DOCUMENT INFO

TITLE OF DOCUMENT

# PR 5.2 - Information Security Management System

DOCUMENT CODE

PR 5.2

DATE

01 Feb 2023

REVISION

0

DISTRIBUTION

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

LIST OF REVISIONS

## REVISIONS

| Revision | Date | Description | Author |
|---|---|---|---|
| 0 | 01/02/2023 | Original document | eCore |

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

# 1. Scope

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

# 2. Information Security Policy

**eCore** is the Holding of these companies:

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

In line with the Vision[i] of ELFO S.r.l. and the Vision[ii] of Reimagine, the **eCore organization** (hereinafter **eCore** for brevity) is committed also to preserving the confidentiality, integrity, and availability of all the physical and electronic information assets throughout their organisation to preserve high availability, regulatory and contractual compliance and commercial image.

Information and information security requirements will continue to be aligned with the **eCore** goals and the ISMS is intended to be an enabling mechanism for information sharing, for electronic operations, for data management and for reducing information-related risks to acceptable levels.

**eCore** current strategic business plan and risk management framework provides the context for identifying, assessing, evaluating, and controlling information-related risks through the establishment and maintenance of an ISMS.

The Risk Assessment, Statement of Applicability and Risk Treatment Plan identify how information-related risks are controlled. The Chief Operating Officer (COO) will be responsible for the management and maintenance of the risk Assessment. Additional risk assessments may, where necessary, be carried out to determine appropriate controls for specific risks.

In particular, businss continuity, operational controls of ICT infrastructure, access control to systems and information security incident reporting are fundamental to this policy. Control objectives for each of these areas are contained in this document and are supported by specific documented policies and procedures.

All Employees/Staff of **eCore** and certain external parties identified in the ISMS are expected to comply with this policy and with the ISMS that implements this policy. All Employees/Staff, and certain external parties, will receive the requirements and will be required to provide appropriate training. The consequences of breaching the information security policy are set out in the Organization's disciplinary policy and in contracts and agreements with third parties.

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

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

**eCore** is committed to achieving certification of its ISMS on the International Standard ISO/IEC 27001:2022.

This policy will be reviewed to respond to any changes in the risk assessment or risk treatment plan, and at least annually.

**In this policy, 'information security' is defined as:**

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

**Preserving**

This means that management, all full time or part time Employees/Staff, sub-contractors, project consultants and any external parties have, and will be made aware of, their responsibilities (which are defined in their job descriptions or contracts) to preserve information security, to report security breaches (in line with the policy and procedures) and to act in accordance with the requirements of the ISMS. All Employees/Staff will receive information security awareness training and more specialised Employees/Staff will receive appropriately specialised information security training.

**the availability,**

This means that information and associated assets should be accessible to authorised users when required and therefore physically secure. The computer network must be resilient and **eCore** must be able to detect and respond rapidly to incidents (such as viruses and other malware) that threaten the continued availability of assets, systems, and information.

**confidentiality**

This involves ensuring that information is only accessible to those authorised to access it and therefore to preventing both deliberate and accidental unauthorised access to **eCore** information and proprietary knowledge and its systems including its network(s), website(s), extranet(s), and monitoring system.

**and integrity**

This involves safeguarding the accuracy and completeness of information and processing methods, and therefore requires preventing deliberate or accidental, partial or complete, destruction or unauthorised modification, of either physical assets or electronic data. There must be appropriate contingency including for network(s), system(s), website(s), extranet(s) and data backup plans and security incident reporting. **eCore** must comply with all relevant data-related legislation in those jurisdictions within which it operates.

**of the physical (assets)**

The physical assets of **eCore** organization are under control and procedure/policy that apply to Cloud System, application, process information, racks, server, laptops and personal computers, data cabling, smartphones, filing systems and physical data files.

**and information assets**

The information assets include information stored electronically on servers, intranet(s), Cloud Services, PCs, laptops, mobile phones and information transmitted electronically by any means.  In this context, 'data' also includes the sets of instructions that tell the system(s) how to manipulate information (i.e. the software: operating systems, applications, utilities, etc).

**of eCore organization.**

[i] To each company its own custom software. ELFO brings technological excellence, expertise and passion: the customer chooses everything else. People building tomorrow's success together.

[ii] Making software products to simplify business processes