UTIA Information Technology Security Standard: IT0017 UTIA - Information Security Incident Response Reporting Procedures	
Version: 04	Effective Date: 09/01/2014

Objective:
This document describes the appropriate procedures for reporting a security incident as detailed in UTIA IT0122 – Information Security Incident Response Plan.

Scope:
These Incident Response Reporting Procedures apply to all units of the University of Tennessee Institute of Agriculture (UTIA), including contractors and consultants who manage or utilize IT assets, as well as individuals accessing those assets. These procedures must be followed in the event of a security incident or possible incident. Reportable information security incidents will be treated as an incident until procedures have ruled out an actual incident.

Reportable Information Security Incidents:
Although not an all-inclusive list, any of the following can be considered a security incident:

- Suspicious computer activity including, but not limited to:
    - Unusual connections
    - Unusual logon attempts or successful logons
    - Excessive bandwidth consumption
    - Copyright infringement
    - Malicious network or system sweeps or scans
    - Significant degradation of computer performance
- Suspected compromise of IT resources including, but not limited to:
    - Ransomware attacks
    - Spear phishing attacks
    - Stolen UTIA-owned IT assets
    - Malicious attacks against systems
    - Denial of service attacks
    - Malware
        - Phishing attempts
        - Clicking on suspicious links
        - Opening unrequested email attachments
    - Compromised user accounts
- Suspected breaches of moderate or internal use data. Examples of moderate data include:
    - Personally Identifiable Information (PII)

- HIPAA data
- FERPA data
- PCI data
- Legally protected Human Resources data
- Research data protected by contract
- Self-declared critical data
- Patent data

- Misuse of IT assets according to UTIA standards and procedures; University policies; industry and government standards; and applicable local, state, and federal laws

Procedures for Reporting a Security Incident:

- End User Responsibilities
  1. Stop all work on the computer and contact your local or regional IT support personnel.
  2. Advise the local or regional IT support personnel if your system is classified as low, moderate, high, or business critical.
     - ❖ If a local or regional IT support person is not available, immediately contact the UTIA Chief Information Security Officer (CISO).
     - ❖ Please contact the OIT HelpDesk for reporting a security incident only in the event you are unable to reach a local or regional IT support person, or the UTIA CISO and be certain to tell them you are with UTIA.
- Local/Regional IT Support Personnel Responsibilities
  1. Quickly and briefly investigate system anomalies to assess if an information system security incident is in progress or has occurred.
  2. Create a trouble ticket in utk.teamdynamix.com, completing all mandatory fields. If a security incident has not occurred, please proceed to step 5.
  3. If the system is classified as moderate, high, or business critical, then
     a. Do not turn the system's power off.
     b. Disconnect all network connections.
     c. Contact the UTIA CISO immediately.
     d. Wait for direction from the incident response team before taking any further action.
  4. If the system is classified as low, then
     a. Run necessary scanning services as listed on UTIA's Security website.
     b. Contact the UTIA CISO for additional support, if necessary.
     c. Remediate the IT asset by reimaging or per other departmental guidelines if necessary (i.e., scan hard drive with additional tools, rebuild, etc.).
     d. Update the ticket in FootPrints, logging results.
  5. Local/regional IT support personnel will close utk.teamdynamix.com security tickets for systems classified as low, while the UTIA CISO will review and close all tickets for systems classified as moderate, high, or business critical as related to security incidents.

- UTIA CISO Responsibilities
  1. Provide advice and assistance to all users.
  2. Determine who is on the Incident Response Team and provide oversight.
  3. Provide a checklist to the Incident Response Team to ensure all procedures are completed.
  4. Work with the Incident Response Team to determine if an incident has occurred and the severity of the incident.
  5. Perform follow-up activity with the Incident Response Team.
  6. Maintains all documentation for all system security incidents.
  7. The UTIA CISO will submit a detailed report to the UT System Administration CISO for appropriate state reporting.

Work should be conducted within the UTIA organizational tree to quantify the personnel time required for dealing with the incident (including time necessary to restore systems). Analyzing the personnel work time associated with an incident will help those who may be prosecuting any suspected perpetrators and will aid in the justification of funding for future security initiatives.

Refer to UTIA IT0122 – Information Security Incident Response Plan to ensure that all other requirements have been met.

References:
UTIA Glossary of Information Security Terms
UTIA IT0122 – Information Security Incident Response Plan
UT Policy IT0122 – Security Incident Reporting and Response
UTIA IT0115 – Information and Computer System Classification Standard
UTIA IT0110 – Acceptable Use of Information Technology Resources Security Plan (AUP)

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