Technical Panel
of the
Nebraska Information Technology Commission

Standards and Guidelines

Draft Document
30-Day Comment Period

Title: Remote Access Standard

Notes to Readers:

1. The following document is a draft standard under review by the Technical Panel of the Nebraska Information Technology Commission (NITC). This document is available in both PDF and Word versions at http://www.nitc.state.ne.us/standards/index.html.
2. If you have comments on this document, you can send them by e-mail to rick.becker@nitc.ne.gov, or call 402-471-7984 for more information on submitting comments.
3. The comment period for this document ends on November 21, 2006.
4. The Technical Panel will consider this document and any comments received at their meeting on November 22, 2006. Information about this meeting will be posted on the NITC web site at http://www.nitc.state.ne.us/.

Nebraska Information
Technology Commission

STANDARDS AND GUIDELINES

Remote Access Standard

Category	**Security Architecture**
Title	**Remote Access 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 as outlined in section 3.2
Guideline - Adherence is voluntary.

Status	☐ **Adopted** ☑ **Draft** ☐ **Other:_________**
Dates	**Date: Draft October 20, 2006** **Date Adopted by NITC:** **Other: Previous Guideline adopted by the NITC on September 30, 2003.**

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

It is the responsibility of all State of Nebraska agencies to strictly control remote access from any device that connects from outside of the State of Nebraska network to a desktop, server or network device inside the State of Nebraska network and ensure that employees, contractors, vendors and any other agent granted remote access privileges to any State of Nebraska network utilize one of the approved secure remote access products listed in Appendix A. (Approved Remote Access products).

2.0 Purpose and Objectives

As employees and organizations utilize remote connectivity to the State of Nebraska networks, security becomes increasingly important. Accompanying and contributing to this trend is the explosive growth in the popularity of broadband connections and other technologies for remote access. These standards are designed to minimize the potential exposure from damages which may result from unauthorized use of resources; which include loss of sensitive or confidential data, intellectual property, damage to public image or damage to critical internal systems, etc. The purpose of this document is to define standards for connecting to any State of Nebraska agency from any host.

Objectives include:

- Provide guidance to State of Nebraska agencies for employees, contractors, vendors and any other agent that requests remote access to any State of Nebraska network.
- Provide a high level of security that uses standardized technology and remains adaptable in the face of changing technology products.
- Ensure a solution that is scalable to meet the current and future needs of state agencies, their employees, clients and customers, and business partners.
- Meet federal security requirements for remote access control.

3.0 Applicability

3.1 State Government Agencies

All State agencies, boards, and commissions are required to comply with the standard listed in Section 1.0. All existing Agencies utilizing non-standard remote access applications must convert to the standard listed in Section 1.0 as soon as fiscally prudent, unless the application is exempt.

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 requirements; or financial hardship. Requests may be submitted to the Office of the NITC via e-mail. The NITC Technical Panel will consider the request and grant or deny the exemption. A denial of an exemption by the NITC Technical Panel may be appealed to the NITC.

4.0 Responsibility

4.1 NITC

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

4.2 State Agencies

Each state agency will be responsible for developing a policy that ensures that secure remote access to State resources is maintained, and/or implemented, including but not limited to selecting appropriate technologies, software, and tools in a manner consistent with this standard and other state agency security policies.

Each state agency will be responsible for ensuring that the computers connected to State resources contain an Anti-Virus program with current signatures and that the computer is free from Spyware, Adware, and rootkits that would place State resources in jeopardy.

4.2.1 Remote Access from Non-State Owned and/or Managed Devices

All Remote Access Users must sign and renew annually an agreement with the agency which addresses at a minimum the following:

- Remote access users are responsible for all actions incurred during their session in accordance with all State of Nebraska and agency standards and policies.
- All home networks connected to the Internet via a broadband connection should have a firewall installed, updated and operational.
- Web browsers settings should be selected or disabled as appropriate to increase security and limit vulnerability to intrusion.
- Operating systems should contain the most current security patches.
- All home computers must contain an Anti-Virus program with current signatures and that the computer is free from Spyware, Adware, and rootkits.

5.0 Related Documents

5.1 NITC Security Officer Handbook
(http://www.nitc.state.ne.us/standards/security/so_guide.doc)
5.2 NITC Network Security Policy (http://www.nitc.state.ne.us/standards/index.html)
5.3 NITC Incident Response and Reporting Procedures for State Government
(http://www.nitc.state.ne.us/standards/index.html)
5.3 Appendix A
5.4 NITC Acceptable Use Policy
(http://www.nitc.state.ne.us/standards/network/aup_20040309.pdf) and applicable Agency acceptable Use Policies

6.0 References

6.1 National Institute Standards and Technology (NIST) Special Publication, 800-46, “Security for Telecommuting and Broadband Communications”.
(http://csrc.nist.gov/publications/nistpubs/index.html).

Appendix A
Approved Remote Access Products

Product	Version
nFuseCitrix	
State-sponsored VPN solution	
SSH	Version 2 (SSHv2) and above*

Configuration settings for SSHv2

- Change the default port that it listens on, say from TCP/22 to TCP/2222 (or some other value) which will render it invisible to port scans for SSH on the standard port
- Disallow 'root' from logging in directly to the console, which reduces the privilege of a connection even if the logon is guessed and makes its superuser password protection extremely difficult to defeat