NEBRASKA INFORMATION
TECHNOLOGY COMMISSION

# TECHNICAL STANDARDS AND GUIDELINES

## XX-XXX Remote Access Guidelines

| | |
|---|---|
| Category | **Security Architecture** |
| Title | **Remote Access Guidelines** |
| Number | **XX-XXX** |

| | |
|---|---|
| Applicability | ☑ **State Government Agencies**<br>□ All................................................**Not Applicable**<br>☑ Excluding higher education institutions................................................**Guideline**<br>□ **State Funded Entities -** All entities receiving state funding for matters covered by this document.................**Not Applicable**<br>☑ **Other:** All Public Entities..............................**Guideline**<br><br>**Definitions:**<br>**Standard** - Adherence is required. Certain exceptions and conditions may appear in this document, all other deviations from the standard require prior approval of _______________.<br>**Guideline** - Adherence is voluntary. |

| | |
|---|---|
| Status | □ Adopted ☑ Draft □ Other:_________ |
| Dates | Date: August 8, 2003<br>Date Adopted by NITC:<br>Other: |

Prepared by: Technical Panel of the Nebraska Information Technology Commission
Authority: Neb. Rev. Stat. § 86-1506(6)
http://www.nitc.state.ne.us/standards/

## 1.0 Guidelines

1.1 **All home networks connected to the Internet via a broadband connection should have some firewall device installed.** Personal software firewalls installed on each computer are useful and effective, but separate, dedicated, and relatively inexpensive hardware firewalls that connect between the broadband connection and the telecommuter's computer or network can provide greater protection. Organizations should consider using both personal and hardware firewall devices for high-speed connections. When both a software personal firewall and a separate device are in operation, the organization can screen out intruders and identify any rogue software that attempts to transmit messages from the user's computer to an external system.

1.2 **Web browsers should be configured to limit vulnerability to intrusion.** Web browsers also represent a threat of compromise and require additional configuration beyond the default installation. Browser plugins should be limited to only those required by the end user. Active code (such as ActiveX or Java) should be disabled or used only in conjunction with trusted sites. The browser should always be updated to the latest or most secure version. Privacy is always a concern with web browsers. The two greatest threats to this privacy are the use of cookies and monitoring of web browsing habits of users by third parties. Cookies can be disabled or selectively removed using a variety of built-in web browser features or third-party applications.

1.3 **Operating system configuration options should be selected or disabled as appropriate to increase security.** The default configuration of most home operating systems is generally inadequate from a security standpoint. File and printer sharing should almost always be disabled. The operating system and major applications should be updated to the latest and most secure version or patch level. All home computers should have an anti virus program installed and configured to scan all incoming files and e-mails. The anti virus program should have its virus database updated on a regular basis. Another concern for many telecommuters is the surreptitious installation of spyware by certain software applications. This spyware, while usually not intended to be malicious, reports information on users (generally without their knowledge) back to a third party. This information could be general information about their system or specifics on their web browsing habits. A variety of programs are available for detecting and removing this spyware..

1.4 **Selection of wireless and other home networking technologies should be in accordance with security goals.** Several home networking technologies are available for telecommuters who wish to connect their home PCs together to share resources. Some of these technologies are the same as their office counterparts (e.g., Ethernet), and others are designed specifically to meet the needs of telecommuters (e.g., phone- and power-line networking). While most of these technologies can be made relatively secure, some represent a threat to security of both the home network and, sometimes, the office network. In particular, wireless networking has vulnerabilities that should be carefully considered before any installation.

