CLEAN DESK AND CLEAR SCREEN POLICY

Code: POL-TI-009
Revision: 01
Data: 27/02/2023

WWW.DMSLOG.COM

1. OBJECTIVES

The purpose of this document is to establish the minimum requirements for maintaining a "clean" work environment, in which data and information relating to employees, customers, intellectual property, partners and service providers are protected and kept safe, making it difficult for unauthorized persons to access.

Through best practices in the day-to-day of the physical and virtual work environments of DMS LOGISTICS, this regulation outlines guidelines that aim to ensure the privacy, confidentiality, integrity and security of the data held by the company.

2. BACKGROUND

DMS LOGISTICS, in order to use the best practices of the market, adopts ISO 27001, control A.7.7, using the policy of table and clean screen, in order to ensure and align our internal methods with what is practiced in the market.

To improve the security and confidentiality of the company's data, DMS LOGISTICS adopts this Clean Table and Screen Regulations for work environments. This document aims to reduce the risk of unauthorized access, loss or damage to information during and after corporate working hours, or when workstations are empty.

A clear Clean Desktop and Screen policy is an important tool to ensure that all sensitive and confidential materials are removed from the workspace and properly stored when they are not in use or when the user is not present on their workstation. It is a basic but effective initiative to reduce the risk of safety breaches in the workplace, as well as increasing the awareness of employees about the need to protect the company's data and information.

It is applied to employees, outsourced employees, consultants, temporary employees and other employees present in the physical and virtual environments of DMS LOGISTICS, including people related to external service providers.

3. STANDARDS

All employees are required to ensure that all sensitive/confidential information in hard or electronic copy is secure in their area of work at the end of the day and when they are away for an extended period;

- Computer workstations should be locked when the workspace is unoccupied;

- Computer workstations should be completely shut down at the end of the workday;

- Any restricted or sensitive information must be removed from the table and locked in a drawer or in a safe and separate place when the table is unoccupied and at the end of the working day;

- File lockers containing restricted or confidential information should be kept closed and locked when not in use;

- Keys used for access to restricted or confidential information should not be left on an unattended desk;

- Passwords should not be left on sticky notes pasted on or under the computer, nor may they be left in an accessible place;

- Internal or confidential documents in electronic media should be stored in environments with controlled access and passwords to prevent access to unauthorized persons;

- Notes, messages, and reminders should not be left on display on the table or pasted on the desktop, notebook, monitor, bulletin boards, or walls;

- Avoid printing documents that can be read on the desktop and notebook;

- Printouts containing restricted or confidential information should be removed immediately from the printer;

- All printed documents must be destroyed before being disposed of in the trash. Documents classified as confidential and restricted must be

destroyed using defragmenting machinery or incinerated;

- Personal belongings should always be stored, either in your closet or in your purse;

- Your password is personal and non-transferable, so don't pass it on to anyone;

- Do not put on the table glasses with water, juices, coffee, etc.

- Do not write down information classified as restricted, confidential,sensitive in places where the information may be exposed, such as bulletin boards, murals and whiteboard;

- Portable computing devices, such as laptops and tablets, should be locked out of use;

- Mass storage devices, such asCDROM, DVD, or USB sticks, should be protected and stored in secure locations;

The Clean Table and Screen Regulations consider:
- the level of information exposed and its safe handling;

- Legal and contractual requirements that require protection of information;

- Identified Organizational pisces;

- Cultural aspects;

- Measures taken to protect tables, devices and media.

Areas with sensitive information of customers, suppliers, product code, and unauthorized access have locks, as well as drawers and cabinets.

4. PROTECTION OF DEVICES AND INFORMATION SYSTEMS

All computers are password protected in downtime and there is segregation of function and area in the offices.

DMS LOGISTICS adopts restrictions on the use of copying and printing technologies and the adoption of a paperless culture. At DMS LOGISTICS we do not encourage the use of printed matter and employees will be guided to fragment

company and personal documents. Any information sent to printers should be collected as quickly as possible.

The company has guidelines for the proper disposal of information left in meeting rooms. All The information on whiteboards is erased and all pieces of paper used during the meeting are fragmented.

4.1.   ADOPTION OF 5S

Throughout its organizational structure, DMS LOGISTICS adopts the 5S methodology, which is an age management program developed in Japan. The 5S program aims to achieve continuous improvement and quality, being a strategic plan that undertakes efforts to:

1.   **Use and classification:** Keep computers, tools, classified documents. This improve internal efficiency, helping to increase the quality of work and facilitating the identification of problems, ultimately improving productivity, avoiding the acquisition and storage of unnecessary items;

2.   **Organization:** identification and organization of each item in the DMS LOGISTICS employee's work area;

3.   **Cleaning:** The DMS LOGISTICS employee is expected to have the owner's attitude, reflecting on the regular cleaning and maintenance of the common and work areas.

4.   **Standardize:** Simplification, standardization of rules to be followed.

5.   **Support:** Maintain what has been accomplished, including all standards regarding the best practices adopted.

Thus, we aim to eliminate waste and create value through the organization of facilities.

The benefits of adopting the 5S methodology:

- Increased profitability: companies can save hours of work, money and other resources;

- More efficient workforce: with standard procedures, staff can focus on what's important;

- Better service: With a more organized, cleaner and streamlined workplace, employees can spend more time providing excellent services;

- Safer workplace: Employees are less at risk and may feel safer inclean, organized work spaces.

5. 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.

All registration and treatment of Non-Conformity shall be carried out as described in POP-SGI-002 - Treatment of Nonconformities.

6. DECLARATION OF COMMITMENT

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

7. REVISION HISTORY

Revision	Data	Description
00	16/01/2023	Issuance of the document.
01	27/02/2023	Review and standardization of the document.

8. 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

WE NEVER PUT QUALITY OR ETHICS AT RISK IN BUSINESS

WE NEVER COMPROMISE ON QUALITY AND BUSINESS ETHICS