

MEETING AGENDA

NEBRASKA INFORMATION TECHNOLOGY COMMISSION

Tuesday, September 18, 2007, 9:00 a.m.
State Capitol, Room 1524
14th & K Streets
Lincoln, Nebraska

AGENDA

Meeting Documents:
Click the links in the agenda
or [click here](#) for all documents (78 Pages, 670 KB)

9:00 a.m.	Call to Order, Roll Call, Notice of Meeting, & Open Meetings Act Information Approval of June 27, 2007 Minutes * Public Comment
9:05 a.m.	Office of the CIO Project Updates <ul style="list-style-type: none">• LB 1208 Implementation• Public Safety Wireless Update• Microsoft Exchange Conversion Informational Updates <ul style="list-style-type: none">• NITC Joint Briefing, November 9, 2007• Statewide Technology Plan Revision• Office of the CIO Roadmap
9:30 a.m.	Reports from the Councils and Technical Panel <ul style="list-style-type: none">A. Community Council Report<ul style="list-style-type: none">• Community Council Charter*• Podcasting Across Nebraska Update<ul style="list-style-type: none">◦ WebsiteB. eHealth Council Report<ul style="list-style-type: none">• HISPC Final Report (Summary Complete Report)• eHealth Council Work Group-HISPC ContinuationC. Education Council ReportD. State Government Council ReportE. Technical Panel Report

	<ul style="list-style-type: none"> • Standards & Guidelines <ul style="list-style-type: none"> ○ Information Security Policy* ○ Data Security Standard* ○ Password Standard* ○ Email Policy for State Government Agencies* • Project Review Reports <ul style="list-style-type: none"> ○ Retirement Systems ○ Health and Human Services - Medicaid Management Information System (MMIS) ○ Health and Human Services - Laboratory Information Management System (LIMS) ○ Nebraska State College System -Student Information Administrative System ○ University of Nebraska - Student Information System
11:00 a.m.	Other Business
11:15 a.m.	Adjournment

* Indicates action items.

(The Nebraska Information Technology Commission 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.)

The meeting notice and agenda were posted to the NITC website and the [Public Meeting Calendar website](#) on September 12, 2007.

MEETING MINUTES

NEBRASKA INFORMATION TECHNOLOGY COMMISSION

Wednesday, June 27, 2007, 9:30 a.m.

University of Nebraska-Kearney

Nebraskan Student Union-Chancellor's Dining Room

1013 West 27th Street , Kearney, Nebraska

PROPOSED MINUTES

MEMBERS PRESENT:

Lieutenant Governor Rick Sheehy, Chair

Linda Aerni, Chief Executive Officer, Community Internet Systems

Pat Flanagan, Information Services Manager, Mutual of Omaha

Lance Hedquist, City Administrator, South Sioux City

Dr. Dan Hoelsing, Superintendent, Laurel-Concord, Coleridge, & Newcastle Public Schools

Mike Huggenberger, Director-Netlink, Great Plains Communications

Dr. Doug Kristensen, Chancellor, University of Nebraska-Kearney

Dr. Janie Park, President, Chadron State College

Trev Peterson, Attorney, Knudsen, Berkheimer, Richardson, and Endacott, LLP

CALL TO ORDER, ROLL CALL, NOTICE OF MEETING, & OPEN MEETINGS ACT INFORMATION

Lieutenant Governor Sheehy called the meeting to order at 9:35 a.m. There was a full quorum present to conduct official business.

Lieutenant Governor stated that the meeting notice and agenda were posted to the NITC website and the [Public Meeting Calendar website](#) on June 21, 2007. As required by statute, a copy of the Nebraska Open Meetings Act was available at the end of the meeting table.

Commissioner Kristensen welcomed the Commissioners and guests to the University of Nebraska-Kearney campus.

APPROVAL OF FEBRUARY 22, 2007 MINUTES

Commissioner Kristensen moved to approve the [February 22, 2007 minutes](#) as presented. Commissioner Hequist seconded. Roll call vote: Sheehy-Yes, Aerni-Yes, Flanagan-Yes, Hedquist-Yes, Hoelsing-Yes, Huggenberger-Yes, Kristensen-Yes, Park-Yes, and Peterson-Yes. Results: Yes-9, No-0. Motion carried.

PUBLIC COMMENT

There was no public comment.

INFORMATIONAL UPDATES

LB 1208 Implementation - Network Nebraska, Brenda Decker

The Northeast schools connections bids were closed. The bid did not come in as low as anticipated. Imperial schools may have to pay more than the other schools.

Most all schools will pay approximately \$1,500 a month. An RFR for the video equipment has been released. Most of the Northeast Nebraska schools have opted not to buy off the state contract. They are not required to buy off the contract. Installation is scheduled to start July 2nd. Over 90 sites will need to be installed and operational before the school session begins in August. More detailed information on LB 1208 is available on the Network Nebraska website.

One of the issues of discussion has been what to and who is responsible when there is a problem with the network. There are several entities involved such as the Educational Service Units, the schools, the State of Nebraska, service providers, etc. One option that is being discussed is a statewide ticket system.

A RFP for the Phase 2 of LB 1208 will be released in August. Phase 2 will connect schools in the 308 area code. The Office of the CIO will need letters of intent from each school district in order to bid on their behalf. The project is preparing for discussions regarding pricing advantages that could be given back to the Northeast Nebraska school districts.

In addition to the RFP's for LB 1208, the RFP for the Network Nebraska backbone network will go out to bid soon. The State is attempting to aggregate demand. Commissioner Hoelsing commented that the Northeast Nebraska school districts have been in discussions with the Public Service Commission regarding their concerns with the QWEST bid, as well as providing assistance to the schools. The local telephone companies affected the cost. The Northeast school districts have also been meeting with the telephone companies. Schools with Quest service will pay \$1,500 month with other school districts with a different provider pay up to \$2,800/month. Postalization rates for all schools would be beneficial. The LB 1208 incentives to the schools won't be available until 2 more years.

Lieutenant Governor Sheehy commented that these issues should be addressed by the Distance Education Council.