1.5 **Public entities should provide telecommuting users with guidance on selecting appropriate technologies, software, and tools that are consistent with the agency network and with agency security policies.** Users have many approaches to choose from in establishing an off-site office. Sophisticated technologies such as virtual private networks (VPNs) can provide a high level of security, but are more expensive and complex to implement than other solutions. Whenever practical, agencies should provide telecommuting users with systems containing pre-configured security software and necessary hardware. If possible, agency security administrators should update and maintain the systems as well, to minimize reliance on users who are not specialists in security features. (It is not always financially or logistically practical for agencies to provide users with pre-configured systems, and this recommendation should not be taken as a requirement of this publication.) Many users, particularly if they do not require interactive access to agency databases, can obtain an adequate degree of security at very low cost and with little additional software, easing burdens on both the user and system administrators at the central computing system. The benefits and risks of telecommuting are here to stay. Computing resources and access to office networks while on the road or working from home is too valuable for most organizations or employees to give up. While there will always be risks associated with remote access to an organization's resources, most of these risks can be mitigated through careful planning and implementation. By the same token, even though broadband connections generally represent a greater threat than dial-up connections, the threat can be reduced through careful configuration and the judicious use of the security tools and techniques discussed in this document.

## 2.0 Background

### 2.1 Purpose and Objectives

This document sets forth policies and guidelines for acquiring and managing resources used for remote access to the state's network. The following guidelines copy the Executive Summary and other information from the National Institute Standards and Technology (NIST) Special Publication, 800-46, "Security for Telecommuting and Broadband Communications". A full copy of this publication is available at: (http://csrc.nist.gov/publications/nistpubs/index.html).

Anyone implementing remote access should read the entire NIST Special Publication, 800-46, which is incorporated into these guidelines by reference.

These general guidelines do not replace or supercede any specific standards and procedures of operational entities, which have responsibility for managing communications networks.

### 2.2 Executive Summary

Telecommuting has become a popular trend in the workplace. As employees and organizations employ remote connectivity to corporate and government networks, the security of these remote end points becomes increasingly important to the overall security of a network. Accompanying and contributing to this trend is the explosive growth in the popularity of broadband connections for telecommuters. These developments complicate the process of securing organizational and home networks. This document assists organizations in addressing security issues by providing recommendations on securing a variety of applications, protocols, and networking architectures. Recommendations in this publication are designed for State government agencies, educational institutions and other public entities, but may be useful to commercial organizations and home users as well. Home broadband architectures face a variety of threats that, while present on dial-up connections, are easier to exploit using the faster, always-on qualities of broadband connections. The relatively short duration of most dial-up connection makes it more difficult for attackers to compromise telecommuters dialed-up to the Internet. "Always on" broadband connections provide attackers with the speed and communications bandwidth necessary to compromise home computers and networks. Ironically, as governmental and corporate organizations have hardened their networks and become more sophisticated at protecting their computing resources, they have driven some malicious entities to pursue other targets of opportunity. Telecommuters with broadband connections are these new targets of opportunity both for their own computing resources and as an alternative method for attacking and gaining access to government and corporate networks.

State agencies and their employees can take a variety of actions to better secure their telecommuting and home networking resources.

## 3.0 Definitions

**3.1** **Access Point**. A hub or interconnect device on a Local Area Network (LAN) that supports wireless (IEEE 802.11x) devices such as laptops, PDA's, etc. In some cases, the Access Point constitutes a stand-alone LAN where only a few wireless devices that need to communicate or share resources.

**3.2** **Local Area Network (LAN)**. A data communications system that (a) lies within a limited spatial area, (b) has a specific user group, (c) has a specific topology, and (d) is not a public switched telecommunications network, but may be connected to one. For State agencies, LANs are defined as restricted to rooms or buildings. An interconnection of LANs within a limited geographical area, such as a military base, is commonly referred to as a campus area network. An interconnection of LANs over a city-wide geographical area is commonly called a metropolitan area network (MAN). An interconnection of LANs over large geographical areas, such as nationwide, is commonly called a wide area network (WAN).

**3.3** **Metropolitan Area Network (MAN)**. A data communications network that (a) covers an area larger than a local area network (LAN) and smaller than a wide area network (WAN), (b) interconnects two or more LANs, and (c) usually covers an entire metropolitan area, such as a large city and its suburbs.

