WAYNE STATE UNIVERSITY

Computing & Information Technology

Standard for Audit and Accountability

Purpose

This standard establishes the need for the University to maintain appropriate audit record and system logging functionality for university systems and applications in order to efficiently troubleshoot issues, identify possible suspicious or unauthorized activity, and to assist in responding to IT security incidents.

Scope

The scope of this standard covers all electronic systems that provide computer services or store or process university data, whether managed centrally by C&IT or at a departmental support level.

Roles and Responsibilities

University IT staff will configure information systems under their authority with the requisite settings, scripts, or programs to ensure that computing events deemed necessary for security purposes are properly generated, stored, monitored, and reviewed, and that these audit records are made readily available to the C&IT Information Security Office.

University management will include minimum requirements as defined by this standard and related materials for audit records and logging as prerequisites for any information system or application which is purchased, procured, developed, or implemented.

The C&IT Information Security office assist system administrators in ensuring their systems and applications are generating audit records and logs that meet the minimum standards as defined by this standard and related materials.

Audit and Accountability Standards, Procedures, and Guidelines

Detailed procedures, standards, and guidelines will be authored and maintained by the C&IT Information Security Office outlining the specific audit record and logging security controls to be developed and implemented, along with appropriate guidance. New or modified procedures, standards and guidelines will be communicated to all University IT staff once approved by the C&IT Risk & Security Oversight Committee.

Organizational Coordination

The C&IT Information Security Office will solicit feedback from on-campus IT units regarding the effectiveness and applicability of this standard and related materials, taking it into consideration during periodic standard review. This standard and associated documents will be openly published and communicated to all IT staff at a minimum of an annual basis.

Compliance
All university units are required to be in compliance with this standard and any associated materials. Any exceptions to this standard must be approved by the C&IT Information Security office, will be given a deadline for proper compliance, and will be reviewed on an annual basis.

Standard Review
This standard and any associated materials will be reviewed at a minimum on an annual basis by the C&IT Risk & Security Oversight Committee.

Definitions
As used in this standard, *"audit record"* refers to the generation of text output that summarizes details of an individual action or transaction in an information system, and is also commonly referred to as a *"log entry".* An *"audit log"* or *"log file"* is a combination of audit records or log entries for an individual information system.

As used in this standard, *"enterprise systems"* are electronic information systems maintained by C&IT that contain confidential institutional data. Current examples of enterprise systems include Banner, Cognos, and Imaging.

General Standards for Audit and Accountability
The University must use and maintain the following controls in active information systems to maintain a standard and reliable audit and logging structure:

1. Audit Record Capabilities. Given the type and classification of events for information systems that process university data, the following events are minimally sufficient to support proper identification during troubleshooting or incident handling. Information systems must be able to audit or log the following events at minimum:
    - Successful login or session creation;
    - Successful logout or session destruction;
    - Failed login attempts;
    - Read or write access to data elements which contain confidential information;
    - Creation, modification, or removal of standard or administrative user accounts;
    - Creation, modification, or removal of standard or user account privileges;

2. Audit Record Content. Each individual audit record or log entry must contain a timestamp, an event name, the system or application generating the log, the source address or process causing the log event, the result of the event, and any associated username or identity.

3. Information System Logging. Information system components at the operating system and application levels must be able to be produce audit records or system logs via the above specifications immediately on the occurrence of each event, and system administrators must ensure audit records are being generated correctly.

4. Audit Record Retention. Unless specified by regulation or contractual agreement audit records or system logs are kept for a minimum of 90 days on a remote storage system, or local generating device if remote storage is not technically feasible. Any utilized file systems and log storage locations must be sized to retain logs for this duration.

5. Log System Monitoring. The failure of any part of the audit record generation process immediately notifies the system administrator via email, alert, or other noticeable means. In the event of storage failure, information systems should attempt to write to additional locations or overwrite oldest log entries in order to continue logging functionality.

6. Audit Record Review. System administrators review audit record and log file activity for signs of unauthorized access on at least a weekly basis, reporting any suspected abnormalities or incidents to the Information Security Office. Reviews can be performed via either manual or automated means.

7. Audit Record Security. Audit records and log entries are secured via available application or system means from unauthorized access, modification, or deletion. This may include controls such as making the destination file system unwritable by users or by writing the logs to a system out of the control of the system administrator.

8. Accurate Timestamps. Audit records and log entries are tagged or created with a timestamp generated by the issuing system that is within three seconds of Universal Coordinated Time (UTC) and is configured correctly with time zone information.

9. Audit Record and Log File Selection. C&IT Information Security Office coordinates and guides configuration of audit functionality per these specifications. Requirements may change over time based on threat, regulation or active investigation.

10. Audit Log Collection. C&IT Information Security Office may request specific audit logs to support investigation of security incidents or facility threat monitoring. These audit logs must be delivered securely over the network to a central location maintained by C&IT.

Additional Standards for Enterprise Systems

Enterprise systems that store or process confidential data are subject to a higher standard of system auditing and require the following additional security controls:

1. Additional Audit Record Details. Enterprise systems must additionally generate audit records at the operating system level for each command or operation performed by a system administrator, including the full text of any typed commands or parameters.

2. On-demand Audit Record Review. Information systems must permit the viewing, analysis, and export of log data in the event of a security incident without modifying any individual log entries. Logs must me filterable or searchable by timestamp, event name, source IP address, and relevant username.

3. Centralized Audit Record Storage. Audit records or logs are immediately copied and sent over the network to an approved central location which is read-only to any accessing users.

4. Restricted Audit Record Privileges. Write access to audit records and changing audit functionality is further restricted to a minimal number of system administrators. Administrator actions that change audit log settings are immediately sent to a centralized log system for immediate follow-up.

5. Audit Record Automation. Upon request of the ISO, audit records or log entries are sent to and analyzed by the ISO SIEM system which normalizes, correlates, and provides organization-wide situational awareness of potential security issues at the university.

6. Synchronized Timestamps. System and application timestamps are checked against an approved timeserver such as *time.wayne.edu* at a minimum of once per day, updating their internal clock when detected time skew is over one second.

7. Information System Event Review. The list of auditable and logged events for any enterprise university information system is reviewed at a minimum of an annual basis.

Non-Compliance
The C&IT Information Security Office may limit access to or from a system if it does not meet the above guidelines.

Exceptions
Exceptions to these standards may be granted by the Information Security Office given business justification and a satisfactory risk assessment. In such cases, the system owner shall acknowledge the risk and take responsibility for any breaches, incidents, or compromises that occur as a result of not utilizing a supported operating system.