UTIA IT0127 – AUDIT AND ACCOUNTABILITY POLICY

Effective: September 19, 2017
Last Reviewed: March 25, 2019 **Last Updated:** August 02, 2017

Objective:
This policy has been established to adapt and maintain a formal documented program for the monitoring, management, and review of any University of Tennessee Institute of Agriculture (the Institute) IT assets, application, network, or user activity. This policy also includes the procedures for guiding the implementation and management of audit controls and records.

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

Policy:
This policy addresses the following audit controls:

1. Audit events
2. Audit records
3. Audit storage capacity
4. Audit review, analysis, and reporting
5. Audit records retention

Audit events
An event is any observable occurrence within an Institute IT asset. Audit events are identified as those events that are significant and relevant to the security of the Institute's IT assets and the environments in which they operate in order to meet specific and ongoing audit needs. Audit events include any auditable event required by applicable local, state, and federal laws, as well as directives, policies, regulations, and standards.

The details logged for each event may vary, but at a minimum should include:

- Time stamps, mapped to either Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT)
- Event, status, and/or error codes
- Service, command, or application name
- Account associated with an event
- Device used (source and destination IPs, web browser, etc.)

Audit records

An audit record is generated by the IT asset and contains information establishing what type of audit event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of individuals or subjects associated with the event. The audit record content should contain only that information explicitly needed for specific audit requirements, as audit trails and audit logs may produce some information that may be misleading or could make it more difficult to locate the appropriate information. The baseline configuration must include the appropriate content settings to support the centralized management and configuration capability of the Institute's IT assets.

Audit records should include:

- Password changes
- Successful and failed logons
- Failed accesses related to the Institute's IT assets
- Administrative privilege usage
- Third-party credential usage

Audit storage capacity

Audit records should be maintained for a period as designated by the baseline configuration. Sufficient audit storage capacity reduces the likelihood of exceeding capacity, thereby resulting in loss of auditing capability. When possible, off-loading audit records onto a different IT asset than the one that is being audited will preserve the confidentiality and integrity of audit records.

Audit review, analysis, and reporting

Audit review, analysis, and reporting covers information security-related auditing performed by the Institute and may include monitoring of:

- Account usage
- Remote access
- Wireless connectivity
- Mobile device connection
- Configuration settings
- System component inventory
- Use of maintenance tools and nonlocal maintenance
- Physical access
- Use of VoIP

Questionable findings must be immediately reported to the Institute's Chief Information Security Officer (CISO) or to the incident response team for review and analysis. The CISO will integrate the analysis of audit records with the analysis of vulnerability scanning reports, performance data, IT asset monitoring information, and any other monitoring capabilities to further enhance the ability to identify inappropriate or suspicious activity. The CISO will also

correlate information from audit records with records obtained through physical monitoring and non-technical sources (e.g., human resource records or legal requests).

The Institute may need to adjust of the level, scope, and frequency of audit review, analysis, and reporting when there is a change in risk based on new information received. The CISO will oversee any necessary adjustment.

Audit records retention

Audit records must be retained by the Institute until it is determined they are no longer needed for administrative, legal, audit, or other operational purposes. This includes retention and availability of audit records relative to Freedom of Information Act (FOIA) requests, subpoenas, and law enforcement actions. Retention is necessary for any after-the-fact investigations of security incidents, as well as to meet regulatory requirements and UT Policy FI0120 – *Records Management*.

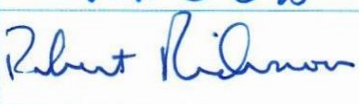
References:

UTIA Glossary of Information Technology Terms
UTIA IT0125 – *Information Technology Configuration Management Policy*
UTIA IT0122 – *Information Security Incident Response Policy*
UTIA IT0122P – *Information Security Incident Response and Reporting Procedures*
UTIA IT0110 – Acceptable Use of Information Technology Resources Security Policy (AUP)
UT Policy IT0127 – *Audit and Accountability*
UT Policy FI0120 – *Records Management*
NIST SP 800-53 – *Security and Privacy Controls for Federal Information Systems and Organizations*

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

Approval of Policy

We approve UTIA IT0127 – *Audit and Accountability Policy* as described in this document.

Name	Title	Signature	Date
Tim Cross, Ph.D.	Chancellor, UTIA		9/18/17
Robert L. Ridenour, Jr.	Chief Information Officer, UTIA		9/17/2017
Sandra D. Lindsey	Chief Information Security Officer, UTIA		09/14/2017