DHHS Information Technology (IT) Audit Standard

Issue Date: October 1, 2013
Effective Date: October 1, 2013
Revised Date:

Number: DHHS-2013-001-F

1.0 Purpose and Objectives

It is Nebraska Department of Health and Human Services (DHHS) Policy that the DHHS Information Security Officer (ISO) will establish and manage an entity-wide oversight and compliance function. This includes a managed review of auditing logs and records of security-related events to provide DHHS with assurance of policy compliance throughout DHHS.

The purpose of this standard is to provide assurance that DHHS maintains log records according to policy and DHHS document retention requirements and maintains evidence that may be necessary for investigations, forensics, or legal discovery purposes. The purpose is also to ensure that all servers deployed at DHHS are configured according to DHHS policies and standards. Servers deployed at DHHS shall be inspected for compliance with this standard at least annually and as prescribed by applicable regulatory compliance.

Logs will be treated as Confidential information and secured appropriately with sufficient capacity to meet audit log retention requirements. DHHS will periodically review audit log records for indications of inappropriate or unusual activity, and report findings to designated DHHS officials.

2.0 Scope

This standard applies to DHHS IS&T systems. It should be noted that additional audit and logging requirements exist for business applications, such as disclosure of protected health information (PHI) for business purposes or application security events. The requirements for auditing and logging of PHI disclosure or handling are not part of the scope of this standard.

All systems that handle Confidential or Highly Restricted information, allow interconnectivity with or from other systems, or make access control (authentication and authorization) decisions, shall record and retain audit-logging information sufficient to answer the following questions:

- What activity was performed?
- Who or what performed the activity, including on what system the activity was performed.
- What the activity was performed on (object)?
- When was the activity performed?

- What tool(s) was the activity performed with?
- What was the status (such as success vs. failure), outcome, or result of the activity?

3.0 Standard

3.1 Log Format, Storage, and Retention

DHHS is required to ensure availability of audit log information by allocating sufficient audit record storage capacity to meet policy requirements. IS&T shall perform annual capacity planning and trend analysis to reduce the likelihood of such capacity being exceeded. The capacity and utilization of log files shall be regularly monitored and reported, and action will be taken to keep an IS&T approved level of freespace available for use. Automated notification of IS&T personnel shall occur if the capacity of log files reaches IS&T defined threshold levels, or the audit logging system fails for any reason.

The Audit Logging process for DHHS is required to provide system alerts to appropriate IS&T or Information Security personnel in the event of an audit processing failure (e.g., shut down information system, unintended overwriting of the oldest audit records, stop generating audit records, etc.). It is required that all system logs shall be sent to a central log review system that is protected from unauthorized access and is backed up for availability and integrity purposes.

The system should 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. Some mechanisms known to support these goals are listed in the DHHS Audit Logging and Monitoring Procedures.

3.2 System and Network Infrastructure Auditable Events

The DHHS System and Network infrastructure are defined as "the LAN, WAN, Servers, firewalls, and Routers/Switches use to provide electronic communication and data /information processing".

Security safeguard regulations require logging and reviewing events that are determined to have a level of risk above low as identified by DHHS Risk Management procedures. Auditable events may be incorporated into system auto logs and change management documents. The following System and Network Infrastructure events should be logged and periodically reviewed, unless the risks of security incidents can be mitigated or made insignificant through other security mechanisms:

- Successful user log-on and log-off events to the DHHS domain
- Failed login or access attempts to the DHHS domain
- Setting of system time
- Adds, changes, or deletes to the audit settings or log files

- Privileged activities such as Systems Administrator function, setting up new accounts, root level activities, etc.
- System, Server, and Network startup and shutdown
- System, Network, or Services configuration changes, including installation of software patches and updates, or other installed software changes
- Hardware installation events
- Initiation or acceptance of a network connection
- Grant, modify, or revoke system access rights, including adding a new user or group, changing user privilege levels, changing file permissions, changing database object permissions, and user password changes
- Modification of Firewall rules or other boundary protection settings
- System configuration changes
- Detection of suspicious/malicious activity such as from an Intrusion Detection or Prevention System (IDS/IPS), anti-virus system, or anti-spyware system
- Physical entrance or access to secured and restricted areas or facilities where system and network infrastructure reside.

DHHS audit logs shall be retained for 90 days, and up to 1 year or longer if requested or required for investigative or legal purposes. Events should be summarized and reported monthly, or on request. Logs governed by Privacy Regulations (such as PHI handling) may have other retention requirements that supersede these standards.

3.2.1 Audit Log Contents

DHHS logs shall contain sufficient information to establish what events occurred, the sources of the events, and the outcomes of the events. The logs shall identify or contain at least the following elements, or enough information in which to infer the following elements with reasonable assurance.

