Auburn University at Montgomery
Policies and Procedures

Title: Clean Desk Policy

Responsible Office: Office of Technology

I. PURPOSE

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

II. POLICY

A clean desk policy can be 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 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.

III. EFFECTIVE DATE

December 1, 2017

IV. APPLICABILITY

This policy applies to all departments, faculty, employees, students and contracted personnel (hereafter referred to employees) who, as a part of their official university employment, have access to PII or SPI sensitive/confidential material.

V. RESPONSIBILITY

Policy Responsible Office: Office of Technology
Policy Responsible Executive: Chief Information Officer (CIO)

VI. DEFINITIONS

Sensitive/Confidential Material pertains to personally identifiable information (PII) or sensitive personal information (SPI). FERPA definitions of PII can be found on the AUM website or obtained from the Registrar's office.

VII. PROCEDURES

1. 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.
2. Computers must be locked when workspace is unoccupied.
3. Any confidential or sensitive information must be removed from the desk and placed in a drawer (locked if available) and the office must be locked when the workspace is unoccupied and at the end of the work day.

4. File cabinets containing confidential or sensitive information must be kept closed and locked (if possible) when not in use or when not attended.
5. Keys used for access to confidential or sensitive information must not be left at an unattended desk.
6. 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.
7. Printouts containing confidential or sensitive information should be immediately removed from the printer.
8. Upon disposal, confidential or sensitive documents should be shredded in the official shredder bins or placed in the lock confidential disposal bins. For disposal of electronic storage media, refer to the Electronic Data Disposal Policy.
9. Whiteboards containing confidential or sensitive information should be erased.
10. Portable computing devices such as laptops and mass storage devices such as CDROM, DVD, USB drives containing confidential or sensitive information must be secured in a locked drawer. Please refer to the Mobile Device Encryption Policy for additional information.

VIII. SANCTIONS

Deliberate disregard of this policy or the protection standards created to implement this policy may be subject to disciplinary action, in accordance with University policies and procedures, and FERPA regulations.

IX. EXCLUSIONS

NONE

X. INTERPRETATION

The Office of Technology CIO has the authority to interpret this policy.

APPROVAL TO PROCEED: ____________ **DATE:** 12-1-17

APPENDICES

NONE