Public Safety Wireless Update, Brenda Decker: The Legislature funded a Public Safety Wireless System for the State of Nebraska. This effort will occur over the next 8 years and will be headed by the Office of the CIO and the NITC. The Office of the CIO received funding to build the infrastructure. The Office of the CIO will be working with NEMA, law enforcement, Games & Parks, and local government. There are Homeland Security federal grant funds available to states for local governments. This will help assure that local government efforts coincide with federal homeland security efforts. There are 10 regions in the State of Nebraska. Regions are counties that collaborate to share standards protocol, resources, etc. Anything purchased from these monies would be used by the State so that regions will be able to connect with each other within the State as well as with other states. The goal is to have interconnectivity and interoperability with the State's network. The first meeting held was with the Omaha Public Power District (OPPD) who already has a system in place. A meeting with the Nebraska Public Power District (NPPD) is being planned. NPPD is getting a new system. OPPD and NPPD would become one region. An RFI will be released in August. The Office of the CIO will provide the NITC with regular updates.

2007 Annual Information Technology Services Report. The report will be completed by June 30th. Commissioners will be sent a copy.

2007 Statewide Technology Plan. The plan was approved at the last NITC meeting

and has been posted to the NITC website.

UPDATE: RECOMMENDATIONS ON TECHNOLOGY INVESTMENTS FOR THE FY2007-2009 BIENNIUM

Rick Becker, Government I.T. Manager

Commissioners were given a chart with an updated funding status for the I.T. projects reviewed by the NITC for the FY2007-2009 Biennium.

REPORT - COMMUNITY COUNCIL REPORT

Anne Byers, Community Information Technology Manager

Membership: At the February meeting, the NITC established an eHealth Council. Several of the Community Council members represented telehealth. The Community Council Chair recommended asking these members decide if they want to continue serving on the Community Council as well. They all felt that the eHealth Council better served their interest. At the May 18th Community Council meeting, membership was on the agenda as an action item. After much discussion, it was decided that the Community Council include a Work Force Development sector in their membership. A nomination committee was established. With the approval of the NITC, the council is recommending the following slate of nominees to serve as members of the Community Council:

- Mitch Arnold, Preferred Partners, LLC.
- Jason Barelman, Wayne State College
- Dean Folkers, Department of Education
- Darla Heggem, Twin Cities Development, Scottsbluff-Gering
- Bethanne Kunz , Valley County Economic Development
- Joan Modrell, Department of Labor
- Caleb T. Pollard, Nebraska Department of Economic Development
- Angie Ramaekers, Columbus Area Chamber of Commerce
- Rivkah Sass, Omaha Public Library
- Dan Shundoff, Intellicom, Kearney

Commissioner Flanagan moved to approve the [membership](#) nominations of new Community Council members as presented. Commissioner Park seconded. Roll call vote: Sheehy-Yes, Peterson-Yes, Park-Yes, Kristensen-Yes, Huggenberger-Yes, Hoelsing-Yes, Hedquist-Yes, Flanagan-Yes, and Aerni-Yes. Results: Yes-9, No-0. Motion carried.

Commissioner Flanagan stated that he would like to see the Community Council to continue the work force development effort in order to keep I.T. graduates here in Nebraska.

Update: Podcasting Across Nebraska: Participating communities in the Podcasting Across Nebraska project are developing podcasts. South Sioux City and the North Platte/Lincoln County Convention and Visitors Bureau have each developed several podcasts. Central City and Fulterton will become part of the Hiway 14 Association Podcast. The association plans to do podcasts on the Santee and Ponca tribes as well. The Panhandle Public Health District plans to do podcasts on the West Nile, nutrition, and the hazards of underage drinking. They have a student who is a filmmaker assisting with the podcasts.

REPORT - EHEALTH COUNCIL REPORT

Anne Byers, Community Information Technology Manager

Charter: The eHealth Council held their first organizational meeting on May 21st. Lieutenant Governor Sheehy presided over the first part. The following Co-chairs were appointed: Kimberly Galt, Keith Mueller, and Dan Greiss. The council charter was discussed at the meeting. The eHealth Council is recommending staggered terms for voting members only. The eHealth Council is recommending the Council Charter to the NITC for final approval.

Discussion occurred regarding the elected officials term. The Commissioners recommended that Ms. Byers draft language regarding the elected officials as ex-officio non-voting members.

Commission Hedquist moved to approve the eHealth [Charter](#) as submitted with an amendment that the elected officials serve as ex-officio members and be appointed annually by the NITC. Commissioner Aerni seconded. Roll call vote: Aerni-Yes, Flanagan-Yes, Hedquist-Yes, Hoelsing-Yes, Huggenberger-Yes, Kristensen-Yes, Park-Yes, Peterson-Yes, and Sheehy-Yes. Results: Yes-9, No-0. Motion carried.

Membership: Bios that were submitted late were distributed to the Commissioners. Ms. Byers stated that the membership slate is well balanced and represented. There was good attendance at the first meeting. With the approval of the NITC, the council is recommending the following slate of nominees to serve as members on the eHealth Council:

State of Nebraska/Federal Government representatives:

- Steve Henderson, Office of the CIO
- Senator Mick Mines, Nebraska Legislature
- Dennis Berens, HHSS, Office of Rural Health
- Congressman Jeff Fortenberry, represented by Marie Woodhead

Health Care Providers:

- Daniel Griess, Box Butte General Hospital, Alliance
- Dr. Delane Wycoff, Pathology Services, PC
- Dr. Harris A. Frankel (alternate)
- Joni Cover, Nebraska Pharmacists Association
- September Stone, Nebraska Health Care Association
- Bill Bivin, Nebraska Health Care Association (alternate)
- John Roberts, Nebraska Rural Health Association

eHealth Initiatives representatives:

- Donna Hammack, Nebraska Statewide Telehealth Network and St. Elizabeth Foundation
- Ken Lawonn, NeHII and Alegent Health
- Harold Krueger, Western Nebraska Health Information Exchange and Chadron Community Hospital
- C.J. Johnson, Southeast Nebraska Behavioral Health Information Network and Region V Systems