- Type of action: Examples include authorize, create, read, update, delete, and accept network connection.
- Subsystem performing the action: Examples includes process or transaction name, process or transaction identifier.
- 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.
- Date and time the action was performed, including relevant time-zone information if not in Coordinated Universal Time.

- Time stamps of the audit logging event, obtained from internal system clocks.
- Whether the action was allowed or denied by access-control mechanisms.
- Description and/or reason-codes of why the action was denied by the access-control mechanism, if applicable.

3.2.2 Audit Review, Monitoring, Findings and Remediation

Security safeguard regulations require regular inspections of system audit logs for indications of inappropriate or unusual activity. Additionally, these logs shall be reviewed by authorized personnel (representative of the data owner) to facilitate investigations of suspicious activity or suspected violations. All reports of findings shall be reported to appropriate officials who will prescribe the appropriate and necessary actions.

- Logs of system capacity and log integrity shall be reviewed on a daily basis.
- Logs used to determine anomalies in system or network utilization shall be reviewed on a daily basis
- Logs of privilege access account creation or modification shall be reviewed at a minimum of every two weeks
- All other logs shall be reviewed at a minimum of monthly

When possible, IS&T will employ automated mechanisms to alert the ISO and designated support staff when inappropriate or unusual activities with security implications are discovered. Any automation used for log analysis will not change the underlying log structure. It is acceptable for log analysis tools to extract data for analytical review, as long as the original audit logs remain unchanged and secured.

All relevant findings discovered as a result of an audit shall be listed in the DHHS tracking system or Information Security Plan of Action and Milestones (POA&M) process to ensure prompt resolution or appropriate mitigating controls. All results and findings generated by the audit or review process must be provided to appropriate DHHS management within one week of project/task completion. This report will be considered Confidential DHHS information.

3.3 Application Logging Review and Monitoring

DHHS requires application development or acquisition activity include applicable application logging for security events. Application logs are invaluable data for identifying security incidents, monitoring policy violations, establishing baselines, providing information about problems and unusual conditions, contributing additional application-specific data for incident investigation which is lacking in other log sources,

and helping defend against vulnerability identification and exploitation through attack detection.

Application logging must be commensurate with audit and logging requirements set down by data sharing agreements or state and federal security regulations. Example of oversight regulations:

> *IRS Data Use Agreement:*
> *IRS Publication 1075 - Within the application, auditing must be enabled to the extent necessary to capture access, modification, deletion and movement of FTI by each unique user. This auditing requirement also applies to data tables or databases embedded in or residing outside of the application.*
>
> *HIPAA Security Standard - Information System Activity Review*
> *Security Rule 45 CFR* ***§ 164.308(a)(1)(ii)(D)*** *– "Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports."*

Application logging might also be used to record other types of events too. Application logging content must be part of the overall system analysis and design activity, and should consider:

1. Application process startup, shutdown, or restart
2. Application process abort, failure, or abnormal end.
3. Significant input and output validation failures
4. Business process monitoring (e.g., activity abandonment, transactions, connections, information requests)
5. Audit trails (e.g., data addition, modification and deletion, data exports)
6. Performance monitoring (e.g., data load time, page timeouts)
7. Compliance monitoring and regulatory, legal, or court ordered actions.
8. Authentication and authorization successes and failures;
9. Session management failures
10. Use of higher-risk functionality (e.g., addition or deletion of application credentials, changes to privileges, assigning users to tokens, adding or deleting tokens, submission of user-generated content - especially file uploads)
11. Legal and other opt-ins (e.g., permissions for mobile phone capabilities, terms of use, terms and conditions, personal data usage consent, permission to receive marketing communications)
12. Suspicious, unacceptable or unexpected behavior

Application logs will be reviewed at least quarterly. Corrective actions to address application deficiencies will be managed through the application development process or the POAM process.

3.4 Audit and Logging Requirements for Business Partners

This standard is intended to be adapted for use in DHHS procurement standards and RFP templates. In this way, DHHS can ensure that new IT systems, whether developed in-house or procured, support necessary audit logging and log management functions.

3.5 Audit and Review Scheduling

The ISO is responsible for maintaining an audit schedule detailing required periodic IT audits. The schedule will detail the yearly dates of each audit, what business unit or program area is responsible for completing the audit, and the date the audit is completed. This schedule at minimum will include:

- Weekly RACF Report Review
- Bi-annual Alter Access review for systems managing highly restricted and confidential data
- Annual Timely Termination Review
- Annual New-Hire Privacy & Security Awareness Training Review
- Annual External Partner Access Review
- Periodic Physical Safeguard Site Review of DHHS Offices and Facilities
- Daily, Weekly, and Monthly review of logs from auditable events

4.0 Revision History

Legal Review – 09-30-2013
Policy Approved – 09-30-2013

Signature:

Eric Henrichsen

Date: 9/30/2013

Eric Henrichsen
Information System & Technology Administrator
Nebraska Department of Health & Human Services