M E E T I N G A G E N D A

Technical Panel

of the
Nebraska Information Technology Commission
Tuesday, June 13, 2006
9:00 a.m. - 10:30 a.m.
Varner Hall - Board Room
3835 Holdrege St., Lincoln, Nebraska

AGENDA

Meeting Documents: Click the links in the agenda
or click here for all documents (PDF xxx KB).

1. Roll Call and Meeting Notice

2. Public Comment

3. Approval of Minutes - April 17, 2006*

4. Standards and Guidelines*

- Recommendations to the NITC
  - Web Cookie Standard (PDF) | Comments Received (None)
  - Wireless Local Area Network Standard (PDF) | Comments Received (None)
  [Related documents: - Wireless Access Point Approval Process (PDF) - Wireless LAN Security Checklist (PDF)]
  - Information Technology Disaster Recovery Plan Standard (PDF) | Comments Received (None)

5. Discussion: Changes to the Project Proposal Form (PDF) and guidance document (PDF) for the upcoming biennial budget review process.

6. Discussion: NIDCAC Resolution Creating the Nebraska Computing and Telecommunications Security Committee (PDF) - Heath Hollenbeck

7. Regular Informational Items and Work Group Updates (as needed)

- Accessibility of Information Technology Work Group
- CAP
- Security Work Group
- Statewide Synchronous Video Network Work Group

8. Other Business

9. Next Meeting Date

Tuesday, July 11, 2006

10. Adjourn

* Denotes Action Item

(The Technical Panel will attempt to adhere to the sequence of the published agenda, but reserves the right to adjust the order of items if necessary and may elect to take action on any of the items listed.)

NITC and Technical Panel Websites: http://www.nitc.state.ne.us/
Meeting notice posted to the NITC Website: 20 APR 2006
Meeting notice posted to the Nebraska Public Meeting Calendar: 20 APR 2006
Agenda posted to the NITC Website: 9 JUN 2006

M E E T I N G M I N U T E S

TECHNICAL PANEL

Nebraska Information Technology Commission

Monday, April 17, 2006, 9:00 a.m.

Varner Hall, 3835 Holdrege

Lincoln, Nebraska

PROPOSED MINUTES

MEMBERS PRESENT:

Mike Beach, Nebraska Educational Telecommunications Commission
Brenda Decker, Chief Information Officer, State of Nebraska
Steve Henderson, Department of Administrative Services, State of Nebraska
Ron Cone, Alt. for Kirk Langer
Walter Weir, University of Nebraska

MEMBERS ABSENT: Christy Horn, University of Nebraska, Compliance Officer

CALL TO ORDER, ROLL CALL, NOTICE OF PUBLIC MEETING

Mr. Weir called the meeting to order at 9:13 a.m. A quorum was present at the time of roll call. The meeting notice was posted to the NITC website and the Nebraska Public Meeting Calendar on March 16, 2006. The meeting agenda was posted to the NITC Website on April 14, 2006.

PUBLIC COMMENT

There was no public comment.

APPROVAL OF MINUTES

Ms. Decker moved to approve the March 14, 2006 minutes as presented. Mr. Beach seconded. Roll call vote: Beach-Yes, Decker-Yes, Henderson-Yes, Cone- Yes, and Weir-Yes. Results: Yes-5, No-O. Motion carried.

STANDARDS & GUIDELINES: NETWORK EDGE DEVICE

Discussion occurred about the public comment received regarding the statement: "Network Nebraska support team familiarity with equivalent devices." Bid specifications will be more specific. After discussion, the following changes were recommended:

- Cover: Under "Applicability", include as a standard for State Government Agencies.

For State Funded Entities, change to not applicable. For Other, stike the word "educational".

- Section 1.0: Strike the last sentence. Change first sentence to read, “All state government agencies, boards, and commissions, and entities electing to connect to Network Nebraska for purposes of transmitting data across the state shall comply with this standard.”
- Sections 1.1 & 1.2: Strike thelast bullet that reads, “Network Nebraska support team familiarity with equivalent devices."
- Section 2.1: Change second sentence to read, “As these contracts reach the end of their terms, network upgrade or replacement will be examined through the bid process”.
- Sections 4.1 & 4.2: Revise to be consistent with the "Applicability" changes made on the cover.

Mr. Beach moved to forward the Network Edge Device Standard for Entities Choosing to Connect to Network Nebraska with the recommended changes to the NITC for final review and approval. Ms. Decker seconded. Roll call vote: Weir-Yes, Cone- Yes, Henderson-Yes, Decker-Yes, and Beach-Yes. Results: Yes-5, No-0. Motion carried.

STANDARDS & GUIDELINES: SCHEDULING STANDARD FOR SYNCHRONOUS DISTANCE LEARNING AND VIDEOCONFERENCING

No public comments were received. Members recommended that Ms. Decker contact Roger Keetle about the standard and discuss implications for the telehealth project. The recommended changes were to strike the second paragraph under Section 1.0, and correct the footer.

Mr. Henderson moved to forward the Scheduling Standard for Synchronous Distance Learning and Videoconferencing with the recommended changes to the NITC for final review and approval. Mr. Beach seconded. Roll call vote: Henderson-Yes, Cone- Yes, Weir-Yes, Beach-Yes, and Decker-Yes. Results: Yes-5, No-0. Motion carried.

STANDARDS & GUIDELINES: SET FOR 30 DAY COMMENT PERIOD

The State Government Council approved the following standards at their meeting on Thursday, April 13, 2006, for review by the Technical Panel.

Web Cookie Policy: The panel recommended that it be a standard rather than a policy.

