interested parties;
- protecting information and corporate assets against unauthorised access, disclosure, loss, alteration, unavailability and destruction;
- promoting personnel awareness and providing appropriate information and training activities to ensure that everyone understands their information security responsibilities;
- encouraging the proper and secure use of IT resources, digital technologies and corporate tools, including Artificial Intelligence systems, in compliance with applicable security requirements and internal policies;

- preventing and managing information security incidents, minimising their impact and contributing, where relevant, to business continuity and the recovery of operations;
- monitoring the performance and effectiveness of the ISMS, periodically reviewing it and pursuing its continual improvement.

3. Applicability and Responsibilities

This Policy applies to all personnel of Intecs Engineering S.p.A. and, according to the activities performed and the relevant obligations, to collaborators, consultants, suppliers, partners and other parties authorised to access information or resources within the scope of the ISMS.
All relevant parties are required to comply with the principles set out in this Policy and with the applicable corporate provisions, procedures and operating instructions, contributing to the protection of information and the timely reporting of security events, anomalies and incidents.
Top Management supports the Information Security Management System, promotes an information security culture and ensures, within the scope of its responsibilities, the resources and competencies required for its implementation and for achieving the defined objectives.
Information security is a shared responsibility.

4. Communication and Review

This Policy is communicated to personnel and made available to relevant interested parties, where appropriate.
The Policy is reviewed periodically and whenever significant changes occur in the Company's business context, risks or applicable requirements, in order to ensure its continuing suitability, adequacy and effectiveness.
Intecs Engineering S.p.A. is committed to continually improving its Information Security Management System in line with its business objectives and the requirements of ISO/IEC 27001.

Doc-ID: IE-ISMS-POL-ENG
Date: 27/10/2026
Version: 1.0

General Manager (M. Mannori)