**3.4** **Personal Digital Assistant (PDA)**. A handheld computer that serves as an organizer for personal information. It generally includes at least a name-and-address database, a to-do list, and a note taker. PDAs are pen-based and use a stylus to tap selections on menus and to enter printed characters. The unit may also include a small on-screen keyboard that is tapped with the pen. Data are synchronized between a user's PDA and desktop computer by cable or wireless transmission.

**3.5** **Smart Card**. A credit card with a built-in microprocessor and memory that is used for identification or financial transactions. When inserted into a reader, the card transfers data to and from a central computer. A smart card is more secure than a magnetic stripe card and can be programmed to self-destruct if the wrong password is entered too many times.

**3.6** **Virtual Private Network**. A means by which certain authorized individuals (such as remote employees) can gain secure access to an organization's intranet by means of an extranet (a part of the internal network that is accessible via the Internet).

**3.7** **Wide Area Network (WAN)**. A physical or logical network that provides data communications to a larger number of independent users than are usually served by a local area network (LAN) and is usually spread over a larger geographic area than that of a LAN. Note 1: WANs may include physical networks, such as Integrated Services Digital Networks (ISDNs), X.25 networks, and T1 networks. Note 2: A metropolitan area network (MAN) is a WAN that serves all the users in a metropolitan area. WANs may be nationwide or worldwide.

**3.8** **Wireless Application Protocol (WAP)**. A standard for providing cellular telephones, pagers, and other handheld devices with secure access to e-mail and text-based Web pages.

**3.9** **Wired Equivalent Privacy (WEP)**. Wired Equivalent Privacy (WEP) is a security protocol, specified in the IEEE Wireless Fidelity (Wi-Fi) standard, 802.11, that is designed to provide a wireless local area network (WLAN) with a level of security and privacy comparable to what is usually expected of a wired LAN.

## 4.0 Applicability

These guidelines are intended to be useful to all public entities that are developing their own security policies and procedures for remote access. They specifically apply to state government agencies, excluding higher educational institutions.

## 5.0 Responsibility

**5.1** **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, including disaster recovery plans for information technology. The authority may delegate this responsibility but delegation does not remove the accountability.

**5.2** **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 disaster recovery planning for information technology.

**5.3** **Agency Security Officer**. In some cases, the Agency Information Officer assigns an Agency Security Officer who is responsible for preparing a disaster recovery plan for information technology. They must understand the risks posed by disruption of computer systems. They must help prepare contingencies and be ready to implement the disaster recovery plan for information technology.

## 6.0 Related Policies, Standards and Guidelines

**6.1** NITC Security Officer Handbook (http://www.nitc.state.ne.us/standards/security/so_guide.doc)

**6.2** NITC Network Security Policy (http://www.nitc.state.ne.us/standards/index.html)

**6.3** NITC Incident Response and Reporting Procedures for State Government (http://www.nitc.state.ne.us/standards/index.html)

## 7.0 References

**7.1** National Institute Standards and Technology (NIST) Special Publication, 800-46, “Security for Telecommuting and Broadband Communications”. A full copy of this publication is available at: (http://csrc.nist.gov/publications/nistpubs/index.html).

