INFORMATION SECURITY POLICY

REVIEW 02

WWW.DMSLOG.COM

TABLE OF CONTENTS

1. CONTEXTUALIZATION

DMS LOGISTICS is a provider of the most modern processes in the global logistics segment, which are made possible by the continuous improvement of its technological services with subsidiaries and partners distributed throughout the five continents of the world.

The information security policy aims to reduce this risk by protecting DMS LOGISTICS from threats and vulnerabilities, and the impact on its assets, which may compromise the confidentiality, integrity and availability of information.

2. PURPOSE

DMS LOGISTICS aims to establish directives and responsibilities for information security management and promote the continuous improvement of procedures related to data and information security, to prevent, detect and reduce vulnerabilities to incidents related to web and cloud environments. Thus, ensuring the availability, integrity, confidentiality, legality, authenticity, and auditability of the information necessary for the fullfillment of the interests of DMS LOGISTICS and its interested parties.

At the sole discretion of DMS LOGISTICS, this information and cyber security policy may be evaluated and reviewed regularly or in the event of circumstances and incidents that justify or require such evaluation and review, in order to ensure its permanent updating, adequacy, effectiveness and protection of the assets of DMS LOGISTICS.

3. Relationship Areas (RECIPIENTS)

The information security Policy, at DMS LOGISTICS, applies to all partners, administrators, officers, managers, representatives, employees, service providers and other third party users authorized by DMS LOGISTICS who may have access to and use, in any capacity and type, in the exercise of their activities, data, information, resources, tools, systems, applications or services owned or controlled by DMS LOGISTICS, including works performed externally that use the Organization's processing environment, or access to information belonging to DMS LOGISTICS.

Disclosure of the policy to DMS LOGISTICS interested parties is made through the DMS website, integration training, recycling and e-mails at least once a year.

This policy also applies to Employees in remote work, including, teleworking and home office. DMS LOGISTICS may establish, at its sole discretion, specific information security policies, processes and directives for these cases.

4. REFERENCE DOCUMENTS

- Law no. 9.279/1996 - Regulates rights and obligations concerning industrial property
- Law 13.709/2018 - General Law on Protection of Personal Data (LGPD)
- Law 13.853/2019 - Amends the General Law on the Protection of Personal Data, published in 2018
- NBR ISO/IEC 27001:2013 – Information Security
- NBR ISO 9001:2015 – Information Security

5. AUTHORITY AND RESPONSIBILITIES

- Officers: DMS Officers are responsible for analyzing, reviewing and approving this Policy whenever necessary. This Policy takes effect on the date of its approval by the Executive Board and repeals any documents to the contrary.
- IT and infrastructure manager: Comply with the directives established in this Policy, maintain it regularly updated to ensure that any changes in the DMS LOGISTICS direction are incorporated into it and clarify doubts regarding its content and application.
- Managers: Manager of each area are responsible for establishing criteria regarding the level of confidentiality of the information (reports and/or media) generated by their area. Information should be classified as: Public, Internal, Confidential or Restricted.
- Employees: Observe and ensure compliance with this Policy and, when necessary, evoke the IT and Infrastructure Manager to consult on situations that involve conflict with this Policy or through the occurrence of situations described in it. It is essential that each person understands the role of information security in their daily activities and participates in awareness programs.

At their sole discretion, the DMS LOGISTICS Officers may implement a committee for the evaluation, review, implementation and inspection of this Policy and its terms and conditions.

If there is doubt or question regarding the provisions of this policy, the Employee must contact the IT and Infrastructure Manager by the following means: [__]

DMS LOGISTICS will promote, develop, update and implement, on a regular and continuous basis, the other policies, processes and practices necessary to enable and consummate this information and cyber security policy, including, but not limited to: (i) business continuity policy, intended to ensure the critical and essential business activities of DMS LOGISTICS; (ii) disaster management and recovery policy; (iii) supplier risk assessment policy; (iv) and other related policies that become necessary or convenient, at the discretion of DMS LOGISTICS.

