



Information Security Policy Statement

Purpose

Espria has implemented an Information Security Management System (ISMS), demonstrating our commitment to protecting the confidentiality, integrity, and availability of our information assets. This commitment aligns with the ISO 27001 standard. Our Information Security Policy serves as a framework to systematically assess business risks, safeguard information assets from potential threats, ensure compliance with legal and regulatory requirements, and foster a culture that prioritises information security throughout the organisation.

Scope

This Information Security Policy is applicable to all employees, contractors, partners, and third parties who access Espria's systems, networks, and information assets. The scope covers all business operations, processes, systems, and information, regardless of format—whether electronic, physical, or otherwise. It includes information stored on computers, transmitted across networks, printed or written on paper, stored on portable media, and shared verbally in conversations or over the telephone.

Leadership Commitment

The senior management team is dedicated to supporting and providing the necessary resources for the effective implementation and maintenance of the ISMS. Management will establish measurable information security objectives that align with the organisation's strategic goals and ensure the continual improvement of the system to address emerging threats and changes in the business environment. Promoting widespread information security awareness across all organisational levels is a key priority.

Information Security Framework

Our ISMS adopts a risk-based approach that involves the identification and assessment of information security risks, considering both external and internal interested parties. Appropriate controls are implemented to mitigate identified risks. The ISMS is regularly monitored, audited, and evaluated to ensure optimal performance. Incident management and the ongoing enhancement of security measures are central to our approach.

Roles and Responsibilities

All Espria personnel are responsible for understanding and complying with this policy, thereby supporting the ISMS. Specific responsibilities are as follows:

- Top Management: Provides oversight, approval, and strategic direction for the ISMS.
- Head of Compliance: Oversees implementation, monitoring, and continuous improvement of the ISMS.
- Managers: Ensure policy implementation within their areas, and guarantee staff adherence.
- Employees and Contractors: Must comply with security policies and procedures and promptly report any security incidents.
- Third Parties: Are required to adhere to contractual information security obligations.

Information Security Objectives

Our policy ensures we meet the following objectives:

- Compliance with UK Data Protection Laws and other applicable privacy laws.
- Identification and understanding of the needs and expectations of all interested parties relevant to our information security management system.
- Assignment of appropriate information security roles and responsibilities.
- Protection, management, and controlled sharing of customer, client, or Group data in accordance with UK Data Protection Laws and, where relevant, the data protection laws of the data owner's country.

- Regular auditing and reporting reviewed by the Executive Board.
- Reporting and investigation of any actual or suspected information security breaches up to Board level.
- Maintenance of information confidentiality.
- Preservation of information integrity.
- Fulfilment of regulatory, legislative, and contractual security requirements.
- Protection against unauthorised access to information.
- Establishment and monthly monitoring of objectives and targets in line with the Espria Continual Improvement Procedure to promote ongoing enhancement of our ISMS.
- Provision of necessary information security training.
- Implementation of procedures and instructions to support this policy.
- Pursuit of continual improvement in our products, services, and ISMS effectiveness.

Climate Change

Espria recognises the impact that climate change may have on our operations, management system, and strategic objectives. In alignment with ISO standards and our commitment to continual improvement, we regularly assess both internal and external factors—including climate change—to ensure our management system remains effective and resilient. We identify and evaluate the requirements of interested parties, including those related to climate change, and integrate these considerations into our planning, implementation, and maintenance activities. By proactively addressing climate-related risks and opportunities, Espria aims to enhance operational performance, fulfill our regulatory and contractual obligations, and support the long-term sustainability of our organisation.

Compliance and Review

Espria ensures compliance with this policy by conducting regular internal audits and reviews of the ISMS. Any nonconformities identified during these reviews are addressed and remediated. The policy is reviewed and updated at least annually, or whenever significant changes arise.

Information Security Awareness Training

All relevant personnel must participate in mandatory Information Security awareness training. This training ensures that employees, contractors, and interested third parties understand their responsibilities and the requirements of the ISMS. Through regular training sessions, individuals acquire the knowledge necessary to comply with policy requirements and actively contribute to the protection of Espria's organisational information assets. Attendance and participation in this training are essential for maintaining compliance with Espria's information security policies and procedures.

Policy Awareness

This policy will be communicated and available to all relevant stakeholders, including employees, contractors, and any interested third parties.

The policy is regularly reviewed to ensure its continued suitability.



Angelo Di Ventura
CEO

January 2026