Public Health representatives:

- David Lawton, HHSS, Public Health Assurance
- Jeff Kuhr, Three Rivers Public Health Department, Fremont
- Rita Parris, Public Health Association of Nebraska, alternate
- Kay Oestmann, Southeast District Health Department
- Shirleen Smith, West Central District Health Department, North Platte, alternate
- Dr. Keith Mueller, UNMC College of Public Health

Payers and Employers:

- Steve Grandfield or Susan Courtney, Blue Cross Blue Shield
- Ron Hoffman, Jr., Mutual of Omaha
- Mary Steiner, HHSS Finance and Support, Medicaid

Consumers:

- Nancy Shank, Public Policy Center
- Alice Henneman, University of Nebraska-Lincoln Extension in Lancaster County
- Jim Krieger, Gallup

Resource Providers, Experts, and Others:

- Henry Zach, HDC 4Point Dynamics
- Marsha Morien, Center for Biosecurity (alternate for Henry Zach)
- Kimberly Galt, Creighton University School of Pharmacy and Health Professions

Commissioner Peterson moved to approve the eHealth [membership](#) nominations with the amendment that the elected officials serve as ex-officio members. Commissioner Park seconded. Roll call vote: Huggenberger-Yes, Hoelsing-Yes, Hedquist-Yes, Flanagan-Yes, Aerni-Yes, Sheehy-Yes, Peterson-Yes, Park-Yes, and Kristensen-Yes. Results: Yes-9, No-0. Motion carried.

Commissioner Flanagan informed the Commissioners that Mutual of Omaha will be exiting the eHealth Council after a year because his office will not be underwriting. The member on the list will serve on the council for a year and will propose a replacement.

[eHealth Clearinghouse](#): The clearinghouse is available from the NITC website. It is hoped that the council members will share information about eHealth initiatives in the state, as well as nationally.

REPORT - EDUCATION COUNCIL REPORT

Terry Haack, Chair

The Education Council has met twice since your last meeting on February 22nd. Agenda items and topics of discussion included the following:

- Two portfolio management systems were presented – one used by the University of Nebraska Computing Services Network under the direction of Walter Weir and a Project management software used by the State CIO's office

to plan and monitor large enterprise I.T. projects.

- Renovo Software provided a presentation on the statewide videoconferencing clearinghouse and scheduling system that was awarded by the State to Qwest/Renovo
- Omaha Public Schools provided a presentation about their credit recovery program and the use of Angel software to deliver learning objects that originated from the National Repository of Online Courses (NROC). The Education Council is appreciative that the NITC Technical Panel has chartered a work group to research and recommend standards for the deployment of content and course management systems across the State.
- LB 1208 discussions and updates. K-12 and higher education entities appreciate the work of the CIO's and University's office to manage and help oversee the LB 1208 network upgrade.

Membership: The council would like to recommend the following slate of nominees for the 2007-09 membership renewals/replacements expiring June 30, 2007 for the higher education sector:

- Yvette Holly, UN System
- Chuck Lenosky, Independent Colleges & Universities
- Mike Chipps, Community College System
- Stan Carpenter, State College System

The council would like to recommend the following slate of nominees for the 2007-09 membership renewals/replacements expiring June 30, 2007 for the K-12 sector:

- Bob Uhing, Educational Service Units DEC
- Craig Pease, Administrators
- Art Tanderup, Public Teachers
- Joe LeDuc, Nonpublic Teachers

Commissioner Park moved to approve the Education Council [membership](#) nominations. Commissioner Kristensen seconded. Roll call vote: Hoelsing-Yes, Huggenberger-Yes, Hedquist-Yes, Kristensen-Yes, Flanagan-Yes, Park-Yes, Aerni-Yes, Peterson-Yes, and Sheehy-Yes. Results: Yes-9, No-0. Motion carried.

The Nebraska Information Technology Commission Education Council would like to recognize Dr. Jack Huck, Mr. Rich Molettiere, and Mr. Ed Rastovski for their many years of distinguished service to the Education Council, in the interest of advising the Commission on matters of education technology initiatives, funding, and policy.

LEGISLATIVE PERFORMANCE AUDIT

[Note: This agenda item may require the Commission to hold a closed session (Neb. Rev. Stat. § 84-1410).]

Don Arp and Angie McClelland of the Legislative Council arrived to the meeting to discuss the Performance Audit with the Commissioners. This agenda item was moved up in the agenda.

Commissioner Hedquist moved that the NITC go into closed session to discuss matters relating to the draft performance audit report prepared by the

Performance Audit Section of the Nebraska Legislative Council. Closed session is necessary because, by statute [Neb. Rev. Stat. § 50-1210], the contents of the draft report may not be released to anyone outside the agency. Commissioner Flanagan seconded. Roll call vote: Kristensen-Yes, Hoelsing-Yes, Park-Yes, Hedquist-Yes, Peterson-Yes, Flanagan-Yes, Sheehy-Yes, Aerni-Yes, and Huggenberger-Yes. Results: Yes-9, No-0. Motion carried.

The Commission went into closed session at 11:07 a.m.

The Commission came out of the closed session at 11:43 a.m.

Commissioner Hedquist moved to accept the draft Legislative Performance Audit Report and that the NITC will work with the Committee's recommendation. Commissioner Park seconded. Commissioner Kristensen offered a friendly amendment that the Commission authorizes the Lieutenant Governor to respond to the Committee's recommendations on behalf of the Commission. Commissioners Hedquist and Park accepted the amendment. Roll call vote: Aerni-Yes, Flanagan-Yes, Hedquist-Yes, Hoelsing-Yes, Huggenberger-Yes, Kristensen-Yes, Park-Yes, Peterson-Yes, and Sheehy-Yes. Results: Yes-9, No-0. Motion carried.

REPORT - STATE GOVERNMENT COUNCIL REPORT

Rick Becker, State Government I.T. Manager

The Council has recommended amending Section 6.2.2.10 of their charter to read as follows:

"Two (2) representatives from the general public with extensive IT experience, to be appointed by the Commission."

