	<b>POLICY</b>	
	<b>Título:</b> Information Security - Extract	<b>Código:</b> POL.TEC.POR.001
	<b>Área:</b> Information Security	<b>Versão:</b> V4.0

## 1 OBJECTIVE

The Information Security Policy ("ISP") establishes guidelines and responsibilities that govern the acceptable use of information and/or technological assets, based on the principles of confidentiality, integrity, and availability of information.

## 2 TARGET AUDIENCE

This document applies to all individuals (employees, members of Boards and Committees, directors, interns, and apprentices) who are part of V.tal, as well as individuals within its economic group and all third parties who act for or represent V.tal—or any company within its economic group.


## 3 GUIDELINES

### 3.1 Acceptable Use of Information Technology Resources

The company's technological resources, such as corporate notebooks, desktops, mobile phones, tablets, corporate email, internet, internal networks, etc., must be used exclusively for professional purposes, in accordance with ethical and legal principles. The company establishes rules for the appropriate use of its technological resources, covering:

- Individual Responsibilities and Ethical Use of Resources
- Access and Identity Control
- Infrastructure and Device Security
- Data Protection
- Safe Practices in the Work Environment
- Reporting of Incidents and Suspicious Behavior

V.tal conducts continuous monitoring of its technological resources, including email and messaging services, to protect the organization, ensure compliance with the rules of this policy, and collect evidence of possible violations. The company reserves the right to, without prior notice, monitor, intercept, record, examine, redirect, retransmit, copy, or disclose data sent or received by its employees, as necessary for institutional purposes or criminal investigations. Therefore, employees should be aware that there is no expectation of privacy in the use of these resources.

	<b>POLICY</b>	
	<b>Título:</b> Information Security - Extract	<b>Código:</b> POL.TEC.POR.001
	<b>Área:</b> Information Security	<b>Versão:</b> V4.0

## 3.2 Information Security Governance

### 3.2.1 Policies and Procedures

The ISP and its regulations must be regularly reviewed, approved, and disseminated, aligned with strategic objectives, regulations, and best practices.

### 3.2.2 Information Security Executive Commission

The Information Security Executive Commission coordinates actions to protect digital assets and achieve strategic objectives, aligning business and technology with organizational and regulatory priorities. It should include representatives from all vice presidencies for integrated and multidisciplinary decisions.

## 3.3 Cyber Risk Management

The company must adopt a structured and proactive approach to manage information security risks, such as cyber threats, misuse, fraud, and vulnerabilities, aiming to minimize financial, operational, reputational, and legal impacts.

## 3.4 Third Party Risk Management

The company must identify, assess, and mitigate supplier risks, ensuring compliance with corporate policies, laws, and applicable regulations.

## 3.5 Business Continuity Management

The company must adopt measures to ensure the continuity of critical operations during disruptions, protecting processes, technological resources, and information assets, aligned with regulatory standards, best practices, and strategic objectives.

## 3.6 Identity and Access Management


The company must implement a structured program to ensure that only authorized individuals access to systems, data, and resources, protecting assets, reducing risks, and ensuring regulatory compliance.

## 3.7 Data Protection

The company must adopt controls to protect business, employee, and customer data, maintaining confidentiality obligations even after termination, in accordance with current policy.

## 3.8 Protection Against Malicious Software

The company must implement controls to prevent, detect, and respond to threats related to malicious software.

 O futuro passa por aqui.	<b>POLICY</b>	
	<b>Título:</b> Information Security - Extract	<b>Código:</b> POL.TEC.POR.001
	<b>Área:</b> Information Security	<b>Versão:</b> V4.0

### 3.9 Application Security

The company must apply secure development practices throughout the software lifecycle, with controls from the planning stage, such as code review, testing, best practices, and automated scanning, ensuring information protection.

### 3.10 Vulnerability and Compliance Management

The company must identify and mitigate vulnerabilities in technological assets, with automated scans, testing, timely fixes, and secure configurations, reducing attack surfaces.

### 3.11 Security of Networks, Workstations, and Smartphones or Tablets

The company must implement controls to protect networks, workstations, and mobile devices against unauthorized access, vulnerabilities, and threats.

### 3.12 Physical Security

The company must establish physical access controls to work, processing, and information storage environments, requiring the visible use of badges by employees, third parties, and visitors, and implementing facility protection controls such as power supply, climate control, and cabling infrastructure.


### 3.13 Information Security Incident Management

The company must implement and maintain structured processes to identify, record, analyze, and respond to cyber incidents that may cause financial losses, reputational damage, or direct and indirect impacts on the company and its customers.

