Overview

This addendum covers the Incident Response policies for IT security incidents at UTHSC.

Purpose

The purpose of this document is to describe the data capture, documentation, escalation, assignment, remediation and reporting of security incidents at UTHSC.

Scope

This addendum applies to all information technology security incidents on the UTHSC.

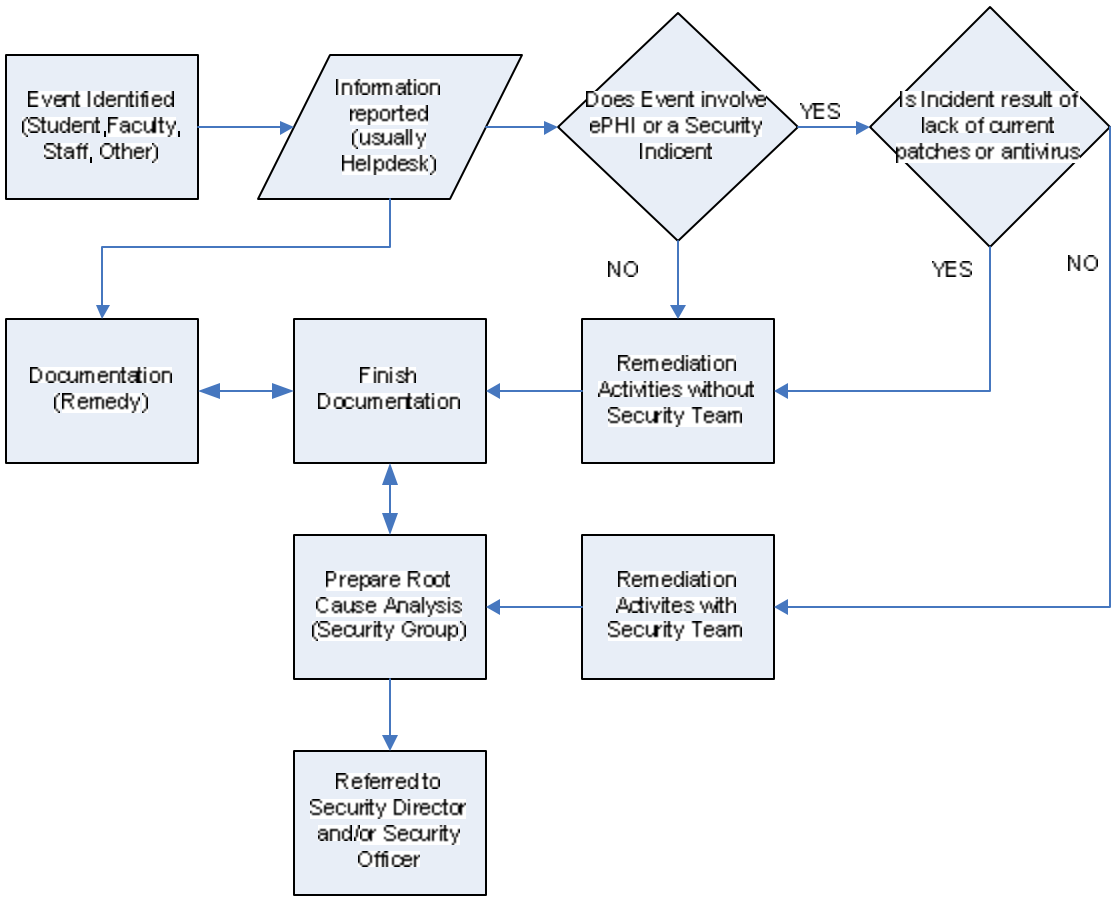
Definitions

Event	A malfunction of an information system that has not yet been investigated and does not have a known cause or an estimate of criticality.
Security Incident	The attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.

Policy

- Faculty, students and staff should report events to the Helpdesk so that initial documentation of the event and remediation may begin.
- Remediation will proceed according to these criteria:
  - If the event does not involve EPHI or is not a Security Incident, then remediation will proceed without involvement of the Security Team.
  - If the event does involve EPHI or is a Security Incident, and is the result of lack of current software patches and/or antivirus protection, the remediation will proceed without involvement of the Security Team.
  - If the incident is not covered by the above criteria, then the Security Team should be notified, and remediation will proceed with the involvement of the Security Team.
- Incident response procedures may detail assignments, escalation and other activities but should be consistent with emergency response or disaster recovery.
- All security incidents will be documented, and Root Cause analyses prepared as appropriate. See **Root Cause Analysis Guidelines** below.
- Documentation of incidents will be reviewed periodically and reported to the Security Director and/or Security Officer as appropriate.

See Flow Chart Below:



Root Cause Analysis Guideline

Guideline Overview

These guidelines documents Root Cause Analyses of security incidents.

Guideline Purpose

Root Cause Analyses are performed to analyze the root causes of security incidents, provide a basis for improved preventive and reactive procedures, establish detailed records for future trouble-shooting, and serve as required documentation under HIPAA for security breaches involving electronic PHI.

Guideline Scope

This addendum applies to all information systems security incidents involving at UTHSC.

Guidelines

Information systems events may result from causes such as equipment failure, user error, programmatic error, and security incidents. Once it has been determined in the incident response process that the event is a security incident, then the preparation of a Root Cause Analysis is required. (See **Incident Response Addendum** above)

The Security group is responsible for documenting Security Incidents, consulting with the Security Team and others who have knowledge of the Security Incident. These Root Cause Analysis reports will include:

- A definitional Problem Description.
- Identification of causal Primary Factors such as timing, process, environment, users, and actors outside UTHSC.
- Identification of a root cause for each of the Primary factors.
- A correction plan, as appropriate, ranking the root causes and corresponding safeguards to be applied.
- A complete appendix of related documentation and communications regarding the Security Incident.

Root Cause Analyses and supporting documentation are classified as Mission Critical data and shall be treated accordingly. (See **Mission Critical Information Addendum**.)

Root Cause Analyses involving EPHI will be forwarded to the UTHSC Security Officer for review and further handling as required.

Enforcement

Reference **Enforcement** in Acceptable Use document.

Additional Information

Any inquires relating to the Incident Response Policy and the and/or the Root Cause Analysis Guidelines should be directed to the Security Director.