Revision	Date	Release Notes
A	**07/10/2022**	Initial review
B	**10/05/2023**	Signed by the General Director
C	**22/01/2024**	Signed by the new General Director
C	**26/09/2024**	Annual review in accordance with the Information Security Policy, no changes
C	**09/12/2025**	Annual review in accordance with the Information Security Policy, no changes

Document approved by all relevant functions.

Quick Reference Guide

Do I need to read this Policy?

This policy defines Ecenarro's high-level principles for managing information security risks in the company.

This policy must be complied with by all employees, third parties, suppliers, contractors, subcontractors and customers of Ecenarro, if applicable.

Compliance with this policy is a mandatory requirement, and will ensure that all information is treated securely, and properly managed according to its classification, and against any legal and contractual requirements.

What is information security and why is it important to Ecenarro?

Information security is the practice of protecting information, systems, and assets by mitigating risks to information security.

It consists of preventing or reducing the likelihood of unauthorized or inappropriate access, unlawful use, disclosure, alteration, deletion, corruption, modification, inspection, recording or devaluation of information, systems and assets.

Information security focuses on protecting the confidentiality, integrity, and availability of information, systems, and assets.

Failure to adequately protect Ecenarro from the risks to the security of the information it manages could adversely affect the organization by:

- Economic losses due to theft, fraud and blackmail.
- Loss of production or inability to operate/supply due to unavailability of data and computer systems.
- Inability to meet contractual requirements for customer information security.
- Breach of contract or other legal breach due to deficiencies, deficiencies or loss of data, including intellectual property.
- Reputational damage.
- Possible security incidents.

Where can I find more information about Ecenarro's information security regulations?

If you need additional information on Ecenarro's information security management, you can consult the intranet, where you will find all Ecenarro information security regulations.

What do I do if I need more help?

If you need further assistance, please contact the Information Security Officer in motaegi@ecenarro.com or xlesmes@ecenarro.com

1.0 Purpose

Ecenarro relies on the confidentiality, integrity and availability of your information to achieve its business objectives.

Any deterioration in the confidentiality, integrity or availability of information, IT systems or (information) assets could disrupt Ecenarro's corporate operations, or expose Ecenarro to commercial, contractual or legal risks.

Therefore, Ecenarro must apply regulations and processes to identify, evaluate and manage the information security risks to which it is exposed, and mitigate these risks to an acceptable level.

The purpose of this policy is to establish the following high-level objectives for information security within Ecenarro, which are adapted to the objectives of the organization:

- Protection of the organization, legally and in accordance with current legislation and regulations.
- Assessment and management of information security threats, vulnerabilities and risks.
- Maintenance of the company's commitment to trust, with its customers and partners.

2.0 Scope

This policy shall apply to:

- All employees, third parties, suppliers, contractors, subcontractors and customers of Ecenarro, if applicable.
- All Ecenarro assets, including information, databases, IT systems, networks, applications and material, as well as all business functions, across all plants.

3.0 Politics

1.1 Information Security Objectives

This Information Security Policy defines the requirements to protect Ecenarro's information, systems and assets by establishing an Information Security Management System (ISMS).

The ISMS is based on the requirements of the Trusted Information Security Assessment Exchange (TISAX), and the international information security standard ISO 27001 to define, control, monitor, maintain and continuously improve information security.

The ISMS guarantees:

- Confidentiality: ensuring that information is disclosed only to authorized parties;
- Integrity: ensuring that only authorized parties and systems can make changes to information, systems or assets;
- Availability: ensuring that authorized parties have access to information, systems and assets; and
- That the legal, regulatory and contractual requirements related to information security are met.

1.2 Information Security Strategy

Ecenarro shall ensure adequate protection of all information, systems, assets, physical locations and persons.

The strategy regarding information security is business-based, oriented to avoid risk, and is managed in accordance with the good practices established in the market, directly aligning with Ecenarro's business objectives.

