California State University Northridge	**Information Technology** Log/Event Management Guidelines	**Page** 1 of 5	
		SOP#: ITIS 90-09-034	**Revision#:** Version 0.4

Prepared by: Leigh Lopez **Date:** May 12, 2009	**Approved by:** Chris Olsen, ISO **Date:** June 8, 2009
Last revised by: Chris Olsen **Date:** June 6, 2009	**Last approved by: Chris Olsen, ISO** **Date: January 12, 2012**

1.0 PURPOSE

Document the guidelines for the management, security, and review of audit logs and security event logs to assist in identifying potential security vulnerabilities, configuration issues, and other anomalies with campus systems, applications, and network devices.

2.0 SCOPE

The scope of these guidelines includes the management, review, and security of audit and security event logs for systems, servers, applications, and network devices.

3.0 RESPONSIBILITY

	Role (Title)	Responsibility
1	Information Security Officer	• Review and authorize access to the central log management server.
2	Information Security Analyst	• Offer guidance to administrators regarding the management, security, and review of audit logs and security events.
3	Network, System, and Application Administrators	• Use guidelines to determine an appropriate approach for managing, reviewing, and ensuring the security of audit/event logs of operating systems, servers, and applications; • Repair or mitigate security vulnerabilities; • Immediately report breaches of security to the IS office.

4.0 GUIDELINES

4.1 Log Management

Collecting, correlating, and reviewing log data can be a daunting task. Where feasible, use log management/correlation and alerting tools and scripts to minimize manual processing overhead.

Irrespective of the device or application, it is imperative that log data have accurate time stamps. Where possible, connect to CSUN's Network Time Protocol (NTP) server.

4.1.1 **Applications**

Applications should log their activity in a manner that correlates well with the business processes the applications support, particularly any operations that modify permissions or access rights. These logs should generally include:

- The business operation that was requested;
- Whether the request was accepted or denied;
- The time and date the operation was performed (Start and end times may be appropriate for long operations.);
- Who initiated the operation;
- System and network resources used;
- Any information needed for business process controls;
- Client hardware and software characteristics;

It should be noted that the "application" may actually be a more generic service, such as a web, file, or print server. In this case, it may be difficult to relate the more generic logs to business processes. When this is the case, appropriate documentation may need to be maintained describing the relationship between the logs and the supported business processes.

4.1.2 **Systems**

Many components of the IT infrastructure generate logs. Examples of these components include:

- Operating Systems
- Web servers
- Database servers
- Print servers
- File servers
- Authentication servers
- DHCP servers
- DNS servers
- Electronic mail server logs

In general, all of these logs have potential value and should be maintained; especially those pertaining to the transmission, access, or modification to university protected data. These logs should include the following types of information:

- Actions taken by any individual with root or administrative privileges;
- Changes to system configuration;
- Access to audit trails;
- Invalid logical access attempts;
- Use of identification and authentication mechanisms;
- Alarms raised by an access control system;
- Activation and de-activation of controls, such as anti-virus software or intrusion detection system;
- Changes to, or attempts to change system security settings or controls.

For each of the above events, the following should also be recorded, as appropriate:

- User identification
- Type of event
- Date and time
- Success or failure indication
- Data accessed
- Program or utility used
- Origination of event (e.g., network address)
- Protocol
- Identity or name of affected data, information system or network resource

4.1.3 **Network/Telephony Devices**

Many components of the network infrastructure generate logs. Examples of these components include:

- Routers
- Switches
- Wireless access points
- Network-based firewalls
- Intrusion detection and prevention systems
- Telephone Switches

These logs typically describe flows of information through the network, but not the individual packets contained in that flow. Information logged for a flow should include:

- Network (IP) addresses or telephone numbers of the end points;
- Service identifiers (port numbers) for each of the end points;
- Whether the flow was accepted or denied;
- Date, time, and duration of the flow;
- Number of packets and bytes used by the flow.

4.2 Review Logs/Alerts

- Alerts involving the potential breach of access/security, or that indicate a problem with availability of a critical resource should be reviewed as soon as possible, and at least weekly;
- Other logs should be reviewed in order of importance; recommended at least monthly.

4.3 Appropriate Use of Log Information

In reviewing log files and event alert information, security incidents involving the potential loss or breach of university protected information should be immediately reported to the Office of Information Security. It will be necessary to retrieve and report log records based on a variety of selection criteria, such as:

- Source(s) of the log records
- Time
- Network address
- Application or service
- User
- Other details surrounding the incident

4.4 Security of Logs

Logs often contain information that, if misused, could represent an invasion of the privacy of members of university. It is necessary to protect log files and provide access only to those with a need to know.

Critical servers or those that transmit or store protected data, at a minimum, should store a copy of log/alert data on a separate protected log server.

5.0 DEFINITIONS:

6.0 REFERENCES:

a. CSUN Protected Data: http://www.csun.edu/it/security/protecteddata.html

7.0 FURTHER INFORMATION:

ITIS-90-08-004 Information Security Incident Response Procedures