	POLICY	
	Code: POL-00032	Version: V3.0
Title: INFORMATION SECURITY		

1 OBJECTIVE

The Information Security Policy ("Policy" or "PSI") aims to establish guidelines, principles and responsibilities, in addition to guiding the execution of actions related to the treatment of information and the appropriate use of assets and/or information by the target audience, in order to mitigate any risks related to external or internal threats, deliberate or accidental, that may impact V.tal's information regarding its integrity, confidentiality and availability.


2 TARGET AUDIENCE

This PSI is applicable to all V.tal, covering all use of devices, access to servers, connections to the network and the internet and any other uses of technological resources or containing V.tal information. It must therefore be complied with and applied in all areas of the Company, including by all individuals or legal entities, whether partners, directors, administrators, employees, apprentices and trainees ("Internal Employees"), as well as service providers, third parties, suppliers and partners of the Company ("External Employees") who, within the scope of their relationship with V.tal, may have access to the areas, equipment, information, files, networks and data owned by the Company. For the purposes of interpreting this Policy, Internal Employees and External Employees will be referred to together simply as "Employees".

3 GUIDELINES

Information is Equity: all information and any data or assets generated, acquired, handled, stored, under custody, transported and/or discarded by Employees on the premises and/or in assets of the Company, due to their link with V.tal or the performance of their activities contracted by the Company ("Protected Information"), are considered assets of V.tal and must be used exclusively for corporate interests. V.tal has a Data Classification Policy aimed at Internal Employees and a Privacy and Personal Data Protection Manual for Third Parties aimed at External Employees, which establish specific rules and obligations on the use of Protected Information, applying them in addition to this PSI.

The responsibility and commitment must be everyone's: all Employees are responsible for the protection and safeguarding of Protected Information, as well as the physical and computer environments to which they have access, regardless of the security measures implemented. Acceptable use of the Company's network infrastructure and services is always ethical, honest, and respects individual rights, including rights to privacy and data protection.

	POLICY	
	Code: POL-00032	Version: V3.0
Title: INFORMATION SECURITY		

Access to information must be managed: logical access, physical access control and the use of information will be approved, controlled, recorded, stored and monitored, in order to adapt Information Security with the execution of the tasks inherent to your position or function.

Security incidents need to be prevented or combated: Information Security incidents, when they cannot be prevented, must be identified, monitored, communicated and properly combated in order to reduce risks in the environment, avoiding interruption of activities, and not affect the achievement of the Company's strategic objectives and customer service.

V.tal's assets and their use may be monitored: the Company may, within the limits of applicable law and as necessary, monitor, film and record the access and use of its technological assets, as well as the environments, services, equipment and information systems, including, but not limited to, emails, files, impressions, browsing history and, in general, networks and computers, so that undesirable or unauthorized actions are detected.

V.tal may audit compliance with security practices: the Company may periodically audit without prior notice, the Information Security practices, in order to evaluate the compliance of the actions of its Employees in relation to what is established in this Policy, in the other guidelines that compose it and in the applicable legislation, including through the monitoring practices mentioned in this PSI.


3.1 Principles of Information Security

These are the security actions or lines of conduct that act as a guide for its implementation and the management of Information Security:

Establish Information Security throughout V.tal: Information Security is handled at the organizational level, in accordance with decision-making that takes into account all of V.tal's critical business processes.

Adopt a risk-based approach: Information Security is based on risk-based decisions such as loss of competitive advantage, compliance, civil liability, operational disruptions, reputational damage and financial losses, misuse, fraud, sabotage, theft and cyberattacks.

Promote a positive security environment: Information Security is structured based on the analysis of human behavior, observing the growing needs of all stakeholders, through the awareness, education and maturity of human capital, strengthening one of the fundamental elements to maintain the appropriate level of Information Security.

