University of Connecticut

Information Security Office

Logging Standard

Revision History

Revision Date	Revised By	Summary of Revisions	Section(s) / Page(s) Revised
6/01/2013	ISO	Initial Release	All

Approvals

Review Date	Reviewed By	Name/Title	Action (Reviewed or Approved)
6/01/2013	CISO	Jason Pufahl, CISO	Approved
6/01/2013	RMAC	Risk Management Advisory Council	Reviewed

Table of Contents

Purpose

Logging is an essential information security control that is used to identify, respond, and prevent operational problems, security incidents, policy violations, fraudulent activity; assist in business recovery activities; and, in many cases, comply with federal, state, and local laws and regulations. The purpose of the Logging Standard is to define logging expectations and requirements regarding University of Connecticut's (UConn) electronic log data collection and analysis.

Underlying Requirements

All systems that handle confidential information, accept network connections, or make access control (authentication and authorization) decisions shall record and retain audit-logging information sufficient to answer the following questions:

1. What activity was performed?
2. Who or what performed the activity, including where or on what system the activity was performed from (subject)?
3. What the activity was performed on (object)?
4. When was the activity performed?
5. What tool(s) was the activity performed with?
6. What was the status (such as success vs. failure), outcome, or result of the activity?

Activities to be Logged

Therefore, logs shall be created whenever any of the following activities are requested to be performed by the system:

1. Create, read, update, or delete confidential information, including confidential authentication information such as passwords;
2. Create, update, or delete information not covered in #1;
3. Initiate a network connection;
4. Accept a network connection;
5. User authentication and authorization for activities covered in #1 or #2 such as user login and logout;
6. Grant, modify, or revoke access rights, including adding a new user or group, changing user privilege levels, changing file permissions, changing database object permissions, changing firewall rules, and user password changes;
7. System, network, or services configuration changes, including installation of software patches and updates, or other installed software changes;
8. Application process startup, shutdown, or restart;
9. Application process abort, failure, or abnormal end, especially due to resource exhaustion or reaching a resource limit or threshold (such as for CPU, memory, network connections, network bandwidth, disk space, or other resources), the failure of network services such as DHCP or DNS, or hardware fault; and
10. Detection of suspicious/malicious activity such as from an Intrusion Detection or Prevention System (IDS/IPS), anti-virus system, or anti-spyware system.

Logging additional items may be deemed necessary for higher risk or business critical systems at the discretion of the System Administrator and Information Security Office.

Elements of the Log

Such logs shall identify or contain at least the following elements, directly or indirectly. In this context, the term "indirectly" means unambiguously inferred.

1. Type of action – examples include authorize, create, read, update, delete, and accept network connection.
2. Subsystems performing the action – examples include process or transaction name, process or transaction identifier.
3. Identifiers (as many as available) for the subject requesting the action – examples include user name, computer name, IP address, and MAC address (Note that such identifiers should be standardized in order to facilitate log correlation.)
4. Identifiers (as many as available) for the object the action was performed on – examples include file names accessed, unique identifiers of records accessed in a database, query parameters used to determine records accessed in a database, computer name, IP address, and MAC address. (Note that such identifiers should be standardized in order to facilitate log correlation.)
5. Before and after values when action involves updating a data element, if feasible.
6. Date and time the action was performed, including relevant time-zone information if not in Coordinated Universal Time.
7. Whether the action was allowed or denied by access-control mechanisms.
8. Description and/or reason-codes of why the action was denied by the access-control mechanism, if applicable.

Formatting and Storage

The system shall support the formatting and storage of audit logs in such a way as to ensure the integrity of the logs and to support enterprise-level analysis and reporting. Mechanisms known to support these goals include, but are not limited to, the following:

1. Microsoft Windows Event Logs collected by a centralized log management system;
2. Logs in a well-documented format sent via syslog, syslog-ng, or syslog-reliable network protocols to a centralized log management system;
3. Logs stored in an ANSI-SQL database that itself generates audit logs in compliance with the requirements of this document; and
4. Other open logging mechanisms supporting the above requirements including those based on CheckPoint OpSec, ArcSight CEF, and IDMEF.

