8045.S600 Logging Elements

Implements:	CSU Policy #8045.0
Policy Reference:	http://www.calstate.edu/icsuam/sections/8000/8045.0.shtml

Introduction

Each campus must identify and implement appropriate logging and monitoring controls for information assets. These controls must take into consideration the technical capabilities of each resource.

1.0 Logging Elements

1.1 At a minimum and as appropriate, taking into account the capabilities of the device or application creating the log entries, such controls must track and log the following events:

a) Actions taken by any individual with root or administrative privileges
b) Changes to system configuration
c) Access to audit trails
d) Invalid access attempts (failed login)
e) Use of identification and authentication mechanisms (logins)
f) Notifications and alerts
g) Activation and de-activation of controls, such as anti-virus software or intrusion detection system
h) Changes to, or attempts to change system security settings or control.

1.2 For each of the above events, the following must be recorded, as appropriate:

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

1.3 Each campus must establish procedures for the retention of logs and monitoring information.

1.4 Critical servers, at a minimum, must store a copy of their log data on another device; this copy must be protected from unauthorized access.

1.5 Each campus must establish methods for time synchronization of logging and monitoring activities.

REVISION CONTROL

Revision History

Revision Date	Revised By	Summary of Revisions	Section(s) Revised
11/15/2011	Macklin	Incorporation of ISAC Comments	All
11/15/2011	Moske	Formatted	All
1/11/2012	Macklin	Format, final review	All

Review / Approval History

Review Date	Reviewed By	Action (Reviewed, Recommended or Approved)
4/23/2013	ISAC	Reviewed, approved and recommended for CISO review
7/16/2013	CISO / Perry	Approved
3/3/2014	CISO	Request to Post