

---

# Security Log Management [1]

## Topics:

[log](#) [2]

PS-08-022 Security Log Management

Issue Date: 3/20/2008

Effective Date: 3/20/2008

## PURPOSE

Developing, implementing and maintaining effective log management practices throughout an enterprise helps ensure that computer security events (actions of users, malicious activity and operational trends) are recorded and stored in sufficient detail and for an appropriate period of time as required by agency, state or federal regulation. Additionally, agencies with federal partners are subject to laws and regulations such as FISMA, GLBA, PCI and HIPAA that require or strongly recommend storage and review of certain logs. This policy establishes the requirement to implement log management practices for State information systems.

## POLICY

Agencies that operate and control State of Georgia information systems shall establish internal policies and procedures for creation, protection and retention of computer security logs and implement a log management infrastructure.

## RELATED ENTERPRISE POLICIES, STANDARDS, GUIDELINES

[Log Management Infrastructure \(SS-08-036\)](#) [3]

## REFERENCES

NIST 800-92 Guide to Computer Security Log Management

## TERMS and DEFINITIONS

**Log** - A record of the events occurring within an organization's systems and networks.

**Computer Security Log Management** - The processes for generating, transmitting, storing, analyzing and disposing of computer security log data.

**Log Management Infrastructure** - Consists of the hardware, software, networks and media used to

generate, transmit, store, analyze, and dispose of log data.

---

**Source URL:** <https://gta.georgia.gov/psg/article/security-log-management>