	Department of Human Services Online Directives Information System	Index: Effective: Review:	POL1902 09/20/2014 11/02/2019

SUBJECT: DHS Information Security Policies

Audit and Accountability Policy

POLICY

This policy establishes the Agency Audit and Accountability Policy, for managing risks from inadequate event logging and transaction monitoring through the establishment of an effective Audit and Accountability program. The audit and accountability program helps DHS implement security best practices with regard to event and transaction logging and the retention of audit evidence.

Authority

1. United States Department of Commerce National Institute for Standards and Technology (NIST)
2. United States Internal Revenue Service
3. United States Department of Health & Human Services
4. Centers for Medicare & Medicaid Services

References

- United States Department of Commerce National Institute for Standards and Technology (NIST) Special Publication 800-53 Security and Privacy Controls for Federal Information Systems and Organizations, Revision 4, April 2013
- United States Department of Commerce National Institute for Standards and Technology (NIST) Special Publication 800-100 "Information Security Handbook: A Guide for Manager" October 2006.
- United States Department of Commerce National Institute for Standards and Technology (NIST) Special Publication 800-92 "Guide to Computer Security Log Management" September 2006.
- 45 CFR Parts 160, 162 and 164 Health Insurance Reform: Security Standards; Final Rule: Audit Controls 164.312(b)
- United States Internal Revenue Service, IRS Publication 1075 Tax Information Security Guidelines For Federal, State and Local Agencies Safeguards for Protecting Federal Tax Returns and Return Information
- Centers for Medicare & Medicaid Services, Catalog of Minimum Acceptable Risk Controls for Exchanges

Applicability

The scope of this policy is applicable to all Information Technology (IT) resources owned or operated by DHS. Any information, not specifically identified as the property of other parties, that is transmitted or stored on DHS IT resources (including e-mail, messages and files) is the property of DHS. All users (DHS employees, contractors, vendors or others) of IT resources are responsible for adhering to this policy.

Definitions

None

Responsibilities

DHS shall adopt the Audit and Accountability principles established in NIST SP 800-53 "Audit and Accountability Control Family guidelines," as the official policy for this domain. The following

subsections outline the Audit and Accountability standards that constitute DHS policy. Each DHS Business System is then bound to this policy, and shall develop or adhere to a program plan which demonstrates compliance with the policy related the standards documented. In conjunction with appropriate tools and procedures, audit trails will assist in detecting security violations, performance problems, and flaws in applications.

- **AU-1 Audit and Accountability Policy**
    1. Senior management, management, and all organization entities are required to coordinate and implement necessary controls for providing and maintaining effective auditing and accountability controls to IT resources and information systems on the basis of business and security requirements.
    2. Periodic reviews of this policy shall be performed and documented at least within every **three years**, or when there is a **significant change**.
    3. Periodic review of audit and accountability procedures shall be performed at least **annually**.
- **AU-2 Auditable Events**
    1. The agency ensures all information systems are capable, at minimum, of auditing the following event types:
        a) Log onto system
        b) Log off system
        c) Change of password
        d) All system administrator commands, while logged on as system administrator
        e) Switching accounts or running privileged actions from another account, (e.g., Linux/Unix SU or Windows RUNAS)
        f) Creation or modification of super-user groups
        g) Subset of security administrator commands, while logged on in the security administrator role
        h) Subset of system administrator commands, while logged on in the user role
        i) Clearing of the audit log file
        j) Startup and shutdown of audit functions
        k) Use of identification and authentication mechanisms (e.g., user ID and password)
        l) Change of file or user permissions or privileges (e.g., use of suid/guid, chown, su)
        m) Remote access outside of the corporate network communication channels (e.g., modems, dedicated VPN) and all dial-in access to the system
        n) Changes made to an application or database by a batch file
        o) Application-critical record changes
        p) Changes to database or application records, where the application has been bypassed to produce the change (via a file or other database utility)
        q) All system and data interactions concerning FTI
        r) Additional platform-specific events, as defined in SCSEMs located on the Office of Safeguards website

2. The security audit function shall be coordinated amongst DHS organizational entities in an effort to enhance mutual support and help tailor the selection of auditable events which helps benefit the agency's security posture.
3. Agency identified auditable events have been validated and shall require continuous review to ensure the events are adequate to support after-the-fact investigations of security incidents. The list of auditable events is reviewed and updated **at least annually** or **when there is a significant change to the information system**.

