

 Georgia Technology Authority	<b>Georgia Technology Authority</b>	
<b>Title:</b>	<b>Log Management Infrastructure</b>	
<b>PSG Number:</b>	SS-08-036.01	<b>Topical Area:</b> Security
<b>Document Type:</b>	Standard	<b>Pages:</b> 2
<b>Issue Date:</b>	3/31/08	<b>Effective Date:</b> 3/31/08
<b>POC for Changes:</b>	GTA Office of Information Security	
<b>Synopsis:</b>	Requires agencies to monitor and analyze systems logs to record events and detect anomalies.	

## PURPOSE

Log management infrastructures perform functions that support the generation, analysis and security of log data such as optimizing system and network performance, recording the actions of users, and providing data useful for identifying malicious activity and investigating security incidents.

This standard establishes requirements to establish and maintain a log management infrastructure for state information systems.

## SCOPE, AUTHORITY, ENFORCEMENT, EXCEPTIONS

See Enterprise Information Security Charter (Policy)

## STANDARD:

Agencies that operate and control State of Georgia information systems shall develop and maintain a security log management infrastructure commensurate with the sensitivity and/or importance of the system or data to the organization or as required by local, state or federal regulations.

The security log infrastructure shall include processes for log generation, monitoring, analysis, protection, storage and disposal. Log management policies shall define and prioritize auditable events and storage/retention requirements.

Systems or applications categorized as high or where required for regulatory compliance shall, at a minimum, log the following auditable information and events:

- User ID
- Dates and times of logon and logoff
- Logon method, location, terminal identity (if possible), Network address
- Unsuccessful system or data access attempts
- All actions performed using administrator, developer, super-user or other

Title:	Log Management Infrastructure
--------	-------------------------------

- privileged access
- System alerts or failures
- Other significant events as appropriate

Log data shall be routinely reviewed and analyzed by trained personnel.

Logging systems, configurations and files shall be protected from breaches of confidentiality and integrity. Access to logs files and log configurations/generators shall be audited, monitored and restricted to need-to-know personnel.

Log files are subject to State retention requirements and shall be stored in sufficient detail and for an appropriate period of time. The integrity and availability of log archives shall be protected.

Security personnel shall monitor log management processes and systems and conduct periodic audits of the security of the log infrastructure.

### **GTA RELATED POLICIES, STANDARDS, GUIDELINES**

- Security Log Management (Policy)

### **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.

- **Event** – An action that occurs within a system or network.
- **Log Archive** - Retaining logs for an extended period of time, typically on removable media, a storage area network (SAN), or a specialized log archival appliance or server.
- **Log Analysis** - Studying log entries to identify events of interest or suppress log entries for insignificant events.

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

**Security Log Infrastructure** - The hardware, software, networks and media used to generate, transmit, store, analyze, and dispose of log data.

Note: The PSG number was changed from S-08-036.01 on September 1, 2008

Effective Date:	March 31, 2008	2 of 2
-----------------	----------------	--------