Commissioner Kristensen moved to approve the State Government [Charter Amendment](#). Commissioner Peterson seconded. Roll call vote: Hedquist-Yes, Park-Yes, Peterson-Yes, Flanagan-Yes, Kristensen-Yes, Hoelsing-Yes, Huggenberger-Yes, Sheehy-Yes, and Aerni-Yes. Results: Yes-9, No-0. Motion carried.

Cyber Security Conference, Steve Henderson. The conference was held on April 18th with approximately 130 participants. There are other state organizations interested in co-sponsoring next year's conference. Lieutenant Governor Sheehy stated that Mr. Henderson has been assisting with the agency directors discussions regarding disaster recovery and business resumption and would like to include cyber security in these discussions.

Email, Brenda Decker. The State Government Council has implemented and support the shared services concept. Email has been an item of discussion. Currently, there are 13 email systems in Nebraska state government. A couple of years ago, the NITC approved a business email system and a basic email system. One of Governor Heineman's goals is to implement one email system for all of state government. The Office of the CIO brought in a consultant to talk with agencies, Lotus Notes and Microsoft Exchange providers. Agencies, boards and commissions have been informed that the State of Nebraska will be moving to a Microsoft Exchange platform and that it will be implemented through the Office of the CIO. This enterprise unified email system effort will be save the state \$500,000 annually

once implemented. The office is working cooperatively with the Secretary of State regarding information sharing and record keeping. It is anticipated that it will take at least 24 months to implement the whole state. Agencies will have two pricing option arrangements: 1) a license can be purchased over six years and pay approximately \$10/month per mailbox, or 2) purchase the license upfront with end of year monies and pay approximately \$7/month per mailbox. The number of staff supporting the current email systems is conservatively estimated at 20 persons in the agencies. After implementation of the new platform, it is estimated to be only 4-5 people for the state.

REPORT - TECHNICAL PANEL REPORT

Walter Weir, Chair

The Technical Panel has held three monthly meetings since the last NITC meeting. The Retirement Systems have provided monthly progress reports. The Technical Panel established a Learning Management System Standards Work Group. Kirk Langer, Technical Panel member, is chairing the work group.

The Technical Panel has recommended approval of the following four standards and guidelines.

STANDARDS & GUIDELINES: REMOTE ADMINISTRATION OF INTERNAL DEVICES

Standard: It is the responsibility of all State of Nebraska agencies to strictly control remote access from any device that connects from inside the State of Nebraska network to a desktop, server or network device elsewhere within the State of Nebraska network (e.g. from a 10.x.x.x device to a 10.x.x.x device) and ensure that employees, contractors, vendors and any other agent granted remote access privileges adhere to common methods of secure remote administration which shall include but are not limited to:

- Use of strong authentication mechanisms (e.g., strong passwords, public/private key pair, two factor authentication, etc.)
- Utilize device host access (by IP address) lists to restrict remote access
- Use of secure protocols that provide encryption of both passwords and data (e.g., SSL, HTTPS) when reasonable and appropriate, rather than insecure protocols (e.g., Telnet, FTP).
- Grant permissions to only those with a job related need.
- Implement the 'Principle of Least Privilege' to those who are granted permissions.
- Reset factory default device passwords and regularly change any default accounts or passwords for the remote administration utility or application.
- Disable remote capabilities of devices or device accounts if remote access is not employed by the agency.

Purpose: The purpose of this document is to define standards for agencies that connect from any State of Nebraska network or device to any State of Nebraska network or device.

Objectives include:

- Provide guidance to State of Nebraska agencies employees, contractors, vendors and any other agent that access any State of Nebraska network or device.

- Provide a high level of security through industry standards and best practices.
- 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.

Commissioner Flanagan moved to approve the [Remote Administration of Internal Devices](#) Standard. Commissioner Park seconded. Roll call vote: Park-Yes, Flanagan-Yes, Peterson-Yes, Aerni-Yes, Kristensen-Yes, Sheehy-Yes, Hedquist-Yes, Huggenberger-Yes, and Hoelsing-Yes. Results: Yes-9, No-0. Motion carried.

STANDARDS & GUIDELINES: MINIMUM SERVER CONFIGURATION

Standard: The State of Nebraska recognizes the National Institute of Standards and Technology (NIST) as the adopted author of deployment configurations that provide minimum baselines of security for servers on the State of Nebraska network. As such, all state agencies, boards and commissions will comply with NIST standards, guidelines, and checklists as identified in Appendix A. NIST provides instructions, recommendations, and considerations to assist readers in deploying servers in a secure method. All State of Nebraska System Administrators should examine NIST documents when installing and or configuring servers. The documents are not all inclusive, but rather meant as a means of prompting and guiding Administrators through the installation process.

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

Commissioner Peterson moved to approve the [Minimum Server Configuration](#) Standard. Commissioner Kristensen seconded. Roll call vote: Peterson-Yes, Aerni-Yes, Sheehy-Yes, Kristensen-Yes, Park-Yes, Hedquist-Yes, Hoelsing-Yes, Flanagan-Yes, and Huggenberger-Yes. Results: Yes-9, No-0. Motion carried.

STANDARDS & GUIDELINES: SMTP ROUTING STANDARD

Standard: All inbound and outbound SMTP traffic will be routed through the State of Nebraska's SPAM/Anti-Virus appliance that is managed by the Office of the CIO

Purpose and Objectives: All inbound and outbound SMTP traffic must be routed through the State of Nebraska's SPAM/Anti-Virus appliance to ensure that email and attachments within emails are properly scanned for viruses, SPAM, and that all content complies with State of Nebraska policies including privacy concerns.

Commissioner Hedquist moved to approve the [SMTP Routing Standard](#). Commissioner Flanagan seconded. Roll call vote: Flanagan-Yes, Aerni-Yes, Huggenberger-Yes, Peterson-Yes, Sheehy-Yes, Park-Yes, Hedquist-Yes, Kristensen-Yes, and Hoelsing-Yes. Results: Yes-9, No-0. Motion carried.

