

COMMONWEALTH OF PENNSYLVANIA
DEPARTMENT OF HUMAN SERVICES,
INSURANCE AND AGING

INFORMATION TECHNOLOGY POLICY

Name Of Policy: Security Audit Logging Policy	Number: POL-SEC009
Domain: Security	Category:
Date Issued: 05/23/11	Issued By Direction Of: 
Date Revised: 07/19/17	Sandra K. Patterson, CIO Bureau of Information Systems

Table of Contents

1	Introduction	3
1.1	Purpose	3
1.2	Scope	3
1.3	Compliance	3
1.4	Exemptions.....	3
1.5	Policy Review and Update	3
2	Security Audit Log Management.....	3
2.1	Auditable Events	3
2.2	Content of Audit Records	4
2.3	Audit Record Retention	5
2.4	Protection of Audit Information.....	6
2.5	Audit Monitoring, Analysis, and Reporting	6
2.6	Audit Reduction and Report Generation	7
2.7	Response to Audit Processing Failures	7
	Appendix	8
2.1	Supporting DHS Policies.....	8

1 Introduction

1.1 Purpose

This policy establishes requirements for the collection, maintenance and review of audit logs for DHS applications and related network resources, in support of identity management and threat monitoring. This policy also addresses compliance with related DHS, Commonwealth of Pennsylvania (CoPA) and federal requirements.

Audit logs consist of information trails that are used to track and associate user and system activity to events. In conjunction with the appropriate tools and procedures, auditing can assist in detecting security violations, as well as performance problems and application flaws. While the prevention of intrusion is ideal, detection is critical, as is the implementation of an effective information assurance auditing policy.

1.2 Scope

All DHS employees, contractors and other stakeholders are responsible for understanding and complying with this policy. Audit logs include CoPA network access logs, system logs, authentication logs, or any other data which correlate a network or system activity with a user and/or time.

1.3 Compliance

All DHS employees, contractors and other stakeholders are expected to be familiar with and comply with this policy. Violations of this policy may lead to revocation of system privileges and/or disciplinary action.

1.4 Exemptions

Requests for exemption to the policy should be submitted to the Chief Information Security Officer (CISO). Any exceptions granted will be issued a policy waiver for a defined period of time.

1.5 Policy Review and Update

This document, and its supporting standards and procedures, will be reviewed annually, and updated as needed.

2 Security Audit Log Management

Security Audit log (“audit logs”) management includes:

- Maintain Integrity, Confidentiality and accessibility to Agency logs.
- **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.

2.1 Auditable Events

Auditable events are those activities that can be tracked that provide information regarding system resource usage. The following policy addresses the requirement for DHS information systems to generate records for identified auditable events.

DHS Policy

- a. DHS shall identify the systems, applications, or processes that make data vulnerable to unauthorized or inappropriate tampering, uses, or disclosures. For each identified system, application, or process. DHS shall identify user activities (e.g., Create, Read, Update, and Delete) that need to be tracked and audited.
- b. DHS applications and information systems shall, at a minimum, perform an annual review, record, alert and report 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, application/system errors, modification of proxy services)
- a. DHS applications and information systems shall review of identified critical transactions to be reviewed every 30 days
- c. DHS applications and information systems shall have the capability to compile audit records from multiple components throughout the system into a system-wide (logical or physical), time-correlated audit trail.
- d. DHS applications and information systems shall use a synchronized clock for recording timestamps.
- e. 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.
- f. Audit logs from DHS applications and information systems shall be integrated with the Commonwealth's standard Security Information and Event Management (SIEM) solution ("DHS SIEM solution") described in Information Technology Bulletin (ITB)-SEC021.
- g. The CISO shall periodically review the list of DHS-defined auditable events, and update the list as needed. This review shall include consideration of: (a) events that require auditing on a continuous basis, and (b) events that require auditing in response to specific situations based on an assessment of risk.

2.2 Content of Audit Records

The following policy provides guidance to ensure that the information that is included in audit records is sufficient in detail to facilitate the reconstruction of events upon a suspected or actual system compromise or malfunction.

DHS Policy

- a. DHS information systems shall generate audit records that contain sufficient information to establish what events occurred, the sources of the events, and the outcomes of the events. In addition, audit record content shall provide the capability to determine whether a given individual took a particular action.
- b. DHS information systems shall, at a minimum, record the following information:
 - a. Timestamp
 - b. UserID / Domain
 - c. Source IP address or application
 - d. Application or service accessed
 - e. Resource or complete URL
 - f. Module/Function accessed
 - g. Unique Action performed (Read/Update/Create/Delete)
 - h. Primary record identifier
 - i. Data field accessed/updated.

2.3 Audit Record Retention

Audit records are to be kept available to support analysis relating to misuse, penetration reconstruction, or other investigations. The following policy provides guidance to ensure that audit logs are retained in accordance with DHS, CoPA and federal requirements, as well as to provide support for investigations of security incidents.

