pennsylvania
DEPARTMENT OF LABOR & INDUSTRY
OFFICE OF INFORMATION TECHNOLOGY

L&I, Office of Information Technology Policy SEC-012

Name:	Audit, Accountability, and Reporting Policy
Effective Date:	December 2016
Category:	Security
Version:	1.1

1. Purpose:

To provide directions and identify guidelines regarding audit and accountability policies for the Department of Labor & Industry (L&I), while also fulfilling the requirements of Internal Revenue Service (IRS) Publication 1075, NIST SP 800-53, NIST 800-100, NIST 800-66 and NIST 800-92. This policy establishes Enterprise Audit and Accountability policy for managing risks from inadequate event logging and transaction monitoring through an effective audit and accountability program. This accountability will help protect information, including Federal Tax Information (FTI), from unauthorized access and improper disclosure in compliance with safeguards and requirements defined by the Social Security Administration (SSA) and the IRS.

2. Background:

This policy is published under the general authority of the Governor's Office of Administration / Office of Information Technology (OA/OIT) based on requirements of IRS Publication 1075, which identifies key roles and responsibilities regarding audit and accountability, and direction regarding acceptable audit and accountability standards.

L&I systems capture a wealth of information about system health, application performance and security. Data owners, define the contents of the audit record based on federal and state statues. System administrators, and application administrators define their support procedures based on defined triggers, thresholds, or severity of an event. Routine checks of these logs can help L&I Office of Information Technology (OIT) and system owners determine health and availability of their service.

3. Scope:

This policy applies to all employees, contractors, temporary personnel, members of boards, commissions and councils, agents, and vendors in the service of L&I (hereinafter referred to collectively as "L&I Users").

4. Policy:

In accordance with IRS Publication 1075, NIST SP 800-53, AU-1 through AU-11, OIT Enterprise Security and Compliance Section (ESC) will oversee IT audits and will conduct Information Technology (IT) security audits for all systems classified as, "sensitive", or "protected", per OA ITP-SEC019. Each system will be audited for security controls at least once every three (3) years to assess whether the IT security controls implemented are operating adequately and effectively. L&I's Chief Information Security Officer (CISO) is accountable for the oversight of comprehensive monitoring and logging for L&I systems and infrastructure. ESC's Quality Assurance and Release (QAR) Manager is responsible for the IT security audits of L&I systems. The CISO or QAR Manager shall verify IT security audits that are performed by independent parties not associated with the processes or procedures of the system.

A. Auditable Events:

1. At a minimum, all L&I IT systems must be capable of and configured to:
    - Produce audit logs with the necessary event information.
    - Have the ability to off-load audit log data to a log aggregation server.
2. Based on a risk assessment and business needs, the Data Owner (DO) shall determine and report to ESC whether their IT system must be audited for the following events:
    - Authentication attempts
    - Authenticated individual
    - Access time
    - Source of access
    - Duration of access
    - Actions executed
3. Events must be logged in real time, to the fullest extent possible, stored locally, and sent to the central log analysis server as the event is recorded. Systems must ensure the integrity protection and authentication of an event transmitted to the log analysis server.
4. Network devices such as routers, switches, hubs, firewalls, and other devices that facilitate the transfer of packets from one point to another must be configured to log security data as well as errors. Network devices must be configured to transmit recorded events to the central log analysis server as the event is recorded by the network device.
5. Applications, including web services and database services residing on servers that utilize cached or separate authentication capabilities must maintain logs of all security, application, and event-related information.
6. End-user workstations, including but not limited to desktops and laptops, must maintain logs of security-related events. These devices must also forward the security event information to a central log analysis server as the event occurs.
7. The DO shall coordinate the security audit function with other L&I staff that require audit-related information to select auditable events.
8. The DO and CISO shall ensure events selected for the audit log fully support after-the-fact investigations.

B. Content of Audit Records:

1. The System Administrator (SA) shall configure the system so that the audit records contain sufficient information to, at a minimum:
   - Establish what type of event occurred (i.e. event id).
   - When (date and time) the event occurred (i.e. time stamp).
     a. The time may be expressed in Coordinated Universal Time (UTC), a modern continuation of Greenwich Mean Time (GMT), or local time with an offset from UTC.
     b. All systems must utilize Network Time Protocol (NTP) time synchronization.
   - Where the event occurred (i.e. destination IP address).
   - The source of the event (i.e. source IP address).
   - The outcome (success or failure) of the event.
   - The identity of any user/subject associated with the event (i.e. user id/process id).
   - File names involved and access control or flow control rules invoked.
2. The SA shall configure the system to log additional data, commensurate with sensitivity and risk as determined by CISO, DO and system owner.
3. L&I will centrally manage the content of audit records generated by all servers providing application support to the agency, including but not limited to database servers, messaging servers, file servers, print servers, middleware servers, and Domain Name System (DNS) servers.
4. L&I will centrally manage the content of audit records generated by all network devices providing connectivity to the agency, including but not limited to: routers, firewalls, and Intrusion Detection Systems (IDS) / Intrusion Protection Systems (IPS).