STANDARDS & GUIDELINES: DNS FORWARDING STANDARD

Standard: All outbound (Internet) DNS traffic must be forwarded through the State of Nebraska's internal DNS servers.

Purpose and Objectives: All outbound (Internet) DNS traffic must be forwarded through the State of Nebraska's internal DNS servers that are managed by the Office of the CIO.

Commissioner Aerni moved to approve the [DNS Forwarding Standard](#). Commissioner Park seconded. Roll call vote: Sheehy-Yes, Peterson-Yes, Park-Yes, Kristensen-Yes, Huggenberger-Yes, Hoelsing-Yes, Hedquist-Yes, Flanagan-Yes, and Aerni-Yes. Results: Yes-9, No-0. Motion carried.

GOVERNMENT TECHNOLOGY COLLABORATION FUND GRANT – NEBRASKA GEOSPATIAL DATA SHARING AND WEB SERVICES NETWORK

Steve Henderson, I.T. Administrator for Planning and Project Management, and Larry Zink, GIS Coordinator

This proposal is a request for partial startup funding of a two-year project to establish the Nebraska Geospatial Data Sharing and Web Services Network and to lay the foundation for its long-term sustainability. This project is a collaborative interagency, intergovernmental project to develop an enterprise-level GIS/Geospatial Data Sharing Network and Web Services portal for Nebraska. Geospatial data is data that contains information about the physical location (street address, latitude/longitude, etc.) of data elements and can be mapped and/or integrated with other data based on common or proximate locations. This geospatial data portal will facilitate interactive data access and exchange between state, local, federal agencies, the private sector and the general public. The project will provide for both private/secured and open data access protocols for specific datasets.

Commissioner Flanagan moved to approve the [Nebraska Geospatial Data Sharing and Web Services Network](#) Government Technology Collaboration Fund Grant. Commissioner Hequist seconded. Roll call vote: Sheehy-Yes, Aerni-Yes, Flanagan-Yes, Hedquist-Yes, Hoelsing-Yes, Huggenberger-Yes, Kristensen-Yes, Park-Yes, and Peterson-Yes. Results: Yes-9, No-0. Motion carried.

Mr. Henderson, Mr. Zink and the GIS Steering Committee were acknowledged for their work with this collaborative effort.

OTHER BUSINESS

There was no other business to discuss.

ADJOURNMENT

With no further business, the meeting was adjourned.

Meeting minutes were taken by Lori Lopez Urdiales and reviewed by the staff of the Office of the NITC.

Strategic Initiatives

The NITC has identified eight strategic initiatives, which address the NITC's goals of supporting the development of a robust telecommunications infrastructure; supporting community and economic development; promoting the efficient delivery of government and educational services; and ensuring the security of data and network resources and the continuity of business operations. These initiatives would materially advance the vision and statewide goals as identified by the NITC. By emphasizing selected strategic initiatives, the NITC hopes to encourage funding of these initiatives and to encourage state agencies to work together to advance these initiatives. This year's plan includes one new strategic initiative and an expanded initiative. Public Safety Communications was added this year in recognition of the Office of the CIO's expanded involvement in public safety communications. The eHealth strategic initiative builds on and expands the scope of the Nebraska Statewide Telehealth Network initiative included in earlier plans. One strategic initiative from earlier editions of the statewide technology plan has been completed. With implementation of a statewide K-12 distance learning network underway as a result of the passage of LB 1208 by the Legislature in 2006, the Statewide Synchronous Video Network strategic initiative has been completed.

Supporting the Development of a Robust Telecommunications Infrastructure

Network Nebraska. In order to develop a broadband, scalable telecommunications infrastructure that optimizes the quality of service to every public entity in the state of Nebraska, the Office of the CIO and the University of Nebraska engaged in a collaborative partnership that used existing resources to aggregate disparate networks into a multipurpose core backbone extending from Norfolk, Omaha, Lincoln, Grand Island, Kearney and North Platte to the Panhandle. Benefits of Network Nebraska include lower network costs, greater efficiency, interoperability of systems providing video courses and conferencing, increased collaboration among educational entities, new educational opportunities, more affordable Internet access, and better use of public investments.

Supporting Community and Economic Development

Community IT Planning and Development. The primary objective of this initiative is to foster community and economic development in Nebraska communities through the effective use of information technology. The NITC Community Council has partnered with the University of Nebraska Cooperative Extension and Rural Initiative to form the Technologies Across Nebraska partnership. Technologies Across Nebraska is a partnership of over 40 organizations working to help communities utilize information technology to enhance development opportunities. Through Technologies Across Nebraska's Podcasting Across Nebraska program, communities and regional groups are creating podcasts to promote local attractions and events and to provide information to citizens. Technologies Across Nebraska's quarterly newsletter, *TANGents*, reaches over 1,000 individuals with an interest in technology-related development.

The NITC has identified eight strategic initiatives which address the NITC's goals.

Strategic Initiatives



Promoting the Efficient Delivery of Services

eHealth. eHealth technologies include telehealth, electronic health records, e-prescribing, computerized physician order entry, and health information exchange. The State of Nebraska will build upon the success of the Nebraska Statewide Telehealth Network as it begins to address issues related to the adoption of electronic health records and health information exchange. The widespread adoption of electronic health records is expected to reduce medical errors, improve quality of care, and reduce health care costs for payers.

Public Safety Communications System. The Regional Interoperability Advisory Board, Office of the CIO, and the Nebraska Emergency Management Agency have established strategic goals and grants guidance to improve state and local interoperable communications capabilities. The statewide telecommunications strategy integrates regional communications systems, the mutual aid frequency plan, and the state communications infrastructure. The Office of the CIO has developed a plan for a statewide interoperable communications network that consolidates a core of state agencies on a single system platform.

Digital Education. The primary objective of the Digital Education Initiative is to promote the effective and efficient integration of technology into the instructional, learning, and administrative processes and to utilize technology to deliver enhanced digital educational opportunities to students at all levels throughout Nebraska on an equitable and affordable basis. This initiative will involve the coordination and promotion of several major systems and applications that have either been developed mostly at the local level or have not been replicated statewide.

