UTIA IT0135 – System and Information Integrity Policy

Effective: April 17, 2018
Last Reviewed: April 03, 2018 **Last Updated:** March 08, 2018

Objective:
This policy addresses the implementation of selected security controls for the University of Tennessee Institute of Agriculture's (the Institute) information technology (IT) assets to ensure the regular and timely maintenance of those assets, protecting the integrity of the assets and the data on those assets.

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

Policy:
This policy ensures that reasonable measures are in place to protect IT assets classified as moderate, high, or business critical, protecting these IT assets from threats posed by malware and other malicious or unauthorized activity. This policy also ensures that IT asset flaws are identified and addressed in a timely manner. The policy will be reviewed at least annually and updated as necessary.

These Institute-owned IT assets are protected by using the following security controls:

Flaw Remediation
The Institute's Chief Information Security Officer (CISO) will do regular assessments of IT assets classified as moderate, high, or business critical, identifying, reporting, and correcting software flaws. One way of identifying such flaws is through processes detailed in the UTIA IT0124P2 – *Vulnerability Assessment Procedures*, checking for Common Weakness Enumeration (CWE) or Common Vulnerabilities and Exposures (CVE). The Institute will test software and firmware updates relation to flaw remediation for effectiveness and potential issues before installations. The Institute will install security-relevant software and firmware updates within 30 days of their release, and will incorporate flaw remediation into the Institute's configuration management process.

Malicious Code Protection
IT assets must have an approved antimalware application(s) installed with the intent to detect, block, quarantine or eradicate known malicious code. Any approved application will be

configured to automatically update and to run regular scans, and will alert the user if any such malicious code is detected.

Information System Monitoring

The Institute's CISO or designee will monitor IT assets to detect attacks, indicators of potential attacks, and unauthorized connections. Any detection of such activity will be immediately reported to the Institute's CISO and the IT asset owner. The Institute's CISO will work with the IT asset owner to ensure the integrity of the monitoring tools and the information collected from those tools.

Spam Protection

The Institute will rely on the UT Knoxville's Office of Information Technology email administrators and the spam protection mechanisms they have in place, as OIT owns the email system the Institute uses.

Information Handling and Retention

The Institute handles and retains data within an IT asset, in addition to information output from the IT asset in accordance with Institute policies and procedures; University policies; applicable local, state, and federal laws; and other applicable directives, policies, regulations, standards, and requirements.

References:

UTIA Glossary of Information Technology Terms
UT Policy IT0135 – *System and Information Integrity*
UTIA IT0124P2 – *Vulnerability Assessment Procedures*
UTIA IT0125 – *Information Technology Configuration Management Policy*
UT Policy FI120 – *Records Management*

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

Approval of Policy

We approve UTIA IT0135 – *System and Information Integrity Policy* as described in this document.

Name	Title	Signature	Date
Tim Cross, Ph.D.	Chancellor, UTIA		4/17/18
Robert L. Ridenour, Jr.	Chief Information Officer, UTIA		4/17/2018
Sandra D. Lindsey	Chief Information Security Officer, UTIA		04/16/2018