

Electronic Data Disposal Policy

I. POLICY STATEMENT

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 or if being repurposed or reused within Auburn University. When electronic storage devices cannot be sanitized, the media will be destroyed using The Office of CIO approved vendors and processes.

II. POLICY PRINCIPLES

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

April 30, 2016

IV. APPLICABILITY

This policy applies to all departments, faculty, employees, students and contracted personnel that use or maintain Auburn University information systems or media which contains sensitive or confidential information.

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 the electronic media.

V. POLICY MANAGEMENT

Responsible Office: The Office of the CIO

Responsible Executive: Chief Information Officer

Responsible Officer: Information Security Officer

VI. DEFINITIONS

Sanitation of a hard drive or other electronic medium means placing the medium in a condition so that the prior data stored on it cannot be read or recovered.

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-ROMS, flash/thumb drives, portable drives, cell phones and PDAs.

VII. POLICY PROCEDURES

1. Deans, directors and department heads are responsible for ensuring the sanitation of all AU-owned electronic devices and computer systems in their units prior to removal from the AU campus.
2. All University employees are responsible for the sanitation of reusable and destruction of non-reusable electronic media before disposal.
3. Software used to sanitize computer hard drives must be compliant with Department of Defense standards. Any medium that cannot be sanitized with such software must be physically destroyed.
4. The Office of Information Technology will:
 - a. publish guidelines and approved software on the Information Technology Policy website. Sanitization and disposal forms and additional sanitization and data disposal information can also be found on the website.
 - b. accept for destruction, any electronic data storage medium from any University department.
5. Property Services is responsible for the disposition of surplus computer systems and electronic devices. Any computer system or device sent to Property Services for disposition must have an Electronic Data Disposal Verification form (available from the IT website) affixed to it indicating that the system has been sanitized, the date, the name and phone number of the person responsible for sanitizing the system. Property Services will not accept any computer system without this information. If the original operating system media and certificate of license are available, they should also be sent to Property Services with the computer system.
6. Any disposal of computer systems and media must comply with all environmental regulations.
7. All sensitive and/or confidential University information maintained on electronic media must be carefully removed before the media are made available for re-use within Auburn University.

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 the CIO has the authority to interpret this policy.