	POLICY	
	Code: POL-00032	Version: V3.0
Title: INFORMATION SECURITY		

3.2 Privacy and Protection of Personal Data

This PSI applies to data, including personal data and sensitive personal data, about Employees, customers, end customers and service providers related to V.tal. It is forbidden, without the prior authorization of V.tal, the use of this data for purposes other than those that supported the collection, use, storage and any other cases of data processing, under the terms of this PSI and other policies related to privacy and protection of personal data.

V.tal uses external service providers. If the data being processed is personal, we enter into appropriate contractual agreements and organizational measures are implemented in accordance with applicable legislation to ensure data protection.

The Employee guarantees that all personal data to which he has access will not be disclosed or shared without the express authorization of the Company, nor will it be transmitted or accessed by unauthorized third parties. The Employee also guarantees that he will adopt the best Information Security practices throughout the data life cycle within V.tal, not limited to those described in this PSI.


3.3 Monitoring and Auditing of the Environment

Every physical and digital environment of V.tal is or may be monitored, respecting the limits provided for in current legislation, including the access, use or traffic of information in such environment by any means (such as, for example, e-mail) in order to verify compliance with the Company's security and data protection standards.

Employees are aware that V.tal may:

- Monitor all servers, networks, internet connections, software, equipment and corporate devices, mobile or not, connected to the corporate network;
- Perform physical inspections on the employee's equipment and workstations, periodically or under reasoned suspicion of violation of the Company's internal rules.

The Employee is also aware that the monitoring may identify him and present data on his use of V.tal's technical infrastructure and the material and content handled by the Employee, being certain that all information collected in the course of the monitoring is stored in the Company's backups for audit purposes and may be used as evidence of possible violation of the rules and conditions established by V.tal or by the legislation in force. If requested by the competent bodies, this information may be disclosed to the extent that there is a legal reason or judicial determination to do so.

	POLICY	
	Code: POL-00032	Version: V3.0
Title: INFORMATION SECURITY		

The Employee understands that the monitoring is carried out to safeguard the security not only of the Company's systems and Protected Information, but also of the Employee himself. The data and information monitored can only be accessed by the competent departments and for legitimate purposes, such as investigating complaints and conducting investigations in the work environment. Any and all processing of data for these purposes will be based on the audit report or other appropriate instrument for this purpose and will comply with the specific rules on privacy and protection of personal data.

3.4 Handling of Protected Information

The Employee is responsible for their use of the Protected Information. Thus, the rules below must be observed to ensure a minimum level of Information Security.

3.4.1 Printer and Copier Care

Employees are aware that any and all use of equipment, such as copiers and printers, must be made exclusively within the scope of their professional activities, and use for personal purposes is prohibited. It should be avoided to print documents containing certain types of Protected Information, given that the Internal Employee must follow the guidelines of the Data Classification Policy and the External Employee must follow the guidelines of the Privacy and Personal Data Protection Manual for Third Parties. Any type of printed or copied documents must be removed immediately from the equipment.


3.4.2 Use of Protected Information

The Employee must take the utmost care with his/her use of Protected Information, taking care not to leave notes or manipulate documents containing Protected Information in circulation places, such as meeting rooms or public spaces, such as cafes and airplanes. The reuse of draft papers containing Protected Information is prohibited.

In cases involving the contracting of third-party services that justify the need to share Protected Information, such information may only be shared after a confidentiality agreement or other relevant contractual instruments have been signed with such third parties.

3.4.3 Receiving, Sending and Sharing Files

The Employee is responsible for the files he receives, sends and shares through electronic means and the Company's technological infrastructure, whether equipment owned by the Company made available for the Employee's use, the Employee's own equipment, or cloud services.

	POLICY	
	Code: POL-00032	Version: V3.0
Title: INFORMATION SECURITY		

To ensure minimum levels of security of V.tal's technological infrastructure, the Employee is prohibited from:


- **receive, send and share files that:** (a) have different purposes and not related to the activities of interest of the Company or related to its business; (b) contain pornography or content of a racist, discriminatory or any other nature that violates the legislation in force, morals and good customs; (c) violate the rights of third parties, in particular intellectual property rights, copyrights, image rights, among others; (d) characterize civil or criminal infraction and/or may cause damage to V.tal and third parties; and (e) constitute unfair competition or breach of professional secrecy;
- **send, share and download:** (a) files containing malware, such as viruses and other malicious code; (b) Internal, Confidential or Secret Information in an external environment; and (c) any executable file (.exe) that is not authorized by V.tal.

