ActualSales Group’s Security Policy

I ___________________________ employee of one of the companies that make up the ActualSales Group, hereby declare that I understood and accepted the ActualSales Group Security Policy.

Signature __________________________ Date ___________

ActualSales Group’s Security Policy

1 – GOAL

Provide guidance and support for information security in accordance with business requirements and with the relevant laws and regulations for the best use of available resources and delivery of value to the customer, thus contributing to the financial sustainability of the organization.

2 – SCOPE

This “Security Policy” maintains the integrity in the provision of the service in all units and companies that operate under the ActualSales Group name in accordance with the group’s strategies, current legislation and contractual requirements.

The guidelines established here must be followed by all employees, service providers, suppliers, interns, contractors, partners, and customers who use information from the ActualSales Group.

3 – DEFINITION

The Security policy is a continuous effort to protect information assets against various types of threats to ensure business continuity, minimize risk to the organization, helping companies that are part of the group to fulfill its mission;

It is obtained from the implementation of control objectives and adequate controls to ensure that the organization's business and security objectives are met.

4 – RESPONSABILITY

The ActualSales Group affirms its commitment to the security of information, laws and regulations applicable to the business, based on this “Security Policy”.

5 – SECURITY POLICY’S GOAL

Ensure the reliability index of information security, reflected in the organization's business.

6 – DEFINITION

6.1 – Employees in general

ActualSales Group employees must be aware of Information Security, and their behavior must be consistent with it;

Anyone associated with the improper use of information from the company and / or its customers is prohibited from transmitting it to the competition or third parties, and / or using it for their own benefit and / or storing information, files or emails in another support other than those provided (email and professional cloud storage) by the IT team

It is explicitly prohibited to store or share any type of files or information from the ActualSales Group for any email or cloud storage other than your professional. Send files to personal emails (nome.pessoal@gmail.com), put files in personal or temporary cloud storage (personal Google Drive or WeTransfer).

It is also not allowed to share any information from the Actualsales Group via Instant Messaging, except for customers or suppliers, but in the case of the latter only information directly related to them and on platforms and instant messaging accounts authorized by the administration (namely skype accounts and hangouts provided to employees).

The ActualSales Group reserves the right to automatically store information about the activities of anyone using its resources, including IP address, user, applications, screen / page and conversation carried out within or through the company, and also reserves the right to question the employees of their intentions when detected that they have accessed areas where it is possible to consult personal data of users or more detailed data on the commercial aspect of the business and on relations with suppliers and customers;

Any authentication ID (user and password) on the corporate network or in applications provided by the ActualSales Group is personal and non-transferable and each user will be responsible for storing and using it;

Any password used by users on internal platforms must always be generated by the user himself and communicated to the IT team using an encryption method that does not allow the IT team to have knowledge of the password (MD5). In the case of professional email, the communication of new passwords must as a rule oblige the user to change the password after the first login.

The IT team should therefore not define or be aware of a definitive password either for internal platforms or for professional email, to ensure that all users, including members of the IT team, are only aware of their password. Exception made for platforms with shared use by several users.

Professional e-mail should only be used to deal with matters related to the company, and only business information can only be transmitted by email or other means outside the property of ActualSales Group if this transmission of information is inherent to the business model or there is explicit authorization from management.

No access to the systems and applications of the ActualSales Group or its customers may be shared, with the associated owner of the user being solely responsible for maintaining the confidentiality of his login passwords, users, internet, work files and other applications of the ActualSales Group ;

At the end of the employment and / or contractual relationship, of the associates and / or service providers, the Administrators of the ActualSales Group must formally inform the IT team of the employee's departure and for the disabling of accesses, and the IT team must disable all Authentication ID's used during service provision.

The IT team of the ActualSales Group, given the need for direct access to the business database, should have access to the database and software only through a computer authorized for this purpose (machine's SSH key).

At the end of the employment and / or contractual relationship, any programmer, the ActualSales Group's IT Team must immediately disable the SSH key for that computer so that he no longer has access to the infrastructure, software base and business database.