6. INFORMATION SECURITY PRINCIPLES

- Confidentiality: Ensure that information will only be accessible to authorized persons;
- Integrity: Ensure that the information, stored or in transit, will not undergo any unauthorized modifications, whether intentional or not;
- Availability: Ensure that information is available whenever necessary.
- Compliance: Ensure compliance with the requirements, which may be legal and/or contractual obligations with interested parties and with legal and regulatory aspects.
- Qualification: Encourage training and qualification in the field of information security.

7. INFORMATION SECURITY POLICY

DMS LOGISTIC's policy is to offer our customers high-performance logistics solutions based on creativity and constant optimization of operations, quality management system, information security and security, promoting the continuous improvement of procedures related to data and information security, to prevent, detect and reduce vulnerabilities to incidents related to web and cloud environments. Thus, ensuring the availability, integrity,

confidentiality, legality, authenticity and auditability of the information necessary for the fullfillment of the interests of DMS LOGISTICS and its interested parties.

DMS LOGISTICS is committed to:

1. Provide air and sea freight forwarding services for import and export.
2. Safeguard its information assets to reduce vulnerability and incidents.
3. Ensure the availability, integrity, confidentiality, legality, authenticity and auditability of the information necessary for the fullfillment of the interests of DMS LOGISTICS and its interested parties.
4. Evaluate business risks aiming to ensure customer satisfaction, applicable requirements and financial viability;
5. Align information security management with our business.
6. Ethically and responsibility carry out the processing of information throughout its life cycle.
7. Ensure the confidentiality, integrity and availability of information throughout its life cycle: production, handling, reproduction, transport, transmission, storage and disposal.
8. Identify, analyze, evaluate and process risks that involve information assets, through periodic assessments, at regular intervals.
9. Adopt mechanisms to protect against misuse, fraud, damage, loss, error, sabotage, and theft and attacks, throughout the information life cycle.
10. Continuously monitor information assets and use processes, controls and technologies to prevent and respond to attacks.
11. Disseminate the culture of information security through a permanent program of awareness-raising, awareness and qualification.
12. Preserve information security requirements in contracting services or hiring people and in the relationship with employees, suppliers, third parties, partners, contractors and interns.
13. Grant employees and third parties access solely to the information necessary for the performance of their functions and assignments provided for in a contract or by legal determination.
14. Identify, through access control, each user individually and in duly proven cases of improper processing of corporate information hold the user in case responsible, along with the administrator who granted them the access.
15. Analyze the occurrences of improper processing of corporate information under the legal and disciplinary aspects, attributing responsibility, and under the technical aspect, correcting vulnerabilities.
16. Fully meet the needs of our customers and constantly increase their satisfaction, which is why we give great importance to promoting quality awareness among our employees.
17. Invest in training and qualification of our largest capital, our employees, so that all are integrated into the quality management and information security system.
18. Work on the continuous improvement of Information quality and security processes and systems.
19. Ensure a dedicated and qualified team with entrepreneurial and innovative guideline. Executives guide by setting an example and create the internal environment to achieve quality goals.
20. Ensure that relationships with our suppliers are of mutual benefit. This requires transparent communication, agreement on common goals regarding the customer requirements and cooperation in improving joint processes.

21. Promote associated activities and resources to achieve results across the system and at all levels of hierarchy.

The contracting, maintenance and implementation of systems, applications, programs and other information resources and tools in the DMS LOGISTICS must always take into account the existing security risks and respective measures, controls and mitigation mechanisms. DMS LOGISTICS will perform regular and ongoing assessments, including through third parties, on the security measures, controls and mechanisms of its systems, applications, programs and other information resources and tools, including risk impact analyses.

8. GENERAL OBLIGATIONS

All DMS LOGISTICS Employees must consider information as an asset of the organization, one of the critical resources for carrying out the business, which has great value for DMS LOGISTICS and must always be treated professionally.

At all times, employees must observe and comply with the provisions of this security and cybernetics policy, under penalty of the applicable legal and contractual sanctions and measures. DMS LOGISTICS monitors and supervises, on its own or through the use of third parties, the compliance of its Employees with the provisions of this security and cybernetics policy.

