**Clean Desk Policy**

**Overview**

A clean desk policy can be an import tool to ensure that all sensitive/confidential materials are removed from an end user workspace and locked away when the items are not in use or an employee leaves his/her workstation. It is one of the top strategies to utilize when trying to reduce the risk of security breaches in the workplace. Such a policy can also increase employee’s awareness about protecting sensitive information.

**Purpose**

The purpose for this policy is to establish the minimum requirements for maintaining a “clean desk” – where sensitive/critical information about our employees, our intellectual property, our customers and our vendors is secure in locked areas and out of sight. A Clean Desk policy is not only ISO 27001/17799 compliant, but it is also part of standard basic privacy controls.

**Scope**

This policy applies to all employees and contractors.

**Policy**

* Employees are required to ensure that all sensitive/confidential information in hardcopy or electronic form is secure in their work area at the end of the day and when they are expected to be gone for an extended period.
* Workstations (desktops or laptops) should be locked and inaccessible to others when personnel are away from their desk, even for a short period of time.
* Workstations should be shut down completely at the end of the day.
* Any Restricted or Sensitive information must be removed from the desk and locked in a drawer when the desk is unoccupied and at the end of the work day.
* When outside the home, laptops should either be locked using a cable or not left unattended for any period of time.
* Passwords should not be written down / stored near workstations, but should be entered in 1Password.
* When outside the home, whiteboards containing Restricted and/or Sensitive information should be erased.
* Treat mass storage devices such as CDROM, DVD or USB drives as sensitive and secure them in a locked drawer

**Policy Compliance**

**Compliance Measurement**The Infosec team will verify compliance to this policy through various methods, including but not limited to, periodic walk-thrus, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

**Exceptions**

Any exception to the policy must be approved by the Infosec team in advance.

**Non-Compliance**

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

**Related Standards, Policies and Processes**

None.

**Definitions and Terms**

None.

**Revision History**

|  |  |  |
| --- | --- | --- |
| **Date of Change** | **Responsible** | **Summary of Change** |
| **June 2014** | SANS Policy Team | Updated and converted to new format. |
| **July 2022** | Ivy Astrix | Initial draft |