Wireless Local Area Network Standard: The Security Architecture Work Group recommended the inclusion of the following reference documents rather than include them in the standard – Wireless Access Point Approval Process and the Wireless Local Area Network Security Checklist to allow for regular updates.

I.T. Disaster Recovery Plan Standard: The Shared Services Work Group took over development and review of the standard. It was originally developed the Security Architecture Work Group. Lt. Governor Sheehy has been meeting with agency directors on Disaster Recovery and Business Resumption. It was recommended to make this a standard for State Government Agencies.

Mr. Henderson moved to approve the Web Cookie Standard, Wireless Local Area Network Standard, and the I.T. Disaster Recovery Plan Standard for the 30-day public comment period. Ms. Decker seconded. Roll call vote: Cone- Yes, Henderson-Yes, Decker-Yes, Beach-Yes, and Weir-Yes. Results: Yes-5, No-0. Motion carried.

AGENCY IT PLAN FORM

The State Government Council has approved the reviesed form. Agency I.T. plans are due August 16, 2006.

Mr. Weir moved to approve the Agency I.T. Plan Form. Mr. Henderson seconded. Roll call vote: Decker-Yes, Henderson-Yes, Cone- Yes, Weir-Yes, and Beach-Yes. Results: Yes-5, No-0. Motion carried.

NEW NITC WEBSITE

Members were asked to review the new website and make any suggestions. The NITC will be reviewing it at their meeting on Monday, May 1st.

REGULAR INFORMATIONAL ITEMS

Accessibility. Ms. Horn was not present to provide a report.

CAP, Brenda Decker. The group is meeting today, after the technical panel meeting.

Security Architecture Work Group, Steve Hartman. An RFP has been issued for a security scan of the state's network. Pamphlets were distributed for the Cyber Security Conference being held on May 24, 2006. The conference is aimed at seasoned I.T. security personnel. The luncheon keynote speaker will be broadcasted for students, faculty and instructors. Seating is limited.

OTHER BUSINESS

Mr. Decker announced the new NITC Commissioners: Dr. Dan Hoesing, Laurel-Concord, Coleridge, & Newcastle Public Schools; Lance Hedquist, South Sioux City; Pat Flanagan, Mutual of Omaha; and Mike Huggenberger, Great Plains Communications.

NEXT MEETING DATE/TIME AND ADJOURNMENT

Members will be contacted regarding the May meeting.

Ms. Decker move to adjourn. Mr. Weir seconded. All were in favor. Motion carried.

The meeting was adjourned at 10:48 a.m.

Meeting minutes were taken by Lori Lopez Urdiales and reviewed by Rick Becker of the Office of the CIO/NITC.

Technical Panel
of the
Nebraska Information Technology Commission

Draft Document
30-Day Comment Period

Title: Web Cookie 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 May 22, 2006.
4. The Technical Panel will consider this standard and the comments received at their meeting currently scheduled for June 13, 2006. Final approval of the standard would be considered by NITC at their next meeting following the Technical Panel review. Information about these meetings will be posted on the NITC web site at http://www.nitc.state.ne.us/.

Nebraska Information Technology Commission

STANDARDS AND GUIDELINES

Web Cookie Standard

Category	**E-Government Architecture**
Title	**Web Cookie Standard**
Number	

Applicability

☑ **State Government Agencies**
- ☑ All ..... **Standard**
- ☐ Excluding _____ ..... **Not Applicable**

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

☐ **Other:** _____ ..... **Not Applicable**

Definitions:
Standard - Adherence is required. Certain exceptions and conditions may appear in this document, all other deviations from the standard require prior approval of the Technical Panel of the NITC.
Guideline - Adherence is voluntary.

Status	☐ Adopted ☑ Draft ☐ Other:_____
Dates	Date: Draft April 17, 2006 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

Nebraska.gov and state agencies may use cookies to store user information subject to the following:

1.1 Permanent Cookies

1.1.1 Will not contain personal identifying information (e.g. names, date of birth, social security number, hint answers).

1.1.2 May be used to save personalized web site settings (e.g. font size, color, text type, etc.).

1.1.3 May include an expiration date if appropriate.

1.2 Session Cookies

1.2.1 Will be erased when a user's web browser session ends or the user logs out of the application.

1.2.2 Will only be accessible to the specific application(s) in use.

1.3 Any use of cookies can be made known to the user through the use of appropriate browser settings.

1.4 The Web Cookie Standard is available on the State Portal.

2.0 Purpose and Objectives

The purpose of this standard is to establish guidance for the use of web cookies on web sites, web pages, and web applications created by State of Nebraska agencies, boards and commissions.

3.0 Definitions

3.1 Web Cookie

Any technique of saving state or tokens stored on a user's computer to be exchanged between a web browser and a web server is considered a cookie (an example of an additional type of cookie is a PIE - Persistent Identification Element).

3.2 Web Page

A document stored on a server, consisting of an XHTML file and any related files for scripts and graphics, viewable through a web browser or the World Wide Web. Files linked from a web page such as Word (.doc), Portable Document Format (.pdf), and Excel (.xls) files are not web pages, as they can be viewed without access to a web browser.

3.3 Web Site

A set of interconnected web pages, usually including a homepage, generally located on the same server, and prepared and maintained as a collection of information by a person, group or organization.

3.4 Web Application

An application that is accessed with a web browser over a network such as the Internet or an intranet.

4.0 Applicability

This standard shall apply to all State of Nebraska agencies, boards and commissions.