All users of the company's computer resources are responsible for protecting the security and integrity of information and computer equipment. Violation of this security policy is any act that:

- Exposes DMS LOGISTICS to actual or potential monetary loss by compromising data security, information, or yet loss of equipment;
- Involves the disclosure of confidential data, copyrights, negotiations, patents or unauthorized use of corporate data;
- Involves the use of data for unlawful purposes, which may include the violation of any law, regulation, or any other government provisions.

It is not allowed to remove any devices, equipment, information from DMS LOGISTICS facilities without the security team's express written permission.

For executing activities and services, DMS LOGISTICS may make available to its Employees, at its sole discretion, certain devices, equipment and resources, on loan. At all times, the devices, equipment and resources assigned will remain under the property of DMS LOGISTICS, and the Employee will only have provisional ownership over them. In any case, the ownership of these assigned assets will be transfered to the Employees. At all times, employees must ensure the safekeeping, correct handling and the maintenance in good regular state of conservation of the assigned assets, taking into account the considering the natural wear and tear resulting from their normal and proper use. The use of the assigned assets for purposes other than those for which they are intended is prohibited. The assigned assets must be kept in adequate, appropriate and safe places, in compliance with the DMS LOGISTICS recommendations and guidelines. Whenever requested by DMS LOGISTICS, Employees will return the devices, equipment and resources that have been assigned by DMS LOGISTICS for carrying out their activities. Employees who, in the exercise of their activities, have in their possession and use DMS assets, must return them and cease the use of any tools, resources and services made available by DMS, after the termination of the employment contract, provision of services or applicable legal basis.

Third parties who have access to DMS LOGISTICS information systems, whether suppliers, customers or others, must have access to the applicable information security standards, and agree to their terms and conditions, to secure and ensure DMS LOGISTICS information security, before access is granted, including confidentiality standards.

These suppliers must always adopt the best market practices for information security and shall be regularly monitored to ensure compliance with applicable information security requirements. Contracts must include appropriate provisions to ensure the security of DMS LOGISTICS' information and systems.

Employees must be regularly trained and qualified in information security matters, regarding the kind and types of threats, existing security measures and the need to report suspicions and indications of problems. DMS LOGISTICS is committed to providing mandatory training and qualification to all Employees to ensure information security.

The definitive and permanent disposal of DMS LOGISTICS's media, software, systems and other devices and equipment must be preceded by the elimination and destruction of any data and information contained in such assets. The same procedure will be applied in the event of defect or failure of these assets.

9. INTELLECTUAL PROPERTY

All materials, works, “designs”, processes, flowcharts, research, analysis, creations or procedures developed by any Employee during the exercise of their activities for DMS LOGISTICS are owned by DMS LOGISTICS, without prejudice to the applicability of Brazilian law.

10. USE POLICY

- Do not enter your passwords or users on third-party machines, especially outside the company.
- Only accept technical assistance from a previously introduced and identified member of our technical team.
- Report to the external or internal security team requests that conflict with the topics listed above.

11. EMPLOYEE DATA. employees' devices.

Any Personal Data of Employees that may be stored will be considered confidential data.

Personal Data of Employees will not be transferred to third parties, except when required for our business, and provided that such third parties maintain the confidentiality of such data, including, in this case, the list of electronic mail addresses (e-mails) used by DMS LOGISTICS employees. On the other hand, the employees commit not to store personal data in the premises of DMS LOGISTICS, without prior and express permission by the executive board.

This Policy is also applicable to the Employees' personal devices and equipment which are used for the exercise of their respective activities and services, as appropriate, as long as duly authorized and permitted by DMS LOGISTICS.

DMS LOGISTICS may establish, at its sole discretion, specific information security policies, processes and directives designed to regulate access and use of DMS LOGISTICS data, information, tools, resources and services on personal devices of Employees, suppliers and

authorized users, including the authorized requirements, types, brands. These specific policies, processes and directives may be amended by DMS LOGISTICS from time to time.

