8-503. Minimum server configuration.

The state recognizes the National Institute of Standards and Technology (NIST) along with Center for Internet Security (CIS) Controls and Benchmarks as sources for recommended security requirements that provide minimum baselines of security for servers.

NIST and CIS provide instructions, recommendations, and considerations to assist readers in deploying servers in a secure method. All state system administrators should examine NIST and CIS Control documents when installing or configuring servers. The documents are not all inclusive, but rather meant as a means of prompting and guiding administrators through the installation process.

Agencies must comply with the following NIST standards, guidelines, and checklists: NIST SP 800-53, Security and Privacy Controls for Information Systems and Organizations; NIST SP 800-70, National Checklist Program for IT Products; and NIST SP 800-44, Guidelines on Securing Public Web Servers. Agencies should also strive to implement the highest tier possible for the CIS Controls and Benchmarks.

Server Hardening. All State of Nebraska servers are required to be hardened according to these standards. In addition, these servers must have a published configuration management plan as defined below and approved by the Office of the CIO. The following are server hardening standards:

(1) Servers may not be connected to the state network until approved by the Office of the CIO. This approval will not be granted for servers until these hardening standards have been met or risk levels have been accepted by agency management;

(2) The operating system must be installed by authorized IT personnel only, and all vendor supplied patches must be applied. All software and hardware components must be currently supported by the vendor. All unsupported hardware and software components must be identified and have a management plan for replacement that is approved by the Office of the CIO;

(3) All unnecessary software, system services, system and admin accounts, and drivers must be removed or disabled unless doing so would have a negative impact on the server;

(4) Logging of auditable events, as defined in NIST SP 800-53 control objectives, will be enabled. Audit logs will be secured and only accessible to accounts with privileged access and retained for a minimum of one year or be retained in accordance with federal and state guidance;

(5) Security parameters and file protection settings must be established, reviewed, and approved by the Office of the CIO;

(6) All system software must have security updates and patches applied when made available from the vendor. Priority setting of vulnerabilities will be based on impact to the agency and as referenced in the National Vulnerability Database (https://nvd.nist.gov);

(7) Servers will be scanned monthly for unauthorized software or unauthorized changes to the configuration baselines;

(8) Servers will be monitored with active intrusion detection, intrusion protection, and end-point security monitoring that has been approved by the state information security officer. This monitoring must have the capability to alert IT administrative personnel within 1 hour;

(9) Servers must be loaded from standardized processes and software. These processes and software shall be appropriately configured and protected, with integrity controls to ensure only authorized and documented changes are possible;

(10) All significant changes to servers must go through a formal change management and testing process to ensure the integrity and operability of all security and configuration settings. Significant changes must have a documented security impact assessment included with the change;

(11) Remote management of servers must be performed over secured channels only. Protocols that do not actively support approved encryption, such as telnet, VNC, and RDP, should only be used if they are performed over a secondary encryption channel, such as TLS; and

(12) Agencies must implement prevention techniques to protect against unauthorized data mining of information from public facing systems (e.g. Captcha).

--

History: Adopted on July 12, 2017. Amended on July 8, 2021.
URL: https://nitc.nebraska.gov/standards/8-503.pdf