CALIFORNIA STATE UNIVERSITY
SAN BERNARDINO

CSUSB Log Management Standard

CSUSB, Information Security & Emerging Technologies Office

Last Revised: **09/17/2015**

Final

REVISION CONTROL

Document Title: CSUSB Log Management Standard

Author: Javier Torner

File Reference:

Date	By	Action	Pages
09/15/2015	J Torner/J Macdonell	Created Standard	All
9/17/2015	L Carrizales	Standard approve by ISET Subcommittee on 9/16/15. Made changes to the document based on recommendations from ISET Subcommittee.	All

Review/Approval History

Date	By	Action	Pages
9/16/2015	ISET Subcommittee	Approved Standard	All

Contents

CSUSB

Information Security Standards

Log Management Standard

1.0 Introduction

The CSUSB system/application log management standard identifies event logging requirements, log review frequency, retention period of logs, and general configuration.

System monitoring plays a critical role in securing information resources and aids in detecting unauthorized system activities, monitoring performance, and investigating incidents. An effective implementation of system monitoring requires clear standards, support by management, and well-trained system administrators in the areas of operating systems and applications.

Configuring logging requires individual system evaluation of risk, impact and performance of the system. System monitoring requires dedicated staff to regularly review, analyze and take appropriate action to resolve or mitigate suspicious events and alerts.

2.0 System and Application Monitoring Standard

2.1 Scope

Servers, applications and workstations that process, access or interact with Level 1 or significant amounts of Level 2 information are required to log events and send security logs at a minimum to the log management system.

2.2 Directory and Authentication Servers

All directory and authentication servers must send authentication information at a minimum to the log management system. Directory and authentication management servers include: Active Directory, OpenLDAP, CAS, Shibboleth, Radius, ADFS, OID, Password Management Applications, and Identity Management Systems.

Password recovery and modification systems must send all successful and unsuccessful attempts and IP address information to the log management system.

2.3 Network Security

All network systems that perform authentication transactions must send such events to the log management system. Network device authentication and configuration change

events must be sent to the log management system, including: DNS, IDS, and Firewall logs.

2.4 Audit Logging

Audit logging records system and user activities used for system performance tuning, detecting unauthorized access and to investigate incidents. Audit logs must contain at minimum the event/application/process, user ID, date and time for key events.

If possible, or appropriate, audit logs should identify terminal, location, network addresses and protocols.

The types of events logged must be determined for each system by taking into account an evaluation of risk, impact and performance to the system. Key events that should be logged include:

- Records of successful and failed system access attempts;
- Records of failed data and other resources access attempts;
- Changes to system configuration;
- Use of elevated privileges;
- Use of system utilities and applications;
- Alarms raised by the access control system;
- Changes to protection systems (e.g. firewall, anti-virus, and intrusion detection systems);
- Additional events identified by the vendor or system administrator.

2.5 Log Event Format

Ensure that the details captured for events and activities contain sufficient information to establish what events occurred, the sources of the events, and the outcomes of the events. For each of the events, the following will need to be recorded, as appropriate:

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

Log data should be collected in its original form whenever practical but may also be collected in a normalized form (e.g. comma-separated variable format) if the

normalization takes place at the time of collection and the integrity of the normalized log data is assured.

When appropriate, a California State University (CSU) approved data encryption, checksums, hash or a similar process, should be used to protect the integrity of collected production and archived log data.

2.6 Monitoring of Logs and Events

Monitoring of log events requires regular review and analysis of log files and appropriate event follow-up. Automation can improve the review and analysis of logs. However, log reduction, review, and reporting of log analysis should be conducted without altering original log records.

The log and event management system(s) must be utilized for the collection and processing of security events. It is recommended that a record of log analysis audit history be maintained.

Processed log reports and alerts should be generated and reviewed daily for critical systems, systems containing Level 1 and/or significant amounts of Level 2, and Internet-exposed systems and applications.

Departments/Units monitoring their systems and applications should develop procedures that include the following:

- Individual who is responsible for the overall process and results
- How often reviews will take place
- How often review results will be analyzed
- Types of log data and monitoring procedures that will be needed
- How reports or logs will be reviewed
- Where monitoring reports will be filed and maintained
- Mechanisms implemented to assess the effectiveness of the review process (metrics)
- The plan to revise the review process when needed

The regular review and analysis of logs can detect:

- Anomalous events
- Attempts to gain access
- Failed file or resource access attempts
- Unauthorized changes to users, groups and services
- Suspicious or unauthorized network traffic patterns
- Problem trends

Access to log data should be restricted only to authorized employees.

Requests for the release of log data for internal investigations must be submitted to the Information Security and Emerging Technologies (ISET) Office for review and, when appropriate, may require approval from the Provost/Vice President or their delegate.

Extract of logs to third-parties for diagnostic or troubleshooting purposes is permissible provided that the information is reviewed, specific in scope, and any sensitive or identifiable information is redacted. The inadvertent disclosure of confidential information recorded in logs should be reported to the respective university management.

2.7 Reporting Security Related Events

Security related events must be reported to the ISET office at security@csusb.edu. ISET will review these events and provide corrective measures and escalate as appropriate.

Security-related events include, but are not limited to:

- Brute force attempts
- Accounts that have been automatically locked due to activity not attributed to the account holder
- Multiple simultaneous login events from geo-locations greater than 6,000 miles apart
- Port-scan attacks
- Evidence of unauthorized access
- Anomalous occurrences that are not related to specific applications on the host
- Theft of computing equipment.

2.8 Retention and Protection of Log Information

Log data must be retained for no less than one year except as required by applicable legislation (such as HIPAA) or regulation (such as PCIDSS).

Server and application security logs that include authentication and source IP must be sent to the log management system. The log management system retain logs for no less than one year.

3.0 References

CSU Policy ICSUAM 8045 Information Technology Security Policy

Reference: http://www.calstate.edu/icsuam/sections/8000/8045.0.shtml

CSU Standard ICSUAM 8045.S600 Logging Elements Policy

Reference:http://www.calstate.edu/icsuam/sections/8000/8045.S600_Logging_Elements.pdf