State Government Efficiency. The State Government Council will address multiple items improving efficiency in state government, including implementing shared services and adopting standards and guidelines. The council has identified and is working to implement six shared services for state government agencies. Also, the council will continue to develop standards and guidelines to better coordinate state agency technology efforts. Benefits of these activities include lower costs, easier interoperability among systems, greater data sharing, and improved services.

E-Government. Through the use of technology, state agencies can enhance information sharing, service delivery, and constituency and client participation. Benefits include improved services for citizens and businesses, and increased efficiency and effectiveness for agencies.

Ensuring the Security of Data and Network Resources and the Continuity of Business Operations

Security and Business Resumption. This initiative will define and clarify policies, standards and guidelines, and responsibilities related to the security of the State's information technology resources. Benefits include lower costs by addressing security from an enterprise perspective, cost avoidance, and protecting the public trust.

September 10, 2007

To: NITC Commissioners

From: Anne Byers

Subject: Community Council Report

Community Council Discussions

The Community Council has undergone significant changes in membership and felt that it was time to review its mission, charter and goals. At their meeting on July 16, 2007, members began the process by first identifying community technology needs. They also revised several sections of their charter, including their mission, responsibilities, and membership. I will be asking you to approve the revised charter.

The Community Council is scheduled to meet on September 14, 2007 and will be revising and prioritizing their goals.

Community IT Needs

The list of needs and the number of votes each received in a prioritization exercise are listed below:

- Make technology available to all consumers/Universal technology and Internet access—16
- Direct, efficient link between job seekers and employers and other community information/ Connecting the Pieces/Coordinate access efforts among community engagements—11
- Consolidate community resources to reduce duplication and overlap—9
- Cell phone coverage—9
- New generation workforce training for adults—8
- Competitive business class broadband—6
- People first—Get the people to drive the infrastructure—3
- Soft skills development-1
- Video conference sites

Revised Community Council Mission (Section 5.1 of the Charter)

The mission of the Council is to foster the collaborative, innovative, and effective use of technology through partnerships between public and private sectors to support community and economic development for Nebraska citizens.

Revised Community Council Responsibilities (Section 5.2 of the Charter):

- Assist the Commission in developing, reviewing and updating the statewide technology plan.
- Identify specific community information technology needs in Nebraska.
- Develop strategies to address the unique circumstances of rural areas with sparse population.
- Establish such subcommittees and task forces as necessary and appropriate to advise the Council on specific issues.
- Recommend policies, guidelines and standards that promote economic opportunities, innovation, and entrepreneurship to improve quality of life in communities through the use of information technology.
- Recommend policies and initiatives that promote awareness, access, training, partnerships, and planning for the use of information technology in communities.
- Review and make recommendations to the Commission on requests for funds from the Community Technology Fund.

Revised Membership (Sections 6.1 and 6.2)

The membership section of the charter was also revised, eliminating telehealth as a membership sector.

Podcasting Update

We are wrapping up the Podcasting Across Nebraska project. Twenty-five podcasts have been created through the program. The podcasts are having a positive effect on the promotional and information dissemination efforts of participating communities. Participating in the program has made participants more aware of and more interested in other interactive communication technologies. Participants are also more confident about their ability to learn and use other new technologies. The final report includes additional information on the outcomes and impact of the program. We are discussing ways of expanding the program to include other types of new technologies.

Nebraska Information Technology Commission
Community Council Charter

1. Introduction

The Community Council (hereafter referred to as “Council”) of the Nebraska Information Technology Commission (hereafter referred to as “Commission”) is an advisory committee of the Commission composed of representatives from rural and community IT development, local governments and libraries, resource providers, and other focus areas as deemed appropriate by the Community Council and the NITC. The Council was originally formed by Executive Order 97-7 in November 1997 to identify, prioritize, and coordinate user needs with respect to community information technology. The Community Council first met on January 30, 1998.

2. Purpose of Charter

The purpose of this charter is to provide operational guidance to the Council members and to provide general information to all who read the proceedings and recommendations of the Council.

3. Authority

The authority for the Community Council of the Nebraska Information Technology Commission is derived from Section 6-7 of LB 924 passed April, 1998. "Establish ad hoc technical advisory groups to study and make recommendations on specific topics, including work groups to establish, coordinate, and prioritize needs for education, local communities, and state agencies[.]" NEB. REV. STAT. § 86-516(7).

4. Nebraska Information Technology Commission Responsibilities and Mission

4.1 Commission Mission

"The mission of the Nebraska Information Technology Commission is to make the State of Nebraska's investment in information technology infrastructure more accessible and responsive to the needs of its citizens regardless of location while making government, education, health care and other services more efficient and cost effective."

<http://www.nitc.state.ne.us/>

4.2 Commission Responsibilities:

4.2.1 Adopt policies and procedures used to develop, review, and annually update a statewide technology plan;

4.2.2 Create a technology information clearinghouse to identify and share best practices and new developments, as well as identify existing problems and deficiencies;

4.2.3 Review and adopt policies to provide incentives for investments in information technology infrastructure services;

4.2.4 Determine a broad strategy and objectives for developing and sustaining information technology development in Nebraska, including long-range funding strategies, research and development investment, support and maintenance requirements, and system usage and assessment guidelines;

4.2.5 Adopt guidelines regarding project planning and management, information-sharing, and administrative and technical review procedures involving state-owned or state-supported technology and infrastructure. Governmental entities, state agencies, and political subdivisions shall submit projects that directly utilize state-appropriated funds for information technology purposes to the process established by NEB. REV. STAT. §§86-512 to 86-524. Governmental entities and political subdivisions may submit other projects involving information technology to the Commission for comment, review, and recommendations;

4.2.6 Adopt minimum technical standards, guidelines, and architectures upon recommendation by the technical panel;

4.2.7 Establish ad hoc technical advisory groups to study and make recommendations on specific topics, including work groups to establish, coordinate, and prioritize needs for education, local communities, and state agencies;

4.2.8 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;

4.2.9 Approve grants from the Community Technology Fund and Government Technology Collaboration Fund; and

4.2.10 Adopt schedules and procedures for reporting needs, priorities, and recommended projects.

5. Community Council Mission and Responsibilities

5.1 Council Mission

The mission of the Council is to foster the collaborative, innovative, and effective use of technology through partnerships between public and private sectors to support community and economic development for Nebraska citizens.

