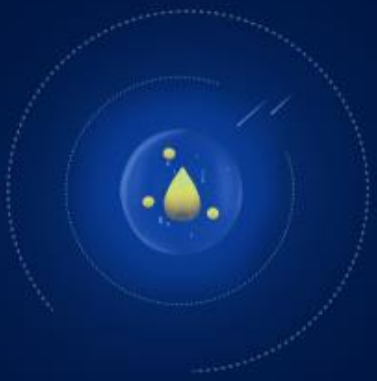
EPICENTER. BETTER INTEGRATION.



Epicenter Information Security Policy

Public

EPICENTER

Table of Contents

1 PURPOSE

The purpose of this policy is to describe the strategic importance of the ISMS for the organization and direct all information security activities in the organization.

Any changes to this document must be approved by the Board of Epicenter.

2 SCOPE

This policy applies to all members of the organization.

3 TERMS AND DEFINITIONS

Information Security
The preservation of confidentiality, integrity, and availability of information.

Confidentiality
The property that information is not made available or disclosed to unauthorized individuals, entities, or processes.

Integrity
The property of accuracy and completeness.

Availability
The property of being accessible and usable upon demand by an authorized entity.

ISMS	information security management system
CISO	Chief Information Security Officer

4 RELATED DOCUMENTS

- ISO/IEC 27001:2022 – clause 5.1
- Statement of Applicability (available internally or on request)
- Internal Policies and Procedures

5 ROLES & RESPONSIBILITIES

5.1 Epicenter Board

The Board of Epicenter is committed to ensure the protection of all information assets in the scope of the ISMS from unauthorized disclosure, alteration and loss of availability. For that reason, the provisioning of sufficient resources to support these efforts is guaranteed.

The Board of Epicenter is aware of the ever-evolving threat landscape and recognizes the need to constantly adapt to arising challenges to keep information assets secure. This circumstance

requires the continual improvement of all activities within the scope of the ISMS and as a result, this document will be updated on a regular basis.

5.2 Chief Information Security Officer (CISO/CTO)

The Chief Information Security Officer is responsible for the maintenance of the IS Policy Document in accordance with the Standard Procedure Document Management plan.
The CISO is also responsible for the following areas: Governance, Asset Management, Information Protection, System and network security, Secure Configuration, Identity and Access Management, Information Security Event Management and Information Security Assurance.
The CISO is responsible for reporting breaches to the regulatory authorities.

5.3 Human Resources Manager

The Human Resources Manager is responsible for the integrity of employee documentation (contracts, attestations, signed agreements).

5.4 Office Manager (Spain)

The Office Manager together with the CISO is responsible for performing the risk analysis related to physical security on an annual basis. The Office Manager is also responsible for monitoring the Clean Desk Policy.

5.5 Chief Commercial Officer

The CCO is responsible for supplier relationship security and facilitating legal and compliance topics that affect the services offered to customers and the functioning of Epicenter.

5.6 Head of Product Management

Responsible for ensuring a secure development lifecycle, that the application developed has built-in security elements that meet the requirements relating to data access within the FIT4Cloud application as well as security testing, change management and secure coding.

5.7 Security Operations Team

Responsible for assurance activities, pen testing, information security policies and specialist information security advice. Incident response for cyber security issues. User awareness.

5.8 All Epicenter Employees

1. understanding the baseline information security controls necessary to protect the confidentiality, integrity and availability of information entrusted;
2. protecting information and resources from unauthorized use or disclosure;
3. protecting personal, private, sensitive information from unauthorized use or disclosure;
4. abiding by the Acceptable Usage Policy
5. reporting suspected information security incidents or weaknesses to the Security Operations Team.
6. Complete the annual, mandatory GPDR training.
7. Receive at least annual security awareness training.

6 POLICY

6.1 Commitment

The Board of Epicenter is committed to supporting and continuously improving our Information Security Management System (ISMS). This commitment includes:

1. Establishing a Clear Information Security Policy.
2. Defining Security Objectives.
3. Resource Provisioning.

Allocating sufficient resources (financial, technological, and human) to implement, maintain, and improve the ISMS.

4. Support and Training:

Ensuring all personnel have the necessary skills, knowledge, and training to fulfill their information security responsibilities.

5. Promoting a Security Culture:

Fostering a culture of security awareness throughout the organization, encouraging all employees to take ownership of information security.

6. Continuous Improvement:

- Monitoring and Review: Continuously monitoring the performance of the ISMS through audits, assessments, and feedback.
- Learning from Incidents: Using lessons learned from security incidents and near-misses to strengthen the ISMS.

7. Risk Management:

- Risk Assessment: Conducting regular risk assessments to identify and evaluate information security risks.
- Risk Treatment: Implementing appropriate measures to mitigate identified risks in line with the organization's risk appetite.

Furthermore, every member of the organization is mandated to contribute to the continual improvement process as far as his or her actions are concerned as deemed necessary by the Chief Security Officer.

