

Overview

Systems monitoring and auditing, at {COMPANY-NAME}, must be performed to determine when a failure of the information system security, or a breach of the information systems itself, has occurred, and the details of that breach or failure.

Purpose

System monitoring and auditing is used to determine if inappropriate actions have occurred within an information system. System monitoring is used to look for these actions in real time while system auditing looks for them after the fact.

This policy applies to all information systems and information system components of {COMPANY-NAME}. 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

Policy Detail

Information systems will be configured to record login/logout and all administrator activities into a log file. Additionally, information systems will be configured to notify administrative personnel if 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 VP of IT or COO.

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.

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.

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.