Technical Panel
of the
Nebraska Information Technology Commission

Draft Document
30-Day Comment Period

Title: Wireless Local Area Network 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 May 22, 2006.
4. The Technical Panel will consider this standard and the comments received at their meeting currently scheduled for June 13, 2006. Final approval of the standard would be considered by NITC at their next meeting following the Technical Panel review. Information about these meetings will be posted on the NITC web site at http://www.nitc.state.ne.us/.
5. Comments may also be submitted on two related documents: Wireless Access Point Approval Process and Wireless LAN Security Checklist. These documents are posted at http://www.nitc.state.ne.us/standards/index.html.

Nebraska Information
Technology Commission

STANDARDS AND GUIDELINES

Wireless Local Area Network Standard

Category	**Security Architecture**
Title	**Wireless Local Area Network 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 4.1).
Guideline - Adherence is voluntary.

Status	☐ Adopted	☐ Draft	☑ Other: Reviewed
Dates	Date: March 17, 2006 (Draft Revisions) Date Adopted by NITC: September 30, 2003 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/

Executive Summary

Wireless communications offer organizations and users many benefits such as portability and flexibility, increased productivity, and lower installation costs. Wireless technologies cover a broad range of differing capabilities oriented toward different uses and needs. Wireless local area network (WLAN) devices, for instance, allow users to move their laptops from place to place within their offices without the need for wires and without losing network connectivity. Less wiring means greater flexibility, increased efficiency, and reduced wiring costs.

In additional to the inherent risks associated with any wired network, wireless technology introduces several unique vulnerabilities. Since wireless signals are radio transmissions, they can be intercepted by suitable radio receiving devices, sometimes even devices operating outside the intended service area. If data transmissions are not encrypted or are inadequately encrypted, the intercepted data can be read and understood in a matter of seconds. Any data transmission sent through the wireless network is at risk, including correspondence, usernames and passwords, financial data, and other sensitive information. Because wireless transmissions circumvent traditional perimeter firewalls, those existing protections established to prevent unauthorized access are ineffective. Advances in wireless signaling technology may increase transmission distances, further exacerbating the problem of unauthorized reception. Unauthorized users may gain access to agency systems and information, corrupt the agency's data, consume network bandwidth, degrade network performance, and launch attacks that prevent authorized users from accessing the network, or use agency resources to launch attacks on other networks.

Also, since wireless network devices operate using radio signals, their proliferation within an area can lead to Radio Frequency Interference (RFI) among these devices and other radio devices using the same frequency bands.

The purpose of this standard is to ensure that only registered and secure WLANs are deployed by state government agencies. This standard provides the following:

1. State agencies must register WLANs, including each Access Point (AP) that connects to the state private network, with the Division of Communications (DOC). [Section 1.1]

2. State agencies must provide for proper management and security of WLANs. [Section 1.2]

3. Provides for resolution of conflicts between wireless devices. [Section 1.3]

4. Requires compliance with other network standards. [Section 1.4]

5. Provides a list of general recommendations for agencies implementing WLANs. [Section 1.5]

Source Notes: A source for portions of the original version of this document and the Division of Communication's Wireless Access Point Checklist was *Special Publication 800-48, "Wireless Network Security 800.11, Bluetooth and Handheld Devices,"* November 2002 published by the National Institute of Standards and Technology (NIST) of the U.S. Department of Commerce. A full copy of that publication is available at http://csrc.nist.gov/publications/nistpubs/index.html. NIST Special Publication 800-48 provides a detailed overview of wireless technology, wireless LANs, wireless personal area networks ("Bluetooth" technology), and wireless handheld devices. Anyone implementing any of these types of wireless systems should read the entire report. Parts of the document were also based on the National Institutes of Health, Wireless Network Policy.

1.0 Standard

This standard applies to state agencies which deploy a Wireless Local Area Network (WLAN).

Wireless services that fall within the definition of Campus Connection, Metropolitan Area Network (MAN), or Wide Area Network (WAN) must be purchased through DAS Information Technology Services (ITS) to comply with state statutes.

1.1 Registration of Wireless Devices

State agencies must register WLANs, including each Access Point (AP) that connects to the state private network, with the Division of Communications (DOC).

1.1.1 Registration

Self-registration is available through a DOC form on the ITS website (See Section 7.1). The registration process will identify: contact information; WLAN device information, including the manufacturer, model, and physical location; and the security/firewall technologies being deployed. Registration should occur prior to deployment.

1.1.2 Review and Approval

The DOC will contact the registering agency after reviewing the registration information.

1.1.3 Naming Convention

Final device names are assigned by the DOC during the registration process to avoid conflicts and confusion, and to aid in incident response and in identifying and locating wireless devices. If technology allows for the broadcast of a device name, standardized names should appear in the broadcast description, along with any unique identifiers assigned to the unit.

1.1.4 Unregistered (Rogue) and Unsecured Devices

Only approved WLANs and access points will be deployed within state agencies. Unregistered (rogue) devices will be removed from service.

Network managers for the DOC will incorporate procedures for scanning and detecting unregistered (rogue) wireless devices and access points. This requires a full understanding of the topology of the network. It also requires performing periodic security testing and assessment, including randomly timed security audits to monitor and track wireless and handheld devices. ITS reserves the right to disable network access for a device, server or LAN if adequate security is not in place.

1.2 Management and Security

1.2.1 Physical Security

Access points must be properly secured within a safe, adequately monitored area to prevent unauthorized access and physical tampering. Devices will not be placed in easily accessible public locations.

1.2.2 Configuration Management

All wireless access points must be secured using a strong password. Passwords will be changed at least every six months. Administrators must ensure all vendor default user

names and passwords are removed from the device. Administration of the device will be prohibited from the wireless network.

1.2.3 Authentication and Encryption

Authentication and encryption is required on all WLANs (see options listed on the registration form for details).

