THE UNIVERSITY OF TENNESSEE
HEALTH SCIENCE CENTER

UT Health Science Center: IT0017-HSC-A Security Incident Response	
Version 5	**Effective Date: 04/18/2016**

Responsible Office: Office of Cybersecurity	Last Review: 03/01/2025 Next Review: 03/01/2027
Contact: Chris Madeksho	Phone: 901.448.1579 Email: mmadeksh@uthsc.edu

Purpose

To maintain the security of the University of Tennessee Health Science Center (UTHSC) IT Resources, including data and information, a framework for proactive detection and prevention, and the reactive identification, containment, eradication, recovery, tracking, and documentation of information security incidents is established.

Scope

This standard applies to Information Security Incidents at the University of Tennessee Health Science Center (UTHSC)

Definitions

Security Incident – an event that compromises the security of information or systems.

Security Information Response Team (SIRT) – a group of individuals that initially respond to an incident or potential incident. Members vary depending upon the type of incident reported.

UTHSC Information Technology (IT) Resource - a broad term for all things related to information technology from a holistic point of view and covers all University owned or managed information technology services, including cloud-based services, that users have access to.

Responsibilities

Any member of the UTHSC community has the responsibility for reporting any information security incident or potential incident. Violations can be reported (anonymously) to the following:

- UTHSC ITS Information Security Team
- Executive Leadership of ITS

- UTHSC ITS Service Desk
- UTHSC Privacy Officer
- Campus Police
- Office of Institutional Compliance
- UT Compliance Hotline

Security Information Response Team (SIRT) is responsible for responding to the report of any incident or potential incident, documenting all incidents, and reporting the finding of the incident to the Vice Chancellor for Information Technology/CIO.
The Chief Information Security Officer (CISO) or designee is assigned as a permanent member and head of the SIRT, is responsible for directing the activities of the SIRT, and will correspond with the UTHSC Emergency Management Team as appropriate.
The Office of Cybersecurity is responsible for activating the SIRT in response to an information security incident report classified as Medium or High.
The Executive Leadership of ITS is responsible for acting on the findings of the IRT.

Standard

1. UTHSC maintains an Information Security Incident Response Plan outlining the goals and objectives of the incident response capability
2. UTHSC maintains a Security Incident Response Team (SIRT) to respond to information security incidents chartered as follows:
   a. Authority
      i. The Chief Information Security Officer (CISO) has final accountability and authority over the activities of the SIRT.
      ii. The CISO charters the SIRT and appoints the permanent members of the SIRT
      iii. The CISO, or designee, directs and prioritizes duties of the SIRT while responding to information security incidents.
      iv. The CISO, or designee is the authority to initiate and terminate an information security incident response.
   b. Composition
      i. The CISO, or designee, is permanent member of the SIRT. They manage, direct, and provide leadership for the SIRT while responding to information security incidents.
      ii. Permanent members of the SIRT include the Office of Cybersecurity.

iii. Members of the Information Technology Services (ITS) staff as appropriate to cope with the incident's scope, severity, and potential impact.
iv. Members of the UTHSC Community as appropriate to cope with the incident's scope, severity, and potential impact.

c. Categorization
   i. Each information security incident will be categorized (Low, Medium, High) per the UTHSC Information Security Incident Response Plan
d. Documentation and Reporting
   i. All investigations and resolutions of information security incidents will be tracked and documented.
   ii. SIRT will follow the procedures outlined in the UTHSC Information Security Incident Response Plan when responding to incidents.
   iii. UTHSC reports, on a periodic basis, all security incidents to the UTHSC CIO and the UTSA CISO.

Policy History

Version #	Effective Date
1	04/18/2016
3	04/07/2020
4	02/27/2023
5	03/01/2025 – new naming convention

References

1. IT0002 - Acceptable Use of Information Technology Resources
2. IT0017-Information Technology Incident Response Management
3. UTHSC Security Incident Response Plan