5.2 Council Responsibilities

5.2.1 Assist the Commission in developing, reviewing and updating the statewide technology plan.

5.2.2 Identify specific community information technology needs in Nebraska.

5.2.3 Develop strategies to address the unique circumstances of rural areas with sparse population.

5.2.4 Establish such subcommittees and task forces as necessary and appropriate to advise the Council on specific issues.

5.2.5 Recommend policies, guidelines and standards that promote economic opportunities, innovation, and entrepreneurship to improve quality of life in communities through the use of information technology.

5.2.6 Recommend policies and initiatives that promote awareness, access, training, partnerships, and planning for the use of information technology in communities.

5.2.7 Review and make recommendations to the Commission on requests for funds from the Community Technology Fund.

6. Membership

6.1 Number of Members

The Council membership includes representatives from each of its focus areas: rural/community IT development, local government and libraries, resource providers, and other groups as deemed appropriate by the Community Council and the NITC. The number of members shall be between 18 and 24. The Commission shall solicit nominations from organizations or individuals with an active interest or involvement in community information technology issues. Nominations shall describe the qualifications of the person relative to the goals of the Community Council. In choosing members, the Council shall strive for a balance of perspectives on community information technology issues.

6.2 Representation

The following focus areas will be represented within the Community Council

6.2.1 Rural and Community IT Development

6.2.2 Local Government and Libraries

6.2.3 At-large, Resource Sector

6.2.4 Other focus areas as deemed appropriate by the Community Council and the NITC

6.3 Member Responsibilities

Each member is responsible for maintaining two-way communication with their sector constituents concerning issues brought before the Council. Failure to provide adequate representation and communication may be grounds for dismissal from the Council.

6.4 Vacancies

Vacancies shall be filled in the same manner as the initial appointments for the remainder of the original term. The seat of a Council member who accumulates absences from more than half of the Council's yearly meetings shall be considered vacant.

6.5 Length of Service

One-half of the members in each sector shall serve for 3-year terms. All other members and all subsequent additions shall serve 2-year terms.

7. Meeting Procedures

7.1 Chair(s)

The elected Chair or Co-Chairs will conduct the meetings of the Council, oversee the establishment, operation and dissolution of committees, propose meeting agendas, and maintain the general operations of the Council. The Chair or Co-Chairs of the Council will serve two year staggered terms, expiring on January 1.

7.2 Quorum

An official quorum consists of 50% of the official members or their voting alternates. No official voting business may be conducted without an official quorum.

7.3 Designated Alternates and Non-voting Alternates

7.3.1 Each member of the Council shall designate one (1) official voting alternate.

This official voting alternate shall be registered with the Office of the Chief Information Officer and NITC and, in the absence of the official member, have all the privileges as the official member on items of discussion and voting.

7.3.2 If the official member and his/her official alternate are unable to attend a Council meeting either in person or electronically, then the sub-sector affected may send a non-voting alternate to gather or share information.

7.4 Meeting Frequency

The Council shall meet not fewer than four times per year (quarterly).

7.5 Subcommittees

The Council may, as it deems necessary, form task forces, teams, work groups, and special, ad hoc, and standing subcommittees to carry out its mission and responsibilities. Each time a new subcommittee is formed under the Council, the following seven sections must be decided and assigned within 30 days of formation.

7.5.1 Authority

The authority of any subcommittee of the Council is obtained and assigned through an official motion of the Commission and/or Council.

7.5.2 Goals

The Chair or Co-Chairs of the Council assign the goals of any subcommittee of the Council.

7.5.3 Charge

The Council delivers the charge to the subcommittee, which includes a quarterly progress report back to the Council at its regular meeting.

7.5.4 Membership

The membership of each subcommittee of the Council shall be determined by appointment, election, or volunteerism, whichever means is most suitable to the Council. The subcommittees may include members from outside the Council as resource persons, as determined by the Council.

7.5.5 Leadership

Each subcommittee of the Council shall have a chair or co-chairs to provide leadership. The Chair(s) of the Council may appoint a chair or co-chairs or the majority of the subcommittee may elect a chair or co-chair.

7.5.6 Duration

The Council shall assign each subcommittee a specific duration to complete its charge. At the conclusion of the duration and delivery of its charge, the subcommittee shall be dissolved. If the subcommittee requires a longer duration than has been assigned, the chair of the subcommittee shall request an extension or renewed duration.

7.5.7 Process

The subcommittees charged by the Council may conduct their own meetings and forums away from the Council's regular meetings. The chair of the subcommittee must inform the Office of the CIO-NITC of the date, time, and location of additional meetings.

7.5.8 Open Meetings

"Sections 84-1408 to 84-1414 of the Open Meetings Law shall not apply to subcommittees of such bodies unless a quorum of the public body attends a subcommittee meeting or unless such subcommittees are holding hearings, making policy, or taking formal action on behalf of their parent body..."

7.6 Expense Reimbursement

81-1182.01 "Any department, agency, Commission, council, committee, or board of the state may pay for the reasonable and necessary expenses for the recruitment, training, utilization, and recognition of volunteers providing services to the state and certain providers of services as established by the Director of Administrative Services."

7.6.1 NAS Policy CONC-005 "Volunteers shall mean those persons providing services to the State who are not being compensated for their time."

7.6.2 Council members needing reimbursement must submit a signed request to the Office of the CIO-NITC using the official state accounting forms.

7.7 Open Meeting Laws and Public Notice

It is the policy of the State of Nebraska that the formation of public policy is public business and may not be conducted in secret. Every meeting of a public body shall be open to the public in order that citizens may exercise their democratic privilege of attending and speaking at meetings of public bodies.