1.2.3.1 Access to Systems and Data

- Agencies and other entities connected to the state's network must employ adequate security measures to protect other systems and data connected to the state's network.
- Once authenticated to an access point, users will either be routed outside the state's firewall(s), or authenticated to the network. Just as with a wired network, state network authentication--whether enterprise-wide or agency-specific-- must satisfy prescribed login/password combinations prior to using enterprise or agency-specific resources that are not normally accessible by nodes outside the state's firewall(s).
- Access control mechanisms such as firewalls must be deployed to separate the wireless network from the internal wired network.
- As the technology permits, wireless networks will employ a combination of layered authentication methods to protect sensitive, proprietary, and patient information.

1.2.4 Risk Management

Agencies using wireless systems must develop general risk mitigation strategies for access points, users, and client devices such as virus protection, password standards, and other preventative measures.

1.3 Disruption and Interference

For state agencies, the DOC will resolve any conflicts between wireless devices in coordination with the affected agencies. Priority is granted to fully supported and registered installations, except in the case of medical, safety, or emergency devices, as appropriate.

1.4 Compliance with Other Network Standards

Agency WLANs must satisfy all existing and future standards pertaining to use and security of the state's network as required by law or established by the Nebraska Information Technology Commission or ITS.

1.5 General Recommendations for Agencies Implementing WLANs

1.5.1 Agencies must not undertake wireless deployment until they have examined and can acceptably manage and mitigate the risks to their information, system operations, and continuity of operations. Agencies should perform a periodic risk assessment and develop a security policy before purchasing wireless technologies, because their unique security requirements will determine which products will be considered for purchase.

1.5.2 Agencies must be aware of the technical and security implications of wireless and handheld device technologies.

1.5.3 Agencies must carefully plan the deployment of 802.11, Bluetooth, or any other wireless technology.

1.5.4 Agencies must be aware that security management practices and controls are especially critical to maintaining and operating a secure wireless network.

1.5.5 Agencies must be aware that physical controls are especially important in a wireless environment.

1.5.6 Agencies must enable, use, and routinely test the inherent security features, such as authentication and encryption that exist in wireless technologies.

1.5.7 Where appropriate, agencies must employ protection mechanisms, such as firewalls and intrusion detection systems will be employed.

1.5.8 State agencies must assure all Federal, State, and agency compliance regulations are addressed prior to implementing wireless technology.

1.5.9 Agencies must educate wireless users in wireless security measures and controls to protect information resources they are accessing.

1.5.10 Agencies must utilize the DOC's Wireless Access Point Checklist (see Section 7.3).

2.0 Purpose and Objectives

The purpose of this standard is to ensure that only registered and secure WLANs are deployed by state government agencies.

3.0 Definitions

3.1 Access Point (AP)
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 are needed to communicate or share resources.

3.2 Campus Connection
Any building with high-speed access (at least 10Mb) to the 501 building.

3.3 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 over a city-wide geographical area is commonly called a metropolitan area network (MAN). An interconnection of LANs over large geographical areas is commonly called a wide area network (WAN).

3.4 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.

3.5 Strong Password

A strong password must be a minimum of 8 characters, and possess 2 of the 3 following attributes.

- Must contain at least one (1) numeric,
- Must contain both upper and lowercase letters,
- Must contain special characters (!@#$%^&*{}).

3.6 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.

4.0 Applicability

This standard applies to state agencies, excluding higher education institutions, which deploy a Wireless Local Area Network (WLAN).

Wireless services that fall within the definition of Campus Connection, Metropolitan Area Network (MAN), or Wide Area Network (WAN) must be purchased through DAS Information Technology Services (ITS) to comply with state statutes.

4.1 Exemption

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

4.1.1 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, 521 S 14th Street, Suite 301, Lincoln, NE 68508). 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.

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 Agency must notify the DOC before implementing a wireless system. Self-registration is available through the ITS website (see Section 7.1). Wireless services that fall within the definition of Campus Connection, MAN or WAN, must be purchased through the ITS to comply with State statutes. The agency authority may delegate this responsibility but delegation does not remove the accountability.

5.2 DAS Information Technology Services Divisions (ITS)
ITS shares responsibility for the security of the state's network. ITS reserves the right to disable network access for a device, server or LAN if adequate security for a wireless connection is not in place.

6.0 Related Documents

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 DOC's Wireless Registration Website
http://wlansupport.ims.state.ne.us/wlan_form.html

7.2 ITS Website
http://its.ne.gov/

7.3 DOC's Wireless Access Approval Process
(LINK TO BE ADDED ~ NITC file URL of appendix)

7.4 DOC's Wireless Access Point Checklist
(LINK TO BE ADDED ~ NITC file URL of appendix)

7.5 NIST Wireless Network Security Special Publication 800-48
http://csrc.nist.gov/publications/nistpubs/index.html

7.6 ITS "Network Security Standards", Draft - February 11, 2003
http://its.ne.gov/

Wireless Access Point Approval Process

1. Review NITC wireless LAN security checklist.
2. Plan wireless installation according to NITC standards.
3. Fill out Wireless Registration Online Form. http://wlansupport.ims.state.ne.us/
4. DOC will verify the Agencies approval of the request.
4. Wait for installation approval from Network Services.
5. Purchase and install equipment
6. Notify Network Services of future replacement or removal of wireless equipment.

Nebraska Information Technology Commission

STANDARDS AND GUIDELINES

Wireless Local Area Network Checklist

The table, below, provides a WLAN security checklist. The table presents guidelines and recommendations for creating and maintaining a secure 802.11 wireless network, based on NIST Special Publication 800-48. Items marked 'REQUIRED" must be fulfilled in order to meet the specifications of this standard. Items marked as "Strongly Advise" might provide a higher level of security, but should be weighed against other considerations.

