Clean Desk and Clear Screen Policy

Code	ICT-POL-010
Control	7.7 Clear desk and clear screen 7.8 Equipment siting and protection
Version	2.2
Date of Version	3/6/2023
Created by	Corina Guardado
Approved by	Angel Yanes
Confidentiality level	Confidential
Authorized users	EMAYA employees

Version Control

Date	Version	Change/reviewed by	Description of the change/review by
7/25/2019	0.1	Corina Guardado	Document creation
10/04/2019	1.0	Executive Team	Reviewed and approved
4/17/2020	1.1	Corina Guardado	Aligned Policy with Internal Audit results
5/26/2021	1.2	Corina Guardado	Included roles and responsibilities chart
10/22/2021	2.0	Angel Yanes	Revision
3/22/2022	2.1	Jorge Huezo	Updated document format and content
3/6/2023	2.2	Jorge Huezo	Updated document code

Contents

Introduction

This document defines practices to ensure sensitive information both in physical and in electronic formats are not left exposed at personal and shared workspaces or with shared equipment, when they are not being used, or if an employee must step away from their workstation.

Purpose

The purpose is to guarantee that all employees block their computers when left unattended and to ensure an acceptable level of compliance of 85% on the Internal Audit quarterly check.

Scope

This policy applies to all EMAYA employees and equipment, shared, or assigned, located on EMAYA premises. This policy's content will be communicated to employees through periodic training and awareness.

Clean desk and Clean Screen policy

Workstation protection

Clean Desk policy

When employees are away from their workstations, no objects other than their CPU, Monitors, Keyboard and Mouse shall remain on the workspace; some decoration items are allowed if they do not interfere with cabling or cause an occupation or an information security incident. All printed material, data storage, and documents shall be withdrawn from the workspace and stored in appropriate (locked) areas, to prevent unauthorized access. Computers should be logged out of the user session completely at the end of the workday, making sure to have logged off from information systems to minimize opportunities for unauthorized access. No smart devices that can record information are allowed on the desk; this includes anything from smartphones to smartwatches.

Employees shall abide by the following:

- At the end of the workday, the employee shall store sensitive documents in a safe place and media containing confidential information.
- When printing, any classified or sensitive information should be immediately removed from the printers by the originator.
- Clearing sensitive or critical information on whiteboards and other types of display when no longer required.

Clean Screen Policy

When users need to step away from their workstations, screens should first be locked to avoid unauthorized access to sensitive information. Any workstation left unattended/ unused will automatically lock itself after 3 minutes and will require the user to provide authentication information to gain access again. Employees should also be aware of prying eyes while displaying sensitive information on their screens, taking care to shield screens from unauthorized viewers.

Eating and Drinking

Below is a table detailing the rules for each type of area, the map can be found on **ICT-POL-021 Physical & Environmental Monitoring Policy**.

Level	Description
Critical	No eating or drinking is allowed in these areas under any circumstance
Highly protected	When near information processing facilities only closed drinking containers are allowed, eating is prohibited.

Protected	When near information processing facilities only closed drinking containers are allowed, eating is prohibited.
Public	Eating and drinking is allowed.

Other Practices for Clear Desk and Screen Policy

Shared areas and devices:

Photocopiers and Scanners are located only in administrative areas and are restricted to administrative use. Employees requiring scanned, copied, or printed materials must request authorization from a manager who will in turn request the printed or scanned materials from the Administration. Printed information must not be left unattended in photocopiers or printers. Any unattended information left in printers and scanners should be immediately destroyed. Reuse of printed paper is strictly prohibited.

Shared workspaces such as meeting rooms and training rooms should be cleaned after each use. This means that all paper used during a meeting and left behind should be properly disposed of. All information on whiteboards should be erased and any electronic devices used should be powered down completely.

The IT Department runs a quarterly Internal Audit that checks for compliance with this policy. The violation of this policy becomes a security incident and noncompliance of the norm.

Roles and Responsibilities

Roles	Responsibilities
All Employees	• All personal items shall be withdrawn from the workspace when away • All personal items shall be stored in the locker space or assigned cabinet
Supervisors	• Responsible to request shared workspace use through a ticket • Cleaning up after using a shared workspace with their team
IT Staff	• Guarantee that equipment borrowed for use in shared workspaces is stored appropriately and maintained. • Run internal audits to ensure compliance with the policy • Establish AD policies that help ensure compliance
Admin Staff	• Remove and dispose of any printed documents left unattended on the printer • Store confidential information in the appropriate locations with the appropriate access control.