SOCIETAT CONCESSIONÀRIA
SON ESPASES
HOSPITAL UNIVERSITARI

Information Security Policy

Modification:	Date	Review
Initial Drafting	21/11/2025	A

CONTENTS

All rights reserved

1. INTRODUCTION

The Management of the **Sociedad Concesionaria Hospital Universitario Son Espases** ("**CHUSE"),** within the framework of its powers to establish the policies and strategies of the organization, has approved this Information Security Policy (hereinafter, the "**Policy**").

The objective of this Policy, aimed at all stakeholders, is to define and establish the principles, criteria and objectives for improvement that govern actions in the field of information security in line with the guidelines set by the ISO 27.001 standard.

2. PURPOSE

CHUSE assumes the security of the information associated with its services as one of the key factors in the performance of its activities in order to guarantee confidentiality, integrity and availability, protecting personal data, information privacy and information systems against improper access and unauthorized modifications.

Part of CHUSE's strategic policy is the implementation and development of an Information Security Management System based on the identification, protection, detection, response and recovery of information systems, with the company's Management providing the necessary resources to achieve it.

CHUSE, aware of the need to integrate all the tools and means necessary to provide its services efficiently, with quality and in a secure information management environment, will focus on all those measures and actions that manage to reduce, minimise, transfer or avoid Risks and allow it to take advantage of the Opportunities for its Management System.

To this end, CHUSE's Management undertakes to continuously improve the Information Security Management System implemented, in the periodic reviews it maintains annually and through the establishment of objectives and improvement actions.

3. GENERAL PRINCIPLES

The Management of CHUSE, through this Policy and the development and implementation of the Information Security Management System, assumes and promotes the following general principles that must guide all its activities:

a) To direct our efforts to the prevention of errors, as well as their correction, control and management.
b) Encourage everyone's participation to achieve the goals set by CHUSE, which will be in the best interest of our employees, customers, and other stakeholders.
c) Take continuous training and awareness as one of the main pillars on which information security is based, providing the necessary training in this area to interested parties, through the establishment of training plans.
d) Ensure that the company complies with all the requirements of customers, the different administrations and public bodies, as well as all applicable legal and regulatory requirements, placing special emphasis on those established by the legislation on information security.

e) Establish the procedures that are necessary for the control, monitoring and prevention of incidents.

f) Equip themselves with tools and procedures that allow them to adapt quickly to changing environmental conditions.

g) Guarantee the confidentiality, integrity, availability, as well as the due protection of data and information systems against improper access, cyberattacks and unauthorized modifications.

h) Guarantee business continuity, in terms of information security, protecting critical processes against significant failures or disasters, developing continuity plans in accordance with internationally recognized methodologies.

i) Carry out an adequate assessment, management and treatment of information security risk to achieve a high level of maturity and minimise risk, prioritising the measures and controls to be implemented in accordance with the identified risks and business objectives.

j) Act appropriately and jointly to prevent, detect and respond to cyber incidents that could affect information security.

k) Establishment of the consequences of security policy violations, which will be reflected in the contracts signed with interested parties, suppliers and subcontractors.

l) Improve the efficiency of the security controls implemented to adapt to evolving risks and new technological environments.

m) Review and evaluate the security of the information periodically, taking the necessary measures to correct any deviations that may be detected.

Accordingly, CHUSE maintains the following application guidelines to be taken into account within the framework of the Information Security Management System (ISMS):

a) The protection of personal data and the privacy of individuals.

b) The safeguarding of the organization's records.

c) The protection of intellectual property rights.

d) The documentation of the information security policy.

e) The assignment of security responsibilities.

f) Education and training for information security.

g) The registration of security incidents.

h) The management of any changes that may occur related to security.

In guarantee of the principles of information security:

- **Confidentiality**: The information processed by CHUSE will be known exclusively by authorised persons, subject to identification, at the time and by the means provided.
- **Integrity**: The information processed by CHUSE will be complete, accurate and valid, and its content will be provided by the affected parties without any type of manipulation.
- **Availability**: The information processed by CHUSE will be accessible and usable by authorized and identified users at all times, guaranteeing its own persistence in the event of any foreseen eventuality.

- **Resilience**: In guarantee of the above, CHUSE has the necessary technical and organizational measures that allow constant adaptation to change and continuous improvement of the duly implemented Information Security Management System.
- **Legality**: Consequently, CHUSE undertakes to ensure compliance with all applicable legislation. And specifically, the regulations in force on data protection, privacy and information security.

4. SCOPE AND SCOPE OF APPLICATION

The principles of action of this Policy are directly applicable to all CHUSE's management activities, as well as to CHUSE's employees.

The policy will be reviewed periodically to ensure its effectiveness and updating in the face of new regulations, technologies or environmental challenges.

Policy approved by the members of the Ethics Committee, dated November 27, 2025.

Palma de Mallorca, 27 November 2025

Carlos Ricci Voltas

Managing Director

Prepared

Name: Aina Guerrero Fullana

Position: Quality and Environment Manager

Reviewed

Name: Izaskun Davalillo

Position: Director of HR and Organization

Approved

Name: Carlos Ricci

Position: General Manager