When requested by DMS LOGISTICS, Employees must promptly make their personal devices and equipment available for: (i) implementation of security measures, such as the update of security systems, services, and applications for the protection and safeguard of DMS LOGISTICS data, information, systems, and resources; (ii) monitoring and analysis of the Employees' compliance with the DMS LOGISTICS' policies, procedures, and practices; (iii) execution of tests and audits of the security of DMS LOGISTICS' environment, resources, systems, applications, and networks; (iv) copies and backup copies of any DMS LOGISTICS information, data, services, and activities contained in the Employees' personal devices and equipment; and (v) removal, disposal and uninstall of DMS LOGISTICS data, information, services, resources, tools from the Employees' personal devices and equipment, particularly, with the termination of the applicable contractual relationship.

12. ILLEGAL PROGRAMS

The use of illegal (Unlicensed) programs in DMS LOGISTICS is strictly prohibited.

Users must not, under any circumstances, install this type of "software" (program) on any DMS equipment, even because, according to the organization's security policy, only IT personnel are authorized to install previously authorized programs. Biannually, the IT Department will undergo verifications on the servers data, Drives and/or users' computers, in order to ensure the correct application of this directive. If unauthorized programs are found, they must be removed from the computers.

All employees sign a term of responsibility and use of DMS equipment and systems, in this term it is detailed that:

- Each individual has their own workstation. This means that everything that is executed from your station will be your responsibility.
- Whenever you leave of your station, make sure you've logged off or locked the console.
- Do not install any type of software / hardware without authorization from the technical or security team.
- Do not have MP3 files, movies, photos and copyrighted software or any other type of piracy on your equipment;
- All data relating to the company must be kept on the DMS drive, which has a daily and reliable backup system.
- If necessary, the employee can contact the technical team to request support.

13. PERMISSIONS AND PASSWORDS

Every user, to access the DMS LOGISTICS network data, must have a login user and password previously registered by the IT department.

The direct manager must provide the data regarding the types of accesses and programs for each employee and fill out a form and deliver it to the HR department. When the registration of a new user in the DMS's "network", systems or computer equipment is necessary, the new user's origin department must communicate this to the IT department, through internal communication or e-mail, informing which type of routines and programs the new user will have the right to access and which will be restricted.

The IT department will register and inform the new user their first password, which must be changed immediately after the first login and every 30 (thirty) days after that. For security, the IT department recommends that passwords always have a minimum security criterion so that they are not easily copied, and cannot be repeated.

All users responsible for electronic approval of documents (example: purchase orders, requests and etc.) must inform the IT department who will substitute them in case of their absence in the DMS, so that permissions can be changed (delegation of authority). When access for external users is necessary, whether temporary or not, the access permission must be blocked as soon as said user has finished their job and in the future, if access becomes necessary again, it must then be unblocked by IT personnel.

14. EMPLOYEE work computer stations

All work computer stations have an administrator user, to ensure that no changes are made to the computer settings.

Users are prohibited by the administrator account from downloading and installing unauthorized applications.

15. E-MAIL MONITORING

The corporate email is accessed through tools provided by DMS LOGISTICS. There is no expectation of privacy as occurs with the employee's personal and private use email. Corporate email is a tool owned by DMS LOGISTICS.

Thus, it is important that the employee does not use corporate email in an improper, negligent or malicious manner

16. DATA SHARING

Sharing folders on company computers, computer desktops and other mobile devices is not allowed. All data must be stored on the DMS Drive, and the authorization to access it must be provided by IT personnel. Periodically, the IT Department will undergo verifications on the drives data and/or on the users' computer, in order to ensure that data considered confidential and/or restricted are not stored in the network.

Printer sharing must be subject to access authorizations by the IT personnel. Sharing mobile devices such as pen-drivers and others is not allowed within the company.

17. DESK AND CLEAN SCREEN

- Documents on paper and electronic media must not remain on the desk, they must be stored in locked drawers or cabinets when not in use, especially outside office hours.
- Physical information classified as sensitive, confidential, restricted or critical to DMS must be stored and locked in a secure and separate location.
- Notes, errands and reminders should not be visible on the desk or pasted on the computer desktop, notebook, monitor, notice boards or walls.

- Do not write down information classified as restricted, confidential, sensitive in places

where information may be exposed, such as notice boards and whiteboards.