3.4.4 Custody and Transfer of Information

All Protected Information that must be stored in physical or digital form, when stored by the Employee, must comply with V.tal's data life cycle rules, as well as the following precautions, according to the classification of the information:

- **Physical support.** All documents containing certain Protected Information must be stored in its own physical files indicated by V.tal, in accordance with the methods of identifying the content, also indicated by the Company, including its filing date. Documents used by the Employee in his workstation, when not being used, must always be stored in a drawer or cabinet, ensuring that such drawers and cabinets remain locked when it comes to more critical information. No annotations related to the Protected Information should be left on display, whether on the table, on the computer or in partitions, even when the Employee is present. When the Employee is not on the Company's premises, the documents containing the most critical information should not be exposed.
- **Digital support.** Any and all files containing Protected Information must be saved on the V.tal corporate network, in a specific directory, which prevents access by unauthorized Employees. If the file is to be stored on a mobile device (such as on laptops, due to external meetings), it is essential that the Employee removes the file from the device after use.

Any and all documents or files containing Protected Information may only be changed, copied and/or moved if there is the possibility of recovery, version control or analysis of the records of such file or document in case of security breaches that result in the loss or misplacement of the Protected Information.

	POLICY	
	Code: POL-00032	Version: V3.0
Title: INFORMATION SECURITY		

3.4.5 Disposal of Information

The disposal of a physical document and/or the deletion of a digital file from the V.tal network containing Protected Information must follow the following disposal rules:


- **Physical support.** Documents that have public information can be discarded in the common garbage; those that have Protected Information must be destroyed manually or, preferably, by a fragmenting device before disposal. In the case of more critical information, the use of a fragmenting device is mandatory and, in the absence of such device, the Employee must call the responsible manager to take the appropriate measures.
- **Digital support.** Files containing Protected Information and stored on flexible digital media, such as CD or DVD, must be destroyed by means of a fragmenting device and, in the absence of such device, the Employee must call the responsible manager so that the necessary measures are taken. On the other hand, those files stored on hard digital media, such as hard disk (HD) and pen drive, must be sent to the Technology Department, in a sealed box, for proper destruction, according to the internal procedure adopted.

Only the person responsible for generating or storing the file or document to be discarded is competent to discard or delete it, unless the person responsible expressly grants authorization for a third party to do so. In addition, all disposal must be recorded, in order to maintain a history that allows audits to be carried out, if necessary. In the case of information involving personal data, the Internal Employee will follow the guidelines described in the V.tal Data Retention Policy and the External Employee will follow the Privacy and Personal Data Protection Manual for Third Parties.

3.5 Business Email

The email addresses provided by V.tal to Employees are individual and intended exclusively for corporate purposes and related to the Employee's activities within the Company. E-mail messages should always include signature with the standard format of V.tal. We add that Employees are prohibited from using V.tal's email to:

- send unsolicited messages to multiple recipients, except if related to the legitimate use of V.tal;
- send any message by electronic means that makes its sender and/or V.tal and its units vulnerable to legal and/or administrative proceedings;

	POLICY	
	Code: POL-00032	Version: V3.0
Title: INFORMATION SECURITY		

- disclose unauthorized information, including, without limitation, screen images, systems, documents and the like without express and formal authorization granted by the person responsible;
- falsify addressing information, tamper with headers to hide the identity of senders and/or recipients, in order to avoid the punishments provided for;
- delete relevant e-mail messages when any of V.tal's units or Employees are subject to any type of investigation.

