Audit Logging Standard

1.0 Purpose

Comprehensive logging from critical systems, applications, and services is essential for security monitoring, incident response, forensic analysis, and compliance verification. Audit logs provide crucial information about activities performed, potential indicators of compromise, and system behavior. The purpose of this policy is to define the minimum requirements for generating, formatting, storing, and protecting audit logs across the organization's information systems. This ensures that sufficient information is captured to reconstruct events, detect anomalies, investigate security incidents, and meet regulatory obligations. These requirements should guide the configuration of existing systems and serve as baseline criteria for developing or procuring new systems.

2.0 Scope

This policy applies to all production systems, applications, network devices, and services operating on the organization's network, particularly those that handle sensitive or confidential information, accept network connections, perform authentication or authorization functions, or are otherwise deemed critical to business operations or security.

3.0 Policy Statements

All systems and applications within the scope of this policy must be configured to generate and manage audit logs according to the following requirements:

3.1 General Logging Requirement

Systems must record and retain audit log information sufficient to establish accountability and answer key questions about activities performed, including:

* **What** activity occurred?
* **Who/What** performed the activity (subject identity, source system/IP)?
* **On What** was the activity performed (object/target)?
* **When** did the activity occur (timestamp)?
* **With What Tool** was the activity performed (application, utility)?
* **What** was the outcome (status, success/failure)?

3.2 Logged Activities

At a minimum, audit logs must be generated for the following types of activities:

*   **Data Access/Modification:** Creation, reading, updating, or deletion of sensitive or confidential information (including authentication credentials like passwords). Creation, update, or deletion of other significant data.
*   **Network Activity:** Initiation or acceptance of network connections (e.g., firewall logs, server connection logs).
*   **Authentication/Authorization:** User login attempts (success and failure), user logouts, elevation of privileges.
*   **Access Control Changes:** Granting, modifying, or revoking access rights or permissions (e.g., adding/deleting users/groups, changing privilege levels, modifying file/database permissions, altering firewall rules, user password changes).
*   **System/Configuration Changes:** Significant changes to system, network, or service configurations, including installation/removal of software, application of patches/updates, modification of critical configuration files.
*   **Application Lifecycle:** Application process startup, shutdown, restart, abort, failure, or abnormal termination, particularly events related to resource exhaustion (CPU, memory, disk, network) or service failures (DNS, DHCP).
*   **Security Events:** Detection of suspicious or malicious activity by security tools (e.g., Intrusion Detection/Prevention Systems, Anti-Virus/Anti-Malware, File Integrity Monitoring).

3.3 Required Log Content (Log Elements)

Each log entry must contain sufficient detail to meet the requirements in section 3.1. Where possible, log entries should include, directly or indirectly (unambiguously inferred), at least the following elements:

*   **Timestamp:** Accurate date and time of the event, including time zone information or use of Coordinated Universal Time (UTC).
*   **Event/Activity Type:** Clear description of the action performed (e.g., login, read, delete, connect, modify_permission).
*   **Subject Information:** Identity of the user, service, or process performing the action (e.g., User ID, service account name, process ID).
*   **Source Information:** Origin of the activity (e.g., source IP address, source hostname, client application name).
*   **Object Information:** Target of the action (e.g., file path accessed, database record ID, target IP address, target hostname, service modified).
*   **Status/Outcome:** Indication of success or failure of the action.
*   **Reason Codes (if applicable):** For denied actions, codes or descriptions explaining the reason for denial (e.g., invalid password, insufficient permissions).
*   **Before/After Values (if feasible):** For update actions on critical data elements, logging the value before and after the change.
*   **System/Service Identifier:** Clear identification of the system, application, or service generating the log entry.

(Standardization of identifiers like usernames and IP addresses across logs is crucial for effective correlation.)

3.4 Log Formatting, Storage, and Protection

*   **Integrity:** Logs must be generated and stored in a manner that prevents unauthorized modification or deletion. Write-once media, secure append-only modes, digital signing, or forwarding to a secure, centralized logging system are required.
*   **Centralization:** Logs from systems within scope should be forwarded in near real-time to the organization's centralized log management system (e.g., SIEM - Security Information and Event Management).
*   **Standard Formatting:** Systems should support logging in a standardized, well-documented format suitable for parsing and analysis by the centralized log management system. Acceptable mechanisms include:
    *   Microsoft Windows Event Logs (forwarded securely).
    *   Syslog (using secure protocols like TLS-encrypted syslog or reliable syslog variants).
    *   Database logging (to tables within an ANSI-SQL compliant database that is itself securely logged).
    *   Other industry-standard formats compatible with the organization's SIEM (e.g., CEF, LEEF, JSON formats).
*   **Retention:** Audit logs must be retained according to the organization's Record Retention Schedule and relevant regulatory/compliance requirements, both online (in the SIEM) for analysis and offline (archived securely) for long-term storage.
*   **Access Control:** Access to audit logs must be restricted to authorized personnel on a need-to-know basis.

4.0 Compliance

4.1 Compliance Measurement

The designated IT authority (e.g., Precision Computer team, Information Security, Internal Audit) will verify compliance with this policy through various methods, including configuration audits, review of log content and coverage, testing log forwarding mechanisms, reviewing SIEM integration, internal/external audits, and assessing incident response capabilities reliant on logs.

4.2 Exceptions

Any exception to this policy (e.g., for legacy systems unable to meet specific requirements) requires formal, documented justification, risk assessment outlining compensating controls, and advance approval from the designated IT authority (e.g., Precision Computer team or Information Security).

4.3 Enforcement

Systems found to be non-compliant with this policy may be required to undergo remediation within a defined timeframe or risk being isolated or removed from the network. Failure by personnel responsible for system administration or development to adhere to this policy may result in disciplinary action, up to and including termination of employment or contract.

5.0 Definitions

*   **Audit Log:** A chronological record of system activities, including events related to security, operations, and data access.
*   **SIEM (Security Information and Event Management):** Technology providing real-time analysis of security alerts generated by applications and network hardware. Combines Security Information Management (SIM) and Security Event Management (SEM).
*   **Syslog:** A standard protocol for sending system log or event messages to a specific server (syslog server).

6.0 Related Policies

*   Information Security Policy (Overall)
*   Data Classification Policy
*   Record Retention Schedule / Policy
*   Incident Response Plan
*   Change Management Policy
*   Secure Development Policy / Standards

Revision #3
Created 28 August 2024 16:53:46 by Daniel O
Updated 16 September 2025 22:10:08 by Travis Woolery