DMS LOGISTICS

INFORMATION SECURITY AWARENESS POLICY

Code: POL-TI-004

Revision: 01

Data: 16/01/2023

CONTROLE DE QUALIDADE
APROVADO DMS LOGISTICS
ISO 9001:2015

1. BACKGROUND

The Information Security Awareness Policy establishes the requirements to assist managers of Information Technology (IT) systems, administrators and users of DMS LOGISTICS' systems and data to ensure that the company's systems and data are adequately protected. Our employees are the front line to protect the company's data assets and this policy will help provide consistent guidance and general approach to security awareness.

The purpose of DMS LOGISTICS' Information Security rules is to ensure the protection of its information assets against threats, internal or external, minimize any risks to information security, reduce exposure to loss or damage resulting from security breaches and ensure that adequate resources are available, maintaining an effective security program and making its Employees aware of it.

DMS LOGISTICS works to establish and continuously improve a corporate culture inInformation Security, compatible with the acceptable use of information and the assets that support it, in order to minimize risks and create a safe environment for the performance of the Company's activities.

2. PRINCIPLES

The basic principles of this Policy are:

- The preservation of the image of the company and its employees;
- The creation, development and maintenance of information and communications security culture;
- That the level, complexity and costs of Information and Communications Security actions are appropriate to the value of DMS LOGISTICS' assets, considering the impacts and the probability of occurrence of incidents;
- The preservation of joint and several liability for data of other companies that travel in the assets of DMS LOGISTICS.

3. INFORMATION SECURITY AWARENESS PLAN

The Information Security awareness plan is a formal process, with institutional procedures to educate employees about the necessary care with the technology resources ofDMS LOGISTICS to ensure the security of the data, devices and programs under the ownership and/or responsibility of the company.

DMS LOGISTICS maintains an annual Information Security Awareness plan in accordance with ISO 27001.

It is understood that awareness is the fundamental agent where DMS LOGISTICS stakeholders acquire critical mass about vectors of threats to their activities and risk awareness.

The goal is to reinforce the faithful understanding and understanding of the pillars:

- Integrity;
- Availability;;
- Confidentiality;
- Authenticity;

They are part of the collective thinking of our organization.

We have an annual Information Security Awareness plan, which follows the following guidelines:

- Training on risk management;
- Training on Information Security;
- Hackathon for IT teams to find vulnerabilities, encouraging PO's (Product Owner) to do a secure development (DEVSECOPS).

According to ISO 27001, control A.6.3 proposes security awareness as mandatory for all employees, including employees, contractors,interns and those who are involved in any way with IT systems. By understanding that DMS LOGISTICS is a "Data Company" company, all our employees receive training.

In an effort to educate DMS LOGISTICS employees in understanding their responsibility in protecting systems and data, information security awareness training will include the following topics:

- The company's policy for the protection of IT systems and data, with special emphasis on sensitive IT systems and data;

- the concept of separation of functions;
- Prevention and detection of information security incidents, including those caused by malicious code;
- Proper disposal of data storage media;
- Proper use of encryption; (bitlocker or other)
- Access controls, including creating and changing passwords and the need to keep them confidential;
- DMS LOGISTICS' acceptable use policies;
- DMS LOGISTICS remote access policies (vpn usage);
- Intellectual property rights, including software licensing and copyright issues;
- Responsibility for data security;
- Phishing.

4. AUTHORITY, RESPONSIBILITY AND DUTIES

The roles and responsibilities of the Information Security Awareness Plan are assigned to individuals and may differ from the individual's actual job title or job title. Individuals may be assigned multiple roles, provided that these assignments provide adequate separation of duties, adequate protection against the possibility of fraud, and do not lead to a conflict of interest.

Employees using DMS LOGISTICS' IT systems must:

- Complete an annual online security awareness training course every twelve (12) months. All newly hired employees must complete the Information Security Awareness Training course within the first 30 days from the date of hiring or before receiving access to the company's IT systems and data .
- Additional security awareness training may be required by all employees at other intervals when the IT infrastructure environment changes.
- Read the "Acceptable Use Policy", Information Security Policy E D and more related to the work performed and sign the Term of Commitment and

Responsibility for Directors and Employees (Annex to the PSI), which recognizes that they are fully aware of the best security practices, their roles in protectingDMS LOGISTICS' systems, data, and information technology resources. Access to DMS LOGISTICS' computer technology environments will not be granted without this agreement.