## APPENDIX

### A. Home Computer Security Checklist

1. **Anti Virus Software --** Anti virus application is installed and is configured to:
   a. Start with the boot of the operating system.
   b. Run in the background and automatically scan all incoming files.
   c. Enable web browser protection, if available.
   d. Automatically update the virus signature database weekly.
   e. Schedule it to be run at least weekly to scan all hard drive files.
   f. Attempt to recognize unknown viruses, if available.
2. **Spyware Removal Tools**
   a. Install and run a spyware removal tool to identify and eliminate (as appropriate) spyware.
   b. On a monthly basis, update and run spyware removal tool, again eliminate discovered spyware if appropriate.
3. **Firewall**
   a. A firewall is an application that is employed to monitor and limit dangerous packets from entering a network, providing the capability to:
   b. Log all suspicious traffic (this is generally true for default installs).
   c. Examine log on a periodic basis.
   d. Block traffic to ports that support services that should not be accessible from the Internet (e.g., NetBIOS, Telnet, etc.).
   e. Automatically lock out network access to the host when network connectivity is not required (e.g., when the screensaver activates or computer is inactive for a fixed period of time).
   f. Notify the user when an application attempts to make an outbound connection.
   g. Medium to high level of security (e.g., “paranoia level”).
4. **Encryption Software**
   a. Ensure that appropriate encryption software is being used.
5. **Securing the Operating System**
   a. Secure or disable file and printer sharing.
   b. Ensure that the latest operating system patches are installed.
   c. Use a password protected screensaver to lock it during periods of inactivity.
   d. Where appropriate use a BIOS password to restrict who is able to start the system.
   e. Turn your system off when it is not being used.
6. **Securing Wireless Networks**
   a. Place wireless base station away from outside walls in order to minimize transmission of data outside of building.
   b. Use additional encryption beyond WEP (VPN, PGP, etc.).
   c. Enable 128-bit WEP encryption.
   d. Change SSID to a hard to guess password.
   e. Enable additional authentication schemes supported by your wireless base station.
   f. Disable broadcasts of SSID in the wireless base station beacon message.
   g. Disable SNMP or change the SNMP community strings to a hard-to-guess password.
   h. Install personal firewall on all wireless clients.
7. **Online Security Assessment**
   a. An online security assessment has scanned the current configuration (including the firewall).
   b. All major vulnerabilities identified by the assessment have been corrected and confirmed by a rescan.
8. **Securing Web Browsers**
   a. Browser(s) configured to limit or disable plugins.
   b. Browser(s) configured to limit ActiveX, Java, and JavaScript.

B. **Laptop Security Checklist**
The need for an explicit laptop security checklist can be illustrated by the fact that, according to Safeware Insurance in 1999, the number of laptop computers stolen outnumbered the number of desktop computers stolen by almost 12 to 1.

1. **Review Home Computer Security Checklist**
   a. Where applicable, the appropriate elements from the home computer security checklist presented previously should be applied to a laptop computer. (Not all elements from home computer security checklist may apply.)
2. **Encryption Software**
   a. Although mentioned above in the home computer security checklist, encryption is vital for protecting sensitive information on a mobile computer. Operating system features such as encrypting file system (EFS) or even discretionary access control (DAC) permissions can provide valuable security for a laptop that is stolen.
   b. Third-party software such as PGP and Norton Internet Security can provide similar levels of protection for laptop data.
3. **Physical Security**
   a. Laptops that spend a majority of their time in two or fewer places should be physically secured with a cable lock.
   b. Cable locks are widely available on the Internet and in computer retail stores.
   c. Almost all major laptop brands contain a slot to attach a lock cable.
   d. Those that do not can have a lock cable glued on.
4. **Set BIOS Password**
   a. Set BIOS password to prompt user every time laptop is powered up.
   b. Check for BIOS updates at least twice a year (or more) to “flash” BIOS.
5. **Use Non-descript carrying case**
   a. Avoid unwanted attention. A leather briefcase or obvious laptop case can attract attention in public places, especially airports, and while on planes.
   b. If traveling with confidential information, pack information or information backup in separate bag from laptop in case of theft.
6. **Identify Laptop with contact information**
   a. Many companies and individuals place decals or markings on the laptop case that are difficult to remove and if done so, indicate obvious tampering.
   b. Record serial number and other identification information about laptop twice, and keep one copy at home or in the office in case of theft. This information can be helpful to authorities searching for the laptop.
7. **Backup all personal data on a regular basis**
   a. In the event that your laptop is stolen, all of your work is essentially useless without a backup of all of your personal data.
8. **Consider purchasing advanced security features**
   a. Should your computing needs or data security warrant it, products that offer increasingly advanced security features such as biometric login, motion sensing, and “Lo-Jack” type location tracking are becoming increasingly cheaper to purchase for laptops.
   b. Software developers are responding to this demand by integrating these new technologies into common tasks of computer usage such as seamlessly logging in to the operating system.