- In periods of absence from the workstation, physical documents must be taken from the desks and other surface areas;
- Documents for internal or confidential use in electronic media must be stored in environments with controlled access and passwords to prevent access from unauthorized persons;
- All printed documents must be destroyed before being disposed of in the trash. Documents classified as confidential and restricted must be destroyed using cutting machine or they must be incinerated.
- Avoid printing documents that can be read on the computer desktop and notebook.
- Always log off when leaving your desk and lock the computer Desktops and notebooks screen.
- Do not leave printers, computer desktops and notebooks logged in when you are absent from the office.
- Personal belongings must always be stored, either in your cabinet or in your bag.
- Your password is personal and non-transferable, so do not share it to anyone.
- At the end of the office hours, or when you'll be absent from work, clean your desktop, store the documents, lock the drawers and cabinets and turn off the computer desktop or notebook.
- Do not put glasses with water, juices, coffee, etc., on the desk.

18. INTERNET ACCESS

- Within DMS facilities, internet access is provided to its authorized users, according to the needs inherent for the performance of their professional activities;
- Internet access can be provided both through the DMS's corporate network, and through the provision of mobile internet services, provided by third parties hired by DMS;
- Only web browsing is allowed. Specific cases which require other protocols must be directly requested to the security team with prior authorization from the manager.
- Recreational use of the internet must not occur during office hours.
- All information accessed, transmitted, received or produced through internet access provided by DMS is subject to monitoring, and there should be no expectation of privacy on the part of the user;
- During the monitoring of internet access, DMS reserves the right, without any notification or warning, to intercept, record, read, copy and disclose by, or to, authorized persons for official purposes, including criminal investigations, all information trafficked, whether originating from its internal network and intended for external networks or otherwise;
- During internet access provided by DMS, it is not be allowed to download, upload, include, make available, view, edit, install, store and/or copy any content related expressly or subjectively, directly or indirectly, to:
  - Any kind of sexual exploitation;
  - Any form of adult content, eroticism, porn;
  - Any kind of Child Pornography;
  - Any form of threat, blackmail and moral or sexual harassment;
  - Any slanderous, defamatory, injurious, vexatious, demeaning acts or acts in violation of society's ethical and proper practices;

- Prejudice based on color, gender, sexual orientation, race, origin, social condition, faith, religion, disabilities and special needs;
- Encouragement of excessive or recurrent consumption of alcoholic beverages, smoking and narcotic substances, whether licit or not;
- The practice and/or incitement of crimes or criminal offences;
- The practice of national or international political propaganda;
- The practice of any unfair commercial activities;
- The disrespect to the image or intellectual property rights of the DMS LOGISTICS;
- The dissemination of malicious code and virtual threats;
- Attempt to expose DMS's computer infrastructure to virtual threats;
- Unauthorized disclosure of any DMS LOGISTICS information classified as confidential, restricted or for internal use;
- Use of websites or services that seek to circumvent internet access controls.
- The use of P2P tools (kazaa, Morpheus, etc.) is prohibited.
- The use of IM (Instant messengers) not approved/authorized by the security team is prohibited.

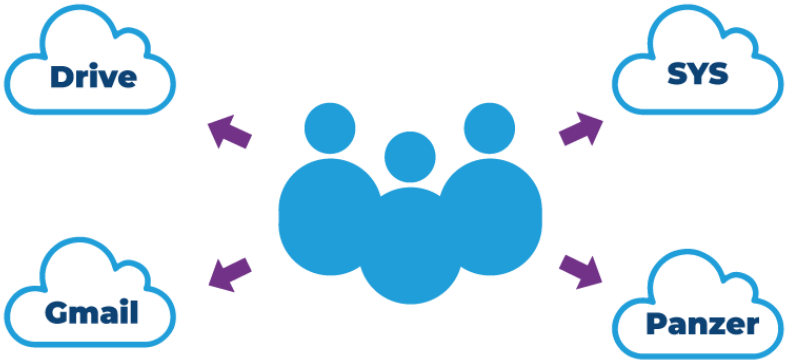
- Remembering again that the use of the internet will be constantly audited as well as the user.
- The employee will be responsible for the use of the devices, equipment, resources, tools and services made available by DMS LOGISTICS for carrying out their activities.