3.6 Internet

All the rules of V.tal are basically aimed at the development of an ethical and professional behavior in the use of the internet. To ensure the rational use of these resources, as well as the security of data and software, the Company reserves the right to use tools to verify the content of corporate emails and monitor the use of the internet and the corporate network.

Any attempt to change the safety parameters, by any Employee, without proper accreditation and authorization to do so, will be deemed inadequate and the related risks will be informed to the Employee and the respective manager. The use of any resource for illegal activities may result in administrative actions and penalties arising from civil and criminal proceedings, and in these cases, the Company will actively cooperate with the competent authorities.


Employees with internet access may download only software approved at V.tal and directly linked to their activities.

Employees may not:

- use the resources of V.tal to download or distribute software or data without proper licenses;
- upload, for its customers, partners and other third parties, any software licensed to V.tal or data owned by it, without the express authorization of the person responsible for the software or data;

3.7 Social Networks and Personal Emails

V.tal may suspend, without prior notice and at its sole discretion, the use and access to social networks, personal emails and messaging services for personal purposes, on the Company's physical premises and devices, for governance and/or Information Security reasons.

	POLICY	
	Code: POL-00032	Version: V3.0
Title: INFORMATION SECURITY		

3.8 Access to the file network

Access to information stored in V.tal's technical infrastructure may be carried out differently (by physical, logical or remote means), depending on the type of format. For each type of format, different rules of conduct will be applied, namely:

3.8.1 Physical Access to Information

The places where the Company's data centers are installed or where its physical files are stored are considered a critical part of its technological infrastructure, which is why the care taken with protection and security must be doubled. There are different types of accesses and, for each of them, different rules and restrictions, as shown below:

- **permanent access:** allowed only to employees of the Company who have the need for cleared access to perform their activities;
- **sporadic access:** allowed to other Employees or external visitors, with prior authorization from V.tal, with registered access (name, date and time).
- **external access:** allowed to those who are not internal Employees of the Company (external contractors), upon authorization and registration (name, date and time), provided that justifies this access.


3.8.2 Logical Access

Access to the information stored in the Company's technological infrastructure will be restricted to each Employee, depending on the access profile assigned to them by the Technology Department, according to the rules set forth in item 3.9 - *Identification and Passwords*. Each profile presupposes the release of access to certain directories within the Company's network, which are assigned by the Technology Department, so that the information can be accessed according to the level of access defined by V.tal.

3.8.3 Remote Access

When the Employee is not on V.tal's premises, he may access the Company's private network remotely, through technologies authorized by V.tal, which may include the use of VPN. Remote access will only be granted to the Employee in cases where there is a proven need. Once the need is verified, remote access will be granted by the Access Management system according to the profile of the employee.

Remote access is only allowed for the execution of the Employee's professional activities that are linked to V.tal. The Employee is responsible for all activities carried out when using remote access, being accountable for any irregular use, including by another person in possession of his or her access.

	POLICY	
	Code: POL-00032	Version: V3.0
Title: INFORMATION SECURITY		

In the event of theft, robbery or loss of mobile equipment that has remote access to the Company's VPN configured, the Employee must immediately seek a police authority to draw up a police report and, subsequently, report the incident to the Technology team, presenting a copy of the police report drawn up.

All remote accesses will be recorded by the Technology team and such records will be available for consultation in case of audit.

3.9 Identification and Passwords

All Employees have certain privileges to access Protected Information, according to their position and duties, according to the rules set forth in item 3.8 - *Access to the File Network*. Some examples of privilege are external access to email, clearances in internet access and logical access, external use of certain V.tal equipment, freeing up hard disk space, use of mobile devices, among others.


The Employee will receive a login and a password, according to the profile assigned to him, which will allow him to be identified when accessing the Company's infrastructure. Thus, the Employee will only have access to V.tal's infrastructure areas that are authorized considering their profile. V.tal reserves the right to review, at any time and without prior notice, through the competent departments, the privileges of any Employee, in order to safeguard the Company's Information Security levels.

