



ASU System Audit Requirements Standard

Version 0.1
November 2008

Table of Contents

1 DOCUMENT CLASSIFICATION: UNIVERSITY CONFIDENTIAL.....	3
2 DOCUMENT REVISION	3
3 STANDARD	4
3.1 Underlying requirements	4
3.2 Activities to be logged	4
3.3 Elements of the log.....	4
3.4 Formatting and storage	5
4 ENFORCEMENT.....	5

1 Document Classification: University Confidential

Physical and Administrative Controls	Reproduction	Distribution	Destruction/Disposal
Each employee is responsible for controlling usage and access on a need-to-know basis. This policy also applies to contractors.	Limited copies may be made only to employees or contractors who have signed a non-disclosure agreement.	Internal: Use University envelope whenever possible. External: Use sealed envelope.	Use document destruction bins. Shred or erase magnetically recorded documents if unable to recycle.

2 Document Revision

Date	Revision	Revised By	Basis for Revision & Description

Document Change/Correction Request

Your feedback is valuable. Anyone who uses this document is invited to use this form is used to submit requests for changes or corrections to this document. Please complete all of the sections and mail to:

Document Identification

Document title
Date of Document
Master File Location

Requester Identification

Name	
Department	
Phone Number	() -
Email Address	

Request

The following Change is requested:

Please describe the change and reason(s) why the change is requested.

Correction:

Section __, page __ contains the following erroneous information:

This information should be changed to:

Attach additional sheets if necessary to fully describe the change or correction.

3 STANDARD

3.1 Underlying requirements

All systems that handle high-risk and/or confidential information, accept network connections, or make access control (authentication and authorization) decisions should record and retain audit-logging information sufficient to answer the following questions:

- What activity was performed?
- Who or what performed the activity, including where or on what system the activity was performed from (subject)?
- What was the activity was performed on (object)?
- When was the activity performed?
- What tool(s) was the activity performed with?

- What was the status (such as success vs. failure), outcome, or result of the activity?

3.2 Activities to be logged

Logs should be created whenever any of the following activities are requested to be performed by the system:

- Create, read, update, or delete confidential information, including confidential authentication information such as passwords;
- Create, update, or delete information not covered in the previous bullet point;
- Initiate a network connection;
- Accept a network connection;
- User authentication and authorization for activities covered in the first and second bullet points such as user login and logout;
- Grant, modify, or revoke access rights, including adding a new user or group, changing user privilege levels, changing file permissions, changing database object permissions, changing firewall rules, and user password changes;
- System, network, or services configuration changes, including installation of software patches and updates or other installed software changes;
- Application process startup, shutdown, or restart;
- Application process abort, failure, or abnormal end, especially due to resource exhaustion or reaching a resource limit or threshold (such as for CPU, memory, network connections, network bandwidth, disk space, or other resources) and/or the failure of network services such as DHCP or DNS, or hardware fault;
- Detection of suspicious/malicious activity such as from an Intrusion Detection or Prevention System (IDS/IPS), anti-virus system, or anti-spyware system.

3.3 Elements of the log

Such logs should identify or contain at least the following elements, directly or indirectly. In this context, the term "indirectly" means unambiguously inferred.

- Type of action – examples include authorize, create, read, update, delete, and accept network connection
- Subsystem performing the action – examples include process or transaction name, process or transaction identifier
- Identifiers (as many as available) for the subject requesting the action – examples include user name, computer name, IP address, and MAC address. Note that such identifiers should be standardized in order to facilitate log correlation.
- Identifiers (as many as available) for the object the action was performed on – examples include file names accessed, unique identifiers of records accessed in a database, query parameters used to determine records accessed in a database, computer name, IP address, and MAC address. Note that such identifiers should be standardized in order to facilitate log correlation.
- Before and after values when action involves updating a data element, if feasible

- Date and time the action was performed, including relevant time-zone information if not in Coordinated Universal Time
- Whether the action was allowed or denied by access-control mechanisms
- Description and/or reason-codes of why the action was denied by the access-control mechanism, if applicable

3.4 Formatting and storage

The system shall support the formatting and storage of audit logging in such a way as to ensure the integrity of the logs and to support enterprise-level analysis and reporting. Note that the construction of an actual enterprise-level log management mechanism is outside the scope of this document. Mechanisms known to support these goals include but are not limited to the following:

- Microsoft Windows Event Logs collected by a centralized log management system
- Logs in a well documented format sent via *syslog*, *syslog-ng*, or *syslog-reliable* network protocols to a centralized log management system
- Peoplesoft logs collected
- Logs stored in an ANSI-SQL database that itself generates audit logs in compliance with the requirements of this document
- Other open logging mechanisms supporting the above requirements including those based on MARS, CheckPoint OpSec, ArcSight CIF, and AD, LDAP, Kerberos