INFO DOCUMENT

DOCUMENT TITLE.

PR 5.2 - Information Security Management System Policy

DOCUMENT CODE
PR 5.2

DATA
27/09/2024

REVISION
3

SCOPE OF APPLICATION

DISTRIBUTION

Restricted	[ ]
Internal only	[ ]
Stakeholder	[ ]
Public	[●]

LIST OF REVIEWS

REVISIONS

Revisions	Date	Description	Author
1	01/02/2023	Original document - ITA version	eCore
2	19/07/2024	Renamed document	Mirko Bersani
3	27/09/2024	Updated Vision	Mirko Bersani

eCore Holding s.r.l
via Pastore 3
29017 Fiorenzuola d'Arda (Piacenza) Italy
Tel 0523.985811 www.ecoreholding.it

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).

2. Information Security Policy

eCore is the holding company for these companies:

- ELFO S.r.l. (custom software development)
- Reimagine S.r.l. (Sales of digital products and services)

In line with ELFO S.r.l.'s Purpose[i] and Reimagine's Vision[ii] , **eCore Holding** (hereafter **eCore**) is committed to preserving the confidentiality, integrity, and availability of all physical and electronic information within its organization to ensure its high availability, regulatory and contractual compliance, and business image.

Information security requirements will continue to be aligned with **eCore**'s goals, and this ISMS is intended as an enabling mechanism for information sharing, digital operations, data management, and the reduction of information risks to acceptable levels.

eCore's current strategic business plan and risk management model provide the framework for identifying, assessing, and controlling information-related risks through the creation and maintenance of an ISMS.

The Steering Committee of eCore assigned ELFO the responsibility to carry out all activities related to ISO 27001 for all group companies.

The Risk Assessment, Applicability Statement, and Risk Treatment Plan identify how information-related risks are controlled. The Chief Operating Officer (COO) will be responsible for managing and maintaining the risk assessment. When necessary, additional risk assessments may be conducted to determine appropriate controls for specific risks.

Specifically, business continuity, ICT infrastructure operational controls, systems access control, and information security incident reporting are central to this policy. The control objectives for each of these areas are contained in this document and are supported by specific documented policies and procedures.

All employees and contractors of **eCore** and certain external individuals identified in the ISMS are required to comply with this policy and the ISMS that implements it. All employees/collaborators, and certain external figures, will receive the necessary requirements and will be required to undergo appropriate training. The consequences of violating the information security policy are defined in the Organization's disciplinary policy, contracts and agreements with third parties.

The ISMS is subject to continuous and systematic review and improvement.

The **eCore** Steering Committee has established an **Information Security Committee**, chaired by the Chief Operating Officer (COO), Chief Innovation Officer (CIO), Chief Technology Officer (CTO), and ICT Team to support the ISMS framework and periodically review the security policy.

eCore is committed to obtaining certification of its ISMS to the international standard ISO/IEC 27001:2022.

This policy will be reviewed at least annually in response to any changes in risk assessment or risk treatment plan.

In this policy, "information security" is defined as:

Preserving the availability, confidentiality and integrity of the physical resources (assets) and information of the eCore organization.

Preserve

Means that management, all full- and part-time employees and staff, freelancers, project consultants, and all external parties have, and will be made aware of, their responsibilities (defined in their job descriptions or contracts) to preserve information security, to report security breaches (in line with policy and procedures), and to act in accordance with ISMS requirements. All employees will receive information security training and more specialized employees will receive specialized information security training.

availability,

It is understood that information and associated assets must be accessible to authorized users when needed and therefore physically secure. The IT network must be resilient and **eCore** must be able to detect and respond quickly to incidents (such as viruses and other cyber threats) that threaten the availability of assets, systems, and information.

confidentiality

It is intended to ensure that information is accessible only to those authorized to access it and thus prevent unauthorized access, whether deliberate or accidental, to eCore's proprietary information and knowledge and its systems, including the network, website, extranet, and monitoring system.

and integrity

That is, the safeguarding of the correctness and completeness of information and processing methods, i.e., the prevention of 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 those for networks, systems, websites, extranets, and data backup plans, as well as security incident reporting. **eCore** must comply with all relevant data laws in the jurisdictions in which it operates.

of physical resources (assets)

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

and information

Information resources include information stored electronically on servers, intranets, cloud services, PCs, laptops, cell phones, and all information transmitted electronically by any means. In this context, "data" also includes the set of instructions that tell the system(s) how to manipulate the information (i.e., software: operating systems, applications, utilities, etc.)

of the eCore organization.

[i] We want to re-engineer the boundaries of possibility of software applications in complex organizations.
We work daily to shift the horizon of our clients' innovation starting with their growth objectives.
We want to share technological excellence, expertise and passion to build memorable relationships.

[ii] Making software products, to simplify business processes.