The Employee's login and password are personal and, consequently, the Employee is responsible for the secrecy and secure maintenance of his password linked to the login, being prohibited the sharing of login and password with third parties, including other Employees, under penalty of bearing the sanctions not only provided for in this Policy, but also the civil, criminal and labor penalties, responding, including, for any and all damage it causes to the Company.

In addition to the Employee's login, he/she will also receive a physical identification that will grant him/her access to certain physical areas of the Company. Such identification will be made by means of a badge, the use of which is personal and non-transferable, and will have the purpose of registering the entry and exit of V.tal's premises.

3.10 Devices

Physical devices capable of storing Protected Information, such as computers, notebooks, tablets and others, made available to Employees for the execution of their activities, are the property of V.tal, and each one is responsible for using and handling them correctly for the activities of interest to the Company, as well as complying with the recommendations contained in the operational procedures provided by the Technology Department.

	POLICY	
	Code: POL-00032	Version: V3.0
Title: INFORMATION SECURITY		


Equipment must be individually identified, inventoried and protected from improper access. Computers should have automatic operating system updates enabled by default and antivirus software installed, activated, and updated frequently. The user, in case of suspected viruses or problems in functionality, must call the Technology Department.

Personal files and/or files not relevant to V.tal's business (photos, music, videos, etc.) should not be copied/moved to network drives, as they may overload storage on the computer's disk. If the existence of these files is identified, they can be permanently deleted.

Documents essential for the activities of the Employees and/or for the Company's business must be saved in a directory with backup service and with availability for access. Such files, if recorded only locally on computers (for example, on drive C:), will have no backup guarantee and may be lost in the event of a computer failure, being therefore the responsibility of the Employee himself.

The Employee understands that he/she is responsible for any and all damage he/she causes to the equipment, by intent or fault, and is aware and agrees to observe the following rules:


- The Employee is responsible for the equipment and undertakes to use all necessary care, as if the device were his/her own;
- The devices must always be within their reach and cannot be left in public places, in vehicles or in any other place, outside V.tal's premises, where there may be access to the equipment by unauthorized persons, in order to prevent the theft and/or robbery of this equipment, as well as the leakage of the Protected Information contained therein;
- Employees must inform the technical department of any identification of a foreign device connected to their computer;
- The opening or handling of computers or other computer equipment for any type of repair that is not carried out by an IT technician of V.tal or by third parties duly hired for the service is prohibited;
- The Employee must maintain the configuration of the equipment made available by V.tal, following the appropriate security controls required by this Policy and by the Company's specific rules, assuming responsibility as custodian of information. In case of configuration change/tampering, it will be subject to the applicable sanctions according to item 3.14.
- All devices, including computer terminals and printers, must be password protected (blocked) when not in use;

	POLICY	
	Code: POL-00032	Version: V3.0
Title: INFORMATION SECURITY		

- All technological resources acquired by V.tal must immediately have their default passwords changed;
- If, during the use of the device, the Employee has doubts about its handling or finds failures that imply the need for its replacement or maintenance, the Employee must open a call with the Technology Department which, in turn, in addition to providing the necessary clarifications, must guide him to deliver the equipment to the place indicated for its replacement or repair;
- If the use of a device is sporadic, the Employee must return it to the Technology Department in perfect conditions of use, together with any accessories that have been delivered to him, such as bags, cases, films, etc., as soon as the period necessary for use ends. In case of non-return of the equipment, within the determined time and place, the Employee will be responsible for refunding the costs of such equipment to the Company, without prejudice to other legal and administrative measures to be taken by V.tal; and
- In the event of loss, theft, or damage to the equipment, the Employee must immediately notify the Technology Department, which will proceed with the removal of the corporate content contained in the device.