Management

Status	Tasks
REQUIRED	1. Develop an agency security policy that addresses the use of wireless technology, including 802.11.
REQUIRED	2. Maintain a complete inventory of all APs and 802.11 wireless devices.
REQUIRED	3. Ensure that wireless networks are not used until they comply with the agency's and the state's security policies.
Strongly Advise	4. Ensure that the client NIC and AP support firmware upgrade so that security patches may be deployed as they become available (prior to purchase).
Strongly Advise	5. Perform comprehensive security assessments at regular and random intervals (including validating that rogue APs do not exist in the 802.11 WLAN) to fully understand the wireless network security posture.
Strongly Advise	6. Ensure that external boundary protection is in place around the perimeter of the building or buildings of the agency.
Strongly Advise	7. Place APs in secured areas to prevent unauthorized physical access and user manipulation.
Strongly Advise	8. Complete a site survey to measure and establish the AP coverage for the agency.
Strongly Advise	9. Ensure that users on the network are fully trained in computer security awareness and the risks associated with wireless technology.
Strongly Advise	10. Perform a risk assessment to understand the value of the assets in the agency that need protection.
Strongly Advise	11. Locate APs on the interior of buildings instead of near exterior walls and windows as appropriate.
Optional	12. Deploy physical access controls to the building and other secure areas (e.g., photo ID, card badge readers).

Technical

Status	Tasks
REQUIRED	13. Change the default SSID in the APs
REQUIRED	14. Ensure that AP channels are at least five channels different from any other nearby wireless networks to prevent interference
REQUIRED	15. Disable all insecure and nonessential management protocols on the APs.
REQUIRED	16. Enable all security features of the WLAN product, including the cryptographic authentication and privacy feature.
REQUIRED	17. Ensure that encryption key sizes are at least 128-bits.
REQUIRED	18. Install antivirus software on all wireless clients.
REQUIRED	19. Ensure that all managed APs have strong administrative passwords.
REQUIRED	20. Enable user authentication mechanisms for the management interfaces of the AP.
Strongly Advise	21. Empirically test AP range boundaries to determine the precise extent of the wireless coverage.
Strongly Advise	22. Make sure that the reset function on APs is being used only when needed and is only invoked by an authorized group of people.
Strongly Advise	23. Restore the APs to the latest security settings when the reset functions are used.
Strongly Advise	24. Understand and make sure that all default parameters are changed.
Strongly Advise	25. Make sure that shared keys are periodically replaced by more secure unique keys.
Strongly Advise	26. Install a properly configured firewall between the wired infrastructure and the wireless network (AP or hub to APs).
Strongly Advise	27. Install personal firewall software on all wireless clients.
Strongly Advise	28. Deploy MAC access control lists.
Strongly Advise	29. Consider installation of Layer 2 switches in lieu of hubs for AP connectivity.
Strongly Advise	30. Deploy IPsec-based Virtual Private Network (VPN) technology for wireless communications.
Strongly Advise	31. Ensure that encryption being used is sufficient given the sensitivity of the data on the network and the processor speeds of the computers.
Strongly Advise	32. Fully test and deploy software patches and upgrades on a regular basis.
Strongly Advise	33. Ensure that all passwords are being changed regularly.
Strongly Advise	34. Ensure that the “ad hoc mode” for 802.11 has been disabled unless the environment is such that the risk is tolerable. Note: some products do not allow disabling this feature; use with caution or use different vendor.
Strongly Advise	35. Ensure that management traffic destined for APs is on a dedicated wired subnet.
Strongly Advise	36. Use SNMPv3 and/or SSL/TLS for Web-based management of APs.
Optional	37. Make sure that APs are turned off during when they are not used (e.g., after hours and on weekends).
Optional	38. Disable the broadcast SSID feature so that the client SSID must match that of the AP.
Optional	39. Validate that the SSID character string does not reflect the agency’s name (division, department, street, etc.) or products.
Optional	40. Disable file sharing on wireless clients (especially in untrusted environments).
Optional	41. Deploy user authentication such as biometrics, smart cards, two-factor authentication, and PKI.

Optional	42. Use static IP addressing on the network
Optional	43. Disable DHCP.

Operational

Status	Tasks
REQUIRED	44. When disposing access points that will no longer be used by the agency, clear access point configuration to prevent disclosure of network configuration, keys, passwords, etc.
Strongly Advise	45. Configure SNMP settings on APs for least privilege (i.e., read only). Disable SNMP if it is not used. SNMPv1 and SNMPv2 are not recommended.
Strongly Advise	46. Enhance AP management traffic security by using SNMPv3 or equivalent cryptographically protected protocol.
Strongly Advise	47. Consider other forms of authentication for the wireless network such as RADIUS and Kerberos.
Strongly Advise	48. Deploy intrusion detection agents on the wireless part of the network to detect suspicious behavior or unauthorized access and activity.
Strongly Advise	49. Deploy auditing technology to analyze the records produced by RADIUS for suspicious activity.
Strongly Advise	50. Fully understand the impacts of deploying any security feature or product prior to deployment.
Strongly Advise	51. Designate an individual to track the progress of 802.11 security products and standards (IETF, IEEE, etc.) and the threats and vulnerabilities with the technology.
Strongly Advise	52. If the access point supports logging, turn it on and review the logs on a regular basis.
Optional	53. Use a local serial port interface for AP configuration to minimize the exposure of sensitive management information.
Optional	54. Deploy an 802.11 security product that offers other security features such as enhanced cryptographic protection or user authorization features.
Optional	55. Enable utilization of key-mapping keys (802.1X) rather than default keys so that sessions use distinct keys.
Optional	56. Wait until future releases of 802.11 WLAN technologies incorporate fixes to the security features or provide enhanced security features.

