THE UNIVERSITY OF TENNESSEE

System-wide Policy: IT0017 - Information Technology Incident Response Management	
Version: 1	**Effective Date: 01/23/2025**

SECTION 1. Policy Statement

I. Objective

This policy provides guidance and structure for the University to develop and maintain a thorough written incident response plan that includes a written process for Users to report incidents and guidance for security issues that cross multiple campus and institute boundaries.

II. Incident Response Management Policy

The Central IT Department must communicate the requirements and processes for incident response management to the campus community annually to engage campus communities and individuals in the shared responsibility of security incident response management. In all cases within this policy where the Central IT Department is required to create a process to implement an IT security control, training and guidance must also be provided to the campus or institute community related to the control itself and the associated process.

1. The campus or institute CISO/DISL must develop and maintain a written incident response plan that is approved by the campus or institute CIO/DTL and meets the following:

a. This plan must include a process for responding to incidents.

b. At a minimum, the incident response process must be reviewed on an annual basis. This review may also occur following an incident or tabletop exercise.

c. An incident manager and backup incident manager must be specifically identified by name within the plan.

i. If an external party, such as an IT Service Provider or law enforcement, is the incident manager, then one University approved internal individual must be specified to oversee the response process.

ii. Contact information must be recorded in the incident response plan.

e. The categorization of the Data affected must be included in the plan response structure (reference System-wide Policy: IT0005 – Data Categorization for more information on Data categorization).

f. All parties that need to be made aware of a security incident must be documented.

g. The plan must address any regulatory or other compliance requirements.

h. The plan must address both internal and external communications.

i. The plan must provide mechanisms for inclusion of all Data Owners affected by the incident.

2. The campus or institute CISO/DISL must maintain a written process for users to report incidents.

a. This process must include approved methods for reporting incidents:

i. Primary and secondary methods for reporting.

ii. Specific recipients to receive incident reports.

iii. Any minimum information that is needed.

iv. Timeframes for reporting incidents.

b. At a minimum, the incident reporting process must be reviewed on an annual basis.

3. When a Security incident crosses multiple campus and institute boundaries the University CISO will determine who the owner of the incident is. The assigned owner is responsible for entering and/or ensuring that all documentation for the incident is created and maintained. Incidents that cross multiple campus and institute boundaries will use the central ticketing process to track the incident and communicate the resolutions.

4. All IT Service Providers must provide documentation that they have a written incident response plan that is tested at least annually. While all Central IT Department staff are required to follow the written incident response plan, IT Service Providers involved in the incident response process must be managed by the incident manager.

5. All Users are required to report suspected or confirmed security incidents according to the campus's incident response plan.

Implementation Group 2 and 3 Controls

Note that Implementation Group 2 (IG2) controls are not required to be implemented until January 1, 2027, and Implementation Group 3 (IG3) by January 1, 2029.

6. The campus or institute CISO/DISL must establish and maintain an incident response process that addresses roles and responsibilities, compliance requirements, and a communication plan (IG2)., which must be reviewed annually.

7. The campus or institute CIO/DTL must assign key roles and responsibilities for incident response, including staff from legal, IT, Data security, facilities, public relations, Human Resources, incident responders, analysts, and Data Owners as applicable (IG2) and review the responsibilities annually. The campus or institute CISO/DISL will determine which primary, and secondary mechanisms will be used to communicate and report during a security incident (IG2). The mechanisms can include electronic chats, phone calls, emails, or letters and must be reviewed annually.

8. The campus or institute CISO/DISL will plan and conduct routine incident response exercises and scenarios for key personnel involved in the incident response process to prepare for responding to real-world incidents (IG2).

a. Exercises need to test communication channels, decision making, and workflows.

b. Testing will be conducted on an annual basis, at a minimum.

9. The campus or institute CISO/DISL will conduct post-incident reviews. Post-incident reviews help prevent incident recurrence through identifying lessons learned and follow-up action (IG2).

10. The campus or institute CISO/DISL will establish and maintain Security Incident thresholds, including, at a minimum, differentiating between an incident and an event (IG3) and review these thresholds annually.

III. Exceptions

The University's Chief Information Officer is authorized to grant exceptions to the University's Information Technology Policies. Campus or institute CIOs/DTLs are authorized to grant exceptions to campus or institute processes and procedures.

SECTION 2. Reason for the Policy

This policy establishes the requirements for information technology incident response management as described in CIS Control 17 (Incident Response Management) for the University of Tennessee in support

of System-wide Policy: IT0001 – General Statement on Information Technology Policy. All Users must familiarize themselves with System-wide Policy: IT0001.

SECTION 3. Scope and Application

This policy applies to all Users of IT Resources owned, operated, or provided by the University of Tennessee, including its campuses, institutes, and administration (University and/or campuses).

SECTION 4. Procedures

Each campus/institute will adopt procedures related to this policy.

SECTION 5. Definitions

See IT0001 – General Statement on Information Technology Policy for definitions of terms.

SECTION 6. Penalties/Disciplinary Action for Non-Compliance

Any violation of this policy may subject the User to discipline as a violation of one or more provisions of the general standard of conduct in the student handbook or to discipline under the Code of Conduct (HR0580 – Code of Conduct) in the Human Resources Policy and Procedures.

The University may temporarily or permanently remove access to its information technology Resources if an individual violates this policy.

SECTION 7. Responsible Official & Additional Contacts

Subject Matter	Office Name	Telephone Number	Email/Web Address
Policy Clarification and Interpretation	System Chief Information Officer and System Chief Information Security Officer	(865) 974-4810 or (865) 974-0637	cio@tennessee.edu or iso@tennessee.edu
Policy Training	System Chief Information Security Officer	(865) 974-0637	iso@tennessee.edu

[Text Wrapping Break]_____

SECTION 8. Policy History

Revision 1:

SECTION 9. Related Policies/Guidance Documents

A. University Policies

a. IT0001 – General Statement on Information Technology Policy

b. IT0002 – Acceptable Use of Information Technology Resources

c. IT0003 – Information Technology Security Program Strategy

d. IT0004 – Information Technology Risk Management

e. IT0005 – Data Categorization

f. IT0014 – Security Awareness Training Management

g. IT0102 – Information Technology Asset Management

h. IT0311 – Information Technology Data Access, Management, and Recovery

i. IT0506 – Information Technology Account and Credential Management

j. IT1318 – Information Technology Network Monitoring and Defense and Penetration Testing

k. IT1516 – Information Technology Service Provider Management Application Software Security Management

l. IT4912 – Information Technology Secure Configuration Management

m. IT7810 – Information Technology Vulnerability Management, Audit Log Management, and Malware Defense

B. Center for Internet Security Critical Security Controls Navigator

https://www.cisecurity.org/controls/cis-controls-navigator/
