UTIA IT0124P2 – VULNERABILITY ASSESSMENT PROCEDURES

Effective: November 18, 2016
Last Reviewed: March 16, 2018 **Last Updated:** October 13, 2016

Objective:
To ensure compliance with the Vulnerability Management section of UT Policy IT0124 - *Risk Assessment*, certain University of Tennessee Institute of Agriculture (the Institute) systems will be subject to routine vulnerability assessment. Vulnerability assessment will consist of identifying networked assets, scanning for vulnerabilities and potential vulnerabilities, and remediation of all vulnerabilities, including potential vulnerabilities.

Scope:
These procedures apply to all Institute-owned IT assets classified as moderate, high, or business critical. All users are required to be familiar with and comply with these procedures.

Procedures:
The Institute's Chief Information Security Officer (CISO) will initiate the vulnerability scans on a monthly basis during a time that will not affect normal network operations. These scans will be run using Qualys Enterprise Suite.

The Institute's CISO will produce a report for each system that has been scanned. The report will include all vulnerabilities and potential vulnerabilities associated with the system. The report will also include pertinent information such as the actual threat, impact, and suggested solution. The report will be sent via UT's Secure Courier email system to the system's owner/administrator. The system owner/administrator will review the report and complete remediation of vulnerabilities based on the level of the vulnerability as outlined below:

Vulnerability Level	Time Frame for Remediation
Urgent	Immediately
Critical	Within 7 days
Serious	Within 30 days
Medium	Within 90 days
Minimal	Within 90 days

Each system owner/administrator will confirm the successful completion of the remediation steps and notify, in writing, the Institute's CISO of completion. The Institute's CISO will run a new vulnerability scan on the system(s) to verify remediation of vulnerabilities. This procedure will continue until all vulnerabilities are remediated and verified by the Institute's CISO.

References:

UTIA Glossary of Information Technology Terms
UTIA IT0124 – *Information Technology Risk Assessment Plan*
UTIA IT0124P1 – *Information Technology Risk Assessment Procedures*
UT Policy IT0124 – *Risk Assessment*

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

Approval of Procedures

We approve UTIA IT0124P2 – *Vulnerability Assessment Procedures* as described in this document.

Name	Title	Signature	Date
Sandra D. Lindsey	Chief Information Security Officer, UTIA		11/18/2016
Robert L. Ridenour, Jr.	Chief Information Officer, UTIA		11/18/2016
Charles Lambrecht	Computer Operations Manager, UTCVM		11/18/16
Brent Lamons	Director of Advising, CASNR		11/18/16
Joel Lown	Coordinator, AgResearch		11/15/16
Emily Tipton	IT Coordinator, UTIA ITS		11-18-16
Cynthia Walker	IT Administrator, Plant Sciences		11-18-16