- **AU-3 Content of Audit Records**
    1. Configure information systems to generate audit records containing sufficient information to establish what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or subjects associated with the event. At a minimum, the following elements shall be identified within each audit record:
        a) What type of event occurred
        b) When (date and time) the event occurred
        c) Where the event occurred
        d) The source of the event
        e) The outcome (success or failure) of the event
        f) The identity of any user/subject associated with the event
        a) Audit records are created such that they contain sufficient amounts of detail required to reconstruct events if unauthorized activity or a malfunction occurs or is suspected. At a minimum, audit records shall record for audit events identified by type, location, or subject.

- **AU-4 Audit Storage Capacity**
    Audit record storage capacity has been established, and shall be maintained to reduce the likelihood of exceeding capacity. The agency retains audit records for the required audit retention of **seven years** to meet agency retention requirements.
- **AU-5 Response to Audit Processing Failures**
    1. Designated organizational or service provider officials are alerted in the event of an audit processing failure.
    2. System operational status is monitored using operating system or system audit logs. Functions and performance of the system are also verified.
    3. Identified personnel are notified when allocated audit record storage volume is reaches maximum audit record storage capacity.
- **AU-6 Audit Review, Analysis, and Reporting**
    1. Information system audit records shall be reviewed at least **weekly** (or more frequently at the discretion of the information system owner) for indications of inappropriate or unusual activity related to potential unauthorized access (e.g. access to FTI). Unauthorized access found via audit records review is immediately reported to supervision and OIT Security.
    2. Unauthorized disclosures of FTI are reported in accordance with the agency's Incident Response Plan, Treasury Inspector General for Tax Administration (TIGTA) requirements, and the IRS Office of Safeguard contact requirements.
    3. The agency adjusts the level of audit review, analysis, and reporting within the information asset when there is a change in risk to organizational operations, organizational assets, individuals, other organizations due to credible intelligence.

- **AU-7 Audit Reduction and Report Generation**
    1. Agency service providers provide audit reduction and report generation to support on-demand audit reviews, analysis, reporting requirements and after-the-action investigations of security incidents
    2. Mechanisms to prevent the altering of data in its original content or time ordering of audit records are employed.
- **AU-8 Time Stamps**
    1. Internal system clocks are utilized in order to generate time stamps for audit records to facilitate logging and monitoring.
    2. Time stamps for audit records are recorded to ensure that audit records can be mapped to Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT).
    3. The internal information system clocks are compared and synchronized to approved authoritative time sources (e.g. NIST, Naval Observatory).
- **AU-9 Protection of Audit Information**
    1. The agency ensures that audit information and audit tools are protected from unauthorized access, modification, and deletion by ensuring appropriate access controls are implemented and maintained.
    2. Explicit authorization is required for access to manage audit functionality, and is restricted only to designated security administrator(s) or staff other than system or network administrators.
    3. System and network administrators do not have the ability to modify or delete audit log entries.
- **AU-10 Non-Repudiation**
  The agency protects against an individual falsely denying having performed a particular action on company information assets by ensuring appropriate non-repudiation mechanisms are implemented.
- **AU-11 Audit Record Retention**
  Audit records on agency information systems that **DO NOT** host, store, and transmits FTI data are maintained for **90 days** and archive old records for **one year.** Audit records for information systems which host, store and transmits FTI data to support after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements are maintained for **seven years**.
- **AU-12 Audit Generation:** DHS shall:
    1. Audit record generation capability for the list of auditable events defined in AU-2 for information systems is implemented.
    2. Designated organizational personnel select which auditable events are to be audited by specific components of the system.
    3. Audit records for the list of audited events defined in AU-2 with the content as defined in AU-3 are generated.
- **AU-16 Cross-Agency Auditing**
  DHS employs mechanisms for coordinating the access and protection of audit information among external organizations when audit information is transmitted across agency boundaries.

History
None