6.2 Information security principles

The following information security principles provide overarching governance for the security and management of information at Epicenter.

6.2.1 Information classification

Information should be classified according to an appropriate level of confidentiality, integrity and availability (see Section 8.1. Information Classification and Labelling) and in accordance with relevant legislative, regulatory and contractual requirements.

6.2.2 Information Handling

Users with responsibilities for information (see Section 5. Roles and Responsibilities) must: a. handle that information in accordance with its classification level; b. abide by Epicenter policies, procedures, and any contractual requirements.

6.2.3 Information Security

Information should be both secure and available to those with a legitimate need for access in accordance with its classification level. a. Access to information will be on the basis of least privilege and need to know.

6.2.4 Information Protection

Information will be protected against unauthorized access and processing.

6.2.5 Breach Reporting

Breaches of this policy must be reported (see Section 7.4 Incident Handling).

6.2.6 Continuous improvement

Information security provision and the policies that guide it will be regularly reviewed, including through the use of annual external audits and penetration testing.

6.3 Information security objectives

Information security management system related to the design, development, implementation and operation of custom software as an extension of transformation and delivery of customer data via third party systems integration, according to the Statement of Applicability version 1.0

The information security policy is the guideline for the management and coordination of the various security processes within Epicenter. The goal is to set up a balanced system of security measures aimed at risk management.

For Epicenter there are two main objectives in this respect.

1. Epicenter strives to never provide unauthorized access to Epicenter information. No access should be possible without an account. With an account, only the information authorised for that account should be available. No information which is unauthorised for that account should be available
2. Epicenter strives never to communicate unfairly. In the context of information security, measures are taken to limit the risks associated with the risk sources listed below, or to limit subsequent damage.

Risks can arise from, among other things:

- The functionality desired by the organization or customers;
- The users of information systems;
- The vulnerability of ICT infrastructure;
- Internal causes (for example careless behaviour or unauthorized use);
- External causes (for example fire, leakage or bankruptcy of a supplier).

In the context of information security, measures are taken to limit the risks associated with these sources of risk, or to limit subsequent damage.

These objectives have resulted in the formulation of Key Performance Indicators that are reviewed at least during each quarterly management review and more frequently if changes occur in the context of the organization.

6.4 Communication

6.4.1 Internal

The information security policy shall be communicated to all persons within the scope of the ISMS by publishing on the Epicenter ISO 27001 Sharepoint site by 15th March 2025.

6.4.2 External

This policy may be shared and communicated with interested parties and stakeholders. As such it will be published and made publicly available via the Epicenter website.

7 COMPLIANCE

7.1 Measurement

The organization will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

7.2 Exceptions

Any exception to this policy must be approved by the Chief Information Security Officer in advance.

7.3 Violations

Members of the organization found to have violated this policy may be subject to disciplinary action, up to and including termination of employment, fines and legal action. Details of the disciplinary procedure are shared with Epicenter employees in the Epicenter Information Security Detailed Document.

7.4 Incident Handling

If an employee is aware of an information security incident then they must report this immediately to the Security Operations Team (secops@epicenter.eu).

8 Information Protection

8.1 Information Classification and Labelling

Internally, all information and assets listed are classified with an Availability, Integrity and Confidentiality rating - also known as an AIC rating - according to one of the following levels of Availability, Integrity and Confidentiality as described in the tables below

The following table provides a summary of the information classification levels related to Confidentiality:

Confidentiality level	Measure	Characteristics of information
High (Highly Confidential/All Employees)	Only available on a need-to-know basis	Information accessible to a limited group of people. Violation of this classification can cause serious harm to Epicenter or to Epicenter's customers. This includes Personal Health Information, Customer information, access portals and personnel files.
Medium (Confidential/All Employees)	Information accessible to Epicenter employees	Information accessible by Epicenter employees. Confidentiality is medium. If this information is released, the damage for Epicenter is limited. Security measures are limited to the integrity of the information. This includes company-wide quarterly updates, company policies and Epicenter organization data.
Low (public)	No measures	Information accessible to everyone. This includes Published data such as the website and PR material.

8.2 Personnel Security

Labelling of information

It is known to all Epicenter employees that customer data is information of a high confidentiality level. It is not possible to apply labelling to this information but it must be treated as Highly Confidential. Information that is highly confidential must be encrypted when it is required to be transferred. Data is only granted to employees who need it to perform their duties. The authorization policy of Epicenter is periodically evaluated and updated to ensure that only necessary access is granted. Epicenter regularly checks access rights.

8.3 Protection of Personal Data and Applicable Laws

Since 25 May 2018, the GDPR (General Data Protection Regulation) is in force. Epicenter processes so-called 'ordinary' personal data and may also process special categories of data according to the Data Processing Agreement with each client.

Epicenter also follows the legal provisions and the guidelines of the Data Protection Authority.