Any observed or suspected incidents must be reported immediately to the Information Security team via the SOC (Security Operation Center) at the email (vtal-soc@vtal.com) or by phone +55 11 5128-8375. Additionally, any individual who becomes aware of or suspects any event that violates the rules of this policy or complementary information security regulations may report anonymously through the Confidential Channel.

### 3.14 Security Awareness

The company must maintain a continuous security awareness program to educate and train employees on protecting people, technological assets, and information, following best practices, regulatory standards, and the company's ISP, promoting an integrated security culture at all levels.

	<b>POLICY</b>	
	<b>Título:</b> Information Security - Extract	<b>Código:</b> POL.TEC.POR.001
	<b>Área:</b> Information Security	<b>Versão:</b> V4.0

### 3.15 Disciplinary Measures and Exceptions

Formal acceptance and compliance with the ISP are mandatory for all employees. Non-compliance may result in disciplinary measures such as guidance, warnings, or dismissal, in accordance with legislation and internal regulations. Exceptions to the rules, required for specific demands, must be submitted to the Information Security management for analysis and formal approval.

### 3.16 Policy Review

This policy may be reviewed, updated, and amended at planned intervals or at any time, at the company's sole discretion, whenever any relevant fact or event warrants its revision.

## 4 ROLES AND RESPONSIBILITIES

### Board of Directors and Senior Management

- Approve the policy and support the cybersecurity strategy aligned with organizational objectives;
- Appoint a director responsible for the policy and ensure the necessary resources for its execution;
- Monitor security indicators and promote a culture of information protection.

### Information Security

- Develop and maintain policies and standards, conduct risk assessments, and implement security controls;
- Monitor threats, coordinate incident responses, and conduct post-event analyses;
- Promote awareness, support internal areas, provide reports to senior management and the board of directors, and make the ISP execution report available to Anatel, as defined in the resolution or upon request.


### Information Security Executive Commission

- Evaluate and monitor the information security strategy and prioritize initiatives based on risks;
- Monitor the execution of critical projects and the effectiveness of implemented controls;
- Promote awareness and leadership engagement in security topics;
- Be informed of high-impact incidents and monitor response and mitigation plans;
- Report the status of initiatives and performance indicators to the Board of Directors, when applicable.

### Business Area Managers

- Ensure employee compliance with security policies and guidelines, identify and mitigate specific risks in their areas in partnership with the Information Security area;
- Disseminate the security culture by actively participating in training and campaigns.

### General Employees

	<b>POLICY</b>	
	<b>Título:</b> Information Security - Extract	<b>Código:</b> POL.TEC.POR.001
	<b>Área:</b> Information Security	<b>Versão:</b> V4.0

- Be familiar with and follow Information Security policies, standards, and guidelines;
- Protect credentials, passwords, and other authentication methods, which must not be shared under any circumstances;
- Immediately report incidents or violations to the security team;
- Use IT resources in an authorized manner and in compliance with this policy's guidelines;
- File a police report in case of loss, theft, robbery, or misplacement of a mobile device configured with company applications, and subsequently report the incident to the Technology team, providing a copy of the report.

## 5 REFERENCES


- ISO/IEC 27001:2022 - Information Security Management Systems - Requirements
- ISO/IEC 27002:2022 - Information Security Controls
- General Data Protection Law – Lei Geral de Proteção de Dados (LGPD) - Law No. 13.709/2018
- V.tal Code of Ethics and Conduct
- Data Classification Policy
- Business Continuity Policy
- Security Controls Policy
- Identity and Access Management Policy
- Vulnerability Management Policy
- Information Security Risk Management Policy
- Information Data Loss Prevention Policy
- Data Retention Policy
- Security Incident Response and Prevention Plan
- Third-Party Privacy and Personal Data Protection Manual
- Third-Party Code of Ethics and Conduct
- NIST Cybersecurity Framework: Version 2.0
- Anatel Resolution No. 740/2020

## 6 GLOSSARY

Not Applicable

## 7 ATTACHMENTS

Not Applicable

	<b>POLICY</b>	
	<b>Título:</b> Information Security - Extract	<b>Código:</b> POL.TEC.POR.001
	<b>Área:</b> Information Security	<b>Versão:</b> V4.0

## 8 APPROVAL TABLE

NAME	POSITION	AREA
Sandro Simas	Vice President	Technology

APPROVED BY V.TAL'S BOARD OF DIRECTORS ON: 14/05/2025

**THIS DOCUMENT REVOKES PREVIOUS VERSIONS**