Standard: Event Monitoring

Executive Summary

The Event Monitoring Standard defines the requirements for Information Security event monitoring within SJSU computing resources to ensure that information security policies, procedures and controls are being followed and are effective in securing information resources with the goal in of safeguarding the confidentiality, integrity, and availability of information stored, processed, and transmitted. The campus systems should comply with all relevant legal requirements applicable to its monitoring and logging activities.

Information Security Standards

Event Monitoring

Standard #	IS-EM	Effective Date	11/10/2015	Email	security@sjsu.edu
Version	4.1	Contact	Information Security Team	Phone	408-924-1530

Revision History

Date	Action
11/10/2015	Incorporated changes from campus constituents – Distributed to Campus.
11/18/2020	Reviewed. Nikhil Mistry
10/19/2021	Reviewed. Cole Gunter
11/30/2022	Reviewed. Cole Gunter

Table of Contents

Introduction and Purpose

This standard defines the requirements for Information Security event monitoring within SJSU computing resources. It is intended to ensure that SJSU's information security policies, procedures and controls are being followed and are effective in ensuring the confidentiality, integrity and availability of SJSU's information resources.

Scope

This standard applies to all SJSU State, Self-Fund, and Auxiliary ("campus") public (internet and campus facing) firewalls, VPNs, network authentication points and servers.

Standard

Sensitive systems should be monitored and information security events should be recorded, reviewed consistently and acted upon accordingly in a timely manner. Operator logs and fault logging should be used to ensure information system problems are proactively identified. The campus systems should comply with all relevant legal requirements applicable to its monitoring and logging activities. System monitoring should be used to check the effectiveness of security controls implemented and to verify adherence to the access control standard.

Logging Requirements: Nature of Information and Retention Period

The following table delineates the nature of audit log information and retention period, for each type of application or system. All audit logs must include a date, timestamp, source address, and destination address (where applicable). All audit logs should record logs in a standardized format such as syslog. If systems cannot generate logs in a standardized format, log normalization tools can be deployed to convert logs into this standard format.

System Type	Audit Log Information	Retention Period	Mirror or Backup
Firewalls, Inbound/Outbound Proxy, Network IPS/IDS	● User log on (successful or failed attempts) ● User log off ● All Privileged commands (configuration changes) ● Activation and De-activation	60 days	Mirrored in real-time to central logging server
Network Infrastructure (Routers, Switches, WLAN Controllers)	● User log on ● User log off ● All Privileged commands (configuration changes)	60 days	Mirrored in real-time to central logging server
Wireless Network Clients	● User WLAN association, including source IP address, username, dates, times, and duration of access.	60 days	Backup Required
VPN	● User log on and log off ● Authenticated username	60 days	Mirrored in real-time to central logging server

	● VPN client source IP address ● Source IP address of remote connection ● Dates, times, and duration of access.		
Endpoints (Workstations, Laptops, Tablets, Mobile Computing devices)	● User log on and log off ● Business applications accessing L1 or L2 information audit events	30 days	Stored locally on endpoint
Active Directory servers	● User log on and log off ● Creation/edit/deletion of all accounts ● All Privileged commands (configuration changes)	60 days	Backup Required
Servers with L1 Data/ Web App Internet Facing	● Where possible, read and write of sensitive level 1 or 2 information, including application, username, source IP address ● User log on and log off ● Creation/edit/deletion of all accounts ● Any exceptions when authorization is denied due to improper permissions ● Changes to system configuration and access control	60 days	Stored locally and mirrored to central logging server
SIEM	● All information security events ● User log on and log off ● Creation/edit/deletion of all accounts ● Activation and De-activation ● All Privileged commands (configuration changes)	60 days	Stored locally and mirrored to central logging server
Physical Security Information (S2 Logs, Key Boxes)	● All checkin/checkout events, including user, date and time.	90 days	Stored on appropriate device or server.

System administrators are responsible for the initial, correct audit log configuration on each managed device. After the device is setup with correct logging, security personnel and/or system administrators should run biweekly reports that identify anomalies in logs. Logs should be actively reviewed, documenting the findings by authorized personnel or monitored by software which is configured to alert personnel in the event of suspicious activity.

Sensitive Application Systems Logs

All production application systems that handle sensitive campus information must generate logs that capture every addition, modification, and deletion to such sensitive information.