Whenever possible, the logs should be forwarded to the University Logging Central Repository that is managed by the Information Security Office.

Required Logging Practices

- Systems should be time-synchronized via a network time source (preferably time.uconn.edu). If possible, log events should include an indication of time zone.
- Log data must be transmitted securely via an encrypted mechanism when possible to preserve integrity and confidentiality. This could include encrypting data prior to transmission or providing an encrypted tunneling mechanism. (Compliance can be achieved several ways – contact the Information Security Office if you need assistance or to assure you are forwarding your logs to the University Central Log Repository).
- When possible, audit the access to and modification of log data.
- All administrator or root access and operations must be logged (including read-only administrator access).
- Log data should be housed centrally (unless isolation is dictated for compliance reasons), and robust role-based access controls should be utilized for data analysis and retrieval.
- Alarms raised by University IT resources (e.g., console alerts or messages; system log exceptions; network management alarms; alarms raised by access control systems) must be logged and retained for a specified period.
- Activation/deactivation of protection systems such as anti-virus, intrusion detection, and file integrity systems must be logged.
- The following data must never be included in University server log data:
    - Social Security Numbers
    - Clear text authentication credentials (e.g., passwords)
    - PII or financial information (e.g., financial account numbers, credit card numbers, etc.)
- Timestamps should be recorded in ISO-8601 format, whenever possible:
    - Minimally : 2013-04-03
    - Acceptable: 2013-04-03 23:45
    - Ideally: 2013-04-03T23:45Z (in UTC)

  (This is critical data that assists when investigating the timeline of an incident.)
- Logging facilities and log information should be protected against tampering, modification, destruction, and unauthorized access. Where possible, system administrators should not have permission to erase, deactivate, or modify logs of their own activities.
- Minimally, logs are expected to include the details as explained in “System and common application logs” (https://plone.uconn.edu/workspaces/splunk/system-and-common-application-logs)

Log Reviews

Logs should be reviewed at least on a monthly basis. Logs must be reviewed within a 24 hour period in response to suspected or reported security problems on systems containing confidential data or as requested by the Information Security Office.

System Stewards are responsible for determining which systems require scheduled log review.

Log review shall include investigation of suspicious activity, including escalation to the Information Security Office or the campus incident response process as appropriate.

Individuals shall not be assigned to be the sole reviewers of their own activity.

Log Retention Schedules

The retention schedule applied for log data depends heavily upon the policies, regulations, and/or standards that govern the type of data recorded in log events (and/or the purpose of the systems of origin). At minimum, as a state entity the University is governed by the Connecticut State Library schedules for data retention. In the realm of Information Technology, Schedule S6 "Information Systems Records" guides retention requirements for log data. This policy provides significant latitude for retention, stating that data must be retained "Until no longer administratively valuable." Log data is encompassed by this requirement (see S6-100).

Data not governed by any other consideration should be interpreted as subject to Schedule S6 as appropriate, allowing system administrator and/or data steward discretion in selecting a log retention period. However, when data is governed by other regulations/standards, the strictest common denominator for retention requirements should be selected.

References

a. "Information Security Policy Manual" http://policy.uconn.edu/wp-content/uploads/2012/05/Information-Security-Policy-Manual.pdf
b. Connecticut State Library Schedule S6 : Information Systems Records, revised 12/2010 http://www.cslib.org/publicrecords/stateretsched/S6InfoSystms2010.pdf
c. CT state HIPAA policies / requirements http://www.ct.gov/best/lib/best/State_HIPAA_Security_Policies_Release_2.0_-_Letter_Print.pdf
d. SANS Information System Audit Logging Requirements http://www.sans.org/security-resources/policies/audit.php