Solano Community College
Logging and Monitoring Department Policy

Purpose

The purpose of this policy is to document the practices for logging and monitoring of district systems and data.

Scope

This IT policy applies to Solano Community College employees, contractors, subcontractors, vendors, consultants, advisor, and other personnel who have access to Solano Community College information assets without regard to data ownership.

Definitions

Audi Controls – Technical mechanisms that track and record computer activities.

Audit Trail – A chronological set of logs and records used to provide evidence of a system's performance or personnel activity that took place on the system, used to detect misconfigurations, and identify intruders.

Process

Solano Community College is committed to conducting business in compliance with all applicable laws, regulations and Solano Community College policies. Solano Community College has adopted this standard to set forth the internal audit process for protecting Solano Community College data.

To ensure data security, Solano Community College will implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain sensitive Solano Community College data. Solano Community College will clearly identify all critical systems that process sensitive information. Solano Community College will implement security standards to regularly review the records of information system activity on all such critical systems that process sensitive information.

Solano Community College will monitor the physical environment and the network to identify potential activity that could indicate a potential security incident. Monitoring for unauthorized personnel, unauthorized remote access, connections, devices, and software will be performed.

Logging Requirements

- All systems will be configured with their default operating system logging enabled
- All transactional databases will maintain transactional logs, backed up nightly and archived for 30 days
- Firewalls will log and monitor traffic, including source and destination IP addresses and ports, an when discernable, username
- Access to systems logs will be limited to those granted elevated privilege

Revision History

Version:	Date:	Description:
1.0	10/5/2022	Initial document