19. Corporate behavior in social media and networks

When accessing their private accounts on social media and networks, employees, service providers and third-party contractors must observe the following restrictions:

- The publication of content or comments directly related to DMS, its employees, third party contractors and service providers is not permitted;

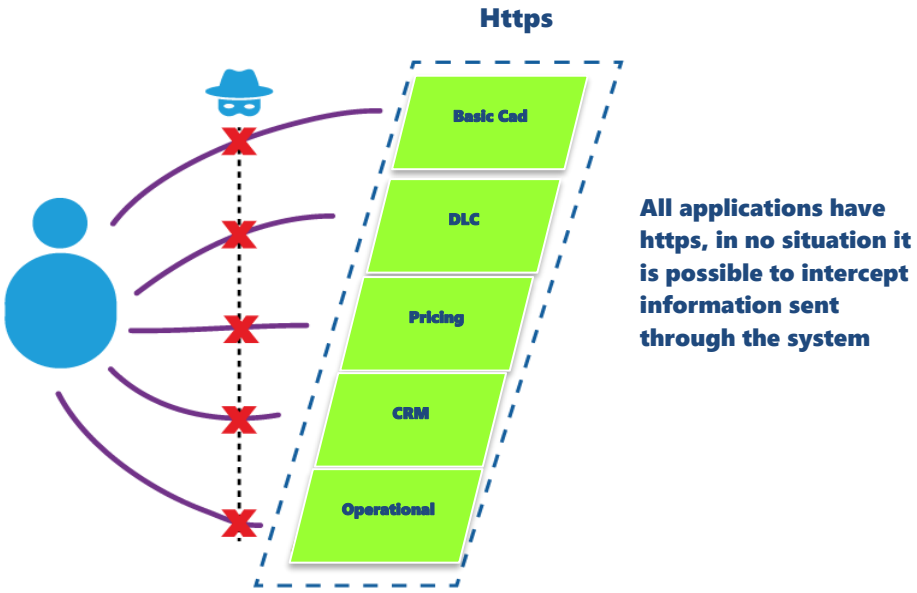
20. BACKUP, SECURITY AND RELIABILITY



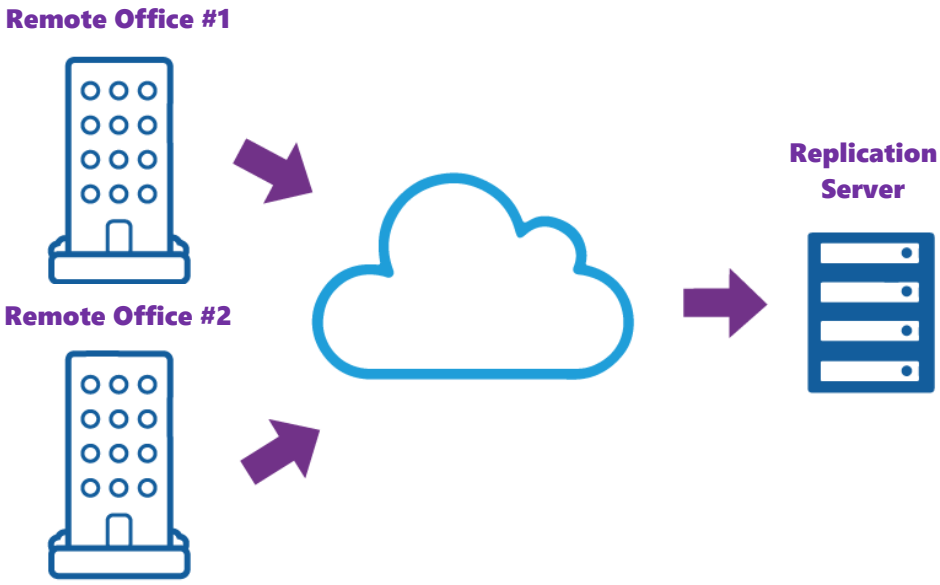
The management of the database is of sole responsibility of the IT Department, as well as the maintenance, alteration and updating of equipment and programs.