Separation of Duties

System administrators shall not have write/delete permission nor disable logs forwarding to mirrored central logging servers. A “golden master” central logging server must be maintained for the purposes of security forensics. This may be accomplished either through dual logging servers or granular permission lists.

Production Application System Log Contents

All computer systems running campus production application systems must include logs that record, at a minimum, user session activity including user IDs, logon date and time, logoff date and time, as well as applications invoked, changes to critical application system files, changes to the privileges of users, and system start-ups and shut-downs.

Logging Security-Relevant Events

Computer systems handling sensitive, valuable, or critical information must securely log all significant security relevant events including, but not limited to, password guessing attempts, attempts to use privileges that are not authorized, modifications to production application software, and modifications to system software.

Logging Logon Attempts

Whether successful or not, all user initiated logon attempts to connect to SJSU production information systems must be logged.

Systems Architecture for Logging Activities

Application and/or database management system software storing confidential Level 1 or Level 2 data must keep logs of all user activities, and statistics related to these activities, that will in turn permit them to detect and issue alarms reflecting suspicious business events.

Computer System Audit Logs

Logs of computer security-relevant events must provide sufficient data to support comprehensive audits on the effectiveness of, and compliance with security measures.

Privileged User ID Activity Logging

All user ID creation, deletion, and privilege change activity performed by Systems Administrators and others with privileged user IDs must be securely logged.

Privileged System Command Accountability and Traceability

All privileged commands issued by computer system operators must be traceable to specific individuals through the use of comprehensive logs.

Password Logging

Unencrypted passwords, whether correctly typed or not, must never be recorded in system logs.

System Log Review

Computer operations staff or information security staff must review records reflecting security relevant events on all production multi-user machines in a periodic and timely manner.

On all internal servers containing Level 1 or Level 2 information, SJSU must establish and operate application system logs, and other unauthorized activity detection mechanisms specified by the Information Security Office.

Electronic Mail Message Monitoring

Messages sent over SJSU internal electronic mail systems are not protected by law from wiretapping or monitoring, and may therefore be captured, read, and used by campus managers and Systems Administrators as deemed appropriate in ICSUAM8105.

SPAM/Fraud Detection

To be able to immediately detect and respond to phishing attacks, SJSU must mount an on-going real-time analysis of spam messages currently traversing the Internet. This activity may alternatively be performed by a third party service specializing in this type of fraud detection.

Protection of Log Information

Logging facilities and log information should be protected against tampering and unauthorized access in accordance with the Data Center Security Standard.

System Log Modification Controls

Where possible, all SJSU production information systems must employ cryptographic MD5 or SHA-1 checksums to verify integrity of system logs.

Log Deactivation, Modification, or Deletion

Mechanisms to detect and record significant computer security events must be resistant to attempts to deactivate, modify, or delete the logging software and logs.

System Log Protection

All SJSU production computer system logs must be protected with digital signatures or Active Directory credentials must document log entry sequence numbers.

Data/Information Exfiltration Controls

The border firewall logs must be automatically monitored for sudden increases in size of data being sent off campus, being sent to known bad location, failures of digital signatures, and gaps in log entry sequence.

Access to Logs

All system and application logs must be maintained in a form that cannot be readily viewed by unauthorized persons. Authorized persons have a readily demonstrable need for such access in order to perform their regular duties. All others seeking access to these logs must first obtain approval from the Information Security Office.

Centralized Log Host Required

Server system logs must be recorded on both the involved servers and also a central or departmental log host separate from production application servers. These logs must be securely maintained for the time periods stated in server configuration guidelines issued by the Information Security Office.

Restricted Disclosure of Fields Recorded In System Logs

The specific nature of the information recorded in SJSU audit trails and system logs is restricted to those who have a demonstrable need for such information in order to carry out their jobs.

Administrator and Operator Logs

System administrator and system operator activities should be logged.

Computer Operator Logs

All SJSU multi-user production systems must have computer operator logs that show production application start and stop times, system boot and restart times, system configuration changes, system errors and corrective actions taken, and confirmation that files and output were handled correctly.

Clock Synchronization

The clocks of all relevant information processing systems within an organization or security domain should be synchronized with the campus central NTP service.

All multi-user computers connected to the SJSU internal network must always have the current time accurately reflected in their internal clocks.