STATE OF ALABAMA

Information Technology Policy

POLICY 675-00: VULNERABILITY MANAGEMENT

Timely patching of security vulnerabilities is critical to maintaining the operational availability, confidentiality, and integrity of information technology (IT) systems. Vulnerability management is a security practice designed to proactively prevent the exploitation of IT vulnerabilities through a systematic, accountable, and documented process for managing the timely deployment of patches and other threat remediation practices.

OBJECTIVE:

Maintain a consistently configured environment, secure against known vulnerabilities in operating system and application software, using a managed remediation process.

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:

Create (or participate in) a comprehensive vulnerability management program with documented, and accountable processes for identifying and addressing vulnerabilities, threats, and remediation within the organization's area of responsibility.

Ensure System/Network Administrators maintain secure system/application configurations by:

- Applying all applicable fixes, patches and updates in a timely manner
- Routinely reviewing vendor sites, bulletins, and notifications
- Implementing vulnerability mitigation strategies in accordance with the organizational vulnerability management program

ADDITIONAL REQUIREMENTS:

In accordance with the recommendations of the National Institute of Standards and Technology (NIST) found in Special Publication 800-40: Creating a Patch and Vulnerability Management Program, State of Alabama vulnerability management programs shall implement the following tasks:

- Create an inventory of all information technology assets
- Create a patch and vulnerability group (recommended)
- Continuously monitor for vulnerabilities and threats using automated and manual methods
- Prioritize patch application; use phased deployments as appropriate
- Test patches before deployment
- Deploy enterprise-wide automated patch management solutions whenever possible
- Create a remediation database (see IT Dictionary)
- Use automatically updating applications as appropriate
- Verify vulnerabilities have been remediated
- Train applicable staff on vulnerability monitoring and remediation techniques

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

DOCUMENT HISTORY:

Version	Release Date	Comments
675-00	09/01/2011	Replaces Policy 670-03 and Standard 670-03S1