ADMINISTRATIVE REGULATION 3729

SOUTH ORANGE COUNTY COMMUNITY COLLEGE DISTRICT

GENERAL INSTITUTION

INFORMATION SECURITY- LOGGING AND MONITORING

I. PURPOSE AND SCOPE

The objective of this administrative regulation is to document the requirements for logging and monitoring at the South Orange County Community College District (SOCCCD). SOCCCD 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 regulations maintained by the District IT department designed to protect the SOCCCD information systems.

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

II. LOGGING AND MONITORING

Monitoring helps speed 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:

1. Alarms generated by network management devices or access control systems;
2. All actions taken by any individual with administrative privileges;
3. Changes to the configuration of major operating system network services / utilities / security software;
4. Anti-virus software alerts;
5. Access to all audit trails or log records; and
6. Failed or rejected attempts to access *Restricted* data or resources.

These events should be tracked by:

1. User identification (User ID / account name).
2. Type of event.
3. Date and time stamp.
4. Success or failure indication.
5. 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

SOCCCD reviews and analyzes audit records for evidence of suspicious, unusual, and inappropriate activity.

SOCCCD 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.

SOCCCD 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.

SOCCCD 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.

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

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

F. Log Review Schedule

The following table lists logging checks to be performed on a daily, weekly basis or ongoing/as needed basis.

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

The following additional network controls are specific to network locations in-scope for PCI:

1. Use file-integrity monitoring or change-detection software on logs to ensure that existing log data cannot be changed without generating alerts (although new data being added should not cause an alert).
2. Review logs for all system components at least daily. Log reviews must include

those servers that perform security functions like intrusion-detection system (IDS) and authentication, authorization, and accounting servers.

3. Retain audit trail history for at least one year, with a minimum of three months immediately available for analysis (for example, online, archived, or restorable from back-up).

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
HIPAA 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)