**Policy Template**

# Overview

One essential element of information security is a clean desk policy. Keeping your workspace neat and orderly helps prevent theft, loss, and unauthorized access to sensitive data. When not in use, desks, work areas, and shared spaces should be free of confidential materials. This guideline offers best practices for doing so.

# Purpose

This guideline's objective is to offer best practices for keeping a safe and hygienic workspace. By making sure that all private materials are appropriately stored and that workspaces are kept neat and clear of unattended papers or electronics, it seeks to lower the possibility of unwanted access to sensitive data.

# Scope

This policy is applicable to all CITE Managed Services (CITEMS) employees, consultants, contractors, temporary workers, and other staff members. It includes all workspaces where business information is handled, such as offices, meeting rooms, and common areas. Both digital and physical materials, including documents, notebooks, electronic devices, removable media, and any other objects that might display or contain sensitive information, are covered by the guideline.

# Policy

Employees of CITE MS are required to always keep their workspaces tidy and safe. Maintaining a clean desk helps prevent theft, loss, and unauthorized access to private and sensitive data. When not in use, particularly at the end of the workday or when leaving a workstation unattended, we advise that all papers, electronic devices, and removable storage media be securely stored.

When not in use, sensitive materials must be kept safely in locked cabinets, safes, or drawers. Mobile devices should either be kept in the employee's possession or locked in a secure location, and computers and terminals must be locked or turned off when not in use.

It is imperative to promptly retrieve and securely store printed materials that contain proprietary or confidential information from printers. Instead of being thrown in the regular trash, documents meant for disposal should be shredded or put in special confidential waste bins.

After talks or meetings are over, private information should be removed from whiteboards and other display surfaces. Workers are required to make sure that no sensitive notes, passwords, or access credentials are written down or left in plain sight.

# Policy Compliance

* 1. Compliance Measurement

The information security team will use a number of techniques, such as but not restricted to:

* Regular walkthroughs and inspections of the workspace
* Managers or the information security team may conduct sporadic spot checks.
* When appropriate, video surveillance of office spaces
* Checklists for employees' or departments' self-evaluations
* Business tool and facilities management system reports
* Mechanisms for reporting incidents and receiving employee feedback

# Exceptions

The Information Security team must examine and approve any exceptions to this policy beforehand. Only valid reasons will be allowed for exceptions, and to preserve security and compliance, suitable compensating controls must be put in place.

# Non-Compliance

Workers who violate the Clean Desk Policy will be reminded first, and they might also get more training or direction. If there is persistent non-compliance, additional measures may be taken to guarantee that the policy is adhered to and the workplace is kept safe and orderly.

# Related Standards, Policies and Processes

* CITEMS Password Policy
* ISO 27001

# Definitions and Terms

Proprietary: Owned by a private individual or corporation under a trademark or patent.

# Revision History

|  |  |  |
| --- | --- | --- |
| **Date of Change** | **Responsible** | **Summary of Change** |
| 30/10/2025 | Samuel Bailey – CITEMS Cyber Security Team Member | Created Clean Desk Policy |