UTIA IT0122P – Information Security Incident Response and Reporting Procedures

Effective: September 1, 2014
Last Reviewed: March 28, 2019 **Last Updated:** September 13, 2018

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

Scope:
These procedures apply to all units of the University of Tennessee Institute of Agriculture (the Institute), including contractors and consultants who manage or utilize IT assets, as well as individuals accessing those assets. Use these procedures if you believe that you have encountered a security incident.

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
- Compromised IT resources including, but not limited to:
  - Stolen Institute IT assets
  - Malicious attacks against systems
  - Denial of service attacks
  - Malware
  - 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

Procedures:

Reporting a Security Incident

- End User Responsibilities
  1. Stop all work on the computer and contact your local IT representative.
  2. Advise the local IT representative if your system is classified as low, moderate, high or business critical.
- Local IT Representative 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 FootPrints ticket, 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 Institute's Chief Information Security Officer (CISO) at once;
     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 Institute's Security website;
     b. Contact the Institute's 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 IT representatives will close FootPrints security tickets for systems classified as low, while the Institute's CISO will review and close all tickets for systems classified as moderate, high, or business critical as related to security incidents.
  6. The Institute's CISO will submit report to the UT System Administration CISO for appropriate state reporting.

References:

UTIA Glossary of Information Security Terms
UTIA IT0122 – *Information Security Incident Response Policy*
UT Policy IT0122 – *Security Incident Reporting and Response*
UTIA IT0115 – *Information and Computer System Classification Policy*
UTIA IT0110 – *Acceptable Use of Information Technology Resources Policy*
NIST SP 800-61 – *Computer Security Incident Handling Guide*

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

Approval of Procedures

We approve UTIA IT0122P – *Incident Response and Reporting Procedures* as described in this document.

Name	Title	Signature	Date
Sandra D. Lindsey	Chief Information Security Officer, UTIA		01/18/2017
Robert L. Ridenour, Jr.	Chief Information Officer, UTIA		1/20/2017
Charles Lambrecht	Computer Operations Manager, UTCVM		1-20-17
Brent Lamons	Director of Advising, CASNR		1-20-17
Joel Lown	Coordinator, AgResearch		1/20/17
Emily Tipton	IT Coordinator, Extension		1-20-17
Cynthia Walker	IT Administrator, Plant Sciences		1-18-2017