UTIA IT01XX – SYSTEM AND SERVICES ACQUISITION POLICY

Effective: May 22, 2018
Last Reviewed: April 03, 2019 **Last Updated:** April 09, 2018

Objective:
This policy is to establish and maintain an information security system and services acquisition program that will be used to evaluate third party services and third party products which are acquired to process information. These services and products include all information technology (IT) assets purchased by the University of Tennessee Institute of Agriculture (the Institute).

Scope:
This policy applies to IT assets purchased, owned, operated, or provided by the Institute, as well as all students, faculty, staff, and users who purchase, access, use, or handle the Institute's assets.

Policy:
This policy ensures system development and acquisition are protected by integrating certain security controls into processes used for system and services acquisition, including internal development, purchasing, and outsourcing to ensure information assets are protected. The policy will be reviewed at least annually and updated as needed.

Allocation of Resources
Funds must be allocated for the protection of IT assets. This includes resource allocation for IT asset or service acquisition, sustainment, and supply chain concerns throughout the system development life cycle.

System Development Life Cycle
A system development life cycle process provides the foundation for the successful development, implementation, and operation of Institute-owned IT assets. The Institute will implement a technology refresh schedule of five years for replacing hardware. This schedule will rotate so that in year one, selected hardware will be replaced, followed by a different list of hardware in year two, and so on until completed in year five. At that point all hardware should be replaced and year one begins the refresh cycle again. Replacing obsolete IT assets will decrease security and privacy risks, such as unsupported assets, assets unable to meet security requirements, slow or inoperable assets, or assets from untrusted sources. IT assets that cannot be replaced must documented and approved through UTIA IT0302 – *Information Technology Formal Exception Policy*.

When replacing old and outdated assets, please follow UTIA IT01xx – *Media Protection Policy*.

Acquisition Process

All purchases of IT assets, including systems, system components (i.e., hardware, software, firmware), or system services must follow all requirements in UT Policy FI0405 – *Procurement*. In addition, the following requirements must be included in any acquisition contract for IT assets and should be reviewed by the Institute's Chief Information Officer (CIO), the Institute's Chief Information Security Officer (CISO), or designee:

1. Security and privacy functional requirements;
2. Strength of mechanism requirements;
3. Security and privacy assurance requirements;
4. Security and privacy documentation requirements;
5. Requirements for protecting security and privacy documentation;
6. Description of the system development environment and environment in which the system is intended to operate;
7. Allocation of responsibility or identification of parties responsible for information security, privacy, and supply chain risk management; and
8. Acceptance criteria.

External System Services

The Institute requires that providers of any external system services comply with all security and privacy requirements in Institute policies and procedures, as well as University policies. Any user roles and responsibilities for external service providers will be assigned on a need to know basis and will be clearly documented. In addition, the Institute will monitor security and privacy control compliance by external system services providers on an ongoing basis.

References:

UTIA Glossary of Information Technology Terms
UTIA IT01xx – *Media Protection Policy*
UT Policy FI0405 – *Procurement*
UTIA IT0124 – *Information Technology Risk Assessment Policy*
UTIA IT0302 – *Information Technology Formal Exception Policy*

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

Approval of Policy

We approve UTIA IT01xx – *System and Services Acquisition Policy* as described in this document.

Name	Title	Signature	Date
Tim Cross, Ph.D.	Chancellor, UTIA		5/21/18
Robert L. Ridenour, Jr.	Chief Information Officer, UTIA		5/18/2018
Sandra D. Lindsey	Chief Information Security Officer, UTIA		05/22/2018