UTIA IT0127P – AUDIT AND ACCOUNTABILITY PROCEDURES

Effective: April 25, 2018
Last Reviewed: March 23, 2018 **Last Updated:** March 23, 2018

Objective:
These procedures have been established to detail the implementation and management of audit controls and records based on UTIA IT0127 – *Audit and Accountability Plan* for any University of Tennessee Institute of Agriculture (the Institute) IT assets, application, network, or user activity.

Scope:
These procedures apply 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 IT assets.

Procedures:
These procedures address 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
Audit events include any auditable event required by Institute policies and procedures; University policies; Office of General Counsel; Human Resources; applicable local, state, and federal laws; as well as industry directives, policies, regulations, and standards.

The details logged for each event can vary, but may 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.)
- Password changes
- Successful and failed logons
- Failed accesses related to the Institute's IT assets
- Third-party credential usage

Audit Policy, in the Windows Local Security Policies, will be configured differently for those IT assets classified as low and those IT assets classified as moderate, high, or business critical. These will be a part of the baseline configuration.

Audit records

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:

- Type of event that occurred
- When the event occurred
- Where the event occurred
- Source of the event
- Outcome of the event
- Identity of any individuals or subjects associated with the event

Audit storage capacity

Audit records should be maintained for a period as designated by the baseline configuration. When possible, off-loading audit records onto a different IT asset than the one that is being audited (i.e., large capacity external hard drive) 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 non-local 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 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 CISO will oversee any necessary adjustment of the level, scope, and frequency of audit review, analysis, and reporting when there is a change in risk based on new information received

Audit records retention

Appropriate retention is necessary for any after-the-fact investigations of security incidents, as well as to meet UT Policy FI0120 – *Records Management*. Audit records retention will be consistent with the requirements in all Institute IT security plans and procedures; University policies; industry and government standards; and state, local, and federal laws.

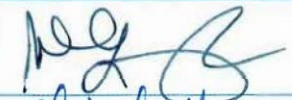
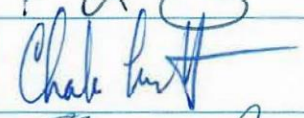
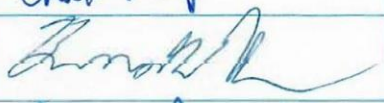
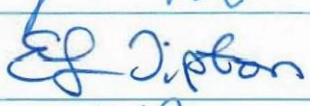
References:

UTIA Glossary of Information Technology Terms
UTIA IT0127 – *Audit and Accountability Plan*
UTIA IT0125 – *Information Technology Configuration Management Plan*
UTIA IT0110 – *Acceptable Use of Information Technology Resources Security Plan (AUP)*
UTIA IT0122 – *Information Security Incident Response Plan*
UTIA IT0122P – *Information Security Incident Response and Reporting Procedures*
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 Procedures

We approve UTIA IT0127P – *Audit and Accountability Procedures* as described in this document.

Name	Title	Signature	Date
Sandra D. Lindsey	Chief Information Security Officer, UTIA		04/24/2018
Charles Lambrecht	Computer Operations Manager, UTCVM		4/20/18
Brent Lamons	Director of Advising, Herbert College of Agriculture		4/20/18
Joel Lown	Coordinator, AgResearch		4/20/18
Emily Tipton	IT Coordinator, Extension		4/23/18
Kristy Keel-Blackmon	Communications Specialist, Forestry, Wildlife and Fisheries		4/20/18
Joanne Logan	Associate Professor, Biosystems Engineering and Soil Science		4/20/18