C. **Telecommuting Security Checklist**
This checklist originally appeared in a Department of Energy publication. Not all items in the list will apply to every organization or telecommuter, but it provides a helpful starting point for an organization or individual to review the security of home computer systems. The checklist also includes considerations for organizations that have telecommuting users who regularly access the organization’s central network.

1. **User Identification and Authorization**
   a. Is the telecommuter authorized by their supervisor/manager to telecommute?

   b. Is the telecommuter authorized by the system owner to access the system(s) remotely?
   c. Does the telecommuter have a unique user ID and password for remote access and for access to sensitive applications?

2. **Access Controls**
   a. Are system access controls in place and functioning to log the identification of each remote access user, device, port, and user activity?
   b. Are system audit logs protected from unauthorized access?
   c. Are banners displayed regarding monitoring for unauthorized access and misuse?
3. **Auditing**
   a. Does the remote access system record alarms and authentication information?
   b. Does the system audit log identify date and time of access, user, origin, success or failure of access attempt?
   c. Are system audit logs retained to support reviews by computer security personnel?
   d. If dial-up access is allowed, does the system record details of access attempts?
4. **Information Availability**
   a. Are Government information assets (hardware, software, data, records) in a physically secure location and protected from theft, fire, smoke, hazardous material, etc.?
   b. Is backup media maintained, secured, and easily retrieved to support established contingency and disaster recovery plans?
   c. Is a physical inventory periodically conducted of Government information assets used for telecommuting?
   d. Can Government information assets be retrieved in the event of employee termination?
   e. Is there a process in place to ensure the most current version of anti virus software is installed on the telecommuting computer?
   f. Are Government information assets adequately secured when not in use by the telecommuter?
   g. Are user IDs and passwords protected from unauthorized use?
5. **Information Confidentiality**
   a. Is Government information protected from unauthorized disclosure (family, friends, eavesdroppers)?
   b. Is encryption used when transmitting sensitive unclassified information?
6. **Remote Access Security Administration**
   a. Is organizational, system administrator, and user responsibility for remote access security defined?
   b. Are justifications for remote access users periodically revalidated to support continued access privileges commensurate with job duties (at least annually)?
   c. Are incident reporting procedures in place to address handling of security breaches?
   d. Is regular system monitoring performed to detect unauthorized access attempts, denial of service, or other security weaknesses?
   e. Is access to network management tools restricted to authorized users?
   f. Is software used for telecommuting legally purchased, and are software-licensing agreements properly maintained?
   g. Are telecommuting equipment hard drives degaussed or overwritten to remove sensitive information in accordance with established best business practices?
7. **Architecture and Network Topology**
   a. Is the telecommuting equipment used interoperable with the computing architecture deployed at the home office?
   b. Does the network adequately separate traffic according to user communities? Does the remote access equipment and system protect the internal trusted network from the external (public) untrusted network?
   c. Are network topology maps documented and kept current?
8. **Education, Awareness, and Enforcement**

   a. Are telecommuters and their supervisors trained in the specific risks, threats, vulnerabilities, and proper use of a secure telecommuting environment?
   b. Is the telecommuter current on their computer security training?
   c. Is the telecommuter aware of the consequences for violation of Condition of Use agreements?

9. **Modem Use**
   a. Is there a single (or otherwise restricted) point of entry via modem into the internal network or server?
   b. Are all dial-up numbers protected from unauthorized disclosure?
   c. Is the telecommuter instructed to disconnect modem connectivity to the home office network or server when not in use?