PUBLIC DOCUMENT

Cybersecurity, Information, and Privacy Policy

Italtel Brasil

Date of issue	22/04/2025
Class of Confidentiality	Public Document
References	ANATEL Resolution No. 740, of December 21, 2020

Indice

1 OBJECTIVE

This document establishes the principles, concepts, values, and references to be adopted to ensure the confidentiality, integrity, and availability of information and data belonging to or controlled by ITALTEL Brasil, and the information systems used by it. This allows ITALTEL Brasil to prevent, detect, reduce, and address vulnerabilities to incidents related to information security and the cyber environment. It also aims to protect the fundamental rights of freedom and privacy, and the free development of the natural person's personality.

2 TARGET AUDIENCE

This document is directed at any and all individuals who have access to information and data belonging to or controlled by ITALTEL Brasil, and the systems used by it, including but not limited to partners, administrators, collaborators, employees (whether or not), minor apprentices, interns, correspondents, service providers, and third parties.

3 SECURITY PRINCIPLES

ITALTEL Brasil's actions are governed by the following principles:

i. **Confidentiality:** Limiting access to information, allowing access only to authorized individuals and in circumstances where access is genuinely necessary, protecting information that should only be accessible by a specific group of users against unauthorized access.
ii. **Availability:** Guaranteeing access for duly authorized individuals to information whenever access is necessary, preventing interruptions to ITALTEL Brasil's operations through physical and technical control of data system functions, as well as the protection of files, their correct storage, and the performance of backups.
iii. **Integrity:** Guaranteeing the truthfulness, accuracy, and completeness of information and the methods of its processing and any eventual handling of the information, ensuring that it is not altered while being transferred or stored, preventing the information from being exposed to handling by an unauthorized person and preventing unapproved changes without the control of the information owner (corporate or private).

4 ROLES AND RESPONSIBILITIES

The assigned responsibilities are distributed as follows

4.1 **Cybersecurity and Information Security Policy, Action Plan, and Incident Response**: The Cybersecurity, Information, and Privacy Policy, as directed by ISO ABNT 27001:2022, is the responsibility of Senior Management, represented by the CISO. Regarding the Action Plan and Incident Response, and the continuous improvement of technical procedures related to the topic, the internal SOC of ITALTEL Brasil is responsible for supporting the CISO.

4.2 **Registration, Cause and Impact Analysis, and Control of Relevant Incident Effects**: the registration, cause and impact analysis, and control of the effects of relevant incidents are the responsibility of the Cybersecurity Committee.

4.3 **Execution of Periodic Tests and Scans for Vulnerability Detection**: the execution of periodic tests and scans for vulnerability detection are the responsibilities of the Red Team area and the internal SOC of ITALTEL Brasil.

4.4 **Maintenance of Data and Information Backups**: the execution of backups, regardless of the computing platform, as well as the disposal of magnetic media originating from the backup process, when applicable, are the responsibilities of the Information Technology Area.

4.5 **Documentation of Capacity Verification of Potential Service Providers, Corporate Governance Practices, and Evaluation of the Relevance of the Service to be Contracted**: the activity of documenting information regarding the capacity verification of potential service providers, corporate governance practices, and regarding the evaluation of the relevance of the service to be contracted, are the responsibilities of the Compliance Area with the assistance of the Information Technology Area and the Information Security Area.

4.6 **Preparation of the Annual Report on the Implementation of the Action Plan and Incident Response**: the preparation of the annual report on the implementation of the action plan and incident response is the responsibility of the CISO.

4.7 **Communication of Security Incidents Impacting Privacy to the National Data Protection Authority**: In accordance with Article 48 of Law No. 13,709/18 (General Data Protection Law - LGPD), the Data Protection Officer (DPO) will be responsible, after being informed by the Information Technology Area, for communicating to the National Data Protection Authority (ANPD) and the data subjects the occurrence of a security incident that may pose a significant risk or damage to the data subjects.

