8-503. Minimum server configuration.

The state recognizes the National Institute of Standards and Technology (NIST) as a source for recommended security requirements that provide minimum baselines of security for servers.

NIST provides instructions, recommendations, and considerations to assist readers in deploying servers in a secure method. All state system administrators should examine NIST 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.

Server Hardening. All servers that store, process, or have access to CONFIDENTIAL or RESTRICTED data 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 state information security officer. 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 sensitive 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 IT authorized personnel only, and all vendor supplied patches must be applied. All software and hardware components should be currently supported. All unsupported hardware and software components must be identified and have a management plan that is approved by the state information security officer;

(3) All unnecessary software, system services, accounts and drivers must be removed 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;

(5) Security parameters and file protection settings must be established, reviewed, and approved by the state information security officer;

(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 (http://nvd.nist.gov);

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

(8) Hardened servers will be monitored with active intrusion detection, intrusion protection, or 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 changes to hardened 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; and

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

--

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