Technical Panel
of the
Nebraska Information Technology Commission

Draft Document
30-Day Comment Period

Title: Information Technology Disaster Recovery Plan 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 May 22, 2006.
4. The Technical Panel will consider this standard and the comments received at their meeting currently scheduled for June 13, 2006. Final approval of the standard would be considered by NITC at their next meeting following the Technical Panel review. Information about these meetings will be posted on the NITC web site at http://www.nitc.state.ne.us/.

Nebraska Information Technology Commission

STANDARDS AND GUIDELINES

Information Technology Disaster Recovery Plan Standard

Category	**Security Architecture**
Title	**Information Technology Disaster Recovery Plan 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 of _____.
Guideline - Adherence is voluntary.

Status

☐ **Adopted** ☐ **Draft** ☑ **Other: Review**

Dates

Date: April 17, 2006
Date Adopted by Nebraska Information Technology Commission: April 23, 2001
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

Each agency must have an Information Technology Disaster Recovery Plan that supports the resumption and continuity of computer systems and services in the event of a disaster. The plan will cover processes, procedures, and provide contingencies to restore operations of critical systems and services as prioritized by each agency. The Disaster Recovery Plan for Information Technology may be a subset of a comprehensive Agency Business Resumption Plan which should include catastrophic situations and long-term disruptions to agency operations.

The Information Technology Disaster Recovery Plan should be effective, yet commensurate with the risks involved for each agency. The following elements, at a minimum, must be included:

- Identification of critical computer systems and services to the agency's mission and business functions.
- Critical systems and services preservation processes and offsite storage strategy and methods to protect storage media.
- Documented dependencies upon other State agency's or entities that support critical systems and services.
- Contingency plans for different types of disruptions to critical systems and services, i.e. hardware failure, etc.
- Information technology responsibilities for implementation and disaster management.
- Procedures for reporting events, as well as escalating an event within an agency.
- Identification of copy distribution and multiple site storage of plan documents.
- Multi-year training, exercising, and improvement plans.
- Annual plan review, revision, and approval process.

2.0 Purpose and Objectives

The purpose of this document is to define, clarify, and standardize Information Technology Disaster Recovery Planning of State government agencies.

2.1 Background

Information Technology Disaster Recovery Plans are based on the following premises:

2.1.1 *Information is an asset.* It has value to the organization and needs to be suitably protected.

2.1.2 *Information resources must be available when needed.* Continuity of information resources and supporting critical systems and services must be ensured in the event of a disruption to business or a disaster.

2.1.3 *Risks to information resources must be managed.* Procedures required to ensure critical systems and services can be recovered and business continuity sustained must be cost effective and commensurate with the value of the assets being protected.

2.2 Objectives

The primary objectives of this Standard are:

2.2.1 To communicate responsibilities for the continuity of government operations;

2.2.2 To establish a plan for restoration of operations following a disaster.

2.2.3 To reduce the risk of loss of state information assets.

2.2.4 To provide a process for the recovery of critical systems and services.

3.0 Definitions

3.1 Agency

Any governmental entity, including state government, local government, or third party entities under contract to the agency.

3.2 Agency Business Resumption Plan

Documents how an agency will continue to function during a disaster.

Note: Items found in an Agency Business Resumption Plan may include, but is not limited to:

- *Business impact analysis, including risk assessment, asset classification, and potential disruption to stakeholders.*
- *Mitigation strategies and safeguards to avoid disasters. Safeguards include, but are not limited to, protective measures such as redundancy, fire suppression, power source protection, and environmental issues.*

3.3 Critical Systems and Services
Those systems, system components (hardware, data, or software), or services that if lost or compromised would jeopardize an agency's ability to continue agency operations.

3.4 Disaster
Any event that threatens or causes the destruction or availability of critical systems and services.

4.0 Applicability

This standard applies to all state government agencies, except Higher Education and those agencies receiving an exemption under Section 4.1. Compliance with Nebraska Information Technology Commission (NITC) standards will be a requirement during consideration of funding for any projects requiring review by the NITC and may be used in audit reviews or budget reviews.

4.1 Exception

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

4.1.1 Exception 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, 521 S 14th Street, Suite 301, Lincoln, NE 68508). 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.

5.0 Responsibility

5.1 NITC

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

5.2 Agency and Institutional Heads

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

6.0 Related Documents

6.1 Agency IT Disaster Recovery Plan Standard Content

6.2 Information Security Management Policy

http://www.nitc.state.ne.us/tp/workgroups/security/policies/security_policy.pdf

6.3 Security Breaches and Incident Reporting Policy

http://www.nitc.state.ne.us/tp/workgroups/security/policies/incident_reporting_policy.pdf

Nebraska Information Technology Commission

Project Proposal Form

New or Additional State Funding Requests
for Information Technology Projects

FY2005-07 Biennium
(2006 Deficit Budget Requests)

Project Title	
Agency/Entity	

About this form…
The Nebraska Information Technology Commission ("NITC") is required by statute to "make recommendations on technology investments to the Governor and the Legislature, including a prioritized list of projects, reviewed by the technical panel, for which new or additional funding is requested." In order to perform this review, the NITC and DAS-Budget Division require agencies/entities to complete this form when requesting new or additional funding for technology projects. For more information, see the document entitled "Guidance on Information Technology Related Budget Requests" available at http://www.nitc.state.ne.us/forms/.

Electronic versions of this form are available at http://www.nitc.state.ne.us/forms/.

