SAAI Clean Desk Policy

Document Name: SAAI Clean Desk Policy
Last Updated Date: 24 April 2021
Version: 1.0
Disclaimer

This policy, its attachments, and any rights attaching hereto are, unless the context clearly indicates otherwise, the property of SAAI. It is confidential, private and intended for the addressee only, and may only be used by the addressee for the particular purpose for which the policy has been requested. The addressee shall furthermore treat all personal information that comes to its knowledge or into its possession as confidential and shall not disclose it without the consent of SAAI.

SAAI accepts no liability whatsoever for any loss or damages, whatsoever and howsoever incurred or suffered, resulting or arising from the use of the information in the policy or its attachments.
Overview

SAAI stands committed to the development of secure policies and practices, and in doing so, has implemented this Clean Desk Policy to increase physical security at SAAI's offices. This policy ensures that confidential information and sensitive materials are stored away and out of sight when they are not in use or when the workspace is vacant.

This policy sets forth the basic requirements for keeping a clean workspace, where sensitive and confidential information about SAAI employees, SAAI Members, clients, vendors, and intellectual property is secured.

The policy shall apply to all SAAI employees, contractors, and affiliates.

Policy

1. Employees are required to secure all sensitive/confidential information in their workspace after the workday and when they are expected to be away from their workstations for an extended period. This includes both electronic and physical hardcopy information.
2. Computer workstations/laptops must be locked (logged out or shut down) when unattended and at the end of the workday. Portable devices like laptops and tablets that remain in the office overnight must be shut down and stored away.
3. Mass storage devices such as CD, DVD, USB drives, or external hard drives must be treated as sensitive material and locked away when not in use.
4. Printed materials must be immediately removed from printers or fax machines. Printing physical copies should be reserved for moments of absolute necessity. Documents should be viewed, shared, and managed electronically whenever possible.
5. All sensitive documents and restricted information must be placed in the designated shredder bins for destruction or placed in the locked confidential bins.
6. File cabinets and drawers containing sensitive information must be kept closed and locked when unattended and not in use.
7. Passwords must not be written down or stored anywhere in the office.
8. Keys and physical access cards must not be left unattended anywhere in the office.

It is the responsibility of each Department Manager to ensure enforcement of the policies above. Repeated or serious violations of the clean desk policy can result in disciplinary actions.

If you notice that any of your devices or documents have gone missing, or if you believe your workspace has been tampered with in any way, please notify the company's Information Officer immediately.

This policy needs to be read in conjunction with the policy called “Information Security Policy” to ensure that all the employees in the company, including temporary employees, contractors, and visitors with temporary access to services and partners with limited or unlimited access time to services are aware of the limitations, restrictions, and processes regarding the safeguarding, destruction, deletion or the shredding of documents containing personal information.