FUNDAMENTAL PRINCIPLES OF THE INFORMATION SECURITY POLICY

CONTENTS

1. PURPOSE
2. OUR COMMITMENT
3. SCOPE
4. INFORMATION SECURITY PRINCIPLES
5. HOW WE FULFIL OUR COMMITMENT
6. MONITORING AND CONTINUOUS IMPROVEMENT
7. COMMITMENT TO OUR STAKEHOLDERS
8. REFERENCE DOCUMENTATION

1.Purpose

At GES, information is an essential asset for carrying out our activities and for maintaining the trust of our customers, partners and other stakeholders.

For this reason, Management establishes and promotes an Information Security Policy aimed at adequately protecting information and the systems that process it, managing security risks and ensuring compliance with applicable requirements.

2.Our commitment

GES is committed to managing information security in accordance with the applicable principles and requirements of ISO/IEC 27001, adopting a risk-based approach and promoting the continuous improvement of its Information Security Management System.

The purpose of this commitment is to adequately preserve information, contribute to business continuity, reduce security risks and respond to the needs and expectations of stakeholders.

3.Scope

This Policy applies to the people, processes, systems and resources included within the scope of the GES Information Security Management System.

Furthermore, its security principles and requirements shall apply, where appropriate, to suppliers, partners and third parties that access, manage or process GES information in the course of the services provided.

4.Information security principles

Information security management at GES is based on the following principles:

- CONFIDENTIALITY Ensuring that information is accessible only to duly authorised persons, entities or systems.
- INTEGRITY Protecting the accuracy, consistency and reliability of information, preventing unauthorised modifications.
- AVAILABILITY Ensuring that the necessary information and systems are available to authorised persons when required.
- COMPLIANCE Meeting legal, regulatory, contractual and other applicable commitments regarding information security and data protection.
- RISK-BASED MANAGEMENT Identifying, analysing, assessing and treating risks that may affect information security, adopting measures proportionate to their nature and criticality.

- ❖ CONTINUOUS IMPROVEMENT Continuously reviewing and improving the effectiveness of the Information Security Management System.

5.How we fulfil our commitment

To put these principles into practice, GES undertakes to:

- Establish the policies, standards, procedures and measures necessary for the proper management of information security.
- Identify, assess and treat information security risks through a systematic risk management process.
- Set information security objectives aligned with the objectives and needs of the organisation.
- Promote information security training and awareness.
- Identify and comply with legal, regulatory, contractual and other applicable requirements.
- Assign the responsibilities and resources necessary for the proper functioning of the Information Security Management System.
- Manage information security incidents and take the necessary measures to reduce their impact and prevent their recurrence.
- Periodically evaluate the effectiveness of the measures implemented and take any necessary improvement actions.

GES will communicate this Policy to all its staff and keep it available for consultation.

6.Monitoring and continuous improvement

GES monitors compliance with this Policy and the effectiveness of its Information Security Management System through the monitoring, evaluation and audit mechanisms established by the organisation.

The Policy will be reviewed periodically and whenever relevant changes occur that may affect the Information Security Management System, in order to ensure it remains suitable for the organisation's needs, its risks and the applicable requirements.

7.Commitment to our stakeholders

GES makes this Information Security Policy available to its stakeholders as a demonstration of its commitment to information protection, security risk management, compliance with applicable requirements and continuous improvement.

8.Reference documentation

POL-CL-01-01 CL Grupo Industrial Information Security Policy.