Status **Active** PolicyStat ID **17257988**

Origination	12/2024	Chapter Lead	Nohemy Ornelas: Chapter 3(CC),4&5
Last Approved	12/2024	Policy Area	Chapter 3 General Institution
Effective	12/2024	References	Non CCLC
Last Revised	12/2024		
Next Review	12/2034		

AP 3729 Information Security Logging & Monitoring

1. PURPOSE AND SCOPE

   The objective of this Administrative Procedure is to document the requirements for logging and monitoring at the San Bernardino Community College District (SBCCD). SBCCD monitors its information technology (IT) infrastructure so that potential security incidents can be detected early and dealt with effectively.

   This is one of a series of information security Administrative Procedures maintained by the District IT department designed to protect the SBCCD information systems.

   Please refer to AP-3725–Information Security Program Overview applicability of assets, application to staff, and external parties.

2. LOGGING AND MONITORING

   Monitoring helps speed the resolution of system problems and aids in the identification of access control policy violations. The monitoring program also verifies correct operation and the overall success or failure of network, server, and application security controls.

   a. Logging Responsibilities and Tools

      The District IT infrastructure must provide district-wide network logging and monitoring services. Appropriate college Technology department managers and staff will have access to these services. Centralized log analysis and event correlation of operating system event logs is performed continuously.

   b. Basic Logging Requirements

      Automated audit trails should reconstruct the following events for all firewalls,

routers, database servers, and critical servers including:

i. Alarms generated by network management devices or access control systems;
ii. All actions taken by any individual with administrative privileges;
iii. Changes to the configuration of major operating systems/network services/utilities/security software;
iv. Anti-virus software alerts;
v. Access to all audit trails or log records; and
vi. Failed or rejected attempts to access Restricted data or resources.

These events should be tracked by:

- User identification (User ID/account name).
- Type of event.
- Date and time stamp.
- Success or failure indication.
- Name of affected data, system component, or resource.

c. Log Access and Retention

Access to audit files must be limited to authorized administrators, District IT management, and college Technology department management. Only individuals with a job-related need should be able to view, initialize or create audit files.

Audit files must be kept secure so that they cannot be altered in any way, through file permissions or other means. Precautions must also be taken to prevent files or media containing logs from being overwritten and that sufficient storage capacity is present for logs.

Logs must be kept for the minimum period specified by any business or legal requirements. If no specific requirements exist, logs should be retained for at least one year.

d. Protection of Logs

Audit records are protected against modification and deletion to prevent unauthorized use.

Audit records for external-facing technologies (e.g., wireless, firewalls, DNS, etc.) are stored on a server located on the internal network.

e. Log Monitoring, Review, Analysis & Reporting

SBCCD reviews and analyzes audit records for evidence of suspicious, unusual, and inappropriate activity. SBCCD reports anomalous auditable events and related security incidents to the Vice Chancellor of Technology and Learning Services, who is responsible for reporting security issues to the Executive Leadership Team as

appropriate. SBCCD adjusts the level of audit review, analysis, and reporting within systems when there is a change in risk to operations, assets, individuals, and other organizations based on law enforcement information, intelligence information, or other credible sources of information.

SBCCD establishes procedures for monitoring the use of systems and facilities to test the effectiveness of access control and security mechanisms. The results of the monitoring activities are reviewed on a regular basis. Monitoring activities include execution of privileged operations, authorized access, unauthorized access attempts, and system alerts or failures.

SBCCD meets all applicable legal requirements related to monitoring authorized access and unauthorized access attempts.

SBCCD System Administrator activities are logged and reviewed on a regular basis.

f. Log Review Schedule like the sample below.

IT Security Event	Frequency	Responsibility
Alarms generated by network management devices or access control systems	Daily	District IT or college Technology department staff
All actions taken by any individual with administrative privileges	Daily	District IT or college Technology department staff
Anti-virus software alerts	Daily	District IT or college Technology department staff
Access to all audit trails	Daily	District IT or college Technology department staff
Failed or rejected attempts to access *Restricted* data or resources	Daily	District IT or college Technology department staff
Changes to the configuration of major operating system network services / utilities / security software	Weekly or as required	District IT or college Technology department staff
Application logs (e.g., SIS)	As required	District IT or college Technology department staff

g. Payment Card Industry (PCI Requirements)

Refer to AP 3737 Information Security - Payment Card Industry Requirements (PCI).

References:
NIST SP 800-53 Rev. 4 AC-2, AU-12, CA-7, CM-3, CM-8, SC-5, PE-3, PE-6, PE-20,SC-7, SI-4
IPAA Security Rule 45 C.F.R. §§ 164.308(a)(1)(ii)(D), 164.308(a)(5)(ii)(B), 164.308(a)(5)(ii)(C), 164.308(a)(8), 164.310(a)(1), 164.310(a)(2)(ii), 164.310(a)(2)(iii), 164.310(b), 164.310(c), 164.310(d)(1), 164.310(d)(2)(iii),164.312(b), 164.312(e)(2)(i), 164.314(b)(2)(i)

Approval Signatures

Step Description	Approver	Date
Approved per Level 2 process in AP 2410	Kelly Goodrich: PPAC Support	12/2024