For questions or comments about this form, contact the Office of the CIO/NITC at:

Mail: Office of the CIO/NITC
521 S 14th Street, Suite 301
Lincoln, NE 68508
Phone: (402) 471-3560
Fax: (402) 471-4608
E-mail: info@cio.state.ne.us

Submission of Form
Completed forms must be submitted by the same date budget requests are required to be submitted to the DAS Budget Division. Completed project proposal forms must be submitted via e-mail to info@cio.state.ne.us. The project proposal form should be submitted as an attachment in one of these formats: Microsoft Word; WordPerfect; Adobe PDF; or Rich Text Format. Receipt of the form by the Office of the CIO will be confirmed by e-mail. If an agency is unable to submit the application as described, contact the Office of the CIO prior to the deadline, to make other arrangements for submitting a project proposal form.

Section I: General Information

Project Title	
Agency (or entity)	

Contact Information for this Project:

Name	
Address	
City, State, Zip	
Telephone	
E-mail Address	

Section II: Executive Summary

Provide a one or two paragraph summary of the proposed project. This summary will be used in other externally distributed documents and should therefore clearly and succinctly describe the project and the information technology required.

Section III: Goals, Objectives, and Projected Outcomes (15 Points)

1. Describe the project, including:
   - Specific goals and objectives;
   - Expected beneficiaries of the project; and
   - Expected outcomes.

2. Describe the measurement and assessment methods that will verify that the project outcomes have been achieved.

3. Describe the project's relationship to your agency comprehensive information technology plan.

Section IV: Project Justification / Business Case (25 Points)

4. Provide the project justification in terms of tangible benefits (i.e. economic return on investment) and/or intangible benefits (e.g. additional services for customers).

5. Describe other solutions that were evaluated, including their strengths and weaknesses, and why they were rejected. Explain the implications of doing nothing and why this option is not acceptable.

6. If the project is the result of a state or federal mandate, please specify the mandate being addressed.

Section V: Technical Impact (20 Points)

7. Describe how the project enhances, changes or replaces present technology systems, or implements a new technology system. Describe the technical elements of the project, including hardware, software, and communications requirements. Describe the strengths and weaknesses of the proposed solution.

8. Address the following issues with respect to the proposed technology:
   - Describe the reliability, security and scalability (future needs for growth or adaptation) of the technology.
   - Address conformity with applicable NITC technical standards and guidelines (available at http://www.nitc.state.ne.us/standards/) and generally accepted industry standards.
   - Address the compatibility with existing institutional and/or statewide infrastructure.

Section VI: Preliminary Plan for Implementation (10 Points)

9. Describe the preliminary plans for implementing the project. Identify project sponsor(s) and examine stakeholder acceptance. Describe the project team, including their roles, responsibilities, and experience.

10. List the major milestones and/or deliverables and provide a timeline for completing each.

11. Describe the training and staff development requirements.

12. Describe the ongoing support requirements.

Section VII: Risk Assessment (10 Points)

13. Describe possible barriers and risks related to the project and the relative importance of each.

14. Identify strategies which have been developed to minimize risks.

Section VIII: Financial Analysis and Budget (20 Points)

15. Financial Information

Financial and budget information can be provided in either of the following ways:

(1) If the information is available in some other format, either cut and paste the information into this document or transmit the information with this form; or

(2) Provide the information by completing the spreadsheet provided below.

Instructions: Double click on the Microsoft Excel icon below. An imbedded Excel spreadsheet will be launched. Input the appropriate financial information. Close the spreadsheet. The information you entered will automatically be saved with this document. If you want to review or revise the financial information, repeat the process just described.

Excel Spreadsheet
(Double-click)

16. Provide a detailed description of the budget items listed above. Include:
    - An itemized list of hardware and software.
    - If new FTE positions are included in the request, please provide a breakdown by position, including separate totals for salary and fringe benefits.
    - Provide any on-going operation and replacement costs not included above, including funding source if known.
    - Provide a breakdown of all non-state funding sources and funds provided per source.

17. Please indicate where the funding requested for this project can be found in the agency budget request, including program numbers.

Nebraska Information Technology Commission
Project Proposal Form
Section VIII: Financial Analysis and Budget

(Revise dates as necessary for your request.)

	Estimated Prior Expended	Request for FY2005-06 (Year 1)	Request for FY2006-07 (Year 2)	Request for FY2007-08 (Year 3)	Request for FY2008-09 (Year 4)	Future	Total
1. Personnel Costs							$ -
2. Contractual Services							
2.1 Design							$ -
2.2 Programming							$ -
2.3 Project Management							$ -
2.4 Other							$ -
3. Supplies and Materials							$ -
4. Telecommunications							$ -
5. Training							$ -
6. Travel							$ -
7. Other Operating Costs							$ -
8. Capital Expenditures							
8.1 Hardware							$ -
8.2 Software							$ -
8.3 Network							$ -
8.4 Other							$ -
TOTAL COSTS	$ -	$ -	$ -	$ -	$ -	$ -	$ -
General Funds							$ -
Cash Funds							$ -
Federal Funds							$ -
Revolving Funds							$ -
Other Funds							$ -
TOTAL FUNDS	$ -	$ -	$ -	$ -	$ -	$ -	$ -

Nebraska Information Technology Commission

Guidance on Information Technology Related Budget Requests
Project Proposal Form Requirements

Issue:

Does an information technology project in your agency's budget request require the completion of a Project Proposal Form?

Background:

The Nebraska Information Technology Commission ("NITC") is required by statute to "make recommendations on technology investments to the Governor and the Legislature, including a prioritized list of projects, reviewed by the technical panel, for which new or additional funding is requested." Neb. Rev. Stat. §86-516(8)

The NITC developed the Project Proposal Form to aid in the review and prioritization of information technology funding requests. The Statewide Technology Plan provides that "[a]ll state agencies and public higher education institutions requesting state appropriations for information technology must prepare a project proposal for each information technology project."

