THE UNIVERSITY OF UTAH®

Title: Log Management and Monitoring
Number: G4-004L
Responsible Office: Information Security and Privacy Office
Last Revision: July 2011

I. OVERVIEW
   a. This document provides guidance for the implementation of the Information Security Policy – Section L: Log Management and Monitoring.

II. DEFINITIONS
   a. Log means a record of the computer action or an event that has occurred.
   b. Network Time Protocol (NTP) means a tool for synchronizing the system clock over a data network.
   c. Logging facility means a University Information Technology (UIT) or Information Technology Services (ITS) approved central logging facility.

III. GUIDELINES
   a. Time Synchronization
      i. The system's clock should be set to synchronize with time.utah.edu.
   b. Log Retention
      i. Audit logs should be retained for sixty days on disk. Audit logs older than sixty days may be moved to long term storage or archived.
      ii. Archive logs for sensitive and restricted data should be retained for six years in a form that is retrievable within fifteen days following a request.
   c. Audit Log Elements
      i. When supported, audit logs should include the following items
         1. Source and target network address
         2. The user ID
         3. User creations or deletions
         4. Changes to a user's privilege or rights
         5. Date and time of the event
         6. Type of event
         7. Files or data accessed
         8. Successful and rejected access attempts
         9. Changes to system and application configurations
         10. Access to programs and applications
         11. Privileged or administrative access
         12. System alarms
         13. Access to audit logs
         14. Logging failures or exceptions to logging
      ii. Audit logs should NEVER include:
         1. Social Security Numbers
         2. Payment card numbers
         3. Clear text authentication credentials
         4. Clear text personally identifiable financial or healthcare information.
   d. Review and monitoring
      i. Audit logs should be reviewed at least daily for tier 1 or tier 2 systems. Log harvesting, parsing and alerting tools may be used to fulfill this requirement.

ii. Logs for all other systems should be regularly reviewed based on the system risk assessment but never less than once a quarter.
iii. Review of audit logs will be documented.

e. Logging Facility
   i. In addition to audit log storage on the local system, logs should be sent to a central log aggregation facility.
   ii. UIT/ITS logs should be sent to a UIT/ITS central log facility
   iii. The logging facility should provide appropriate security controls to protect logs from alteration.
   iv. Access to audit logs must be limited to those with a business need to know.
   v. Change management, including appropriate testing, should be completed prior to the implementation of logging to ensure system availability.
   vi. The IP addresses of UIT logging facilities and implementation help may be obtained by contacting the Service Desk (Helpdesk):
      1. Website - https://cmsworkflow1.srvr.uhsc.utah.edu/webticket/
      2. Telephone number:
         a. 801-581-4000 (Campus)
         b. 801-587-6000 (Health Sciences)

f. Resources
   i. NIST – Guide to Computer Security Log Management, Special Publication 800-92:
   http://csrc.nist.gov/publications/nistpubs/800-92/SP800-92.pdf

   ii. Sans – Five Essential Log Reports
   http://www.sans.org/security-resources/top5_logreports.pd

   iii. Data Classification Resource -
   http://www.secureit.utah.edu/pdf/policy/draft/Draft%20-%20Data%20Classification%20Rule.pdf