

# INFORMATION SECURITY POLICY

This policy is mandatory for all CNAG employees and external users of CNAG's Cluster.

In order to comply with the basic principles, CNAG management undertakes to support the management of information security by means of the establishment of guidelines by management, which guarantee:

- Commitment to and promotion of continuous improvement of the Information Security Management System.
- Provide the material, economic and human resources necessary to carry out the tasks related to Information Security.
- Accept as strategic assets of the company, the information and systems that support it, expressing its determination to achieve the necessary security levels that certify its protection in a profitable way, guaranteeing security and controlled access to the information, and thus improving the quality of the services offered by the company to its customers.
- Implement relevant controls to ensure information processing in operations and appropriate security measures in the networks over which the information is transmitted.
- To raise awareness among users so that CNAG's Information Security policy has the maximum impact within the organisation, developing short, medium, and long-term goals and incorporating specific motivation and training techniques.
- Adopt the Information Security Policy as the main tool for guaranteeing information security and business objectives, promoting, and ensuring compliance with it for all CNAG employees and collaborators. Likewise, regulations, standards and administrative or operational procedures will be defined with a more limited scope within the Information Security Management System.
- Establish contractual relationships with suppliers and partners with appropriate security requirements. Security incidents will be managed promptly, effectively, and appropriately to minimize their impact.
- Establish defined roles and responsibilities for the proper management of the Information Security Management System.
- Identify and act on current and potential risks and threats to CNAG's information security.
- Compliance with legal, regulatory or contractual requirements related to Information Security and applicable to CNAG.

This Policy will be reviewed annually and complemented with established quality and security objectives for each year. It is available to all stakeholders through its publication on the website, and internally by dissemination to the different areas of the organization.

Ivo Glynne Gut  
*Director of CNAG*

DOC-018	TLP: PUBLIC	Revision: 01	Date: 17/03/2025	Page: 1 de 1
---------	-------------	--------------	------------------	--------------