Some, but not all, information technology budget requests will require the completion of the Project Proposal Form. This document is intended to provide guidance on which projects require completion of this form.

Definitions:

Information technology is defined as "computing and telecommunications systems, their supporting infrastructure, and interconnectivity used to acquire, transport, process, analyze, store, and disseminate information electronically." Neb. Rev. Stat. § 86-507. Supporting infrastructure includes both the physical infrastructure such as computers or networks and non-physical components such as personnel, training, customer support, and software.

A **significant project**, for the purposes of this document, means a project which: 1) costs more than $250,000; OR 2) costs more than $25,000 AND has a major effect on a core business function OR has an impact that affects multiple agencies. This definition does not include on-going operational costs of information technology such as replacement of computers, operating system upgrades, routine data processing costs, existing support personnel, or application maintenance.

Guidance:

A Project Proposal Form is required for all significant information technology projects. Review the definitions above and complete the Worksheet on the following page to determine if your project requires a Project Proposal Form.

ALL requests for funding, whether or not a Project Proposal Form is completed, must still be provided for in the standard agency budget requests submitted to the DAS Budget Division.

Agencies should contact their budget analyst with any questions about whether specific projects require the completion of a Project Proposal Form. The Budget Division will consult with the Office of the CIO / NITC on these questions.

References:

Nebraska Information Technology Commission - http://www.nitc.state.ne.us/
Project Proposal Form - http://www.nitc.state.ne.us/forms/
Statewide Technology Plan - http://www.nitc.state.ne.us/stp/
DAS Budget Division - http://www.budget.state.ne.us/

WORKSHEET

1. Is this an information technology related funding request? YES or NO

   If YES, continue.
   If NO, STOP. A project proposal form is not required.

2. Is the funding request for on-going operational costs such as replacement of computers, operating system upgrades, routine data processing costs, existing support personnel, or application maintenance? YES or NO

   If YES, STOP. A project proposal form is not required.
   If NO, continue.

3. Is the cost of the project more than $250,000? YES or NO

   If YES, STOP. A PROJECT PROPOSAL FORM NEEDS TO BE COMPLETED.
   If NO, continue.

4. Is the cost of the project more than $25,000? YES or NO

   If YES, continue.
   If NO, STOP. A project proposal form is not required.

5. Does the project have a major effect on a core business function? YES or NO

   - OR -

6. Does the project have an impact that affects multiple agencies? YES or NO

   If you answered YES to either question 5 or 6, A PROJECT PROPOSAL FORM NEEDS TO BE COMPLETED.
   If you answered NO to both questions 5 and 6, a project proposal form is not required.

DRAFT

N I D C A C

Resolution
Creating the Nebraska Computing and Telecommunications Security Committee
May 19, 2006

Whereas Section 86-542 (2), R.S.N., 1943, authorizes the Nebraska Intergovernmental Data Communications Advisory Council (NIDCAC) to "study and make recommendations concerning the data processing and communications needs of the state and its political subdivisions," and

Whereas Computing, telecommunications, and network equipment have been installed in public buildings throughout the state, and

Whereas Unauthorized access to these computing and telecommunications facilities may result in disruption of state and local government services, and

Whereas The Committee has determined that securing these facilities, both physically and electronically, is necessary to protect state and local computing and telecommunications systems from inadvertent or surreptitious access, and

Whereas Section 86-545, R.S.N., 1943, grants the council "the power to appoint representatives of state agencies and governmental subdivisions which are affected by a proposed project to serve as developmental subcommittees of the council on the development of the proposed project,"

Now, Therefore be it resolved:

Section 1. That a Computing and Telecommunications Security Committee be created as a subcommittee of NIDCAC pursuant to Section 86-545, R.S.N., 1943.

Section 2. That the Committee shall undertake the following tasks:

a) Evaluate existing security practices including physical and electronic access to computing and telecommunications equipment,
b) Identify risks, problems and constraints of current security practices,
c) Review the current level of security technology available to local governments throughout the state,
d) Evaluate opportunities to better protect state and local computing and telecommunications resources,
e) Evaluate requirements necessary to achieve a secured computing and telecommunications infrastructure,
f) Investigate specific measures that ensure secure access to computing, network, and telecommunication systems,
g) Identify key technologies that can be made available to local governments to allow these agencies to secure their computing resources,
h) Document the requirements for secured computing and telecommunications infrastructure,
i) Prepare and publish the committee's findings including recommendations for best practices to ensure the security of the state and local computing resources, and
j) Coordinate with the Technology Council of the NITC to establish recommended security practices.

Section 3. That NIDCAC invite the Technical Panel of the NITC to participate as a joint sponsor of this resolution.

Section 4. The Chair of NIDCAC shall invite representatives of agencies enumerated, below, to participate on the committee. Those who accept shall constitute the membership of the Committee. The Committee may expand its membership by inviting additional representatives of other organizations to join the study as voting or non-voting members. The Committee may establish planning groups to undertake specific tasks of the study. Invitations to participate on the Steering Committee shall include, but be not limited to:

Representatives of any county, city, or other political subdivision
Local law enforcement or other local agencies that perform building security
Local political subdivisions with a data processing center
Office of the Nebraska Chief Information Officer
Nebraska State Building Division
Technical Panel of the NITC

Section 5. The authority for the Committee and its working groups shall exist beginning from the date of passage of this Resolution, and shall continue until January 1, 2007 or until such time as the Committee has completed its tasks, except that NIDCAC may abolish or extend the Committee.

Section 6. The Chair of NIDCAC shall provide or arrange such planning, facilitation, administration, and financial support as is necessary and available to support the work of the Committee.