



UTIA IT0122 – INFORMATION SECURITY INCIDENT RESPONSE POLICY

Effective: September 1, 2014

Last Reviewed: July 01, 2021

Last Updated: July 22, 2021

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. Any user, be it faculty, staff, leadership, student, friend, volunteer, third-party vendor, or any others, must follow this policy.

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

Incident Response Policies and Procedures

This policy requires multiple controls be in place, in addition to a set of Institute Response Procedures. Please refer to [UTIA IT0122P – Information Incident Response Plan and Reporting Procedures](#) for those specific roles and responsibilities for reporting and handling a security incident. It is critical to properly report incidents and possible incidents in order to comply with the State of Tennessee's rules and regulations for appropriate reporting to our cyber insurance provider, as well as to comply with specific federal laws and industry regulations.

Incident Response Training

The Institute requires annual security awareness training per UTIA IT0123 – Security Awareness, Training, and Education Policy. The Institute's Chief Information Security Officer (CISO) prepares role-based training based on this policy. This training does include Incident Response training modules for everyone, however IT staff must complete additional modules in this annual training on how to recognize an incident and handle it or any possible incident in the appropriate manner.

In addition to the role-based training, the Institute's CISO also includes raising awareness and education through the following:

1. Monthly e-newsletters are sent by the CISO to inform all faculty and staff of new threats, such as a new form of spear phishing or ransomware attack.
2. The monthly e-newsletters also give reminders of threats and how to identify an incident or possible incident.
3. The [UTIAsecurity website](#) also contains information on recognizing an incident or possible incident, as well as guidelines on reporting.
4. The UTIA IT Community is given additional information by the CISO on reporting, system recovery, remediation, etc., at this group's regular meetings.

Incident Response Testing

The Institute's CISO works with the local and regional IT support personnel and/or the Incident Response Team (see below for responsibilities and membership) to test the effectiveness of the incident response procedures. The CISO distributes checklists to the Incident Response Team that will be used for following [UTIA IT0122P – Information Incident Response Plan and Reporting Procedures](#).

Incident Handling

The Institute's CISO maintains [UTIA IT0122P – Information Incident Response Plan and Reporting Procedures](#) so they include the most appropriate details for preparation, detection, analysis, containment and recovery, keeping in mind any federal and/or industry regulations for handling a specific incident.

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 (e.g., MS-ISAC, REN-ISAC) may detect issues by recognizing unauthorized activity or abnormal behavior on their systems and reporting the activity to the University.

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.

When an incident or possible incident affects business critical systems the CISO will work with the system owner and system administrator to coordinate contingency planning activities.

Incident Response Monitoring

The Institute's CISO tracks and documents all system security incidents. This documentation includes records about an incident or possible incident, whether it is actually an incident, the status of an incident, and all details about an incident, including detection and reporting.

Incident Reporting

The Institute's CISO is to be immediately notified of any incident or possible incident. 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 procedures.

Please see [UTIA IT0122P – Information Incident Response Plan and Reporting Procedures](#) for specific requirements and responsibilities.

Incident Response Assistance

The Institute's CISO will work with all users for advice and assistance regarding the handling and reporting of any security incident or possible incident.

Incident Response Plan

The Institute's CISO will maintain [UTIA IT0122P – Information Incident Response Plan and Reporting Procedures](#), that includes:

1. Roadmap for incident response;
2. High-level approach to incident response for the overall Institute;
3. Unique requirements based on the Institute's mission, size, structure, and functions;
4. Defined reportable information security incidents;
5. Metrics for measuring incident response capabilities;
6. Defines the resources needed to maintain and mature the Institute's incident response capabilities;
7. Is reviewed and approved by
 - The Institute's CISO
 - The Institute's CIO
 - The Institute's Senior Vice President and Senior Vice Chancellor

The CISO will review and update [UTIA IT0122P – Information Incident Response Plan and Reporting Procedures](#) when changes are necessary and make available to everyone via the [UTIA Policies and Procedures](#) site. Specific incident response details will not be made available except on a need-to-know basis to protect those specifics from unauthorized disclosure and modification. The CISO will distribute a copy of any specifics to those with a justifiable need to know.

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 incident officer, i.e., the Institute’s CISO and/or the Institute’s Chief Information Officer (CIO).

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 the CISO 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 or Institute CIO, if necessary
- Local and/or Regional IT Support Personnel
- Other personnel, as needed

References:

[UTIA Glossary of Information Security Terms](#)

[UTIA IT0122P – Information Security Incident Response Plan and Reporting Procedures](#)

[UT Policy IT0122 – Security Incident Reporting and Response](#)



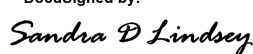
[UTIA IT0110 – Acceptable Use of Information Technology Resources Security Policy \(AUP\)](#)

[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
Tim Cross, Ph.D.	Senior Vice President and Senior Vice Chancellor, UTIA	DocuSigned by:  Dr. Tim L. Cross	7/27/2021 08:05:38 PDT
Angela A. Gibson	Chief Information Officer, UTIA	F81A83AFB474435... DocuSigned by:  Angela A. Gibson	7/27/2021 09:02:07 PDT
Sandra D. Lindsey	Chief Information Security Officer, UTIA	75409DE95BA8458... DocuSigned by:  Sandra D Lindsey	7/27/2021 09:04:22 PDT

213E082B08784A3...