

<b>UT Health Science Center:</b>	
<b>AU-002-Logging and System Activity Review</b>	
<b>Version 2</b>	<b>Effective Date: 03/20/2016</b>

Responsible Office: Office of Cybersecurity	Last Review: 02/14/2023 Next Review: 02/14/2025
Contact: Chris Madeksho	Phone: 901.448.1579 Email: mmadeksh@uthsc.edu

## Purpose

To specify requirements and definite practices for logging and the review of the information system activity involving UTHSC IT resources.

Logging assists to identify, respond, and prevent operational problems, security incidents, policy violations, fraudulent activity; optimize system and application performance; assist in business recovery activities; and, in many cases, comply with federal, state, and local laws and regulations. This standard is also designed to meet compliance requirements for data regulated by federal or state law. This includes, but is not limited to, security requirements and safeguards for the Family Educational Rights and Privacy Act (FERPA), Health Insurance Portability and Accountability Act (HIPAA), or Gramm-Leach-Bliley Act (GLBA).

## Scope

The UTHSC Community and all individuals or entities using any UTHSC IT Resources and all uses of such UTHSC IT Resources that process, store, access or transmit data or information with a classification rating of 3 in accordance with [GP-002-Data & System Classification](#). Requirements established within this document do not supersede any specific requirements imposed by the University of Tennessee policies, State and Federal laws, or contractual agreements.

## Definitions

**Information Technology (IT) Resources** – The collection of data and technology that support the achievement of organizational goals. IT Resources include hardware, software, vendors, users, facilities, data systems, and data.

**Log** – a record of the events occurring within an organization’s systems and networks.

<b>UT Health Science Center:</b> <b>AU-002-Logging and System Activity Review</b>	
<b>Version 2</b>	<b>Effective Date: 03/20/2016</b>

## Responsibilities

The **Owner of the UTHSC IT Resource**, or their designee is responsible for collecting and reviewing Log data on IT Resources within their areas of responsibility. **System and network administrators** are responsible for configuring logging on individual systems and network devices per this Standard.

The **Office of Cybersecurity** is responsible for the management of and execution of this Standard.

## Standard

### Requirements

1. Logging must be enabled, and Log review must take place on UTHSC IT Resources that process, store, access or transmit UTHSC data or information with a level 3 classification in order to identify, respond, and prevent operational problems, security incidents, policy violations, and fraudulent activity; optimize system and application performance; assist in business recovery activities; and to comply with federal, state, and local laws and regulations.
  - a. Logging must be enabled at the operating system, application/database, and system/workstation level; passwords must never be logged
  - b. All electronic logs must be accurately time stamped.
  - c. Log review shall include investigation of suspicious activity, including escalation to the Office of Cybersecurity or the campus incident response process as appropriate.
  - d. Individuals shall not be assigned to be the sole reviewers of their own activity.
  - e. Logs must be accessed, secured, backed-up, and protected commensurate with the criticality of the information they may contain.
  - f. Logs must be kept for a minimum of 90 days.
2. Computer activity logging must be configured as follows:
  - a. Computers must minimally log identity and date/time stamps of the following security events:
    - i. Access or logins and logouts to the computer
    - ii. User creations, privilege escalations and group membership changes that affect user permissions
    - iii. Software installations/de-installations
    - iv. Start-up/shutdown
  - b. Logs for computers configured to provide services to multiple users over the

<b>UT Health Science Center: AU-002-Logging and System Activity Review</b>	
<b>Version 2</b>	<b>Effective Date: 03/20/2016</b>

- UTHSC network (i.e. servers, workstations configured as servers) must be retained for a minimum of 12 months. Other computers must retain logs for a minimum of 30 days.
- c. Logs from computers publicly facing the Internet must be stored in a separate logging server. Logs from computers publicly facing the Internet must be monitored and alerts sent to the system administrator for suspected intrusion or compromise events.
3. Network Infrastructure resources must be configured as follows:
    - a. Minimally log identity and date/time stamps of the following security events:
      - i. Access or logins and logouts to the resources
      - ii. Software installations/de-installations
      - iii. Start-up/shutdown
  4. Any system on the UTHSC network not covered by 1,2, and 3 above may be required to enable logging and be subject to Log review as the result of a risk assessment or at the discretion of the Vice Chancellor for Information Technology or his/her delegate.

### **Definitive Practices**

1. All servers that store, access, or transmit UTHSC data or information with a level 3 classification must connect their logs to the Security Information and Event Management (SIEM) system.
  - a. Contact the Information Security Team for details on how and where to forward logs from servers and security monitoring systems.
2. Required Logs
  - a. Server Authentication Logs must include the following:
    - i. Date/time
    - ii. Username
    - iii. IP address from which the login originated
    - iv. Whether the login was successful
  - b. Logs of any log-based intrusion prevention security application must include the following:
    - i. Date/time
    - ii. Username(s) attempted
    - iii. IP address from which the attempt originated
  - c. Web server access logs (if the server is offering web pages) must include the following:

<b>UT Health Science Center: AU-002-Logging and System Activity Review</b>	
<b>Version 2</b>	<b>Effective Date: 03/20/2016</b>

- i. Date/time
- ii. IP address from which the access originated
- iii. The complete URL of the page that was accessed
- d. Any logs for applications that handle data or information categorized as Confidential or Classified, or authentication/access information must include the following:
  - i. Date/time
  - ii. IP address of server on which the application is running
  - iii. Any critical information on actions performed within the application
- e. Critical information includes any security related actions:
  - i. Failed login attempts
  - ii. Successful logins
  - iii. User creation
  - iv. User deletion
  - v. Credential and permission changes
  - vi. File accesses
  - vii. File downloads and uploads
  - viii. Any other critical actions unique to the application

## References

1. UTHSC Information Security Program
2. [NIST Special publication 800-92](#)
3. [GP-002-Data & System Classification](#)