Auburn University at Montgomery
Policies and Procedures

Title: Electronic Data Disposal Policy

Responsible Office: Office of Technology

I. PURPOSE

All computer systems, electronic devices, and electronic media must be properly cleaned of sensitive and confidential data and software before being transferred outside of Auburn University at Montgomery (AUM) or if being repurposed or reused within AUM.

II. POLICY

The large volume of electronic data stored on computer systems and electronic media throughout the University includes confidential and sensitive information, such as student records, financial data, personnel records and research information. The University is subject to: federal laws that set forth responsibilities for protecting this information, copyright laws, and software license agreements that protect vendor rights regarding the use of software.

Unauthorized disclosure of sensitive information may subject the University to legal liability, negative publicity, monetary penalties and loss of funding. Therefore, all sensitive information and licensed software must be properly removed when disposing of computer systems and other electronic media.

This policy outlines the responsibilities for carrying these protective measures.

III. EFFECTIVE DATE

June 1, 2017

IV. APPLICABILITY

This policy applies to all departments, faculty, employees, students and contracted personnel that use or maintain AUM information systems or media.

V. RESPONSIBILITY

The primary responsibility for sanitizing and/or disposal of data that resides on computer systems or electronic media devices rests with the units that procured, purchased, or leased and/or manages the electronic media.

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

VI. DEFINITIONS

Electronic Media refers to any device that can store data and includes, but is not limited to, computers (servers, desktop, laptop and tablets), disk drives, portable disks, backup tapes, CD/DVD-ROMS, flash/thumb drives, portable drives, printers, copiers, cell phones and PDAs.

Sanitization of a hard drive or other electronic medium is the process to render access to target data (the data subject to the sanitization technique) on the media infeasible for a given level of recovery effort.

The categories of sanitization are defined as follows:

- "Clear" applies logical techniques to sanitize data in all user-addressable storage locations for protection against simple non-invasive data recovery techniques; typically applied through the standard Read and Write commands to the storage device, such as by rewriting with a new value or using a menu option to reset the device to the factory state (where rewriting is not supported).
- "Purge" applies physical or logical techniques that render Target Data recovery infeasible using state of the art laboratory techniques.
- "Destroy" renders Target Data recovery infeasible using state of the art laboratory techniques and results in the subsequent inability to use the media for storage of data.

Confidential and sensitive information include, but are not limited to, Social Security Numbers, student educational records, health care records, bank account and other financial information, research data, personnel data, other confidential or sensitive University business information, or any Personal Identification Information (PII) data not listed here.

VII. PROCEDURES

1. Deans, directors and department heads are responsible for ensuring the sanitation of all AUM-owned electronic media in their units.
2. All University employees are responsible for the sanitization of reusable and destruction of non-reusable electronic media before disposal.
3. Software used to sanitize electronic media must be compliant with Department of Defense standards. Any medium that cannot be sanitized with such software must be destroyed using the Office of Technology CIO approved vendors and processes.
4. The Office of Technology will accept for sanitization, any electronic media from any University department.
5. Payment and Procurement Services/Campus Services, referred to as University Surplus, are responsible for the disposal of surplus computer systems and electronic media. University Surplus may either reuse surplus assets within the university or send it off campus to the State Surplus. Any electronic media sent to University Surplus for disposal must have an Electronic Data Disposal Verification form completed by ITS and a "Sanitized" sticker affixed to it indicating that the system has been sanitized. ITS will retain a copy of the completed Electronic Data Disposal Verification form.
6. University Surplus will not accept any electronic media without a" Sanitized" sticker. If the original operating system media and certificate of license are available, they should also be sent to University Surplus with the computer system.
7. Any disposal of electronic media must comply with all environmental regulations.
8. All sensitive and/or confidential University information maintained on electronic media

must be carefully removed in accordance with this Policy before the media are made available for re-use within AUM.

9. Any materials removed from electronic media must be reviewed by the department in accordance with the University Records Disposition Authority and a determination made as to whether the materials need to be retained in another format or location. Additional information and assistance can be obtained from the University State Records Commission Liaison.

VIII. SANCTIONS

Deliberate disregard of this policy or the protection standards created to implement this policy will be considered a Group I infraction under the University Personnel Manual and is subject to disciplinary action, up to and including dismissal.

IX. EXCLUSIONS

NONE

X. INTERPRETATION

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

APPROVAL TO PROCEED: _____ **DATE:** 6-1-17

APPENDICES

Electronic Data Disposal Verification form

AUBURN
MONTGOMERY

Print Reset

ELECTRONIC DATA DISPOSAL VERIFICATION

Owner Information

Description:

Property Control # (if applicable):

CPU Serial #:

Employee Name:

Department:

Campus Telephone #:

Disk Sanitation Information

Date Cleaned:

Cleaned By:

Campus Telephone #:

I verify that all data, programs and the operation system have been removed from this computer in accordance with Auburn University at Montgomery's Information Technology Electronic Data Disposal policy.

X_____ _____

Date