– Supervisors, Managers and Directors, shall:

- Ensure that each employee under their supervision has participated in and completed the Safety Awareness Training and include the training as part of the employee's annual performance evaluation.
- Keep a copy of each employee's Security Awareness Training certificate in the department's personnel file.
- Managers will ensure that DMS LOGISTICS members who manage, manage, operate or design IT systems receive additional information security training based on their roles as they deem appropriate and that is compatible with their level of expertise, role and responsibilities.

– System owners and administrators shall:

- Facilitate and participate in hands-on cybersecurity training exercises on an *ad hoc* basis that simulates cyberattacks and threats for situational and business readiness.
- Complete annual role-based training (or more frequent breaks based on company needs) and keep training records.

– Data Owners shall:

- Complete annual role-based training (or more frequent breaks based on company needs) and keep training records.

– Chief Information Security Officer shall:

- Align The Information Security Awareness Program of DMS LOGISTICS with the best practices of the sector.
- Supervise DMS LOGISTICS' Information Security Awareness program, including development, implementation and testing.
- Coordinate, monitor and follow the completion of the Information Security Awareness Training for all members of DMS LOGISTICS and report

incomplete training to the person in charge.

- Develop role-based training and maintain training records for the entire program.

5. IMPLEMENTATION AND UPGRADE

The Information Security Awareness Plan of DMS LOGISTICS must be updated whenever necessary or in an interval not exceeding 01 (one) year.

6. NON-CONFORMITY

In cases where it is determined that a violation of DMS LOGISTICS' policies has occurred, corrective measures will be taken, including restriction of access to services or initiation of disciplinary action, which may result in dismissal.

7. APPENDIX A - SCHEDULE OF CAMPAIGNS OF THE INFORMATION SECURITY AWARENESS PLAN

The performance of training in Information Security is a requirement required by ABNT NBR ISO 27001 through control A.6.3, which determines that all members of the organization must receive appropriate training, education and awareness.

The need for this is due to the fact that an employee can also become a vector of vulnerability for the organization when he does not understand concepts of Information Secret, that is, to ensure even more security for the company's systems and data, it is necessary that its employees understand fundamental concepts about Information Security.

This document aims to present an action plan for the realization of the lectures on Information Security Awareness of DMS LOGISTICS.

7.1. Training

These trainings are held internally at DMS LOGISTICS, with lectures and winds for the employees of the organization to know more about Information Security.

The trainings are subdivided into 3 phases of development:

- Preparation - Refers to the integral process of preparation of the training, choice of theme,lectures, activities performed, date of execution;

- Execution - Covers the entire phase of dissemination of the training, going through the realization of the event, until it is finalized;
- Collection of evidence - In this last stage, evidence is collected about the performance of the training and about the presence of the employees in the event.
  - XX/2023

First training with the DMS LOGISTICS team in the year 2023, during the first semester.

In this training the theme addressed was XX.

Training XX/2023			
Month/Year	**Theme**	**Objective**	**Accountable**
XX	XX	XX	XX

Speakers	Beginning	Progress	Status	End
XX	XX	0%	XX	XX

8. DECLARATION OF COMMITMENT

When there are new DMS LOGISTICS Officers, Employees, Service Providers and Partners, they undertake to follow and implement the DMS LOGISTICS Policies.

9. REVISION HISTORY

Revision	Data	Description
00	16/01/2023	Issuance of the document.
01	27/02/2023	General revision for coding in the document.

10. APPROVAL AND CLASSIFICATION OF INFORMATION

Prepared by:	CyberSecurity Team	
Reviewed by:	Leonardo Sabbadim	
Approved by:	Victor Gonzaga	
Level of Confidentiality:	X	Public Information
		Internal Information
		Confidential Information
		Confidential Information

DMS LOGISTICS

WE NEVER PUT QUALITY OR ETHICS AT RISK IN BUSINESS

WE NEVER COMPROMISE ON QUALITY AND BUSINESS ETHICS

WWW.DMSLOG.COM