COMMONWEALTH OF PENNSYLVANIA DEPARTMENT'S OF PUBLIC WELFARE, INSURANCE AND AGING

INFORMATION TECHNOLOGY STANDARD

Name Of Standard: **Audit Logging Standard**	Number: **STD-ENSS026**
Domain: **Security**	Category:
Date Issued: **09/07/2012**	Issued By Direction Of: Shirley A. Monroe Shirley A. Monroe, Dir of Div of Technical Engineering
Date Revised: **08/28/2013**	

Abstract:

This standard describes the Department's minimum audit logging requirements within the department's Information Technology environment.

The security audit log management process includes:

- **Creation and Storage of Audit Logs** – Audit logs must be retained in sufficient detail to facilitate reconstruction of events and determination of the causes of compromise and magnitude of damage, in response to a malfunction or a security violation.
- **Review and Analysis** – Timely and effective review of audit logs is required to allow identification of security incidents, policy violations, fraudulent activity, and operational problems; while providing information useful for resolving such problems.
- **Establishment of Supporting Processes and Resources** – Processes and resources must be established to support internal investigations, forensic analysis, establishment of baselines, and identification of operational trends and long-term issues.

The minimum audit logging requirements for auditable events, requirements for content of audit records and a list of IT systems for which these requirements apply, are discussed below.

General:

Audit Logging Standard applies to the Department of Public Welfare ("Department") IT system and application logs. The requirements outlined in this document are the minimum required to be considered adequate for meeting the log management requirements at the Department.

Standard:

Auditable Events: System owners shall ensure department applications and information systems shall, at a minimum, record for the following events:

- Successful and unsuccessful access to log files.
- Successful and unsuccessful authentication events.
- Successful and unsuccessful authorization events.
- Successful and unsuccessful resource access events.

- Successful and unsuccessful privileged operations.
- Creation, modification and deletion of user accounts, group accounts and objects including files, directories and user accounts.
- Creation, modification and deletion of command line changes, batch file changes and queries made to databases.
- Creation, modification and deletion of security policy.
- Changes to logical access control authorities (e.g., rights, permissions).
- System and/or applications shutdowns, reboots/restarts, errors.
- All system changes with the potential to compromise the integrity of audit policy configurations, security policy configurations and audit record generation services.
- All logging information as part of perimeter devices, including firewalls and routers (e.g., log packet, packet screening/filter, user account management, modification of proxy services)

Log Aggregation: System owners shall ensure department applications and information systems have the capability to compile audit records from multiple components throughout the system into a system-wide (logical or physical), time-correlated audit trail.

Time Synchronization: System owners shall ensure department applications and information systems use a synchronized clock for recording timestamps.

Continuous Auditing: System owners shall identify for each system under their purview, which events require auditing on a continuous basis and which events require auditing in response to specific situations based on an assessment of risk.

SIEM Integration: The department Chief Information Security Officer (CISO) or his/her designee shall ensure logs from DEPARTMENT applications and information systems are integrated with the department's Security Information and Event Management (SIEM) solution – RSA enVision. Department applications that record multiple actions (e.g. read, write, delete) into a single log entry, should separate each performed action into an individual log entry before SIEM integration. Applications that implement custom logging formats should follow the audit log content requirements specified in the SIEM integration guideline for that application.

Auditable Events Review: All security events and operational logs will be reviewed to detect deviation from policy and to test the effectiveness of access control and security mechanisms.

Audit log reports shall be generated on a periodic basis, and made available for management review. A risk analysis shall be conducted to determine the frequency for reviewing audit logs for specific systems and applications based on their criticality and risk profile. Review of the audit logs shall be conducted by authorized personnel.

The CISO or his/her designee shall periodically review the list of DEPARTMENT-defined auditable events, and update the list as needed. This review shall include consideration of:

- Events that require auditing on a continuous basis
- Events that require auditing in response to specific situations based on an assessment of risk.

Audit Log Retention: System owners shall integrate department systems and applications with the RSA enVision for centralized storage and archival of audit logs. Audit logging systems shall provide a warning when allocated audit record storage volume reaches 80%. The following table describes the log retention requirements for audit logs:

Audit Log Compliance Requirements	**Local System Log Retention**	**SIEM Log Retention**	**Archive Log Retention**
Social Security Administration (SSA)	Undefined	Undefined	7 years
Internal Revenue Service (IRS)	Undefined	Undefined	5 years
Department of Public Welfare (DPW)	3 weeks	2 years	2 years

Log Type	**Retention Period**
Blue Coat Logs (Internet)	12 Full months
Siteminder	7 years
Firewall	12 full months
IPS database and system backup	6 years

Audit Log Protection: System owners shall permit read only access to audit logs for the appropriate system administrators and CISO.

Audit Log Reporting:

System owners shall periodically review audit records for inappropriate or unusual activity, investigate suspicious activity or suspected violations, and report findings to the CISO. Automated mechanisms shall be implemented to:

- alert on audit log failure, audit storage capacity near maximum; and
- Facilitate the review of audit records shall be implemented for moderate- or high-impact systems.

The following table describes a list of department applications and the corresponding audit content requirement for each:

	Audit Log Content Requirement	CA SiteMinder	Application FGAC	Database	Active Directory	IBM Tivoli Identity Manager	Microsoft IIS
1	Timestamp	X	X	X	X	X	X
2	User ID	X	X	X	X	X	X
3	Source IP address or application	X	X	X	X	X	X
4	Application or service accessed	X	X	X			X
5	Resource page name	X	X				X
6	Module/Function accessed	X	X		X	X	X
7	Action performed (Read/Update/Create/Delete)	X	X	X	X	X	X
8	Primary Record Identifier (Consistent)	X	X	X			
9	Data field accessed/updated (contains the previous and current value)		X	X			
10	User roles and account information a. Date added b. Last modified c. User introducing the change		X	X	X	X	

The following table describes a list of department infrastructure systems and the corresponding audit content requirement for each:

	Audit Log Content Requirement	Firewall	Antivirus	Intrusion Detection	SIEM
1	Timestamp	X	X	X	X
2	User ID		X	X	X
3	Source IP address or application	X	X	X	X
4	Application or service accessed	X	X	X	X
5	Resource page name				X
6	Module/Function accessed			X	X
7	Action performed (Read/Update/Create/Delete)		X	X	X
8	Primary Record Identifier (Consistent)				X
9	Data field accessed/updated (contains the previous and current value)				X

Exemptions from this Standard:

Any exemptions to comply with this standard should be discussed with the Departments' Chief Information Security Officer (CISO).

Refresh Schedule:

All standards and referenced documentation identified in this standard will be subject to review and possible revision annually or upon request by the DPW Information Technology Standards

References:

1. POL-SEC009: Security Audit Logging Policy
2. ITB-SEC021: Security Information and Event Management Policy

Standard Revision Log:

Change Date	Version	Change Description	Author and Organization
09/07/2012	1.0	Audit Logging	Clifton Van Scyoc
08/28/2013	1.1	Auditable Events, Audit Review	Mathieu Saury