Log Management Standard

Applies To:	All	Policy Number:	ITS-0038
Issued By:	AVP for IT	Policy Version Number:	1.0
Date Issued:	July 1, 2016	Last Review Date:	July 1, 2016
		Last Revised Date:	July 1, 2016

Scope
This document applies to all servers and network devices that handle, accept network connections, or make access control (authentication and authorization) decisions for University Protected information, as defined within the Data Classification section of the University's Acceptable Use & Security Policy.

Purpose
To identify the specific requirements that information systems must meet in order to generate appropriate audit logs and integrate with the University's log management strategy.

Standard

Underlying requirements
All covered systems shall record and retain audit-logging information sufficient to answer the following questions:

1. What activity was performed?
2. Who or what performed the activity, including from where or from which system the activity was performed?
3. What the activity was performed on the covered system?
4. When was the activity performed?
5. With which program(s) was the activity was performed?
6. What was the status (such as success vs. failure), outcome, or result of the activity?

Activities to be logged
Logs shall be created whenever any of the following activities are requested to be performed by a covered system:

1. Create, read, update, or delete University Protected or University Sensitive information, and authentication information, such as passwords
2. Initiate a network connection
3. Accept a network connection
4. User authentication and authorization for activities covered in 1, such as user login and logout

5. 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
6. System, network, or service configuration changes, including installation of software patches and updates, or other installed software changes
7. Application process startup, shutdown, or restart
8. 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), the failure of network services such as DHCP or DNS, or hardware fault
9. Detection of suspicious/malicious activity such as from an Intrusion Prevention System (IPS), anti-virus system, or other security systems.

Elements of the log

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

1. Type of action – examples include authorize, create, read, update, delete, and accept network connection.
2. Subsystems performing the action – examples include process or transaction name, process or transaction identifier.
3. 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.
4. 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.
5. Before and after values when action involves updating a data element, if feasible.
6. Date and time the action was performed, including relevant time-zone information if not in Universal Time. This date and time shall be synchronized using the University's NTP servers.
7. Whether the action was allowed or denied by access-control mechanisms.
8. Description and/or reason-codes of why the action was denied by the access-control mechanism, if applicable.

Formatting and storage

The system shall support the formatting and storage of audit logs in such a way as to ensure the integrity of the logs and to support enterprise-level analysis and reporting. All audit logs must be kept for one year, with three months available online.

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:

1. Microsoft Windows Event Logs collected by a centralized log management system;
2. Logs in a well-documented format sent via syslog, syslog-ng, or syslog-reliable network protocols to a centralized log management system; and
3. Logs stored in an ANSI-SQL database that itself generates audit logs in compliance with the requirements of this document.

Access to Log Files

All access to log files and audit trails shall be limited to a user's job-related need-to-know, as per the ITS Access Control Policy. Audit trails shall be protected from unauthorized modifications.

History and Updates

July 1, 2016: Initial Standard