



# Nebraska Information Technology Commission

## STANDARDS AND GUIDELINES

### Remote Access Standard

Category	<b>Security Architecture</b>
Title	<b>Remote Access Standard</b>
Number	

Applicability	<input checked="" type="checkbox"/> State Government Agencies <input type="checkbox"/> All.....Not Applicable <input checked="" type="checkbox"/> <b>Excluding higher education institutions</b> .....Standard <input type="checkbox"/> State Funded Entities - All entities receiving state funding for matters covered by this document .....Not Applicable <input checked="" type="checkbox"/> Other: <b>All Public Entities</b> ..... Guideline  <b>Definitions:</b> <b>Standard</b> - Adherence is required. Certain exceptions and conditions may appear in this document, all other deviations from the standard require prior approval of _____. <b>Guideline</b> - Adherence is voluntary.
---------------	---

Status	<input type="checkbox"/> Adopted <input checked="" type="checkbox"/> Draft <input type="checkbox"/> Other:
Dates	<b>Date: Draft September 7, 2006</b> <b>Date Adopted by NITC:</b> <b>Other: Previous Guideline adopted by the NITC on September 30, 2003.</b>

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

# DRAFT

## 1.0 Standard

It is the responsibility of all State of Nebraska agencies to strictly control remote access and ensure that employees, contractors, vendors and any other agent granted remote access privilege to any State of Nebraska network utilize one of the following approved secure remote access products (See 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 or letter. The NITC Technical Panel will consider, in consultation with representatives of the Nebraska GIS Steering Committee, 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

# DRAFT

Each state agency will be responsible for ensuring that remote access to State resources is developed, maintained, and/or implemented, including but not limited to providing guidance on 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 Users

- 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 device installed.
- 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.

## 5.0 Related Documents

### 5.1 NITC Security Officer Handbook

([http://www.nitc.state.ne.us/standards/security/so\\_guide.doc](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

## 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>).

# DRAFT

## Appendix A Approved Remote Access Products

Product	Version
Citrix	
VPN	
SSH	