UNIVERSITY OF DENVER
POLICY MANUAL
WORKSTATION SECURITY AND CLEAR DESK

Responsible Department: Information Security Office **Recommended By**: VC Information Technology, Chief Information Security Officer **Approved By**: Chancellor	**Policy Number** IT 13.01.012	**Effective Date** 10/27/2021

I. INTRODUCTION

The University has implemented certain technical, physical, and administrative controls and safeguards to ensure that workstations restrict access to authorized users. In addition, paper documents must also be secured and protected against unauthorized access.

II. POLICY OVERVIEW

Faculty and staff shall follow appropriate guidelines and procedures for using workstations and maintaining the security of documents in desk and office areas.

III. PROCESS OVERVIEW

WORKSTATIONS

A. Physical access to workstations is restricted to authorized personnel.

B. Faculty and staff must prevent unauthorized viewing of sensitive information on a workstation screen:

1. Faculty and staff must ensure that monitors are positioned away from public view.

2. Faculty and staff must manually activate a password protected screen saver when they leave their desk for an extended period of time.

3. Systems must have a password protected screen saver automatically activated within a short timeout period to ensure that unattended workstations are protected.

C. Prior to leaving for the day, faculty and staff must:

1. Exit running applications and close any open documents.

2. Ensure workstations are left on but logged off in order to facilitate after hours updates.

D. Faculty and staff shall use University workstations for authorized University purposes only.

E. Only approved personnel may install pre-approved software on University workstations.

F. All sensitive information must be stored on network file shares.

G. Laptops shall be secured through the use of cable locks or locking laptops up in drawers or cabinets.

H. The IT Department shall ensure that all workstations use a surge protector (not just a power strip) or a UPS battery backup.

I. Faculty and staff shall keep food and drink away from University workstations in order to avoid accidental spills.

J. University workstations shall have vendor-issued critical security updates and patches installed in a timely manner.

K. University workstations shall have active and updated anti-malware protection software.

L. Faculty and staff shall not disable anti-malware protection software.

<u>DESK AND OFFICE AREAS</u>

M. Faculty and staff who work with sensitive information should have lockable space available for storage of non-electronic information when such information is not in use. Faculty and staff must check with their immediate supervisor or university management if they are not sure what information must be locked up or what lockable storage is available.

N. When leaving their work area, faculty and staff shall ensure that their desk and work area is clear (clear desk) of papers and removable storage media containing sensitive information.

O. Faculty and staff who work with sensitive information should have lockable space available for storage of non-electronic information when such information is not in use. Faculty and staff must check with their immediate supervisor or university management if they are not sure what information must be locked up or what lockable storage is available.

P. Papers and devices containing electronically stored sensitive information (e.g., flash drives, laptops, tablets, etc.) must be locked in a drawer when faculty or staff leave their desks for extended periods of time. Storage areas containing sensitive information must be kept locked when faculty or staff are away from their work areas for extended periods of time. Keys to secure storage areas must not be left in the lock or accessible by unauthorized personnel.

Q. To prevent unauthorized disclosure or access, devices that transmit or print sensitive information (e.g., fax machines, printers) shall have the documents immediately removed from the device by an authorized individual.

R. Documents waiting to be shredded shall not be accessible by unauthorized personnel.

S. The Chief Information Security Officer (CISO) shall ensure processes are in place to:

1. Identify sensitive information (hardcopy and electronic) that must be protected from unauthorized access or disclosure.
2. Identify workstations that must be shut down at the end of the workday vs. powered on at night so they can receive security updates.
3. Laptops containing sensitive information must be secured per Policy IT 2.30.066 - *Mobile Device Use*.

IV. DEFINITIONS

A. **“Sensitive information”** means any information for which loss, alteration, misuse or disclosure could adversely affect the interests of the University or its administration, faculty, staff, students, applicants or relations therein. By default, this includes any such information held by the University whether or not such information is subject to legal protections or restrictions.

V. RESOURCES

A. Policy IT 13.10.010 - *Computer and Network Use*
B. Policy IT 02.30.066 - *Mobile Device Use*
C. Policy IT 13.10. 013 - *Passwords*
D. Policy IT 13.10.014 - *Wireless Access*

Revision Effective Date	**Purpose**