I. PURPOSE AND SCOPE

The objective of this Administrative Regulation is to document the requirements for logging and monitoring at South Orange County Community College District (SOCCCD). SOCCCD monitors its 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 Information Technology (IT) department designed to protect SOCCCD information systems.

Please refer to AR-3725 – Information Security Program Overview Applicability of Assets, Application to Staff, and External Policies.

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.

1. Logging Responsibilities and Tools

The District IT Infrastructure team serves as the primary focal point for network logging and monitoring. The College IT departments have tools and systems for monitoring network and desktop systems which can also be used by District IT as requested.

Centralized log analysis and event correlation of operating system event logs is performed continuously.

2. 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:

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

3. Log Access and Retention

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

4. Log Review Schedule

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

<table>
<thead>
<tr>
<th>IT Security Event</th>
<th>Frequency</th>
<th>Responsibility</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alarms generated by network management devices or access control systems</td>
<td>Daily</td>
<td>District IT Management staff</td>
</tr>
<tr>
<td>All actions taken by any individual with administrative privileges</td>
<td>Daily</td>
<td>District IT Management staff</td>
</tr>
<tr>
<td>Anti-virus software alerts</td>
<td>Daily</td>
<td>District IT Management staff</td>
</tr>
<tr>
<td>Access to all audit trails</td>
<td>Daily</td>
<td>District IT Management staff</td>
</tr>
</tbody>
</table>
5. 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).