California State University | Division Of TECHNOLOGY & INNOVATION | CHANNEL ISLANDS

Process Number:	BP-05-005	**Effective Date:**	05/08/2017
Approved By:	A. Michael Berman VP for Technology & Innovation		**Page 1 of 4**

Business Practice for Information Asset Monitoring

PURPOSE:

Provide support of ICSUAM Policy 8045.500 for Information Asset Monitoring related to Information Technology Security.

BACKGROUND:

To support ICSUAM policy 8045.500, CI must implement appropriate controls on the monitoring of information systems and network resources to ensure that monitoring is limited to approved activities. Monitoring must not be conducted for the purpose of gaining unauthorized access, "snooping", or for other activities that violate the CSU Responsible Use Policy. Records created by monitoring controls (e.g. logging) must be protected from unauthorized access and reviewed regularly. Campuses must ensure that only individuals who have a "need-to-know" are granted access to data generated from monitoring controls.

Data generated by monitoring must be retained for a period of time that is consistent with effective use, CSU records retention schedules, regulatory, and legal requirements such as compliance with litigation holds.

At a minimum, server administrators are required to scan regularly, remediate, and report un-remediated vulnerabilities on critical systems or systems that store protected information within a prescribed timeframe. The risk level of a system determines the frequency at which logs must be reviewed. Risk factors to consider are:

- Criticality of business process.
- Information classification associated with the system.
- Past experience or understanding of system vulnerabilities.
- System exposure (e.g., services offered to the Internet).

Business Practice for Information Asset Monitoring

BUSINESS PRACTICE:

Accountability:

Vice President for Technology and Innovation
Director, Infrastructure Technology

Applicability:

All CI connected devices, applications, and computing services

Definitions:

1. **Logs** – Files capturing data regarding authentication and authorization of accessing systems and services.
2. **Logging Elements** – Defined pieces of data that are required to me be included in log data collection.

Text:

General

CI must identify and implement appropriate logging and monitoring controls for information assets. These controls must take into consideration the technical capabilities of each resource and the capabilities of the device or application (or service) creating the log entries. Such controls must track and log the following events prescribed in ICSUAM standard 8045.S600 which include:

Logging Elements:

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.

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.

CI must establish procedures for the retention of logs and monitoring information. Critical servers, at a minimum, must store a copy of their log data on another device; this copy must be protected from unauthorized access. CI must establish methods for time synchronization of logging and monitoring activities

Business Practice for Information Asset Monitoring

Assessment Requirements

Assessment requirements and history are listed in the grid below.

Description	Frequency	Role Assigned
Assessment of business practice	Annual	Director, Infrastructure Technology

Revision History

BP Nbr:	BP-05-005	**Enacted Date:**			
Revision Nbr:	999	**Revision Date:**	99/99/9999	**Revised By:**	