



CLEAR DESK AND CLEAR SCREEN POLICY

Document Version	24.1.01
Date	May 30, 2024

TABLE OF CONTENTS

1. INTRODUCTION.....	3
2. SCOPE.....	3
3. POLICY.....	3
3.1. POLICY STANDARD.....	3
4. COMPLIANCE.....	5
5. OWNERSHIP AND REVIEW.....	5
5.1. CONTACT INFORMATION.....	5
5.2. DOCUMENT RACI.....	6

1. INTRODUCTION

The ***Clear Desk and Clear Screen Policy*** shall provide for a clear desk free from any sensitive information. Additional intent is to reduce the risks of unauthorized access, loss of and damage to information during and outside normal working hours. Safes or other forms of secure storage methods might also protect information stored therein against disasters such as fire, earthquake, flood, or explosion.

The ***Clear Desk and Clear Screen Policy*** refers to practices related to ensuring that sensitive information and assets (e.g., paper notebooks, laptops, cellphones, tablets, etc.) are not left unprotected at personal workspaces such as the office and public workspaces such as coffee shops, airports, or hotel business centers. This applies when assets are not in use or when someone leaves their workstation, either for a short time or at the end of the day.

Since information and assets at a workspace are in one of their most vulnerable places, the adoption of a ***Clear Desk and Clear Screen Policy*** is one of the top strategies to utilize when trying to reduce the risk of security breaches.

2. SCOPE

This Policy applies to SMA Technologies employees who collect, generate, use, or otherwise handle restricted or confidential information. Since all employees have the potential to handle the types of information described, no employee is exempt and therefore, shall be subject to this ***Clear Desk and Clear Screen Policy***.

3. POLICY

All workers of SMA Technologies (employees, contingent workers, or contractors) who handle confidential or proprietary information shall follow the clear desk policy for papers and removable media storage and clear screen for information processing systems.

3.1. POLICY STANDARD

1. Workers shall be required to ensure that all sensitive/confidential information in hardcopy or electronic form is secure in their work area when they expect to be away from their work area for an extended period of time and at the end of the day.
2. Computer workstations shall be locked with a publicly viewable image when workspace is unoccupied, and all previous work shall not be visible on the screen when locked.
3. Laptop computers require privacy screen protection film to prevent “shoulder surfing” in public areas such as coffee shops, airports, or hotel business centers.

4. Computer workstations shall enforce a limit of 5 invalid login attempts by user in a 20-minute period, and automatically lock the account until unlocked by Business Technology & Information Services if the limit for invalid login attempts is reached.
5. Any confidential, sensitive, or secret authentication information shall be secured during business hours if the employee is away from their desk for an extended period of time. At the end of the day, the information shall be removed from the desk and secured for privacy.
6. File cabinets containing confidential, sensitive, or secret authentication information shall be kept closed and locked when not in use or when not attended for extended periods of time.
7. Keys used for access to confidential, sensitive, or secret authentication information shall not be left at an unattended desk.
8. Common areas should be secured. White boards, easel pads and computer screens displaying sensitive information should not be left unsecured or be visible through outside windows.
9. Computer screens shall be set to display a password-protected screensaver after a maximum of 10 minutes of inactivity.
10. Secret authentication information, such as passwords, shall not be left on sticky notes posted on or under a computer, inside an unlocked desk drawer or file cabinet, nor may they be left written down in an accessible location at any time. Account credentials should be stored in the company sponsored password manager.
11. Users shall mark all media containing confidential or sensitive data indicating the distribution limitations, handling caveats, and applicable security markets in accordance with the **Information Classification and Handling Standard**.
12. All media containing confidential or sensitive data that is to be transferred from the in-scope location shall be recorded, protected, and handled in accordance with the Information Transfer Policy as outlined in the **Information Classification and Handling Standard**, as applicable. Any media to be transferred shall only be transferred by authorized users.
13. Printouts containing confidential, sensitive, or secret authentication information shall be immediately removed from the printer.
14. Secure printing requiring a user to authenticate to the printer before their document is printed shall be used if available by the printer manufacturer.
15. When no longer needed, confidential and/or sensitive documents shall be shredded. For remote workers, such documents should be shredded using a cross-cut shredder prior to final disposal. At no time should such documents be left in an unsecured area.
16. Treat mass storage devices as restricted or confidential information and secure them in a locked compartment when not in use. Some examples of mass storage are, but not limited to: CDROM, DVD R/W, USB, portable HDDs or SSDs, and cell phones.
17. Mass storage devices shall be reported as a security incident when such devices have no identifiable owner.
18. Media to be disposed of shall be securely protected until disposal is confirmed and documented complete.

4. DISPATCH AND RECEPTION OF MAIL IN THE US OFFICE IS HANDLED BY THE EXECUTIVE ASSISTANT OR THEIR DESIGNEE ACCESSIBLE ONLY BY KEY. COMPLIANCE

Periodic evaluations of the employees' compliance with this policy shall be performed. Any violations of this policy could lead to disciplinary action up to and including termination of employment.

5. OWNERSHIP AND REVIEW

This policy is owned by the ISMS Manager.

This policy shall be reviewed on an annual basis.

Changes to this document shall be in accordance with the *ISMS Document and Records Control Standard*.

5.1. CONTACT INFORMATION

Gordy Drost
ISMS Manager/Director of Security
(281)446-5000
gdrost@SMAtechnologies.com

5.2. DOCUMENT RACI

Responsible	Assigned to do the work	ISMS Manager
Accountable	Final decision, ultimately answerable	Executive Leadership Team
Consulted	Consulted BEFORE an action or decision is taken (proactive)	ISMS Steering Committee
Informed	Informed AFTER a decision or action has been taken (reactive)	Named participants in this document. Other parties affected by the change.