	Information Security Policy	Z-POL 5.1
Policy	Version 4.0	1/3

Index

[Index](#)

[Change Control](#)

[Scope](#)

[Validity](#)

[Security Policy](#)

Change Control

Version	Written by	Revised by	Approved by	Date of publication
1.0	Security area	Safety Committee	Management	15/02/2012
1.1	Security area	Safety Committee	Management	06/06/2017
2.0	Security area	Safety Committee	Management	15/02/2019
3.0	Security area	Safety Committee	Management	26/02/2021
4.0	Security area	Safety Committee	Management	02/01/2022

Scope


This Security Policy applies to all personnel accessing Zitro's information or communications networks, whether used by employees, collaborators, or third parties.

This policy applies to:

- Zitro group personnel.
- Contractors and subcontractors who provide a service to the Organization, in the matters provided in the respective contract and agreements.
- Personnel who, without having an employment relationship with the Organization, have access to information at any time during its life cycle.

Validity

This policy came into effect on 02/15/2021 and will remain in force during subsequent revisions, until the company is notified of its termination.


	Information Security Policy	Z-POL 5.1
Policy	Version 4.0	2/3

Security Policy

The Zitro group management considers that the achievement of the objectives is subject to compliance with various requirements aimed at guaranteeing Information Security within the Company.

In this way, Information Security is established as a priority for the Zitro group and for this purpose, this Policy establishes the following guidelines:

- Information owned by the Zitro group must be accessible only to duly authorized persons, whether or not they belong to the Organization.
- This Security Policy, as well as the rest of the documents related to information security standards, must be accessible to all members of the company, as well as to personnel outside the company who are related to one or more companies of the group, through one of its processes.
- The Zitro group, and therefore its employees, must comply with all applicable legal, regulatory, and statutory requirements, as well as contractual requirements.
- Confidentiality of information must be always guaranteed and considered a principle within the company.
- The integrity of the information must be ensured through all processes that are managed, processed and stored.
- The availability of information and internal processes must be ensured through adequate backup and business continuity measures.
- All personnel must have adequate training and awareness of Information Security.
- Any incident or weakness that may compromise or has compromised the confidentiality, integrity and/or availability of the information must be communicated through the available means established by the Company and analyzed in order to apply the corresponding corrective and/or preventive measures.
- Assuming security risks must be approved by an appropriate management level, the higher the risk, and always bearing in mind that the person assuming the risk must have competencies or power of decision over the affected area.

	Information Security Policy	Z-POL 5.1
Policy	Version 4.0	3/3

- The Company's management establishes and maintains a Security Committee, responsible for implementing, maintaining and improving this Policy as well as establishing, monitoring, measuring and improving security controls and needs in relation to the Company.

- Every member of the Zitro group must ensure compliance with this policy and the rules derived from it.

<div style="text-align: center;">  Joel Mendizabal IT & Risk Manager </div>	<div style="text-align: center;">  Escriba el texto aquí Sant Quirze del Valles 02/01/2023 Management of Zitro Laboratory </div>
--	---