INFORMATION SECURITY- LOGGING AND MONITORING

1.0 Purpose and Scope

The objective of this Administrative Regulation is to document the requirements for logging and monitoring at Yosemite Community College District (YCCD). YCCD monitors its technology 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 Information Technology Services (ITS) department designed to protect YCCD information systems.

2.0 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.

2.1 Logging Responsibilities and Tools

The District ITS Networking and Operations team serves as the primary focal point for network logging and monitoring.

Centralized log analysis and event correlation of operating system event logs shall be performed continuously utilizing a tool yet to be determined.

2.2 System Vulnerability Scanning

YCCD ITS will quarterly perform internal vulnerability scanning of all YCCD ITS controlled servers. External vulnerability scanning will be performed by an 3rd party vendor annually scanning all external facing servers for security vulnerabilities.

2.3 Basic Logging Requirements

Automated audit trails should reconstruct the following events for all firewalls, routers, database servers, and critical servers, including:

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

These events should be tracked by YCCD ITS System Administrators.

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

2.4 Log Access and Retention

Access to audit files must be limited to authorized administrators and ITS 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.

2.5 Log Review Schedule

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

Security Event	**Frequency**	**Responsibility**
Alarms generated by network management devices or access control systems	Daily	YCCD ITS System Administrators
All actions taken by any individual with administrative privileges	Daily	YCCD ITS System Administrators
Anti-virus software alerts	Daily	YCCD ITS System Administrators
Access to all audit trails	Daily	YCCD ITS System Administrators
Failed or rejected attempts to access *Restricted* data or resources	Daily	YCCD ITS System Administrators

Changes to the configuration of major operating system network services / utilities / security software	Weekly or as required	YCCD ITS System Administrators
Application logs (e.g., SIS)	As required	YCCD ITS System Administrators

2.6 Payment Card Industry (PCI) Requirements

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

- 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).
- 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.
- 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).