Information Security Management System

Doc. **PO-ISMS.001.EN** Ed. **1** - Rev. **0** del **09/01/2025**
Classification: **C1 PUBLIC**

Information Security Policy

Ai Engineering s.r.l.
Legal and operational headquarters
C.so Francesco Ferrucci, 112 - 10138 Torino (TO)
VAT IT 06764910011
C.F/Business Register TO 01066850064
Cod. REA: TO – 632269

1 DOCUMENT SHEET

List of changes:

Ed.	Rev.	DRAFTED	CHANGE SUMMARY	VERIFICATION AND APPROVAL	
				APPROVED	DATE
1	0	ISM	First Draft within the ISMS	CEO	09/01/2025

2 TABLE OF CONTENTS

3 INTRODUCTION

Ai Engineering S.r.l. (hereinafter referred to as "Ai Engineering" or "the organization") provides integrated consulting and highly specialized services in civil engineering, serving both public entities and private clients. The organization's expertise spans the fields of construction, environment, infrastructure, and transportation, with a multidisciplinary and innovation-oriented approach. In a context where digitalization plays an increasingly central role in production and management processes, and where cyber threats are becoming more sophisticated, Ai Engineering considers the protection of company information as a strategic component of its business. Information security is therefore regarded as an essential element for safeguarding competitiveness, ensuring operational continuity, and reinforcing the trust of clients, partners, and stakeholders.

4 PURPOSE

This Information Security Policy aims to clearly and systematically define the organization's approach to protecting its information assets. The objective is to prevent unauthorized access, loss, manipulation, destruction, or unavailability of managed information. In doing so, the organization seeks to safeguard not only its corporate data but also the interests of individuals and entities with whom it maintains professional and institutional relationships.

5 ORGANIZATIONAL CONTEXT

Ai Engineering operates in a highly competitive and dynamic market where technological and regulatory transformations require continuous evolution of operational methods. As part of the broader Ai Group, the organization regularly faces challenges related to the management of sensitive data, the digitalization of processes, and the use of advanced technological infrastructures, including cloud environments and distributed collaboration solutions. The regulatory environment includes European and national regulations, international technical standards, and contractual obligations deriving from complex projects. This scenario demands constant attention to information security, which should be seen not only as a compliance obligation but also as an organizational value.

6 INTERESTED PARTIES AND THEIR REQUIREMENTS

The organization acknowledges that information security is influenced by the needs and expectations of a diverse range of stakeholders. Clients expect reliable data management and guarantee of confidentiality. Employees and collaborators expect to operate in an environment where information is protected, and risks are minimized. Suppliers and consultants must rely on clear rules governing access and data handling. Regulatory authorities require full compliance with applicable laws and the implementation of management systems aligned with recognized standards. Ai Engineering commits to incorporating these expectations into its management system and to tailoring its security measures accordingly.

7 DEFINITION OF INFORMATION SECURITY

For Ai Engineering, information security comprises the set of measures, controls, and organizational practices aimed at protecting information from events that could compromise its confidentiality, integrity, or availability. Confidentiality ensures that access to information is restricted to authorized personnel only. Integrity guarantees that information is accurate, complete, and protected from unauthorized, intentional, or accidental modifications. Availability means that information and the systems that process it are accessible and usable by authorized users whenever needed.

8 SCOPE OF APPLICATION

This Policy applies to all information processed by Ai Engineering, regardless of its form (digital, paper-based, verbal), nature (technical, commercial, administrative, personal), or classification. It covers all individuals who access, process, transmit, or manage information on behalf of the organization, including employees, collaborators, suppliers, and formally authorized external consultants. The scope also includes information systems, technological infrastructures, devices, and physical or digital premises (including cloud environments and remote locations) involved in the handling of information.

9 OBJECTIVES

The Policy aims to ensure the resilience of the organization's information systems, the protection of know-how and intellectual property, the reduction of the impact of security incidents, and compliance with legal, contractual, and industry-specific requirements. It also seeks to promote personnel awareness regarding information security and to demonstrate the organization's ongoing commitment to its stakeholders. Security objectives are annually translated into measurable targets, formalized within the Annual Information Security Plan, and monitored through specific Key Performance Indicators (KPIs). These indicators are reviewed during Management Review meetings and serve as a basis for corrective and improvement actions.

