GIS POLICIES MANUAL

Information Security Policy

Effective from	Replaces	Control Number	Page
January 19th, 2023	(C) GIS-SEG- 001 (May 15th, 2016)	(C) GIS-SEG- 001	1 of 4

I. OBJECTIVE

Establish the Information Security Policy and business continuity within Grupo Industrial Saltillo, S. A. B. de C. V. (GIS).

II. SCOPE

This Policy is of general application to all companies that make up GIS.

III. POLICY DESCRIPTION

1. Information Security Framework

For the proper administration of information security, GIS bases this policy on the ISO/IEC 27001, TISAX, NIST CSF standards, as a reference framework.

2. Information Security Principles

GIS protects the confidentiality, integrity and availability of its own information, of its clients and of authorized third parties that it manages, as well as the continuity of its operational and business processes; managing risks at an acceptable level and implementing controls based on good security practices, complying with the applicable legal, regulatory and contractual framework; GIS develops, implements, maintains and continuously improves the Information Security Management System.

IV. INFORMATION SECURITY GOVERNANCE MODEL

The Security Governance model is based on the Information Security Management System, whose objectives, in relation to information security, are:

1. **Identify** risks systematically.
2. **Protect** from threats, through the development of applicable security technologies.
3. **Detect** threats by using multiple intelligence sources to be able to proactively manage them.
4. **Respond** to Cybersecurity incidents through corporate protocols:
   a. limiting their impact on the company
   b. ensuring the continuity of operations that depend on IT services
5. **Recover and restore** any capacity or service that has been affected due to a Cybersecurity event.

V. USE OF INFORMATION

Each collaborator must be able to access only the information they need for their work and no unauthorized person must be able to access it.

The information and the assets used to store it exist to achieve the business objective and should be used only for this purpose.

VI. INFORMATION PROTECTION

The collaborator must apply and understand the guidelines defined by GIS for the protection of information.

VII. INFORMATION RESTRICTION

Collaborators, clients and authorized third parties must have access only to the information that is strictly necessary to carry out the activities related to the assigned work.

VIII. DISCLOSURE OF INFORMATION

The access to confidential or restricted information granted to GIS Collaborators does not confer the authority to allow access to third parties inside and outside GIS, nor for its disclosure to any person.

IX. SANCTIONS

Violation of the principles of this Policy, guidelines or subsequent procedures will result in the application of disciplinary measures in accordance with the current GIS Code of Ethics.

X. GLOSSARY OF TERMS

Concept	Definition
Information Asset	Any resource that has a value to GIS, where the following categories can be considered: ● Information Systems: Assets formed by the combination of hardware, software (example: operating system, databases, applications, others) and information ● Human Resources: Asset related to the knowledge and experience of the personnel ● Services: Assets related to carrying out activities and providing benefits to the organization, such as: support, maintenance, operation and administration. Includes internal services and services provided by external suppliers ● Facilities: Assets related to the physical infrastructure where the

	information systems and personnel are housed. ● Information: Data that has meaning. Includes databases, data files, contracts and agreements, systems documentation, research information, user manuals, training material, operational or support procedures, continuity plans, audit evidence, archived, among others.
Logical Access	It is the act of accessing information stored in an Information System.
Threat	Potential cause of an unplanned incident, which may result in damage to an Information Asset.
Availability	Assurance that the information will be accessible and usable under the requirement of an authorized entity.
Information	Data that has meaning. It includes databases, data files, contracts and agreements, systems documentation, research information, user manuals, training material, operational or support procedures, continuity plans, audit evidence, archived information, among others.
Security Incident	An Information Security incident is an event that materializes a threat by exploiting a vulnerability and that causes an affectation in one or more information properties of an information asset, which can be: ● *Integrity ● *Availability ● *Confidentiality
Integrity	Guarantee of the accuracy and completeness of the Information and the methods of its processing.
Risk	Consequence of a Threat in relation to the Information Asset.
Security of the information	Preservation of Confidentiality, Integrity and Availability of information.
ISMS	Information Security Management System.
Information Technology (IT)	Technology required for the acquisition, storage, manipulation, administration, control, exchange, transmission, reception, processing, analysis or display of data or information. Includes computer equipment, communications, auxiliary equipment, commercial software or developed in-house, services and related resources acquired or leased, or under the responsibility of the Company.
Third Party	Employee or representative of an organization other than GIS.

Collaborator	Person or entity that uses or requires access to an Information System to perform one or more tasks. The user can be an employee or a third party (supplier, consultant, external user).

XI. RELATED POLICIES AND PROCEDURES

1. GIS-SEG-002 Classification, Administration, Backup and Recovery of Information
2. GIS-SEG-003 Access Control to Information Technology Systems
3. GIS-SEG-004 Remote Access Control to GIS Infrastructure
4. GIS-SEG-005 Assignment of Password Use
5. GIS-SEG-006 Use of Email Service
6. GIS-SEG-007 Use of Internet Browsing
7. GIS-PROC-SEG-001 Classification, Labeling and Information Management

This Policy was approved by the Information Security Committee at its session held on January 19, 2023.