The user can only access the server through our local IP.

Backups are automatically done in our cloud and server, so there is no risk of data loss.



All our data from the cloud is replicated to another server, so even if there is some kind of issue with the cloud, our data will still be saved in the server.



21. ADMISSION, LEAVE AND DISMISSAL OF EMPLOYEES

21.1. IDENTIFICATION OF NEED

The DMS LOGISTIC Personnel Recruitment and Selection department must inform the IT department any and all activity related to the admission, suspension, interruption and dismissal of its employees, so that the latter can be registered in or excluded from DMS systems. This includes the provision of their password and registration of their username in the systems, by the IT department.

It is up to the hiring department to inform the IT department of the routines to which the new contractor will have the right to access. In the case of temporary workers and/or interns, the period for which the contractor will provide services to DMS must also be informed, so that on the date of their termination, activities related to their right to access the systems may also be withdrawn. In the case of dismissal, the HR department must inform as soon as possible the IT staff of the fact, so that the dismissed employee is excluded from the DMS systems.

It is up to the HR department to make DMS LOGISTICS Information Security Policy known to the new contractors, as well as obtain the latter's appropriate signature of agreement. No employee may be hired without having expressly agreed to this policy.

21.2.ACCESS TO CORPORATE EMAILS AND PLATFORMS - LEAVE

During the period of leave from the company, the IT department will suspend the employee's access to computerized systems and emails and will automatically redirect the emails to another member of the team. We will also keep our customers and partners informed of the employee's leave for the determined period according to the decision of the respective Manager.

21.3.RETURN TO WORK

After the return to work is approved, the HR must inform the IT department that the employee's access to the computerized systems and emails have been authorized and that the automatic redirection of emails must be suspended.

22. PROMOTION AND TRANSFER OF EMPLOYEES

When an employee is promoted or transferred from a department or management, the HR department must inform the IT department of the fact, so that the necessary adaptations are made for the access of said employee to the DMS computerized systems.

23. PENALTIES

Failure to comply with the DMS LOGISTICS Information Security Policy may result in the enforcement of measures and sanctions, including, but not limited to, the termination of employees according to the type and severity of the occurrence.

24. INFORMATION AND COMMUNICATION

All recipients of this Policy, when identifying a risk situation related to violation of this Policy, and of other standards of similar content, have the responsibility to communicate the fact to the Management and to the DMS Quality Department.

For this purpose, the following communication channels may be used:

- Channel disk-report: ouvidoria@dmslog.com (in the case someone wants to make an anonymous complaint);
- Called through DMSYS.

For example, Employees must inform, as soon as possible, any situation, fact or event, including mere suspicion or attempt, involving, among others:

(i) Unauthorized use, access, transmission, disclosure, sharing, or any other type of unauthorized processing of data and information owned or controlled by DMS LOGISTICS;

(ii) Any internal or external initiative intended to interfere with, impair, compromise the security, availability, authenticity, confidentiality and integrity of data and information, or the operation and performance of DMS LOGISTICS' devices, equipment, resources, tools, services and security measures;

(iii) Loss, damage, failure, defect of devices, equipment owned or controlled by DMS, or even the employees' personal devices and equipment, through which they have access to data and information owned or controlled by DMS LOGISTICS;

(iv) Any non-compliance that may be identified as pertaining to this Policy and other applicable to Employees, such as confidentiality and provision of services agreements, employment contracts, among others; and

(v) Any other situations, facts or events that, by their kind, may represent an information and cyber security risk to DMS LOGISTICS.

