INFORMATION SECURITY POLICY

Approved by MAIRE group CEO on 03/09/2025

MAIRE

1 SCOPE

MAIRE group ("the Group") is a technology and engineering Group that develops and implements innovative solutions to enable the Energy Transition to accelerate decarbonization across industries.

The Group operates through two business units: Sustainable Technology Solutions to fully enable energy transition through innovative and sustainable processes, optimizing conventional ones and creating new processes from non-fossil feedstock. Integrated Engineering and Construction Solutions to bring to reality complex plants and frontier projects designed to provide access to the latest technologies.

This Information Security Management Policy defines the scope of the Group's Information Security Management System (ISMS), which is designed in accordance with ISO 27001 and applicable legal, regulatory, and contractual requirements.

The Information Security Management System (ISMS) is aligned with the Group's policy frameworks, which promote operational excellence, digital transformation, and responsible innovation. Digital transformation, cybersecurity, and AI-driven technologies are integral components of MAIRE's business and security strategy. This integration embeds information security into the Group's culture, governance, and strategic decision-making processes, thereby positioning MAIRE to deliver secure, reliable, and sustainable solutions to its stakeholders.

Simplicity is a key aspect of MAIRE's strategy and is also incorporated into the Information Security Management System. By promoting streamlined procedures and clearly defined responsibilities, MAIRE ensures that all personnel understand how to manage information securely and effectively across all business functions. This simplification supports the implementation of security controls, facilitates adherence to policies, and fosters a culture of continuous improvement — key to maintaining a resilient and adaptive ISMS. It also enables consistent application of best practices and promotes knowledge sharing across the Group.

1.1 Applicability and distribution

This policy applies to MAIRE group entities, personnel, and third parties who access or manage Group information assets. It covers all business functions and operational areas where information is handled, processed, stored, or transmitted. It encompasses both physical and digital environments, covering the full lifecycle of information assets.

The policy is available on the MAIRE S.p.A. website to all interested parties involved in the Group's operations. Compliance with this policy is mandatory, and responsibilities for its implementation are shared across all organizational levels.

1.2 Approval and Review

The policy is approved by the Chief Executive Officer of the MAIRE group. It is subject to revision to reflect regulatory updates, strategy changes, or contextual evolutions.

1.3 Governance

The management and implementation of this policy is entrusted to all MAIRE group personnel.

All Responsible are accountable for enforcing the policy within their areas of responsibility and ensuring that personnel are aware of and comply with the ISMS requirements.

The Chief Information Security Officer (CISO) is responsible for defining and maintaining the Group's information security strategy, establishing processes to limit digital technology risks, and ensuring maximum protection against cyber-attacks, also establish IT security guidelines for interactions with Third Parties (e.g. clients, suppliers, subcontractors, partners, licensors), verify and ensure the adoption of necessary cybersecurity measures, suspend IT system activities in emergencies, and inform the personnel about actions taken to data protection and cyber security.

The Transformation Enabling & System Quality function is responsible for maintaining this policy, coordinating its implementation, and supporting continuous improvement in alignment with ISO 27001.

Top Management ensures continuous commitment and support for the effective implementation of the Information Security Management System (ISMS) across the organization.

2 COMMITMENT

MAIRE Group is firmly committed to safeguarding its information assets, ensuring protection against unauthorized access, preserving its confidentiality and maintaining its integrity throughout business processes. This commitment is rooted in the adoption of a robust Information Security Management System (ISMS), aligned with ISO/IEC 27001:2022 standard, and supported by the Group's Code of Ethics.

The Group is also dedicated to the early detection and effective management of anomalous events, incidents, and vulnerabilities within its information systems aimed at minimizing any potential impact on business activities and ensuring resilience.

Compliance with all applicable legal and regulatory requirements is a fundamental principle of MAIRE approach to meet evolving obligations and industry standards.

To foster a culture of security, the Group conducts regular training programs that raise awareness and keep all personnel informed about current information security practices and emerging threats.

Finally, MAIRE pursues the continual improvement of its ISMS. This includes ongoing evaluation of risks, performance monitoring, and the implementation of enhancements to ensure the system remains effective, responsive, and aligned with the Group's strategic objectives.

3 OBJECTIVES AND STRATEGIES

The objectives of MAIRE's Information Security Management System (ISMS) are designed to support the Group's strategic vision, operational excellence, and digital innovation. This objective informs the development of a living framework capable of addressing complex risks, adapting to emerging technologies, and supporting the human factor at the heart of cybersecurity.