The misuse of V.tal's devices will subject the Employee to the applicable sanctions, depending on the severity of the conduct practiced. There are some cases of misuse:

- Attempting or obtaining unauthorized access to another computer, server or network;
- Circumvent any security systems;
- Access confidential information without the explicit authorization of the owner;
- Secretly watching others for electronic devices or software, such as packet analyzers (sniffers);
- Disrupt a service, server or computer network by any unlawful or unauthorized method;
- Use any type of technological resource to commit or be complicit in crimes or unlawful acts, such as sexual harassment, embarrassment, stalking or manipulation or suppression of copyright or intellectual property without the proper legal authorization of the holder;
- Hosting pornography, racist material or any other content that violates the legislation in force in the country, morals, good customs and public order; and
- Use pirated software, an activity considered criminal according to national legislation.

	POLICY	
	Code: POL-00032	Version: V3.0
Title: INFORMATION SECURITY		

3.11 Data Center and Cloud

V.tal uses various proprietary and third-party software in the course of its operations and the Employee may not:

- use such software for personal purposes or in any way that compromises the security of the Company's infrastructure;
- delete, modify, copy, transfer, reverse engineer or assign access to such software to third parties, or perform any act that is in disagreement with applicable law;
- install on the network or on the Company's devices any pirated software, not licensed or not authorized by the IT area, and any unauthorized software downloaded by the Contributor will be deleted by the Technology team.

V.tal makes available only the resource(s) for the external storage of files, software and systems. Thus, the use by the Employee of cloud storage services not made available through the Company's technological infrastructure is prohibited.

3.12 Employee Termination or Movement


At the end of the Employee's relationship with V.tal, their access to the Company's technological infrastructure will be revoked. The Employee must return, in perfect conditions of use, any and all devices owned by V.tal that are in his possession, together with any accessories have been delivered to him. The obligations of secrecy and non-reproduction of the Protected Information, assumed by the Employee in this PSI, will remain in force even after the Employee's dismissal.

In case of non-return of the equipment, within the determined time and place, the Employee will be responsible for refunding the costs of such equipment to V.tal.

If the Employee changes department or role within V.tal, he/she must also have his/her accesses reviewed, starting to view only the systems and network folders necessary for the performance of his/her new function.

3.13 Reporting of Information Security Incidents

To avoid undue exposure of the Protected Information, V.tal employs security measures, both internal and external, which meet the legal obligations in force. However, it is essential that the Employee complies with the security obligations assumed in this Policy, since such incidents may occur due to human, technological or systemic failures.

	POLICY	
	Code: POL-00032	Version: V3.0
Title: INFORMATION SECURITY		

If the Employee becomes aware or suspects any event that violates the rules of this Policy or endangers the security of the Company's information, he must immediately communicate to the Confidential Channel. V.tal will investigate the causes and effects of the incident, in order to then take the measures of containment, impact assessment and need to communicate about the incident to the competent body and/or the holders of the Protected Information, according to the Information Security Incident Response Procedure involving V.tal Personal Data.

In order for an audit to be carried out on the incident, V.tal will analyze any and all information, as well as the available evidence that can identify the cause of the problem. The information and evidence will be compiled and attached to a report to formalize what happened.

3.14 Commitments and Penalties

All guarantees necessary to comply with this Policy are formally established with V.tal Employees.

Failure to comply with the Policy is considered a serious misconduct and may result in the application of sanctions provided for by law, as well as warnings, suspensions or termination of the employment contract, according to internal procedures and contractual provisions.

All legal provisions and other V.tal standards, such as the Code of Ethics and Conduct, must be strictly observed.

3.15 Training, Update and Disclosure

V.tal has an ongoing security awareness program that aims to raise awareness, train and instruct people, following international best practices, contributing to the dissemination of the Information Security culture for V.tal Employees.

The content of the Policy is widely and frequently updated and disseminated. The re-reading of this Policy, even if not directly requested, must be done periodically for better understanding.


3.16 Final Provisions

Exceptions to the rules established by this Policy to meet any specific demand must be submitted to V.tal for evaluation and approval.

This Policy may be reviewed, updated and amended at any time, at the sole discretion of V.tal, whenever any relevant fact or event motivates its review.

