RESOURCE INF-010G

Systems Monitoring and Auditing Guideline

Purpose

This guideline provides guidance around monitoring and auditing an information system to determine whether or not inappropriate actions have occurred.

Overview

At Coast Mountain College (CMTN), systems monitoring and auditing must be performed to determine when a failure of the information system security, or a breach of the information system, has occurred, and the details of that breach or failure.

Definitions

System Monitoring: The process of looking for inappropriate actions in real time within an information system.

System Auditing: The process of looking for inappropriate actions after the fact within an information system.

Scope

This guideline applies to all CMTN information systems and information system components. Specifically, it includes:

- mainframes, servers, and other devices that provide centralized computing capabilities
- devices that provide centralized storage capabilities
- desktops, laptops, and other devices that provide distributed computing capabilities
- routers, switches, and other devices that provide network capabilities
- firewall, intrusion detection/prevention (IDP) sensors, and other devices that provide dedicated security capabilities.

Details

Purpose of Information Systems

Information systems will be configured to record login/logout all administrator activities into a log file. Additionally, information systems will be configured to notify administrative personnel when inappropriate, unusual, and/or suspicious activity is noted. Inappropriate, unusual, and/or suspicious

activity will be fully investigated by appropriate administrative personnel and findings reported to the Director of Information Technology.

Information Storage

Information systems are to be provided with sufficient primary (on-line) storage to retain 30-days' worth of log data and sufficient secondary (off-line) storage to retain one year's worth of data. If primary storage capacity is exceeded, the information system will be configured to overwrite the oldest logs. In the event of other logging system failures, the information system will be configured to notify an administrator.

Frequency of Reviews

System logs shall be manually reviewed weekly. Inappropriate, unusual, and/or suspicious activity will be fully investigated by appropriate administrative personnel and findings reported to appropriate security management personnel.

Log Access

System logs are considered confidential information. As such, all access to system logs and other system audit information requires prior authorization and strict authentication. Further, access to logs or other system audit information will be captured in the logs.

Related Policies, Guidelines, and Other Resources

- None