4.8 **Communication of Contracting Relevant Data Processing, Storage, and Cloud Computing Services**: The Information Security Area will be responsible, after being informed by the Information Technology Area, for the contracting of relevant data processing, storage, and cloud computing services.

4.9 **Person in Charge of Personal Data Processing**: In accordance with Articles 5, item VIII; 23, item II; and 41, caput and paragraphs, all of Law No. 13,709/18 (General Data Protection Law - LGPD), in the capacity of "Person in Charge of Personal Data Processing," this person indicated by the controller will act as a communication channel between the controller, the data subjects, and the National Data Protection Authority (ANPD). The identity and contact information of the person in charge must be disclosed publicly, clearly, and objectively, preferably on the controller's website.

5 CYBERSECURITY GUIDELINES

5.1 **Guidelines for Information Handling**: Information must receive adequate protection in observance of the principles and guidelines of ITALTEL Brasil's Cybersecurity, Information, and Privacy throughout its lifecycle, which includes: Generation, Handling, Storage, Transportation, and Disposal.

5.2 **Guidelines for Data and Information Classification**: Information and data under the responsibility of ITALTEL Brasil will be classified as described in the action plan, to adapt the organizational and operational structures to the principles and guidelines of the cybersecurity policy.

5.3 **Guidelines for Developing Incident Scenarios Considered in Business Continuity Tests**: Incident scenarios that imply damage or risk of damage to the reliability, integrity, availability, security, and confidentiality of data and information systems used by ITALTEL Brasil, which have or may have the capacity to cause disruptions in the company's business processes, must be developed within the scope of business continuity tests.

5.4 **Guidelines for Defining Procedures and Controls Aimed at Preventing and Handling Incidents to be Adopted by Service Providers**: When developing procedures and controls aimed at preventing and handling incidents to be adopted by service providers or partners, considering the characteristics of the service to be provided and levels of complexity, scope, and precision, incident scenarios that imply damage or risk of damage to the reliability, integrity, availability, security, and confidentiality of data and information systems used must be analyzed.

5.5 **Guidelines for Defining Parameters to be Used in Assessing the Relevance of Incidents**: The parameters to be used in assessing the relevance of incidents must consider the frequency and impact of incident scenarios that imply damage or risk of damage to the reliability, integrity, availability, security, and confidentiality of data and information systems used, which have or may have the capacity to cause interruption in ITALTEL Brasil's business processes.

5.6 Guidelines for Defining Parameters to be Used in the Retention and Disposal of Personal Data: Information must receive adequate protection in observance of the principles and guidelines of ITALTEL Brasil's Cybersecurity, Information, and Privacy throughout its lifecycle, including proper Disposal for digital and/or physical information.

6 PROCEDURES AND CONTROLS

To reduce ITALTEL Brasil's vulnerability to incidents and meet the other objectives of cybersecurity, information security, and privacy, the organization, including in the adoption of new technologies, will adopt the following specific policies by topic:

* Incident Response Policy;
* Vulnerability Management Policy;
* Backup Policy;
* Supplier Management Policy;
* Privacy Policy;
* Data and Information Classification Policy;
* Access Management Policy;
* Cryptography Policy;
* Acceptable Use Policy;
* Business Continuity Policy;
* Secure Software Development Policy;
* Data Retention and Disposal Policy;

The document related to the Cybersecurity, Information, and Privacy Policy must always be available, as well as other documentation: action plans, specific policies by topic, annual reports, monitoring and control records of the implementation effectiveness of the policies.

7 DISCIPLINARY MEASURES

Violations of this policy are subject to the disciplinary sanctions provided for in ITALTEL Brasil's internal regulations and in the legislation in force in Brazil and in the countries where the company is located.

8 REVIEW

This policy will be documented and reviewed every two years, or in a shorter period following a significant change in processes, people, or technologies that impact the Information Security Management System. The policies derived from this one must follow the same mentioned periodicity.