Log Management Standard

Effective Date: 7/28/2015

1.0 INTRODUCTION

The California State University, Chico 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 system and applications. Configuring logging requires individual system evaluation of risk, cost and performance to the system. System monitoring requires dedicated staff to regularly review, analyze, and take appropriate action to resolve or mitigate unauthorized events.

Implements: CSU Policy ICSUAM 8045 Information Technology Security

Implements: CSU Standard ICSUAM 8045.S600 Logging Elements

2.0 SYSTEM AND APPLICATION MONITORING STANDARD

2.1 Required Logging

Servers, applications and Workstations:

- All campus servers and “high-risk” workstations must send security logs at a minimum to the campus log management system.
- Applications that process, or access Level 1 data must send authentication related log events 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 campus log management system. Directory and authentication management servers include: AD, 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.
Network Equipment:

- All network systems that perform authentication transactions must send such events the campus log management system.
- Network device authentication and configuration change events must be sent to the campus log management system.
- DNS, IDS, and Firewall logs must be retained in a log management system.

2.3 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. Key events are:

- 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.

The types of events logged must be determined for each system taking into account an evaluation of risk, cost and performance to the system.

2.4 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
- Origination 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, or a similar process, should be used to protect the integrity of collected, production, and archived log data.

### 2.5 Monitoring of Logs and Events

Monitoring requires regular review and analysis of log files and appropriate event follow-up. Daily log monitoring is required for critical systems or systems containing Level 1 protected information, or systems exposed through the border firewall. The campus Log and Event management system must be utilized for the collection of security events as well as daily review.

It is recommended that a record of log analysis audit history be maintained. Access to log data should be restricted to the appropriate members as determined by management.

Log review procedures should address the following topics:

• Who is responsible for the overall process and results
• How often reviews will take place
• How often review results 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

Automation can improve the review and analysis of logs. However, log reduction, review, and reporting tools should support log analysis without altering original log records.
The inadvertent disclosure of confidential information recorded in logs should be reported to the respective university management.

### 2.6 Reporting Security-Related Events

Security-related events must be reported to the Information Security Office (x6212) or security@csuchico.edu. The Information Security Office will review these events and prescribe corrective measures as needed.

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

- Brute force attempts
- Accounts that have been automatically locked due to failed attempts
- 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.

### 2.7 Retention and Protection of Log Information

Log information must be retained locally for a minimum of 90 days. Server and application security logs that include authentication and source IP must be sent to the campus log management system. The campus log management system should retain logs for 6 months at a minimum.

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Minimum specified duration</td>
<td>Not specified</td>
<td>Not specified</td>
<td>Not specified</td>
<td>Minimum of one year</td>
<td>Not specified</td>
</tr>
<tr>
<td>Retention to meet audit cycle</td>
<td>One year</td>
<td>One year</td>
<td>One year</td>
<td>One year</td>
<td>One year</td>
</tr>
<tr>
<td>Long term retention of logs that may include audit records</td>
<td>Not specified</td>
<td>Not specified</td>
<td>Not specified (Six years for documentation of policies, actions, procedures, or assessments)</td>
<td>Not specified</td>
<td>Not specified (Seven years of documents and communications related to an audit)</td>
</tr>
</tbody>
</table>
Log information must be protected from tampering or modification on systems through ‘need to know’ file access or appropriate security control. Systems with level 1 protected information must store logs on a secure secondary system.

### 2.8 Clock Synchronization
All event generating applications must synchronize to the campus time servers.

### 3.0 Documentation Review & Approval

<table>
<thead>
<tr>
<th>Review Date</th>
<th>Reviewed By</th>
<th>Action (Reviewed, Recommended or Approved)</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>5/11/15</td>
<td>Policies and Standards Group</td>
<td>Reviewed / Recommended</td>
<td>V1.0</td>
</tr>
<tr>
<td>7/21/15</td>
<td>Information Technology Executive Committee (ITEC)</td>
<td>Approved</td>
<td>V1.0</td>
</tr>
</tbody>
</table>