# **Policy 5.9**: Clean Desktop Policy

**Volume**: 1
**Managing Office**: Information Technology Services (ITS)
**Effective Date**: June 27, 2025
**Authority**: Information Technology Services/CIO

---


**Executive Summary**

The clean desk policy is an important tool to ensure that all sensitive/confidential materials are removed from an end user's workspace and locked away when the items are not in use or an employee leaves their workstation. It is an important strategy to utilize when trying to reduce the risk of security breaches in the workplace. This policy is also designed to increase University faculty and staff security awareness in regard to protecting sensitive information.


## I. Purpose

The purpose of this policy is to establish the minimum requirements for maintaining a "clean desk" – where sensitive/critical information about our faculty, staff, students, our intellectual property, our customers, and our vendors is secure in locked areas and out of site. A Clean Desk policy is in line with various information security frameworks and guidelines; it is also part of any organization's standard basic privacy controls.

## II. Scope

This policy applies to all University faculty, staff, and board members.

## III. Policy

The following principles should be followed to ensure the privacy and confidentiality of user data:

A. 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.

B. Computer workstations must be locked when the workspace is unoccupied.

C. Any Restricted or Sensitive information must be removed from the desk and locked in a drawer when the desk is unoccupied and/or at the end of the workday.

D. File cabinets containing Restricted or Sensitive information must be kept closed and locked when not in use or when not attended.

E. Keys used for access to Restricted or Sensitive information must not be left at an unattended desk.

F. Laptops must be stored securely at the end of the business day.

G. Passwords may not be left on sticky notes posted on or under a computer, nor may they be left written down in an accessible location.

H. Printouts containing Restricted or Sensitive information should be immediately removed from the printer.

I. Upon disposal Restricted and/or Sensitive documents should be shredded in the official shredder bins or placed in the lock confidential disposal bins.

J. Whiteboards containing Restricted and/or Sensitive information should be erased.

K. Lock away portable computing devices such as laptops and tablets.

L. Treat mass storage devices such as external hard drives or USB drives as sensitive and secure them in a locked drawer. Microsoft OneDrive, provided by the University, is the approved file storage medium.

M. All printers and fax machines should be cleared of paper as soon as they are printed; this helps ensure that sensitive documents are not left in printer trays for the wrong person to pick up.

## IV. Compliance

Failure to comply with this Policy and/or regulations promulgated hereunder will be deemed a violation of University Policy and subject to disciplinary action in accordance with the disciplinary guidelines as outlined in the Faculty or Staff Handbook, whichever one is applicable to the individual. The Information Technology Services (ITS) Information Security team will verify compliance with 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.

## V. Exceptions

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

## VI. Revision History

- Initially Approved: June 2025 (Board Approval)

**VII. Authority:** President

**VIII. Responsible Office:** President/Chief Information Officer

## IX. Related Documents

- All other ITS policies and procedures

## X. References:

- The SANS Institute