UTIA IT01XX – MEDIA PROTECTION POLICY

Effective: May 24, 2017
Last Reviewed: April 15, 2019 **Last Updated:** March 18, 2019

Objective:
This policy provides the guidance for protecting and sanitizing media at the University of Tennessee Institute of Agriculture (the Institute). Media protection is critical for securing the confidentiality of the Institute's data by guarding the data from unauthorized access and disclosure throughout the lifetime of the media.

Scope:
This policy applies to media owned, operated, processed, or provided by the Institute. Media includes, but is not limited to, paper, hard drives, random access memory (RAM), read-only memory (ROM), disks, flash drives, memory devices, phones, mobile computing devices, networking devices, and all-in-one printers.

Policy:
Media Use and Retention
Paper media must be retained in accordance with UT Policy FI0120 – *Records Management*. In addition to complying with the retention periods noted in FI0120, the person(s) responsible for the paper media will protect any records containing sensitive data by placing these records in a stored and locked area (e.g., filing cabinet, safe, etc.) with limited access to the locked area. The paper media must be restricted on a need-to-know basis, with access granted to privileged users to the least privileges necessary to perform job responsibilities and using role-based access control (i.e., job classification and function).

All electronic media, or Institute IT assets, classified as moderate according to the UTIA IT0115 – *Information and Computer System Classification Policy*, must be kept in a secure location and maintained accordingly. Users must be given access based on a need-to-know basis, using the principle of least privilege and role-based access control.

Users of any Institute IT assets must use individual login accounts. No group access will be allowed without approval through the Institute's formal exception process. Users must never share passwords with anyone, and anyone needing access to any IT asset at the Institute must go through the proper channels to request that access. UTIA IT0110 – *Acceptable Use of Information Technology Resources Security Policy (AUP)* applies to all Institute employees with access to IT assets.

Any records stored on any Institute IT assets must be properly backed up. The storage of electronic records must comply with all Institute and University policies. Always consult with the Institute's Chief Information Security Officer (CISO) before storing sensitive data.

Media Destruction

All paper media must be destroyed after the appropriate retention period has expired (see FI0120) and provided the department does not need the records for legal, research, or other valid purpose. If the paper media is stored at the Records Management facility, then Records Management procedures must be followed for destruction of the media. If the paper media is stored onsite and contains sensitive data, the department must use a crosscut shredder or some other form of destruction that guarantees the records cannot be reconstructed. Otherwise, a secure shredding company must be used and documents with sensitive data must be placed in a locked bin provided by that company.

Computers must not be handed from one user to another without providing the new user with a clean computer. The unit/department/center/region/county must back up any relevant data, then contact the appropriate local or regional IT representative, or the OIT HelpDesk to request that the hard drive be reimaged, placing a clean image with a new account on the drive. If the hard drive contains sensitive data, the Institute's CISO must be contacted to determine if a DOD (Department of Defense) data wipe, or sanitization, is necessary. The sanitization will place a series of random 1s and 0s across the drive multiple times to ensure no sensitive data can be recovered. If sanitization is necessary, the CISO will determine who will do this process, and then the appropriate IT representative will be called for the imaging to be done.

For any computer being removed from usage, it is important to notify the local or regional IT representative, or the Institute's CISO of any software licensing on the computer that can be transferred from the old computer to a new computer. Often this licensing is done based on the computer and not the person.

For electronic media going to Surplus Property, the department must comply with UT Policy FI0610 – *Surplus Property*. When the department prepares the **Computer/Hard Drive Surplus Form and Certification of Sanitization**, the form must indicate that the hard drive has stored sensitive data, and must be sanitized before the computer can be sold. If any electronic media actually requires destruction, the department must indicate on the form that the hard drive requires complete destruction and cannot be sold. Surplus Property personnel will remove the drive and use a degausser to ensure that the drive is irrevocably destroyed.

Electronic media at the Institute's statewide non-campus locations, must also comply with this policy. For destruction of electronic media, the statewide offices must contact the regional offices' IT staff, who will post items on the online auction site provided by UT Surplus, unless other arrangements have been approved by the Institute's Chief Business Officer.

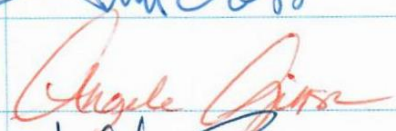
References:

UTIA Glossary of Information Technology Terms
UTIA IT0302 – *Information Technology Formal Exception Policy*
UTIA IT0115 – *Information and Computer System Classification Policy*
UTIA IT0110 – *Acceptable Use of Information Technology Resources Security Policy (AUP)*
UT Policy FI0120 – *Records Management*
UT Policy FI0610 – *Surplus Property*
NIST SP 800-53 – *Security and Privacy Controls for Federal Information Systems and Organizations*
NIST SP 800-88 – *Guidelines for Media Sanitization*

For more information, contact Sandy Lindsey, CISO, at (865) 974-7292, or email sandy@tennessee.edu.

Approval of Policy

We approve UTIA IT01xx – *Media Protection Policy* as described in this document.

Name	Title	Signature	Date
Tim Cross, Ph.D.	Chancellor, UTIA		4/15/2019
Angela A. Gibson	Chief Information Officer, UTIA		4/17/19
Sandra D. Lindsey	Chief Information Security Officer, UTIA		04/15/2019