UTIA IT0131 – Security Assessment and Authorization Policy

Effective: May 22, 2018
Last Reviewed: April 02, 2019 **Last Updated:** March 23, 2018

Objective:
This policy is to establish the security controls required for the University of Tennessee Institute of Agriculture (the institute) security assessment activities.

Scope:
This policy applies to IT assets owned, operated, or provided by the Institute that are classified as business critical; as well as all students, faculty, staff, and users who access, use, or handle these business critical IT assets.

Policy:
The Institute is responsible for developing a security assessment policy that describes the security controls and control enhancements under assessment, as well as the assessment procedures necessary to determine the effectiveness of security controls. This policy also details the assessment environment and the assessment roles and responsibilities. The policy requires that the outcome of the assessment of security controls will be provided in a report to be shared with the Institute's Chief Information Officer, IT asset owner(s), and appropriate leadership.

Security assessments will include, at a minimum, vulnerability management and system monitoring to maintain the security posture of Institute-owned IT assets during the entire life cycle (see UTIA IT01xx – *System and Services Acquisition Policy*). The following controls will also be implemented.

System Interconnections
The Institute authorizes connections from the IT asset to other IT assets through the use of Interconnection Security Agreements. For each interconnection, the interface characteristics, security requirements, and nature of the information communicated will be documented. The Institute will then review and update the Interconnection Security Agreements annually.

Plan of Action and Milestones
The Institute's Chief Information Security Officer (CISO) will develop a plan of action and milestones for each IT asset classified as business critical. The asset owner will document remedial actions to correct system deficiencies noted during assessments and continuous monitoring activities.

Continuous Monitoring

The Institute implements a continuous monitoring program for each business critical IT asset that includes:

- Metrics to be monitored;
- Frequency of monitoring;
- Ongoing security control assessments;
- Ongoing security status monitoring;
- Correlation and analysis of security-related data generated by the assessments and monitoring;
- Response action items resulting from the data analysis; and
- Reporting the results of the assessments.

Penetration Testing

Penetration testing is a specialized type of assessment that is conducted to identify vulnerabilities that could be exploited by adversaries. The Institute may conduct annual penetration testing on certain Institute-owned IT assets. This primarily depends on IT assets with penetration testing based on industry or government requirements.

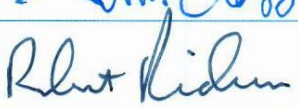
References:

UTIA Glossary of Information Technology Terms
UT Policy IT0131 – *Security Assessment and Authorization*
UTIA IT0115 – *Information and Computer System Classification Policy*
UTIA IT01xx – *System and Services Acquisition Policy*

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

Approval of Policy

We approve UTIA IT0131 – *Security Assessment and Authorization 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