

DOCUMENT TITLE

PR 5.2 - Information Security & Quality Management System Policy

CODICE DOCUMENTO
PR 5.2

DATE
09/10/2026

REVISION
5

DISTRIBUTION

- Restricted []
- Internal only []
- Stakeholder []
- Public [x]

REVISIONS

Revisions	Date	Description	Author
1	01/02/2023	Original document	eCore
2	19/07/2024	Document renamed	Mirko Bersani
3	27/09/2024	Vision updated	Mirko Bersani
4	27/07/2026	Chapter 2 updated (exclusion of Reimagine and roles aligned with the organizational chart)	Paolo Braggion
5	09/10/2026	Integration of the Quality Policy requirements in accordance with ISO 9001:2015	Paolo Braggion

Indice

1. Purpose of the document	3
2. Information Security Policy	3
3. Our principles	5

1. Purpose of the document

The purpose of this document is to describe the general information security principles defined by eCore in order to develop an efficient and secure Information Security Management System (ISMS).

This document constitutes the Information Security Policy pursuant to ISO/IEC 27001:2022 (clause 5.2) and, where relevant, refers to and supplements the Quality Policy established pursuant to ISO 9001:2015 (clause 5.2). It applies to all group companies and to all processes, locations, people and assets included within the scope of the management systems.

2. Information Security Policy

eCore is the holding company of ELFO S.r.l. (custom software development).

In line with the Purpose of ELFO S.r.l. and eCore Holding (hereinafter, “eCore”), the company is committed to:

- providing high-quality software products and services that consistently meet customer requirements, stakeholder expectations and applicable statutory and regulatory requirements;
- preserving the confidentiality, integrity and availability of all physical and electronic information within the organization, in order to ensure high availability, regulatory and contractual compliance, and the company’s business reputation. Information security is considered an integral part of the quality of the services delivered. Therefore, protecting the confidentiality, integrity and availability of customer data and business processes directly contributes to product and service conformity and stakeholder satisfaction;
- promoting a culture of continual improvement of the Integrated Quality and Information Security Management System;
- continuously planning and monitoring the Quality and Information Security Objectives, which are defined and reviewed annually by the Steering Committee.

Information security requirements and quality objectives will remain aligned with eCore’s objectives. This Integrated Management System (Quality and Security) is intended to enable information sharing, digital operations, data management and customer satisfaction, while reducing information-related and business-process risks to acceptable levels.

eCore’s current corporate strategic plan and risk and opportunity management model provide the context for identifying, assessing and controlling risks related to information and service delivery through the establishment, maintenance and continual improvement of an Integrated Management System.

This context is consistent with the analysis of the organization's context, interested parties, risks and opportunities carried out as part of the Integrated Management System, using a risk-based thinking approach.

Quality Policy principles referenced

Within the Integrated Management System, eCore applies the following principles, in line with the Quality Policy:

- customer focus: understanding and meeting the needs and expectations of customers and other interested parties, while protecting their information;
- process and risk-based approach: managing business processes, including those that handle information, by identifying and addressing risks and opportunities;
- compliance: complying with applicable statutory, regulatory and contractual requirements, including all relevant data-related laws in the jurisdictions in which eCore operates;
- people engagement and competence: ensuring awareness, training and accountability across all personnel;
- continual improvement: systematically improving the effectiveness of the management system, processes and security controls;
- management of suppliers and external parties: ensuring that externally provided processes, products and services are also controlled from an information security perspective.

Governance and responsibilities

eCore's Steering Committee has assigned ELFO responsibility for carrying out all activities relating to ISO 27001 and ISO 9001 for all companies in the group.

The Risk Assessment, Statement of Applicability, Risk Treatment Plan and process mapping identify how risks relating to information and service/product levels are controlled. Measurable objectives are defined, monitored and periodically reviewed in line with the quality objectives. The Chief Operating Officer (COO) is responsible for managing and maintaining the risk assessment. Where necessary, additional risk assessments may be carried out to determine appropriate controls for specific risks.