25. TERM AND DEFINITIONS

- Sensitive information: All data that must be protected.
- Sensitive personal data: Personal data on racial or ethnic origin, religious conviction, political opinion, union membership or affiliation to a religious, philosophical or political organization, data regarding health or sexual life, genetic or biometric data, when referring to an individual;
- Information security guarantee: Systems' and organizations' ability to ensure the availability, integrity, confidentiality and authenticity of information.
- Access: Possibility to communicate via device, storage medium, network drive, memory, registry, file, etc. aiming to receive, provide, or delete data
- Storage: Action or result of maintaining or keeping data in storage
- Archiving: Act or effect of maintaining registered data after it has already lost its validity or had its effectiveness exhausted
- Valuation: Act or effect of calculating value on one or more data
- Classification: A way to sort the data according to an established criteria
- Collection: Collection of data for specific purpose
- Communication: To pass on information relevant to data action policies

- Control: Action or power to regulate, determine or monitor actions on the data
- Dissemination: Act or effect of data dissemination, propagation, multiplication
- Distribution: Act or effect of disposing of data according to an established criteria
- Deletion: Act or effect of deleting or destroying data from the repository
- Extraction: The act of copying or removing data from the repository in which it was located
- Modification: Act or effect of changing data
- Processing: Act or effect of processing data
- Production: Creation of assets and services from data processing
- Reception: Act of receiving the data at the end of the transmission
- Reproduction: Copying pre-existing data obtained via any process
- Transfer: Moving data from one storage area to another, or to a third party
- Transmission: Moving data between two points via electric, electronic, telegraph, telephone, radio-electric, pneumatic, etc., devices.
- Use: Act or effect of the use of data.
- Shared use of data: Communication, dissemination, international transfer, interconnection of personal data or shared processing of personal databases by public bodies and entities in compliance with their jurisdiction, or between these and private entities, reciprocally, with specific authorization, for one or more methods of processing permitted by these public entities, or between private entities.

26. THE COMPANY AND THE SECURITY POLICY

All the standards set forth herein are intended to protect the institution against improper access to computerized systems.

Upon receiving a copy of the Security Policy, the employee commits to respect all topics covered herein and is aware that their emails and internet browsing may be monitored.

The security team is fully available to answer questions and provide technical assistance.

27. SITUATIONS NOT COVERED

This Policy presents general directives, and some specific situations may not be covered.

What is expected in these cases is that each one acts with responsibility, prudence and ethical conscience, evaluating the best way forward with the certainty that the appropriate solution will always be governed by the values we cherish.

Any questions not specified in this document and related to the topics ethics and conduct, should be submitted for evaluation by the Executive Board.

It is the responsibility of the Human Resources Department to keep this document up to date, in accordance with the one published by the group internationally, making its content known to all in the DMS Group.

28. TERM

This Code will be in force on the date of its publication, revoking and replacing any previous communication on the subject and will remain in force for an indefinite period.

29. REVIEW HISTORY

Review	Date	Description
00	10/18/2018	Issuance of the document.
01	09/28/2020	General revision to include new commitments to the environment, health and safety of associates and information security and coding in the document.
02	12/01/2020	General revision to change the term web and clouds for web and cloud and modify the document template.

30. APPROVAL AND CLASSIFICATION OF INFORMATION

Elaborated by:	Wellington Ferreira	
Revised by:	Natalie Corrêa	
Approved by:	Eduardo Reis	
Level of confidentiality:	X	Public Information
		Internal Information
		Confidential Information
		Restricted Information

Annex I - Information Security Policy Commitment Term

I hereby declare, for all purposes, that I have received a copy of the Information Security Policy from DMS LOGISTICS, which was in clear and easy to understand language, so that I assume that I am aware of my responsibility and I commit myself to fulfill it and to fully respect it.

I also declare that I am aware of compliance in all situations and circumstances that are directly or indirectly linked to my activities at DMS LOGISTICS.

In the same way, I am aware that failure to comply with any of the terms provided in this Information Security Policy will lead to the formation of an administrative inquiry, which will be constituted to investigate any irregularities.

Continuous act, in view of the finding of irregularities, I hereby declare that I am aware that DMS may take the appropriate measures, both in the administrative and judicial fields, aimed at repairing all damages caused, whether in the criminal, civil or labor spheres..

Finally, in witness whereof, I hereby sign the present instrument.

Place and Date	
Full name	
CPF	
Signature	

WE NEVER COMPROMISE ON QUALITY AND BUSINESS ETHICS

WE NEVER COMPROMISE ON QUALITY AND BUSINESS ETHICS

WWW.DMSLOG.COM