THE UNIVERSITY OF TENNESSEE
HEALTH SCIENCE CENTER

UT Health Science Center: AU-002.01-Logging and System Activity Review	
Version 1	**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 definite practices for logging/information system activity review involving UTHSC IT Resources.

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 categorized as C-3 per the Data Classification Standard.

Practice

1. All servers that store, access, or transmit UTHSC data or information categorized as Confidential or Classified, covered by the *AU-002-Logging and System Activity Review*, 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:

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. AU-002-Logging and System Activity Review
2. GP-002-Data Categorization