STATE OF ALABAMA

Information Technology Standard

STANDARD 662S1-02: SERVER SECURITY

Though operating system vendors have taken steps to make their operating system baseline configurations more secure on a default installation, additional operating system hardening efforts are usually required in order to reduce the exposure of State of Alabama server-based computing resources to cyber-related threats and unauthorized access. Secure operating system baseline configurations are a fundamental countermeasure.

OBJECTIVE:

Define standard configuration settings for a secure computing baseline for State of Alabama server computing resources.

SCOPE:

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

REQUIREMENTS:

To ensure server security, apply the guidelines stated in National Institute of Standards and Technology (NIST) Special Publication 800-123: Guide to General Server Security. The following additional requirements apply to all State of Alabama servers.

SERVER SECURITY STANDARDS

Configuration Standards:

Configure servers in accordance with an appropriate security baseline or hardening script.

The CIS Security Benchmarks Division develops and distributes Security Configuration Benchmarks describing consensus best practices for the secure configuration of IT systems. Download and apply the applicable server and operating system CIS benchmark(s) from:

http://benchmarks.cisecurity.org/downloads/browse/?category=benchmarks

Other sources of acceptable configuration standards include Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIGs) or NIST National Checklist Program (NCP) Repository.

- DISA STIGs are available here: http://iase.disa.mil/stigs/pages/a-z.aspx
- NIST NCP Checklists are available here: https://nvd.nist.gov/ncp/repository

Document the designated operating environment, the server role, and the selected benchmark or guide in system security plans and local operating procedures. Document any differences between the benchmark settings and the final server configuration and provide justification for those differences.

Least Functionality:

Employ the principle of “Least Functionality” (NIST 800-53, CM-7) by configuring systems to provide only essential capabilities.

Prohibit or restrict the use of system functions, ports, protocols, and/or services to only those required for system functionality.

Allowed functions, ports, protocols, and/or services shall be documented in State Standards and made available to State Server Administrators.

Internet Access:

Servers are not allowed to initiate access to the Internet without explicit approval.

All servers shall use ISD's Internal DNS servers for their DNS.

Servers shall be subject to Web Content Management. The following content categories are allowed:

Web Content – Allowed Categories

- Freeware Downloads
- Information and Computer Security
- Information Technology
- Government and Legal Organizations

(Reference: http://www.fortiguard.com/static/webfiltering.html)

Application Control – Allowed Categories

- Update (Windows Update, Adobe Update, Symantec Update, McAfee Update, etc)
- Web.Others

(Reference: http://www.fortiguard.com/encyclopedia/applications/)

All other applications/categories, including unknown applications, will be implicitly blocked. Additionally, known security risks (such as Botnets and Proxies) shall be explicitly blocked.

Requests for access to blocked applications shall be directed to the ISD Help Desk and may require approval by the ISD Director, the State IT Security Council, and/or the Office of Information Technology.

Malicious Code Protection:

In accordance with Malicious Code Protection controls stated in NIST 800-53 (SI-3), ensure all servers employ malicious code protection mechanisms (i.e., anti-virus software and spam protection (when appropriate)). Requirements are stated in State IT Policy 674: Virus Protection.

Physical Security:

Ensure physical security of servers. Requirements are stated in State IT Policy 651: Physical Security.

BIOS Protection:

Because of its unique and privileged position within the system architecture, the unauthorized modification of BIOS firmware by malicious software constitutes a significant threat. Server Administrators shall:

- Ensure system BIOS updates follow a secure process (for further guidance, refer to NIST Special Publications 800-147: BIOS Protection Guidelines, or 800-147 B: BIOS Protection Guidelines for Servers)
- Handle unauthorized BIOS changes following security incident response procedures

Server Software Support:

Operating systems that are unsupported will not receive security updates making them vulnerable and subject to exploitation. Systems shall be maintained at a service pack level supported by the vendor with new security updates. Unsupported systems may be isolated from other network resources until brought up to date.

Maintain application and operating system software by applying service packs, patches, and fixes in accordance with NIST 800-53 (SI-2), State IT Policy 675, local operating procedures, and/or vendor instructions.

COMPLIANCE

Compliance with these server configuration requirements shall be validated by ISD through periodic vulnerability scanning (as defined in State IT Policy 672: Vulnerability Scanning) and through other monitoring activities.

ISD shall notify (as applicable) the agency IT Manager, Agency Director, and/or State IT Security Council of non-compliance with these requirements.

SUPPORTING DOCUMENTS:

- Information Technology Policy 662: Systems Security
- Information Technology Policy 651: Physical Security
- Information Technology Standard 662S2: Client Systems Security
- Information Technology Standard 662S3: Point-of-Sale Systems Security
- Information Technology Guideline 662G1: Systems Security
- Information Technology Policy 675: Vulnerability Management

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

DOCUMENT HISTORY:

Version	Release Date	Comments
660-02B1	12/18/2007	Original Baseline document
660-02B1_A	9/18/2008	Added general security requirements from NIST 800-123 and Windows Server 2008 Security Guide reference.
660-02S3	2/4/2011	Reissued as a Standard
662S1-00	09/01/2011	New number and format
662S1-01	09/21/2012	Replaced Microsoft Security Guide links with CIS Security Benchmark link
662S1-02	06/24/2013	Completely revised