Log Maintenance Policy

Summary

The process of auditing information systems activity is an important aspect of information security. Network devices, file servers, applications, and security systems such as firewalls and virus detection all contain log files. System log files aid in the detection of unusual activity and forensic investigations.

Purpose

This policy sets forth guidelines and responsibilities for information system log file maintenance and retention.

Policy

Although each device and application may have differing log file capabilities, each system should record as much information as possible including:

- Unsuccessful login attempts
- System startup and shutdown activity
- Modifications or deletions of system files
- Modifications to user access privileges
- User session activity including login and logout dates and times
- All activity concerning sensitive data

Log files, classified as sensitive data, must be backed up, protected from unauthorized access, and kept confidential.

The retention period for log files is a minimum of one month.

Procedures and Responsibilities

UITS technical staff, typically network, systems, and database administrators, are responsible for maintaining and regularly analyzing log files. Administrators must investigate and report anomalies to the Information Security Officer.

Related USG Policy

3.2 (IT Handbook) Log Management

Last Update

3/14/2014

Responsible Authority

Chief Information Security Officer