6.2 – Instant Messaging

The use of Instant Messaging tools not approved by the administration and the IT team is forbidden, except for exceptions, when expressly approved by the administration and its effective use in the activities performed by the associate or client is proven;

File transfer by any Instant Messaging and file sharing tool is prohibited, except for authorized exceptions and / or approved and authorized tools.

The authorized platform for communication between employees of the ActualSales Group is Google Hangouts using the professional email account. Employees should only use this tool to communicate with each other, and always through their professional email account. They should not use other platforms or other accounts to communicate professional content themes.

Nor can they place any type of company information on other instant messaging platforms including user data for pages, urls, entities or billing data. It is prohibited and subject to disciplinary proceedings to use platforms other than Google Hangouts to communicate any content related to the ActualSales Group.

For employees who need to use another platform to communicate with customers or employees of other business units in the group, namely Skype, they should communicate their interest in using that platform to the IT team and only use the account provided by it, no staff and in relation to the account provided shall not:
Change account password
Change the email associated with that account

The administration reserves the right to consult any communications made on instant messaging accounts that the employee has installed on the computer, or logged in his / her browser, regardless of whether the account is the professional account or the personal account (if the employee has logged in via your professional computer).

Employees who do not show interest in having an Instant Messaging account on another platform to contact customers and / or suppliers (eg Skype) should not have this software installed on professional computers, nor should they log in to those same platforms in their browsers. Employees who have software or logins made on instant messaging platforms, incur a breach of security policy, susceptible to disciplinary action and inherently authorize access to any instant messaging account in use or with access made on the company's professional computers.

6.3 – Clients, Providers and Other

All creation, invention and development of ideas, processes, systems, products and services performed during the provision of services at ActualSales Group must be transferred to it. Exceptions must be defined in special agreements with the Administration;

It is forbidden for any service provider to improperly use information from the company and its customers, transmit it to competitors, use it for their own benefit and / or store files and emails improperly;

Upon receiving access to any resource of the ActualSales Group, the service provider will be subject to the organization's internal policies and guidelines and to all criteria established in the confidentiality clauses available in the service provision contract signed at the time of contracting;

At the end of the contractual relationship, the person responsible for the contract of the service providers of the ActualSales Group must ensure that the authentication IDs used during the work are deactivated.

6.4 – Assets

Every associate is responsible for ensuring the proper functioning and integrity of any resource provided by the company to carry out its activities and, when applicable, must sign a commitment to use the resource;

All files that are shared with customers and suppliers that contain personal data must always be protected with a password and only the strictest possible number of employees should have access to the files and the respective password. Files with personal data should not be stored either in email or in cloud storage without password protection in the respective files. The password should not be the same for all files

Personal computers are not allowed on the network. Except for exceptions previously authorized by the IT team, access via mobile devices (smartphones, cell phones, tablets, ipad’s, etc.) will be allowed. In these cases, the only responsible for ensuring the operation of these assets is the associate who owns the equipment;

All entry, movement and exit of assets from ActualSales Group units must comply with the company's internal procedures.

6.5 – Process

The company must map all the processes critical to the business and carry out an analysis and risk assessment with controls and deals. They must be known, approved and accepted by the governing body;

The mapping of critical processes should be reviewed whenever impact changes occur in the environment.

6.6 – Risk

The company must define and follow a single risk analysis and assessment methodology for existing processes and technologies and its results must be comparable and reproducible.

Risk analysis and assessment must be able to identify vulnerabilities, threats, impacts and acceptable levels of risk for assets, people, information, systems, application and mapping of the main business processes according to the company's strategies, current legislation and contractual requirements; The risk analysis and assessment must be reviewed at least once a year, or whenever changes in impact occur in the environment.

6.7 – Information

Access to information from Content Ignition or its customers in its business and computing environment is restricted and will be made available only to formally authorized persons;

All confidentiality clauses agreed with customers in relation to their information must be respected by ActualSales Group members or third parties to services that may have access to this information;

It is expressly prohibited for any user who does not have a formal authorization to use, access to any systems and applications or even a simple attempt;

Any and all information generated within the ActualSales Group or on its behalf, which is the result of the work of associates, suppliers or service providers is the right of the Group and only it can determine its destination and purpose;

All creation, invention and development of ideas, processes, systems, products and services, created within the scope of the job or the responsibilities and mission of the associate's role or position in the company, must be transferred to ActualSales Group, with the exceptions defined in special agreements as provided for in the Code of Conduct;

Disclosure of any information of the company or its customers to others who do not belong to the same work group, in public (including photos / footage on social networks) or internal media, without prior authorization or that is linked to the term liability and confidentiality, except for exceptions when provided for in the contract;

Disclosure on public channels includes comments on social networks for the member's private use. Any disclosure must be approved in advance by management.