C. Audit Storage Capacity:

The SA shall ensure audit storage capacity is allocated in accordance with system configuration such that capacity is not exceeded.

D. Response to Audit Processing Failures:

1. The SA shall configure systems to alert the System Owner in the event of an audit failure.
2. All systems classified as sensitive will be configured by the SA to provide real-time alerts when the following audit failure events occur:

   - Recording of authentication attempts, or
   - Escalation of privileges.

3. These Audit Processing Failure events are considered a potential security incident and should be responded to as outlined in the L&I Security Incident Response Policy.

E. Audit Review, Analysis, and Reporting:

1. In order to effectively review, analyze and report audit data, a baseline configuration for the database shall be maintained, as well as appropriate roles and responsibilities that are definitively distinguishable from one another, to ensure that personnel who review and clear audit logs are separate from personnel who perform non-audit administration.
2. The DO shall review and analyze information system audit records at least weekly for indications of unusual activity related to potential unauthorized FTI access, security violations, or unauthorized access. This can be accomplished manually, via a dashboard, or through automation.
3. The SA shall review and analyze information system audit records at least every 30 days for indications of inappropriate or unusual activity, including changes to system-stored procedures, triggers, and any change function. This can be accomplished manually, via a dashboard, or through automation.
4. The SA shall adjust the level of audit review, analysis, and reporting within an information system when there is a change in risk to L&I’s operations, assets, individuals, other agencies, or the commonwealth.
5. All findings will be reported according to L&I’s Security Incident Response policy. If the finding involves a potential unauthorized disclosure of FTI, the appropriate special agent-in-charge, and the IRS Office of Safeguards will be contacted.
6. If a system is classified as sensitive, audit review, analysis and reporting processes must be integrated to support organizational processes for investigation and response to suspicious activities. This integration must correlate records across different repositories to gain agency-wide situational awareness. Further integration of audit records with analysis of vulnerability scanning information, performance data, and network monitoring information must be used to enhance the ability to identify inappropriate or unusual activity.
7. The Infrastructure and Computing Services (ICS) staff shall monitor the infrastructure and log files on a continuous basis and document the activity at least weekly. ESC staff shall analyze Security Information and Event Management (SIEM) information and maintain regular contact with the OA Security Operations Center (SOC), and security research and coordination organizations, such as the United States Computer Emergency Readiness Team (US-CERT).

F. Protection of Audit Information:

1. Audit records, audit settings, and audit reports must be protected from unauthorized access, modification, and/or deletion.
2. Access to audit information must be restricted to System Owners and those authorized to perform IT security audits or investigate security incidents. Audit information must not be accessible by end-users of the resource or any other user or system administrator.
3. Regular backup and archival processes must be in place for audit files in order to protect historical log data and collect new log data processed by the server.
4. A central log analysis server must be built and protected with the highest level of security, as it will contain sensitive data pertaining to all L&I systems. To provide this protection, the central log analysis server must be located on a dedicated network segment and not on web or data zones, or the internal network. The central log analysis server will forward alerts about anomalous events to the ESC staff for review and action.
5. Audit records must be backed-up at least once every twenty-four hours to a different system or media than the system being audited.

G. Audit Record Retention:

L&I will retain audit records consistent with the agency's records retention policy to provide support for after-the-fact investigations of security incidents and to meet regulatory and agency information retention requirements. At a minimum, all audit data shall be maintained for a minimum of seven (7) years.

5. Responsibilities:

A. L&I User responsibilities:

- Report alerts and warnings from monitoring tools and logs; and
- Adhere to all established audit and accountability policies; and
- Fully cooperate with all audit activities.

B. L&I management responsibilities:

- Comply with all L&I policies and ensure employees comply with the policies; and
- Follow this policy and any processes regarding audit and accountability; and
- Ensure users follow this policy.

6. References:

L&I Policy Definitions Document

SEC-008-Security Incident Response Policy

OA ITP-SEC019 Policy and Procedure for Protecting Commonwealth Electronic Data

IRS Publication 1075

NIST SP 800-53 Security Controls for Federal Information Systems and Organizations

NIST 800-66 Introductory Guide for Implementing the (HIPAA) Act Security Rule

NIST SP 800-92 Guide to Computer Security Log Management

NIST SP 800-100 Information Security Handbook: A Guide for Managers

7. Version Control:

Version	Date	Purpose
1.0	06/2016	Base Document
1.1	12/2016	Content updates