Index

REVISION AND APPROVAL HISTORY

Revision No.	Description	Page(s)	Made by	Date	Approved by	Date
1	General Review	All	C.Santos	30/07/2024	B.Azevedo	12/08/2024

Summary

The Clean Desk Screen Policy is a document that reflects the security concerns and considerations regarding the physical protection of the work environment and information assets of ADDVOLT, considering the requirements of the Information Security Management System.

This document aims to achieve the following objectives:

- Regulate the basic pillars of physical security regarding the workplace.
- Establish the base vectors to ensure a clean desk and clean screen to ensure protection against loss and leakage of information.

1. Scope

Physical security at the workplace is an important point for ADDVOLT's Information Security, guaranteeing the implementation of Personal Data Protection and Information Security practices, regardless of their format, by all employees or interested parties, during and after carrying out work activities.
In this sense, this document applies to all employees and stakeholders, regardless of their role, hierarchical position and contractual relationship who have access to a job or information system of ADDVOLT.

2. References, Definitions and Terminologies

None.

3. General Rules

The use of a desk or computer equipment made available by ADDVOLT to its employees, and / or external parties for performing their functions implies responsibilities regarding the exposure of information, either in printed or written format, or in digital format. Following physical security requirements will help ADDVOLT reduce the risk of information theft, fraud or security breach caused by internal, confidential and / or secret information that is available and visible to everyone.

4. Clean Desk Practices

To guarantee the Protection of Personal Data and Information Security in desks and workstations, the following practices must be adopted by all employees interested parties, without exception:

- The desk must be free of documents and objects, except what is essential for carrying out daily tasks;
- Any internal, confidential and / or sensitive information in a physical format must be filed and stored in specific files for that purpose, with conditioned access, whenever the workstation is unoccupied;
- Any information about access credentials should not be left in visible places (e.g. post its on paper or electronically, under computers) let alone be written in places accessible to everyone;
- The printing of confidential and / or secret information must occur under the direct supervision of the issuer of the print order and the documentation must be immediately removed from the printer after printing;
- When disposing of physical documents, whether internal, restricted and / or confidential, they must be shredded using the equipment approved for that purpose;
- Lock and store all portable devices (e.g. portable computers, tablets, smartphones) in case of absence from the workplace when outside Addvolt locations;

- Properly store all mass storage devices (e.g. CD-ROM, DVD, USB) in specific storage locations for this purpose;
- Portable computers must be locked with a locking cable or kept in specific repositories for the purpose;
- Keys that can allow access to cabinets and drawers, or areas that contain internal, confidential and / or secret information, must be stored and kept in a safe place;
- There must be alternative mechanisms (e.g. alternate key) that allow emergency access to documents and information storage devices, but that access should be restricted to authorized personnel only;
- Offices or rooms that contain confidential and / or secret information must be kept closed and locked when not in use;
- Tables of offices and rooms with confidential and / or secret information must be deleted when not needed;
- The keys used to access offices or rooms with confidential or secret information must be handed over to the person responsible for them.

5. Clean Screen Practices

To guarantee the Protection of Personal Data and Information Security on devices such as computers, mobile devices or workstations (i.e. workstations), the following practices must be adopted by all employees and interested parties, without exception:

- The devices must be locked whenever the workstation is unoccupied;
- Devices must be turned off at the end of the workday or for extended periods of absence;
- The automatic screen lock and password protection mechanisms must be configured for a short period of inactivity, up to 5 minutes;
- The locked screen must be protected by a reactivation password.
- Users of mobile devices (e.g. laptops, smartphones, tablets) should pay particular attention to ensuring that the information displayed on the screen is not visible to unauthorized individuals using, for example, blocking filters;
- The computer's working environment must be clean and organized, with no shortcuts to folders, files or locations that contain, or process information considered internal, confidential and / or secret.

5.1. Whiteboards

When it comes to security rules for whiteboards in physical meeting rooms or production plant, here are some best practices to consider:

- Confidential Information: Be cautious about displaying sensitive or confidential information. If you must, ensure the room is secure and only authorized personnel are present.

- Clean Up: Always erase the whiteboard after the meeting to prevent unauthorized access to the information.
- Digital Copies: If you need to keep a record of the whiteboard, take a digital photo or use a whiteboard capture system, then store it securely.
- Access Control: Control who has access to the meeting rooms and monitor entry and exit.
- Awareness: Educate team members about the importance of whiteboard security and the potential risks of leaving information on display.