The information generated within the organization must be stored in a backup process with the guarantee given by the IT team;

It is not allowed to use pendrives, external hard drives or any other type of removable device for transporting or storing data. Exceptions must be formally authorized by the IT team;

At the end of the contractual relationship with the customer or service provider, all information stored in the ActualSales Group's equipment must be deleted;

At the end of the employment and / or contractual relationship, members and / or service providers who may be allowed access to equipment or storage media must eliminate any physical and / or logical traces of information generated or acquired within the ActualSales Group.

6.8 – System and Apps

All software installed on machines owned or operated by the ActualSales Group must have a previously purchased use license or must be installed by the IT team, the installation of software not authorized by IT by the employee will not be allowed without prior validation by the team. IT;

Users are not allowed to uninstall remote access software that allows their computer to be audited.

All computers must have in the operating system a user with administrator permissions (who allows the installation of software) and a normal user to use the computer. The employee must not have access to the password for the administrator profile, nor should he be able to install software without the permission of the admin user.

All security updates and corrections must be implemented according to the rules of each application and approved by the security and information technology team;

All equipment (servers, desktops, notebooks, among others) that allow the installation of antivirus, must have them installed and updated online, and the user cannot disable or uninstall;

All antivirus software must ensure that viruses, worms, spyware, or other existing attack technology are blocked; All e-mail and internet access must be monitored and protected with antivirus and firewall rules.

7 – VIOLATION OF POLICY

7.1 – Violation Report

Security breaches must be reported to management and the IT team by email. Any violation or deviation must be investigated to determine the necessary measures, aiming at correcting the failure or restructuring processes;

7.2 – Policy Violation Examples

- Use of software that is not installed or authorized by the IT team;
- Introduction (intentional or not) of computer viruses;
- Sharing sensitive business information;
- Disclosure of customer information and contracted operations.
- Use of unauthorized instant messaging software
- Use of personal instant messaging accounts or alteration of elements that are not subject to alteration of professional accounts
- Any non-collaboration of any of the security policy points not specified in this list.

7.3 - Universality and adherence

The safety principles established in this policy are fully adherent to all ActualSales Group employees and must be observed by everyone in the performance of their duties;

7.4 - Non-compliance with the guidelines

Non-compliance or non-compliance with the guidelines of this policy or of the other policies and guidelines of the organization are subject to the application of disciplinary proceedings.

8 – AUDIT

8.1 – Universality and Possibility

All associates, as well as third parties that use the technological environment of the ActualSales Group, are subject to random audits of the network, professional computers and the use of applications.

8.2 – Employee’s Computer Audit

The audit can be carried out remotely through remote access software or locally on the employee's computer. The audit request can happen at any time, and from the moment the employee receives the verbal or written indication to do so. From that moment, the employee must not interact with the computer, including to close chat windows, programs, pages or to block access or turn off the computer.

The non-collaboration of the employee with any of these procedures is directly susceptible to disciplinary proceedings regardless of the justifications presented. During the audit, a member of the administration and a member of the IT team must always be present. During the audit the employee may be present, however the presence of the employee is not mandatory. The audit can be assisted by installing remote computer management software.

8.3 – Definition and Communication

The auditing and monitoring procedures will be carried out periodically by the IT team after direct indication from the management, since the communication from the management to employees is not necessarily at the same time or mandatory in a formal way. These audits aim to observe the compliance with the guidelines established in this policy by users and with a view to managing the network's performance;

If there is evidence of activities that could compromise productivity, data security, or other reasons, the management of the ActualSales Group and the respective IT team is allowed to audit and monitor the activities of a user, conversations in the instant messaging accounts, internet traffic in addition to inspect your files and access records.