Specifically, business continuity, operational controls for the ICT infrastructure, system access control, reporting of information security incidents, customer satisfaction, control of outsourced processes and compliance with project specifications are fundamental to this policy.

Control objectives and performance indicators for each of these areas are set out in this document and supported by specific documented policies, procedures and operating instructions.

All eCore employees and collaborators, as well as certain external parties identified in the Integrated Management System, are required to comply with this policy and the system implementing it. All employees/collaborators and certain external parties will be provided with the necessary requirements and must complete appropriate training under the training and skills development plan. The consequences of violating the information security policy and quality procedures are defined in the Organization's disciplinary policy, contracts and agreements with third parties.

The Integrated Management System is subject to continuous and systematic review and improvement.

eCore's Steering Committee has established an Information Security & Quality Committee, chaired by the Chief Operating Officer (COO), the Chief Innovation Officer (CIO), the Chief Technology Officer (CTO), and the ICT / Quality Team, to support the framework and periodically review the integrated policy.

eCore is committed to maintaining its Integrated Management System in compliance with the international standards UNI EN ISO 9001:2015 and ISO/IEC 27001:2022.

This policy will be reviewed at least annually, or as part of the Management Review, to address any changes in the risk assessment, risk treatment plan, organizational context, or the needs of the market and interested parties.

This Integrated Policy is communicated, understood and applied throughout the organization and is made available to relevant interested parties.

In this policy, "information security" and "Quality" are defined as follows:

- *Preserving the availability, confidentiality and integrity of eCore's physical assets and information.*
- *Ensuring the conformity of processes, software products and digital services delivered, with the aim of achieving ongoing customer satisfaction and operational excellence.*

3. Our principles

Safeguarding

This means that management, all employees and full-time or part-time staff, freelancers, project consultants and all external parties have responsibilities—defined in their job descriptions or contracts—to safeguard information security and quality standards, report security breaches and process/product nonconformities (in accordance with the policy and procedures), and act in compliance with the requirements of the Integrated Management System. All employees will receive training in information security and quality management, while employees in more specialized roles will receive specialized training.

Availability

This means that information and associated assets must be accessible to authorized users whenever required and must therefore be physically secure. The IT network must be resilient, and eCore must be able to detect and respond rapidly to incidents (such as viruses and other cyber threats) that threaten the availability of assets, systems and information, thereby ensuring continuity in the delivery of products and services to customers.

Confidentiality

This means ensuring that information is accessible only to authorized persons, thereby preventing deliberate or accidental unauthorized access to eCore's proprietary information and knowledge, customers' data and property, and its systems, including the network, website, extranet and monitoring system.

and Integrity

This means safeguarding the accuracy and completeness of information and processing methods, and preventing deliberate or accidental, partial or complete destruction, or unauthorized modification, of both physical assets and electronic data. Appropriate contingency plans must be in place, including plans for networks, systems, websites and extranets, data backup plans, and the reporting of security incidents and software anomalies. eCore must comply with all relevant laws concerning data and the quality of products/services in the jurisdictions in which it operates.

Physical assets

eCore's physical assets are under its control and subject to the procedures/policies governing cloud systems, applications, process information, racks, servers, laptops and personal computers, smartphones, and physical and digital data storage systems.

and Information

Information assets include information stored electronically on servers, intranets, cloud services, PCs, laptops and mobile phones, as well as all information transmitted electronically by any means. In this context, "data" also includes the set of instructions that tells the system(s) how to process information (i.e. software such as operating systems, applications, utilities, etc.) belonging to the eCore organization.

We want to redefine the boundaries of what software applications can achieve in complex organizations.

Every day, we work to push the boundaries of our customers' innovation, starting from their growth objectives.



of the eCore organization.

We want to share technological excellence, expertise and passion to build memorable relationships.

"To develop software products that simplify business processes while ensuring the highest standards of quality and information security."