4 ROLES and RESPONSIBILITIES

Board of Directors

	POLICY	
	Code: POL-00032	Version: V3.0
Title: INFORMATION SECURITY		

- Approve this Policy, reinforcing the commitment of senior management to the continuous improvement of safety processes and designate in its corporate structure a director responsible for its management.

Information Security Area

- Manage, coordinate, guide, evaluate and promote the implementation of actions, activities and projects related to Information Security at V.tal, promoting actions of interest to the business, educational programs and human capital awareness.

Employees

- Know and comply with the rules and guidelines established in this Policy and other guidelines that compose it;
- Inform situations that compromise or may compromise the security of information through the Confidential Channel made available by V.tal for this purpose;
- All information created, modified in the exercise of functions and any information contained in corporate e-mail messages must be treated as referring to the business of V.tal, and should not be considered as private or confidential, even if filed in the personal folder of the Employees;
- Ensure that the prohibition on sharing or trading credentials (ID, passwords, badges, tokens and the like) is known and complied with;
- Review your accesses whenever you change department or role within V.tal;
- Ensure that Information Security and data protection requirements, policies and processes are included in technological acquisitions and/or implementations and are maintained throughout their life cycle.

5 REFERENCES

ABNT NBR ISO/IEC 27001:2013 Information technology — Security techniques - information security management - Requirements.


ABNT NBR ISO/IEC 27002:2013 Information technology — Security techniques — Code of practice for information security controls.

Confidential Channel: 0800 721 0783 (<https://www.canalconfidencial.com.br/vtal/>)

NIST Cybersecurity Framework Version 1.1.

Data Classification Policy


Data Retention Policy

	POLICY	
	Code: POL-00032	Version: V3.0
Title: INFORMATION SECURITY		

Privacy and Personal Data Protection Manual for Third Parties

6 GLOSSARY

- Authenticity: guarantee of the veracity of the authorship of the information;
- Employees: all Internal Employees and External Employees who, within the scope of their relationship with V.tal, may have access to the areas, equipment, information, files, networks and data owned by the Company;
- External Employees: all employees indirectly hired by the Company, whether service providers, third parties, suppliers and partners of the Company;
- Internal Employees: all employees hired directly by the Company, whether partners, directors, administrators, employees, minor apprentices and trainees;
- Confidentiality: the information must be available and only be disclosed to authorized individuals, entities or processes;
- Compliance: process of ensuring compliance with a requirement, which may be business obligations with interested parties (investors, employees, creditors, etc.) and with legal and regulatory aspects related to the management of companies, within ethical and conduct principles established by Senior Management;
- Availability: Authorized persons must obtain access to the information and the corresponding assets where necessary;
- Integrity: safeguarding the accuracy of information and processing methods;
- Information: it is the gathering or set of data and knowledge resulting from the processing, manipulation and/or V.tal of data, in such a way that it represents a modification (quantitative or qualitative) in the knowledge of the system (human or machine) that receives it;
- Protected Information: all information and any data or assets generated, acquired, handled, stored, under custody, transported and/or discarded by Employees on the Company's premises and/or assets, due to their link with V.tal or the performance of their activities contracted by the Company.
- Information Security Incident: any and all security breaches that, accidentally or not, lead or are capable of leading to the destruction, loss, alteration, blocking, disclosure or unauthorized use or access to personal data or other information processed by V.tal and Employees;

	POLICY	
	Code: POL-00032	Version: V3.0
Title: INFORMATION SECURITY		

- Information Security Risk: risks associated with the violation of authenticity, confidentiality and integrity, as well as the availability of information on physical and digital media or other information properties;
- Information Security (IS): the set of actions and controls that aims to preserve the aspects of confidentiality, integrity, availability, authenticity and compliance of information, contributing to the fulfillment of V.tal's strategic objectives and service to its customers.

7 ANNEXES

Not applicable

THIS DOCUMENT REVOKES PREVIOUS VERSIONS