Information Security Policy

This Security Policy applies to all personnel who access information or communications networks of Zitro, used by workers, collaborators, or third parties.

In particular, this policy applies to:

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

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

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

- The information that the Zitro group owns must only be accessible to duly authorized people, 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 non-member personnel who are related to one or more companies in the group, through any of its processes.
- The Zitro group, its workers and related personnel to whom this policy applies, must comply with all legal, regulatory, and statutory requirements that apply to it, as well as contractual requirements.
- The confidentiality of information must be guaranteed at all times 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 guaranteed through appropriate support and business continuity measures.
- All staff must have adequate training and awareness in 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 to apply the corresponding corrective and/or preventive measures.
- Taking on security risks must be approved by an appropriate management level, the higher risk involved always taken into account that whoever assumes the risk must have powers or decision-making power over the affected area
- The Company's management establishes and maintains a Security Committee, responsible for implementing, maintaining and improving this Policy as well as establishing, controlling, 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.

IT Corporate & Risk Manager

Zitro India Management

Girish Kamath

Date of update: June 2025