

ATENTO

Yes, policies and
procedures are our
responsability



POL.ITD.002.V1.ENG

Corporate Cybersecurity Policy - Public

Version 01

04/22



Summary

1.	OBJECTIVE	3
2.	FIELD OF APPLICATION	3
3.	REFERENCE DOCUMENT.....	3
4.	TERMINOLOGY	3
5.	DEVELOPMENT.....	3
6.	RESPONSIBILITIES	4
7.	REVISION HISTORY	4

1. OBJECTIVE

N/A

2. FIELD OF APPLICATION

N/A

3. REFERENCE DOCUMENT

N/A

4. TERMINOLOGY

N/A

5. DEVELOPMENT

This Corporate Cybersecurity Policy affects the entire organization and expresses the Management's commitment to approve and support the security regulations and procedures necessary for information security management based on this Policy, the current legal regulations and customer requirements.

With this purpose, the Management commits to the following Cybersecurity Strategic Objectives:

1. To consider the information and the systems that support it as strategic assets, thus expressing its determination to achieve the necessary security levels that guarantee its protection in terms of authentication, confidentiality, integrity, availability, and traceability.
2. To establish a Cybersecurity Security Committee that will manage all the guidelines that will enable us to preserve, safeguard and enhance the security of information assets and thus improve the quality of the services offered to our clients.
3. To promote the implementation of the appropriate security levels to protect both the resources of the information systems and the information processed, stored, or transmitted by them, as well as to ensure compliance with the current legislation on the subject and availability of the information; as well as managing security incidents that may affect it.
4. To promote training and awareness actions on Cybersecurity aimed at all personnel and ensure the dissemination of this Policy and the documents that develop it.
5. To create a Cybersecurity management system based on international standards and codes of good practice, identify, quantify, prioritize, and address the risks, as well as evaluate and review the development of the Cybersecurity Policy as a framework for defining the basic security guidelines.
6. To ensure the existence of the necessary mechanisms to provide continuity of Atento's critical activities when faced with severe contingencies affecting the information systems, allowing their recovery within an acceptable period.
7. To ensure compliance with the current legislation and regulations on Cybersecurity.

All Atento personnel and external personnel (Customers and Employees) must know, respect, and enforce compliance within their area of responsibility, with the security measures established for the protection of information.

The access to information and information systems will be conditional on adherence to this Policy and to the regulations that develop it, and these are of mandatory compliance. Its explicit non-compliance may lead to the the appropriate disciplinary measures and, where appropriate, legal liabilities.

Corporate Cybersecurity Policy	POL.ITD. 002	Version: 01	04/22	Page.: 4 de 4
--------------------------------	-----------------	-------------	-------	---------------

6. RESPONSIBILITIES

N/A

7. REVISION HISTORY

Version	Date	Reviewer	Modifications
01	04/22	Internal Controls	Initial Version