DHS Policy

- a. DHS information systems shall leverage the Commonwealth's standard SIEM solution for an integrated and real-time analysis of security alerts and incident management generated by network hardware and applications. This will provide the agencies with a centralized ability for data aggregation, correlation, compliance and alerting of audit logs.
- b. Audit logs shall be retained for at least two years and archive old records for one (1) year to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements, with the following exceptions:
 - DHS information systems and application that should meet Social Security Administration (SSA) security requirements shall maintain the audit logs for seven years.
 - DHS information systems and application that should meet Internal Revenue Service (IRS) publication 1075 security requirements shall maintain the audit logs for six years.
 - DHS information systems and application that should meet the CJIS security requirements shall retain audit record for at least 365 days and shall continue to retain them until it is determined they are no longer needed for administrative, legal, audit or other operation purposes.
 - For PHI data only, DHS shall verify within every (90) days that sensitive information are erased or its use is still required
- c. The organization allocates sufficient audit record storage capacity and configures auditing to reduce the likelihood of such capacity being exceeded. DHS information systems may leverage the agencies standard SIEM solution for centralized storage of audit logs.
- d. System owners shall ensure that the system allocates sufficient audit record storage capacity and configures auditing to reduce the likelihood of such capacity being exceeded. DHS audit processes shall provide a warning when allocated audit record storage volume reaches 80%.
- e. DHS information systems and applications shall maintain up to three weeks of audit logs on the corresponding information system or application. Other audit logs shall be securely stored using

DHS Policy

DHS's archival process or using tape backups.

- f. Access to archived audit logs and tape backups shall be restricted by the corresponding system owners.
- g. DHS SIEM solution shall maintain audit logs for reporting and analysis in the SIEM database. The remaining audit logs shall be securely stored using DHS's archival process or using tape backups.

2.4 Protection of Audit Information

The following policy provides guidance to ensure that audit information is protected.

DHS Policy

- a. DHS information systems shall protect audit information and audit tools from unauthorized access, modification, and deletion.
- b. System owners shall ensure that their audit trails and audit logs are protected from unauthorized modification, access, or destruction while online and during offline storage.
- c. Audit trails are to be protected against unauthorized access, modification, or deletion. The contents of audit log data can be protected in the following ways:
 - Restrict physical access to the system
 - Permit read only access to audit logs for the appropriate system administrators and CISO.

2.5 Audit Monitoring, Analysis, and Reporting

The following policy addresses requirements for monitoring, analysis of audit logs, and the generation of audit reports.

DHS Policy

- a. All security events and operational logs shall be reviewed to detect deviation from policy and to test the effectiveness of access control and security mechanisms.
- b. DHS shall employ automated mechanisms to integrate audit monitoring, analysis, and reporting into an overall process for investigation and response to unauthorized access and unexpected traffic.
- c. DHS shall employ automated mechanisms to periodically review audit records to track and follow unusual activities, or security anomalies:
 - Items defined in the system security plan
 - Audit failure
 - Audit storage capacity near maximum
- d. 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, using DHS SIEM solution.
- e. System owners shall develop and implement a process to periodically review audit records for inappropriate or unusual activity, investigate suspicious activity or suspected violations, and report findings to the appropriate officials. For moderate- or high-impact systems, the system owners shall employ an automated mechanism to facilitate the review of audit records. Audit records related to activities of users with significant information systems roles and responsibilities shall be reviewed more frequently.
- f. System owners shall use automated mechanisms to integrate their audit procedures into DHS's

DHS Policy

- incident response capability, which provides for centralized audit monitoring, analysis, and reporting.
- g. DHS Information systems and application administrators shall review at least once every fourteen (14) days to ensure unauthorized administrators accounts have not been created.
 - h. DHS Information systems and application shall review system records, network traffic log-ons, errors, system processes and performance; and system resources utilization to determine anomalies on demand at least once every twenty-four (24) hours period.
 - i. DHS Information systems and application shall perform manual reviews of system audit records randomly on demand but at least once every thirty (30) days.
 - j. DHS Information system shall use automated utilities to review audit records at least once every seven (7) days for unusual, unexpected, or suspicious behavior.
 - k. DHS shall regularly review / analyze information system audit records for indications of inappropriate or unusual activity, investigates suspicious activity or suspected violations, reports findings to appropriate officials, and takes necessary actions.
 - l. Review of the audit logs shall be conducted by authorized personnel.

2.6 Audit Reduction and Report Generation

The following policy provides guidance to ensure that DHS information systems are capable of processing audit records.

DHS Policy

- a. DHS audit processing shall have audit reduction and report generation capability. DHS information systems may leverage the DHS's SIEM solution for real-time analysis of security alerts and incident management generated by network hardware and applications.
- b. DHS audit log reports shall have the capability to automatically process audit records for events of interest based upon selectable, event criteria.
- c. System owners shall utilize audit reduction, review, and reporting techniques while ensuring that original audit records needed to support after-the-fact investigations are not altered.

2.7 Response to Audit Processing Failures

The following policy provides guidance to ensure that DHS information systems are capable of alerting personnel in the event of an audit processing failure.

DHS Policy

- a. DHS audit processes shall alert appropriate organizational officials in the event of an audit processing failure, and take remediation actions. (System Owners shall make a risk-based decision on which actions the system should take in the event of an audit failure or when audit capacity is being reached.)
- b. DHS audit processes shall provide alert the appropriate system owners when allocated audit record storage volume reaches 80%.

Appendix

2.1 Supporting DHS Policies

Document	Type
ITB SEC021 - Security Information and Event Management Policy	CoPA ITB
MD245.18 - IT Administrator Acceptable Use, Auditing and Monitoring, Incident Notification, and Response Policies and Procedures	CoPA MD

Policy Revision Log:

Change Date	Version	Change Description	Author and Organization
05/23/2011	1.0	Initial Creation	David Johnson
06/17/2011	2.0	Revised per Tom Zarb Review	David Johnson
11/11/2013	2.1	Revised by Brian Stewart	Brian Stewart
07/19/2017	2.2	Annual Revision	John Miknich