THE UNIVERSITY OF TENNESSEE
HEALTH SCIENCE CENTER

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

Responsible Office: Office of Cybersecurity	Last Review: 04/15/2020 Next Review: 04/15/2022
Contact: Chris Madeksho	Phone: 901.448.1579 Email: mmadeksh@uthsc.edu

Purpose

To specify requirements 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.

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 any area. 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.

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 in accordance with the Practices developed by the UTHSC in support of this Standard.

System and network administrators are responsible for configuring logging on individual systems and network devices per this Standard.

Standard

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 classification rating of 3 in any area 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 IT Security 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 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 standard bullet 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.

References

1. UTHSC Information Security Program
2. NIST Special publication 800-92
3. GP-002-Data & System Categorization