Office of the President
University Policy

SUBJECT:	Effective Date:	Policy Number:	
CLEAN DESK AND CLEAR SCREEN	6-14-20	12.12	
	Supersedes:	**Page**	**Of**
	New	1	3
	Responsible Authorities: Provost Associate Provost and Chief Information Officer Vice President, Administrative Affairs Chief Compliance & Ethics Officer		

APPLICABILITY/ACCOUNTABILITY:

This policy is applicable to all employees, volunteers, and contractors of the University with access to University Data in digital or hardcopy form.

DEFINITIONS:

University Data: Any information maintained by the University or information to which a University constituent is provided access based on the constituent's University status.

Mobile Devices: Any portable electronic computing device that can store data including, but not limited to, mobile phones, tablets, and personal data assistants.

Definitions for data classifications (including Level 1, 2 and 3 information) are found in Policy 12.7 System and Data Classifications.

POLICY STATEMENT:

A clean desk and clear screen policy is an important 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 a user leaves his/her workstation. It is one of the main strategies utilized when attempting to reduce the risk of security breaches in the workplace. Such a policy can also increase employee awareness about protecting sensitive information.

Components of the clean desk policy include the following:

1. All computer workstations and laptops regardless of data classification must be locked or logged out when the workspace or laptop is unoccupied, requiring at least a username and password to unlock except for specific kiosk computers and digital signage.
2. Users are required to ensure that all Level 1 or Level 2 information in hardcopy or electronic form is secure in their work area before leaving for the day by ensuring documents or devices are physically locked away or encrypted.
3. Any hardcopy Level 1 or Level 2 information must be removed from the desk and locked in a drawer when the desk is unoccupied and at the end of the workday.
4. File cabinets and other containers housing hardcopy documents containing Level 1 or Level 2 information must be kept closed and locked when not in use or when not attended.
5. Keys used for access to containers housing hardcopy documents containing Level 1 or Level 2 information must not be left accessible at an unattended desk.
6. Offices or suites with Level 3 information in hardcopy format must be locked when the space is unoccupied if the information is not otherwise secure.
7. Unattended mobile devices and laptops containing or accessing Level 1 or Level 2 information must either be locked with a locking cable or locked away in a drawer, cabinet, or other secure storage location unless the device is fully encrypted by a method approved by the CIO, CISO, or designee(s).
8. Passwords may not be written down and left in any accessible location such as on a sticky note near a computer workstation or in password notebooks.
9. Printouts containing Level 1 or Level 2 information must be removed from printers without undue delay.
10. Upon disposal, hardcopy documents containing Level 1 or Level 2 information must be shredded utilizing shredders with crosscut or confetti-cut cutting patterns or shredded by a third party that provides certificates of destruction. If documents are being utilized in a work-from-home environment, documents need to be kept secure per this policy until it is feasible to return the documents to campus for proper disposal.
11. Whiteboards containing Level 1 or Level 2 information must be erased before leaving a work area.

SANCTIONS

Violations of these policies described herein by an employee is grounds for disciplinary action up to and including termination in accordance with applicable University and the Florida Board of Governors regulations and/or collective bargaining agreements. Such disciplinary actions may also include reprimand or suspension. Violations of these policies by volunteers or contractors are grounds for terminating their access rights and other appropriate sanctions.

Disciplinary or other action taken by the University does not preclude the possibility of criminal actions against an individual violating this policy. The filing of criminal charges similarly does not preclude action by the University.

INITIATING AUTHORITY: Associate Provost and Chief Information Officer

POLICY APPROVAL
(For use by the Office of the President)

Policy Number: _12.12_

Initiating Authority
Signature: _____ Date: _____
Name: _____

Policies and Procedures Review Committee Chair
Signature: _____ Date: _____
Name: _____

President
Signature: _____ Date: _____
Name: _____

Executed signature pages are available in the Office of Compliance