

STATE OF ALABAMA

Information Technology Policy

POLICY 676-00: MONITORING AND REPORTING

Changing threat conditions, changes to information systems (including hardware, firmware, software and people), and the potential impact those changes may have on agency operations, assets, or individuals, requires a structured and disciplined process capable of monitoring the effectiveness of the information system security controls on a continuous basis.

OBJECTIVE:

Establish the responsibility for State of Alabama organizations to continuously monitor the security of their information systems, document and report information system security status to the organization's senior management, and make reports available for review by the State CIO's Office.

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:

Ensure that important security-related considerations are included in the design, development, implementation, and operation of State information systems.

Ensure information systems are continuously monitored, assessed, and reported throughout the system life cycle to provide oversight of information system security controls on an ongoing basis.

Select an appropriate set of security controls in the information system to be monitored. Specific threat information, if available, should be used during the system risk assessment to help guide the selection of security controls for the information system.

The IT Manager or senior agency Information Security Officer (ISO) should approve the set of security controls that are to be continuously monitored, and ensure that the security controls (either planned or implemented) for the information system have been documented in a system security plan.

Continuously monitor the designated controls using methods and procedures selected by the information system owner. Security control monitoring methods may include security reviews, self-assessments, automated tools, security testing and evaluation, or audits.

Inform appropriate personnel when changes occur that may impact the security of an information system.

Update system security plans based on proposed or actual changes to the information system (including hardware, software, firmware, and surrounding environment) and the results of the continuous monitoring process.

Create/update a plan of action and milestones that addresses the following:

- Report of progress made on any current or outstanding items listed in the plan
- Vulnerabilities in the information system discovered during security control monitoring
- Describe how the information system owner intends to address those vulnerabilities (i.e., reduce, eliminate, or accept the identified vulnerabilities)

Status reporting should occur at appropriate organization-defined intervals (at least annually) and following significant changes affecting system security posture.

Security status reports shall be provided to the organization's senior management and made available for review by the State CIO's Office.

ADDITIONAL INFORMATION:

An effective organization-wide continuous monitoring program includes configuration management (CM) and change control processes for organizational information systems. CM responsibilities are defined in IT Policy 605 and the CM process is described in IT Guideline 605G1.

Information Technology Policy 605: Configuration Management
http://cybersecurity.alabama.gov/documents/Policy_605_Configuration_Management.pdf

Information Technology Guideline 605G1: CM Process
http://cybersecurity.alabama.gov/documents/Guideline_605G1_CM_Process.pdf

Information Technology Dictionary
http://cybersecurity.alabama.gov/documents/IT_Dictionary.pdf

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

DOCUMENT HISTORY:

Version	Release Date	Comments
676-00	09/01/2011	Combines and replaces Policy 670-02 and Standard 670-02S1