The ISMS adopts a risk-based and process-oriented approach to ensure that information security is embedded in all business activities. and to anticipate, prevent, and respond to evolving threats while maintaining compliance and stakeholder confidence.

This approach integrates robust governance with operational agility, ensuring that security controls facilitate innovation by fostering trust, automation, and assurance. By prioritizing the protection of digital infrastructure and sensitive information—across project delivery platforms, advanced engineering tools, cloud environments, and interconnected assets—our strategy elevates information security as a key enabler of business objectives rather than merely a defensive measure.

To achieve these goals, MAIRE pursues the following strategic objectives:

- **Protect information assets** by safeguarding MAIRE intellectual property, project data, and client information by implementing appropriate technical and organizational controls;
- **Ensure business continuity** through proactive risk assessment, incident response planning, and recovery procedures that minimize disruption to operations;
- **Lead through compliance** MAIRE complies with ISO 27001, GDPR, NIS2, and relevant industry regulations, ensuring business credibility;

- **Promote a cyber-conscious culture** by delivering targeted training, awareness campaigns, and leadership engagement to foster accountability and vigilance. Tailored education, hands-on training, and real-time communications keep personnel aware, alert, and capable of responding to cyber threats;
- **Foster a cybersecurity culture** through targeted training programs, comprehensive awareness initiatives, and active leadership engagement to encourage accountability and vigilance. Providing tailored education, practical training, and timely communications enables personnel to stay informed, vigilant, and well-prepared to respond effectively to cyber threats;
- **Promote security by Design** embedding security principles into every phase of project lifecycle , into digital platforms and all stages of the project lifecycle, ensuring that data protection, risk mitigation, and compliance are proactively addressed from the very beginning;
- **Strengthen third-party security** by requiring suppliers, contractors, and partners to adhere to the same high standards MAIRE set for itself.
- **Continuously improve the ISMS** through internal audits, performance monitoring, lessons learned, and stakeholder feedback, ensuring that the management system evolves with the business and threat landscape.

These strategies are supported by advanced technologies, including automation, data analytics, and artificial intelligence, to strengthen threat detection, response capabilities, and decision-making processes. Furthermore, the ISMS is aligned with MAIRE’s sustainability objectives, fostering responsible data governance, energy-efficient digital operations, and the ethical application of technology.

By embedding these objectives and strategies into daily operations, MAIRE ensures that information security is not only a compliance requirement but a key enabler of innovation, resilience, and long-term value creation.

4 TRANSPARENCY & REPORTING MECHANISMS

In the event that stakeholders become aware of any violation of the principles set out in this Policy, the Group encourages them to make a report.

These reports can be made - even anonymously - through the following channels:

- whistleblowing platform, available at the link: MAIRE Group - Whistleblowing;
- Form SA 8000 , available at the link: Human Rights and Social Accountability | MAIRE.
- ordinary mail: MAIRE S.p.A., Group Corporate Affairs, Governance, Ethics & Compliance Department, Via Gaetano De Castillia 6/A, 20124, Milan, (Italy).

Reports are managed in accordance with the provisions of the Group's "Whistleblowing" Procedure and the Social Accountability 8000 management system for certified MAIRE group companies.

Any form of direct or indirect retaliation, discrimination or penalization against those who have made a report, for reasons directly or indirectly related to the report, is prohibited.

In case of security incidents, Group Personnel can contact the Security Operation Center (SOC) or make the report through the dedicated section of the company portal.

5 REFERENCES

The Information Security Policy is aligned with international standards, regulatory frameworks, and internal policies to ensure compliance, consistency, and continuous improvement. Key references include:

- ISO 27001:2022 – Information Management System
- GDPR – General Data Protection Regulation (EU)
- CSF –Cybersecurity Security Framework (NIST)

- NIS2 Directive – EU Cybersecurity

This Policy embraces the principles expressed in the following Group strategic documents:

- Code of Ethics
- Diversity, Equity & Inclusion policy
- Human rights policy
- Human Resources policy
- Anti-harassment policy
- HSE&SA policy
- Supply Chain policy
- Quality policy
- Security policy

This Policy is implemented through the Manual of the Information Security Management System and related internal organizational procedures of the MAIRE group.