Nebraska Information Technology Commission

STANDARDS AND GUIDELINES

Minimum Server Configuration Standard

Category	Security Architecture
Title	**Minimum Server Configuration Standard**
Number	

Applicability

☑ State Government Agencies

- ☐ **All** ..... Not Applicable
- ☑ **Excluding higher education institutions**..... Standard

☐ State Funded Entities - **All entities receiving state funding for matters covered by this document** ..... Not Applicable

☑ Other: **All Public Entities** ..... Guideline

Definitions:
Standard - Adherence is required. Certain exceptions and conditions may appear in this document, all other deviations from the standard require prior approval (see Section 3.2).
Guideline - Adherence is voluntary.

Status	☐ **Adopted** ☑ **Draft** ☐ **Other:**_____
Dates	**Date: Draft February 7, 2007** Date Adopted by NITC: Other:

Prepared by: Technical Panel of the Nebraska Information Technology Commission
Authority: Neb. Rev. Stat. § 86-516(6)
http://www.nitc.state.ne.us/standards/

1.0 Standard

The State of Nebraska recognizes the National Institute of Standards and Technology (NIST) as the adopted author of deployment configurations that provide minimum baselines of security for servers on the State of Nebraska network. As such, all state agencies, boards and commissions will comply with NIST standards, guidelines, and checklists as identified in Appendix A.

NIST provides instructions, recommendations, and considerations to assist readers in deploying servers in a secure method. All State of Nebraska System Administrators should examine NIST documents when installing and or configuring servers. The documents are not all inclusive, but rather meant as a means of prompting and guiding Administrators through the installation process.

2.0 Purpose and Objectives

Information technology (IT) is a vital resource to the State of Nebraska; therefore it is critical that services provided by these systems are able to operate effectively.

The purpose of this standard is to establish base configurations and minimum server standards on internal server equipment that is owned and/or operated by the State of Nebraska. Effective implementation of this policy will minimize unauthorized access and other IT security related events to the State of Nebraska's information and technology systems.

3.0 Applicability

3.1 State Government Agencies

All State agencies, boards, and commissions, excluding higher education institutions, which deploy servers on the State of Nebraska network.

3.2 Exemption

Exemptions may be granted by the NITC Technical Panel upon request by an agency.

3.2.1 Exemption Process

Any agency may request an exemption from this standard by submitting a "Request for Exemption" to the NITC Technical Panel. Requests should state the reason for the exemption. Reasons for an exemption include, but are not limited to: statutory exclusion, federal government requirement, or financial hardship. Requests may be submitted to the Office of the NITC via e-mail or letter (Office of the NITC, 501 S 14th Street, Lincoln, NE 68509). The NITC Technical Panel will consider the request and grant or deny the exemption. A denial of an exemption by the Technical Panel may be appealed to the NITC.

4.0 Responsibility

4.1 NITC

The NITC shall adopt minimum technical standards, guidelines, and architectures upon recommendation by the technical panel. (Neb. Rev. Stat. § 86-516(6))

4.2 Agency and Institutional Heads

The highest authority within an agency or institution is responsible for the protection of information resources, including developing and implementing information security programs, consistent with this standard. The authority may delegate this responsibility but delegation does not remove the accountability.

4.3 Agency Information Officer

In most cases, the highest authority within an agency or institution delegates the general responsibility for security of the agency's information technology resources to the agency's highest-ranking information technology professional. This responsibility includes development and promulgation of agency-specific information security policies, including installation, and configurations of all servers present on the state's network.

4.4 Agency System or Network Administrator

In most cases, the authority within an agency or institution responsibility for the day-to-day system, network and/or security administration of the agency's information technology resources. This responsibility includes ensuring due diligence to security best practices is performed when any server is made available on the state's network

5.0 Related Standards and Guidelines

5.1 NITC Security Policies
http://www.nitc.state.ne.us/tp/workgroups/security/security_policies.html

5.2 NITC Security Officer Handbook
http://www.nitc.state.ne.us/standards/security/so_guide.doc

Appendix A

NIST Security Configuration Checklists Repository
http://csrc.nist.gov/checklists/repository/index.html

NIST SP 800-70, The NIST Security Configuration Checklists Program,
http://csrc.nist.gov/checklists/download_sp800-70.html

NIST SP 800-68, Guidance for Securing Microsoft Windows XP Systems for IT Professionals: A NIST Security Configuration Checklist, http://csrc.nist.gov/itsec/download_WinXP.html

NIST SP 800-44, Guidelines on Securing Public Web Servers,
http://csrc.nist.gov/publications/nistpubs/800-44/sp800-44.pdf