10 OPERATIONAL STRATEGIES

To achieve the stated objectives, Ai Engineering has adopted an Information Security Management System (ISMS) compliant with ISO/IEC 27001:2022. The organization is committed to conducting periodic risk assessments, implementing controls based on information classification, monitoring security events, and ensuring a prompt and structured response to incidents. Special attention is given to personnel training, awareness-raising on secure behaviours, and the execution of internal audits to verify the effectiveness of the system. These strategies are supported by a systematic approach to continual improvement, realized through performance analysis, lessons learned from incidents, control adjustments, and regular documentation updates.

11 GUIDING PRINCIPLES

Information security at Ai Engineering is based on a few key principles. Information is classified according to its sensitivity, value, and criticality to determine the appropriate level of protection. Access to information is governed by the "need-to-know" principle, ensuring that only duly authorized personnel can access data necessary for their duties. Encryption is mandatory for the protection of highly sensitive information, both at rest and in transit. Measures are in place to ensure data integrity and availability, including backup solutions, redundant infrastructures, and preventive maintenance procedures. Information is retained in compliance with legal and contractual requirements and securely disposed of at the end of its life cycle. All adopted measures are proportionate to the level of identified risk.

12 MANAGEMENT COMMITMENT

The management of Ai Engineering actively promotes an organizational culture focused on information security. This commitment is reflected in the definition of clear objectives, the allocation of necessary resources, the dissemination of this Policy, and the constant verification of system effectiveness. Management plays a leading role in fostering responsible behaviors and ensuring that all organizational levels share responsibility for protecting information. It is also committed to supporting the continual improvement of the ISMS, ensuring that results from assessments, audits, and reports contribute to the ongoing development and strengthening of the system.

13 ROLES, RESPONSIBILITIES, AND AUTHORITIES

The governance of the Information Security Management System is entrusted to the organization’s management, which assigns specific tasks and responsibilities to the relevant company functions. An ISMS Manager is appointed to coordinate and maintain the system. Functional managers are responsible for applying security measures within their operational areas, while IT and privacy representatives provide technical and regulatory support in managing risks and incidents. All employees and collaborators are required to be aware of and comply with corporate rules and procedures regarding information security.

14 EXCEPTIONS

Any exceptions to this Policy must be expressly authorized by management, only in the presence of documented and justified operational needs. Each exception must be formally recorded and periodically reviewed to assess whether the original conditions justifying the exception still apply.

15 VIOLATIONS AND SANCTIONS

Violations of the provisions set out in this Policy or in related documents may result in disciplinary and/or legal actions. Infractions committed by internal personnel or external parties are considered serious breaches of contractual obligations and may lead to termination of employment or collaboration, as well as possible reporting to the competent authorities where required by law.

16 REPORTING VIOLATIONS

Anyone who identifies or suspects a violation of this Policy, or detects vulnerabilities, incidents, or anomalies relating to information security, is required to report them promptly to the ISMS Manager at the dedicated email address: irt@aigroup.it. Reports are treated confidentially and are analysed to determine the appropriate corrective and preventive actions.

17 VALIDITY, REVIEW, AND APPROVAL

This Policy is formally approved by Ai Engineering’s management and is subject to review at least annually or following significant changes in the regulatory, organizational, or technological context. Each new version supersedes the previous one and is promptly communicated to all interested parties, becoming binding for the entire organization and its external partners.

For traceability purposes, each revision includes a version number, approval date, and references to those responsible for drafting and review.

18 NORMATIVE AND DOCUMENTARY REFERENCES

This Policy is based on and complies with the following references:

- ISO/IEC 27001:2022 – Information Security Management Systems.
- EU Regulation 2016/679 (GDPR) – General Data Protection Regulation.
- Applicable national legislation on privacy and security (Italian Legislative Decree 196/2003 and subsequent amendments).
- Other contractual or industry-specific standards (e.g., ISO 9001, ISO 14001).

Any additional supporting documents (procedures, operational instructions, security plans) form an integral part of the management system and are available through the organization's document control system.

Torino, **09/01/2025**
Ai Engineering s.r.l.
The Chairman
Tarchiani Jacopo

END