Yes, policies and procedures are our responsability

POL.SI.002.V04.ENG

Corporate Cybersecurity Policy - Public

Version 04

11/24

#PoliciesThatGuideUs

SUMMARY

1. OBJECTIVE..3

2. APPLICATION SCOPE..3

3. REFERENCE DOCUMENT...3

4. TERMINOLOGY..3

5. DEVELOPMENT..4

6. RESPONSIBILITIES..5

7. REVISION HISTORY...5

1. OBJECTIVE

The purpose of this Policy is to protect the organization's information assets, ensuring their dimensions of availability, integrity, confidentiality, authenticity, and traceability, as well as the infrastructures, systems, and human resources that process, manage, transmit, and store them, always following business requirements and applicable legal and contractual obligations.

2. APPLICATION SCOPE

This Information Security Policy applies to all individuals, systems, and means that access, process, store, transmit, or use information known, managed, or owned by Atento for any of its life cycle activities, creation, capture, reception, transmission, visualization, classification, retention, and elimination.

Personnel subject to this policy include all individuals with access to the described information, regardless of the automated or non-automated support in which it is located, and whether the individual is an Atento employee or not. Therefore, it also applies to contractors, clients, suppliers, or any third party with access to the company's information or systems.

The guidelines outlined in this Policy will be developed in procedures, technical instructions, and guides, in accordance with the Cybersecurity Regulatory Framework.

3. REFERENCE DOCUMENT

- *ISO/IEC 27001:2022*
- *ISO/IEC 27000:2018*
- *ISO/IEC 27701:2019*

4. TERMINOLOGY

Term	Definition
Asset	Any information or element that has value for the organization.
Risk analysis	Systematic use of information to identify sources and estimate risk.
Adaptability	Defines events and the criteria under which a system must be monitored and reviewed for subsequent control.
Authenticity	Seeks to ensure the validity of information in terms of time, form, and distribution. It also ensures the origin of the information, validating the sender to prevent identity impersonation.
Reliability of information	Ensures that the source of the generated information is suitable to support decision-making and the execution of missions and functions.
Confidentiality	Property that determines that information is not available or disclosed to unauthorized individuals, entities, or processes.
Statement of applicability	Document that describes control objectives and the relevant and applicable controls for it.
Availability	Characteristic where information is accessible and usable upon request by an entity.
Risk assessment	Evaluating the importance of the risk by comparing the estimated risk with given risk criteria.
Information security event	Identified presence of a condition in a system, service, or network indicating a possible violation of the information security policy, failure

Term	Definition
	of safeguards, or a previously unknown situation that may be relevant to security.
Risk management	Coordinated activities to direct and control an organization concerning risk.
Information security incident	An unwanted or unexpected event or series of events related to information security, with a significant probability of compromising business operations and threatening information security.
Integrity	Safeguarding the accuracy and complete state of assets.
Protection against duplication	Ensures that a transaction is performed only once unless specified otherwise, preventing recording a transaction for later playback to simulate multiple requests from the same original sender.
Information resources	All essential hardware and software components to ensure efficient functioning and optimization of computer workstations and peripherals, whether at an individual, collective, or organizational levels, while also prioritizing their proper functionality.
Risk	The effect of uncertainty on objectives.
Inherent risk	Level of uncertainty inherent in each activity without the execution of any control.
Residual risk	Remaining level of risk after risk treatment.
Information security	Preservation of the confidentiality, integrity, and availability of information. It may also involve other properties such as authenticity, traceability, non-repudiation, and reliability.
Information Security Management System (ISMS)	Part of the overall management system is based on an approach to the global risks of a business, whose purpose is to establish, implement, operate, monitor, review, maintain, and improve information security.
Information system	Refers to an independent set of information resources organized for the collection, processing, maintenance, transmission, and dissemination of information according to certain procedures, both automated and manual.
Risk treatment	Process of selecting and implementing improvement actions to manage risk.
Risk assessment	Process of analyzing and evaluating risk.

5. DEVELOPMENT

This Corporate Cybersecurity Policy affects the entire organization and expresses the commitment of the Management to approve and support the necessary security regulations and procedures for information security management.

Based on this Policy, current legal regulations, and customer requirements, Grupo Atento assumes the following Cybersecurity Strategic Objectives:

- Consider the information and supporting systems as strategic assets, demonstrating a determination to achieve the necessary security levels to guarantee protection in terms of authentication, confidentiality, integrity, availability, and traceability.

- Establish a Cybersecurity Security Committee to manage all guidelines that allow for preserving, safeguarding, and strengthening the security of information assets, thus improving the quality of services offered to customers.
- Promote the implementation of appropriate security levels to protect both information system resources and the information processed, stored, or transmitted by them, ensuring compliance with current legislation, confidentiality, integrity, and availability of information, as well as managing security incidents that could affect it.
- Promote training and awareness actions on Cybersecurity for all personnel and ensure the dissemination of this Policy, as well as documents to develop it.
- Create a Cybersecurity management system based on international standards and codes of good practice to identify, quantify, prioritize, monitor, and treat risks, as well as to assess and review the development of the Cybersecurity Policy as a framework for defining basic security guidelines.
- Establish essential mechanisms to ensure the continuity of Atento's critical activities in the face of serious contingencies that affect information systems, allowing recovery within an acceptable time frame.
- Ensure compliance with current legislation and regulations regarding Cybersecurity.

All Atento personnel and external individuals such as clients, suppliers, and stakeholders, are obligated to be aware of, respect, and enforce, within their area of responsibility, the security measures established for information protection.

Access to information and information systems will be conditioned on adherence to this Policy and the regulations that develop it, both of which are mandatory. Open violation may result in the initiation of appropriate disciplinary measures and, if necessary, legal responsibilities.

6. RESPONSIBILITIES

The executive committee must ensure that responsibilities and authorities for roles relevant to information security are assigned and communicated.

The executive committee must assign responsibility and authority for:

- Ensuring that the Information Security Management System is developed under the most relevant international standards.
- Reporting on the performance of the Information Security Management System.

7. REVISION HISTORY

Version	Date	Reviewer	Modifications
01	04/22	Internal Controls	Initial Version
02	11/22	Mauricio Baroni / Yovanni Pineda	Addition of points 1,2,3, 4, and 6
03	02/24	Regional CISOs and SI team	Text Update
04	11/24	Regional CISOs and SI team	Text Update