Information security policy

Objective

The purpose of this policy is to establish the basic principles of action that must guide the people, entities, institutions or units, both internal and external, that have access to our information assets (ICT), or to the environment and/or operational assets (OT), to ensure the effective protection of information resources and the sustainability of the services provided, through the implementation of appropriate preventive, detection, reaction and recovery measures against potential security incidents, safeguarding the integrity, confidentiality and availability of the organization's assets and digital processes.

This Policy has been prepared considering the main regulatory references regarding information security and the best national and international practices.

Principles

This Policy is based on essential protection principles designed to ensure that Zelestra can achieve its goals through the secure use of its information/operational systems.

These fundamental pillars, which must be taken into account at all times when making decisions regarding information security/cybersecurity, are described below:

- Define a comprehensive security strategy with both a preventive and proactive approach to ensure a reasonable level of risk.
- Ensure that information security, including data confidentiality, availability and integrity, is in line with business strategy, as well as with current contractual and legal requirements.
- Promote the integration of security into the organizational culture and management framework of the entity.
- Guarantee the right to the protection of personal data of all persons who are related to the companies belonging to the Group, in accordance with the provisions of the Privacy and Personal data protection policy (or regulation that replaces it in the future).
- Prioritize risk analysis and management as a central part of operations.
- Maintain risk levels within minimum acceptable limits through the continuous application of appropriate and updated security measures.
- Safeguard the information resources and technology used by Zelestra against both internal and external threats, whether intentional or accidental.
- Adopt the necessary measures to prevent, neutralize, minimize or restore the damage caused by security threats to the normal development of activities, based on criteria of proportionality regarding potential risks and the criticality and value of the affected assets and services.
- Establish protection composed of multiple layers of security in order to minimize the resulting impact, in the event of failure or incident.
- Effectively and efficiently use of available security knowledge and infrastructure.
- Establish monitoring and reporting procedures to guarantee compliance with the established objectives.
- Any third party that has access to our information systems must comply with the provisions of this policy, as well as with the procedures that emanate from it.
- Guarantee and promote appropriate training programs, both in person and online or by any other method that is appropriate for the duties established by the applicable regulations, with sufficient frequency to ensure the updating of knowledge. Likewise, require suppliers and contractors to receive security training, prior to the beginning of the effective contractual relationship.
- Optimize security investments to efficiently support business objectives.
- Continuously review and update the security procedures and measures implemented to ensure that they remain effective in response to the constant evolution of risks and protection systems.
- The corresponding authority shall impose appropriate disciplinary measures in accordance with our internal procedures, applicable collective agreements and the regulations in force at any given time.

Zelestra's responsibility is to ensure that the security of Information and Communication Technologies (ICT), as well as of operational assets (OT), is integrated into all stages of the lifecycle of information systems, from conception to decommissioning, including development or acquisition decisions, as well as operational activities.

The present Policy was updated by the Board of Directors on November 21st, 2024, and it came into effect upon approval.

Monitoring system

The information security committee or, in its absence, the Digitalization and Cybersecurity area of Zelestra (or the figures that assume its functions at any time), will supervise the definition, continuous review and implementation of this Policy, as well as of the plans that are developed and specified in the territories and for the specific businesses of the Group.

Communication and stakeholder engagement

This Policy is communicated and understood within the scope of the organization, and it is available through the information and communication channels that the company makes available to all its stakeholders.

The Policy is publicly available on the Zelestra website.

In order to make it easier for any person to confidentially and anonymously report any breach of the principles described in this Policy, Zelestra's Ethics Line (https://zelestra.integrityline.com/) guarantees independence, impartiality and the absence of conflicts of interest throughout the process of receiving, processing and resolving such reports.

Scope

This Policy applies to all companies of the Zelestra Group, to ZELESTRA CORPORACIÓN, S.A.U. and those companies of which Zelestra has, directly or indirectly, the majority of the shares, participations or voting rights, or whose governing or administrative body has been appointed or Zelestra has the power to appoint the majority of its members, controlling the society effectively.

In those investee companies in which Zelestra Group companies do not have effective control, Zelestra will promote principles and guidelines consistent with those established in this Policy.

Definitions

Availability: Characteristic, quality or condition of being available to those who must access it, whether they are people, processes or applications.

Confidentiality: The property of preventing the disclosure of information to unauthorized persons or systems. Only authorized persons access the information.

Information Security Committee: Body responsible for the governance of information security.

Integrity: Property that seeks to keep data free from unauthorized modifications. It guarantees the accuracy of the information as it was generated, without being manipulated or altered by unauthorized persons or processes.