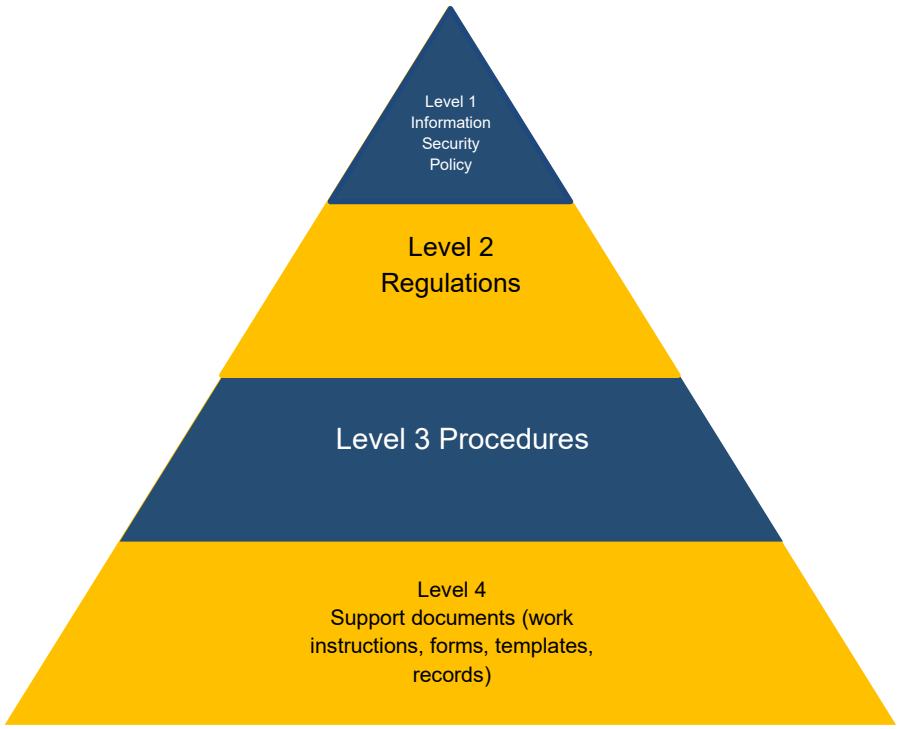
Ecenarro's overall information security strategy has been developed by the Chief Information Security Officer (CISO) and approved by the Board of Directors, to demonstrate the company's commitment to protecting its information, systems and assets.

1.3 Information security regulations

To support this General Information Security Policy, a lower-level set of information security policies, procedures and supporting documents should be maintained to ensure that security objectives continue to be met.

The CISO will manage all supporting documentation, and communicate it to Ecenarro employees and (where appropriate) to external parties, customers, suppliers and others who process Ecenarro information.

Ecenarro's ISMS is based on an information structure that documents security management and controls.



This structure is hierarchical, with high-level regulations and processes near the top of the hierarchy, and detailed subordinate procedures and records below.

1.3.1 ISMS Regulations

The regulations that support the Information Security Policy are:

- Access control, and password and user management.
- Backup and recovery.
- Management of business continuity.
- Configuration management.
- Cryptography.
- Management of information security incidents.
- Classification, labeling and manipulation of information.
- Management of information security assets.
- Information security change management.
- Compliance, assurance and audit of information security.
- Information security risk management.
- Information security training and awareness.
- Network security.
- Physical security.
- Management of portable and mobile devices.
- Records management.
- Technical security audits.
- Management of relationships with third parties and suppliers.
- Vulnerability and patch management.

1.4 Organization and responsibilities for information security

Ecenarro has defined and applied security responsibilities to control the implementation and operation of information security within the company.

1.4.1 Managing Director

The CEO is Ecenarro's highest-ranking executive, whose primary responsibilities include making corporate decisions, managing Ecenarro's overall operations and resources, and being the public face of the company.

1.4.2 Global Information Security Officer (CISO)

The Global Chief Information Security Officer (CISO) sets the information security strategy for the company, and determines the direction for implementing and controlling information security.

The CISO provides information security guidance to the CEO and executive team, recommending appropriate information security investments and practices.

The CISO is responsible for managing information security-related risks, affecting information assets, business continuity planning, crisis management, privacy, and compliance.

1.4.3 Local Information Security Officer (LCISO)

LCISO applies the company's information security strategy locally.

LCISO is in contact with the CISO to approve appropriate information security practices for the designated plant.

LCISO is responsible for managing risks related to information security, physical security, business continuity planning, crisis management, privacy, and regulatory compliance at the designated facility.

1.4.4 Internal Auditor

The internal auditor is responsible for reviewing the proper functioning of the ISMS through his expert knowledge, and for communicating the results of his audit reports to management.

1.4.5 External consultant

In those areas of the ISMS in which it is considered appropriate, Ecenarro can count on external consultants to advise you on the most appropriate way to implement or improve aspects of the management system.

1.4.6 Directors

The directors of Ecenarro are responsible for their respective teams to apply the requirements of this policy.

1.4.7 Employees

All employees play a critical role in the effort to protect and maintain Ecenarro's information assets against loss of confidentiality, integrity, and availability; and report any loss or suspected breach of information or information assets.

To ensure this, all employees must be aware of their responsibility, and they need to be trained and made aware.

1.5 Compliance

The design, operation, use and management of information systems must meet all legal, regulatory and contractual security requirements.

This policy and supplemental material will be reviewed annually by the Ecenarro CISO, when significant risks are identified, or when there are changes in legal or regulatory obligations.

Supporting documents shall conform to any future changes to this policy and, where appropriate, be resubmitted for acceptance by interested parties.

The CISO shall report regularly to Ecenarro's Board of Directors on the state of information security and its effectiveness through appropriate management reports.

Any breach of this policy will be evaluated by Ecenarro's Board of Directors.

1.6 Continuous improvement

Ecenarro's Board of Directors will continuously improve and review the suitability, adequacy and effectiveness of the ISMS.

2.0 Definitions

ISMS	Information Security Management System
CISO	Chief Information Security Officer
LCISO	Local Chief Information Security Officer
Confidentiality	Controlled Disclosure of Information
Integrity	Controlled modification of information
Availability	Access to information

Approved by::

Josu Zaldua, General Director