UTIA IT0122 – Information Security Incident Response Policy

Effective: September 1, 2014
Last Reviewed: March 29, 2019 **Last Updated:** September 06, 2016

Objective:
This policy addresses information security incidents that threaten the confidentiality, integrity, and availability (CIA) of the University of Tennessee Institute of Agriculture's (the Institute) information assets, information systems, and the networks that deliver the information. This policy also assures that the response is conducted in a consistent manner, with appropriate leadership and technical resources, in order to promptly restore operations impacted by the incident and determine the potential loss of CIA.

Scope:
This policy applies to all information technology (IT) assets and services for which the Institute is responsible. It applies to any computing device used by the Institute, regardless of ownership, which is used to store Institute data, or which, if lost, stolen, or compromised, could lead to the unauthorized disclosure of Institute data.

This policy does not cover any human subject research information. Incidents of this nature should be referred to the University's Institutional Review Board.

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
- Compromised IT assets including but not limited to:
  - Stolen Institute-owned IT property
  - Malicious attacks against systems
  - Trojan horses
  - Denial of service attacks
  - Malware
  - Compromised user accounts
- Suspected breaches of moderate or internal use data including but not limited to:
  - HIPAA data
  - FERPA data
  - PCI data

    - Legally-protected HR data
    - Research data protected by contract
    - Self-declared critical data
    - Patent data
- Misuse of IT assets according to Institute policies and procedures; University policies; industry and government standards; and applicable local, state, and federal laws

Event Detection and Incident Confirmation Process:
Events can be detected through a variety of technical and procedural mechanisms. Technical mechanisms include intrusion prevention/detection systems (IPS/IDS), Security Information and Event Management (SIEM) systems, and firewalls which produce alerts when suspicious network activity is detected. Procedural mechanisms include system log reviews, observations of abnormal resource utilization and suspicious account activity. Additionally, sources external to the University (MS-ISAC, REN-ISAC, DMCA) may detect issues by recognizing unauthorized activity or abnormal behavior on their systems and reporting the activity to the University.

Reporting Requirements:
Unless evidence collection and network monitoring are immediately initiated, critical information may be destroyed before investigators have a chance to review it. Institute personnel have the responsibility to report events to their respective IT support personnel in a timely fashion. The IT support personnel will then gather the necessary information to appropriately record the security event using the incident response procedure. Please reference the Institute's security website (https://UTIAsecurity.tennessee.edu) for the IT support personnel contact information.

Analyzing the Cost of the Incident:
Work should be conducted within the 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.

Follow-up:
Performing follow-up activity is one of the most critical actions in responding to incidents. This helps the Institute improve their incident handling processes, as well as aiding in the continuing support of any efforts to prosecute those who have broken the law or abused any Institute-owned IT assets. The incident response team will determine whether a follow-up is needed.

Follow-up actions may include the following:
- Define the "lessons learned"
- Analyze what has transpired and what was done to intervene
- Was there sufficient preparation to prevent the incident?
- Did detection occur promptly? If not, why?
- Could additional tools have helped the detection and recovery process?
- Was the incident sufficiently contained?

- Was communication adequate, or could it have been better?
- What practical difficulties were encountered?

The follow-up phase ensures continuing improvement to the quality of this Incident Response Policy.

Information Security Incident Response Team Responsibilities:
The security incident response team is a group of individuals who have been trained in incident management, each having distinct response roles. The team works under the direction of the Institute's Chief Information Security Officer (CISO), the Institute's Chief Information Officer (CIO), or designated incident officer.

The team is tasked with the following responsibilities:

- Processing IT security complaints or incidents
- Determining incident severity and escalating it, if necessary, with notification to appropriate internal and/or external authorities
- Coordinating security incidents from discovery to closure
- Reviewing incidents, providing solutions/resolutions and closure

The Institute's CISO is responsible for oversight of this process. All questions or concerns related to this policy should be reported to this office for reconciliation.

Information Security Incident Response Team Membership:
Each incident could require various Institute personnel to be available for investigation and remediation. The incident officer will normally follow the outlined team setup but may need to select from the organizational units deemed technically proficient to provide their expertise to a particular incident.

The incident response team will include the following members:

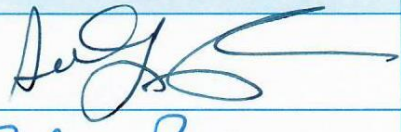
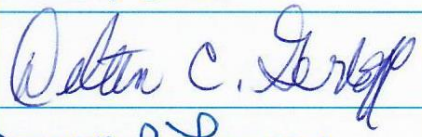
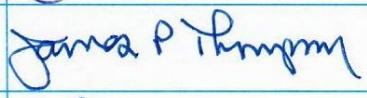
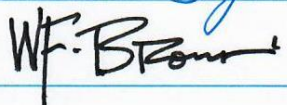
- Institute CISO
- Local IT Representative(s)
- Other personnel, as needed

References:
UTIA Glossary of Information Security Terms
UTIA IT0122P – *Information Security Incident Response and Reporting Procedures*
UT Policy IT0122 – *Security Incident Reporting and Response*
UTIA IT0110 – *Acceptable Use of Information Technology Resources Security Policy (AUP)*
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 Policy

We approve UTIA IT0122 – *Information Security Incident Response Policy* as described in this document.

Name	Title	Signature	Date
Sandra D. Lindsey	Chief Information Security Officer, UTIA		10/14/2016
Robert L. Ridenour, Jr.	Chief Information Officer, UTIA		10/14/2016
Tim Cross, Ph.D.	Interim Chancellor, UTIA		10/17/2016
Delton Gerloff, Ph.D.	Interim Dean, Extension		14/4/16
Jim Thompson, Ph.D.	Dean, VetMed		10.21.16
Caula Beyl, Ph.D.	Dean, CASNR		10-17-16
William F. Brown, Ph.D.	Dean, AgResearch		10/17/16