STATE OF ALABAMA

Information Technology Policy

POLICY 677-00: LOG MANAGEMENT

Log management is essential to ensuring that computer security records are stored in sufficient detail for an appropriate period of time. Log management activities include log generation, transmission, storage, analysis, and disposal; while protecting the confidentiality, integrity, and availability of logs.

OBJECTIVE:

Establish log management responsibilities for the State of Alabama computing environment.

SCOPE:

This policy applies to all Executive Branch agencies, boards, and commissions except those exempt under The Code of Alabama 1975 (Title 41 Chapter 4 Article 11).

RESPONSIBILITIES:

Agency Management, Information Technology Organization:

- Prioritize log management appropriately throughout the organization
- Create and maintain a secure log management infrastructure
- Establish procedures for log management (including incident response)
- Provide proper training for all staff with log management responsibilities

Security Administrators and Information Security Officers:

- Manage and monitor the log management infrastructure
- Configure logging on security devices (e.g., firewalls, network-based intrusion detection systems, antivirus servers)
- Assist others with configuring logging and performing log analysis

System and Network Administrators:

- Configure logging on individual systems and network devices
- Perform regular maintenance of the logs and logging software
- Proactively analyze log data to identify on-going activity and signs of impending problems

Application Developers:

Design or customize applications so they perform logging in accordance with organizational logging requirements and applicable State standards.

SUPPORTING DOCUMENTS:

- Information Technology Standard 677S1: Log Management

By Authority of Director, Information Services Division, Department of Finance

DOCUMENT HISTORY:

Version	Release Date	Comments
677-00	09/01/2011	Replaces Policy 670-06 (number and format change only)