7.7.1 Advance Notice

The Council shall give reasonable advance publicized notice of the time, place, and agenda of each meeting through the use of its web page, <http://www.nitc.ne.gov>. The agenda

will also be available for public inspection during normal business hours at the Office of the CIO-NITC, 501 S. 14th, 4th floor, Lincoln, Nebraska.

7.7.2 Videoconferencing

Meetings of the Council may be held by means of videoconferencing if reasonable advance publicized notice is given; reasonable arrangements are made to accommodate the public's right to attend, hear, and speak; at least one copy of all documents being considered is available at each site; one member of the council is present at each site of the videoconference; and no more than one-half of the Council's meetings in a calendar year are held by videoconference.

7.7.3 Rights of the Public

It is not a violation for the Council to make and enforce reasonable rules and regulations regarding the conduct of persons attending, speaking, reporting, videotaping, photographing or recording its meetings. The Council may not forbid public participation at all meetings but may not be required to allow citizens to speak at each meeting. The Council shall not require members of the public to identify themselves as a condition for admission to the meeting but may do so as a condition for addressing the Council.

7.7.4 Minutes and Voting

The Council shall keep minutes of all meetings showing the time, place, members present and absent and the substance of all matters discussed. Any action taken on any question or motion duly moved and seconded shall be by roll call vote of the Council in open session, and the record shall state how each member voted or if the member was absent or not voting. The roll call shall be called on a rotational basis. Minutes shall be written and available for inspection within ten working days or prior to the next convened meeting, whichever occurs earlier.

Podcasting Across Nebraska

Final Report

2006-2007

Podcasting Across Nebraska is a collaborative effort to help Nebraska communities or regional groups develop podcasts which promote tourism, events, recreation, historic sites, and other activities. Through the program, the City of South Sioux City and South Sioux City Public Schools; the Highway 14 Association; the North Platte/Lincoln County Convention and Visitors Bureau; and Panhandle Public Health District and Panhandle Podcasting Partners received hardware and software as well as training on how to create and produce podcasts.

"I've gotten great feedback," said Sandy Hatton from the Highway 14 Association. "It's been very educational. We didn't know anything about podcasting before participating in this program. We're planning to offer another podcasting training session."

"It's been invaluable in promoting city services and various activities. It is generating economic development opportunities. Departments give us ideas for podcasts all of the time. We definitely plan to keep producing video podcasts."

--Danny Bligh, City of South Sioux City

Participants produced 25 podcast episodes. The podcasts are having a positive effect on the promotional and information dissemination efforts of participating communities.

"It's been invaluable in promoting city services and various activities," said Danny Bligh with the City of South Sioux City. "It is huge for us. It is generating economic development opportunities. Departments give us ideas for podcasts all of the time. We definitely plan to keep producing video podcasts."



Lt. Gov. Rick Sheehy congratulates the South Sioux City participants. Pictured (Left to Right): Greg Koiznan, Lance Martin, Lt. Gov. Rick Sheehy, Lance Swanson, and Danny Bligh. Photo by Jon Wilson, UNL New Media Center.

Participating in the program has made participants more aware of and more interested in other interactive communication technologies. Participants are also more confident about their ability to learn and use other new technologies.

“It opened our eyes and helped us realize that technology isn’t quite so scary. Creating podcasts is easier than we thought and very effective. Participating in the program has given us the confidence to explore other technologies.”

--Muriel Clark, North Platte/Lincoln County Convention and Visitors Bureau.

“It opened our eyes and helped us realize that technology isn’t quite so scary,” said Muriel Clark from the North Platte/Lincoln County Convention and Visitors Bureau. “Creating podcasts is easier than we thought and very effective. Participating in the program has given us the confidence to explore other technologies.”

Project partners include the NITC Community Council, University of Nebraska, Network Nebraska, Department of Economic Development, Division of Tourism, Network Nebraska, Technologies Across Nebraska, Nebraska Lied Main Street program, and Apple Computer. Training was provided by the University of Nebraska Extension educators. Podcasts produced through the project are being hosted by Network Nebraska. Funding was provided through the Nebraska Information Technology Commission Community Technology Fund.

“The communities involved are excited.” said Sandy Patton. “It is great to show what is happening in communities and to promote them.”



Bruce Sandhorst, Lieutenant Governor Rick Sheehy, Todd Jensen, and Karl Schlitt visiting at the University of Nebraska New Media Center. Photo by Jon Wilson, UNL New Media Center



Participants listen to podcasts at the Highway 14 Association training in Fullerton.



Superintendent Jeffrey Anderson, Senator Annette Dubas, Sandy Patton, and Lt. Governor Rick Sheehy at the presentation of podcasting equipment to the Highway 14 Association.



University of Nebraska Extension Educator Connie Hancock gives participants an overview of podcasting.

Outcomes

- Twenty-five podcasts have been created through the program.
- Approximately 30 resource providers were trained at the initial training sessions conducted by the University of Nebraska New Media Center in August 2006.
- 29 individuals from the 4 participating groups received training on podcasting.
- Seven additional training sessions were held, training approximately 100 individuals. Future training sessions are scheduled for Grant, Lincoln, and the Nebraska Rural Institute in Holdrege. Ainsworth and Kimball have expressed interest in a future training session.
- Through a grant from the Digital Story Telling Center, 10 University of Nebraska Extension staff will receive training on podcast production to capture community development in action.

Impact

- **Participating in the program has made participants more aware of and more interested in other interactive communication technologies. Participants are also more confident about their ability to learn and use other new technologies.**

“It opened our eyes and helped us realize that technology isn’t quite so scary,” said Muriel Clark from the North Platte/Lincoln County Convention and Visitors Bureau. “Creating podcasts is easier than we thought and very effective. Participating in the program has given us the confidence to explore other technologies.”

“It has definitely broadened my knowledge,” said Sandy Patton from the Highway Association. “Constantly new things are perking up my ears.”

Jessica Davies from the Panhandle Public Health District commented, “We’re excited for new ways to disseminate health information to young people.”

- **Podcasting is having a positive effect on participating organizations’ promotional and information dissemination efforts.**

“It’s been invaluable in promoting city services and various activities,” said Danny Bligh with the City of South Sioux City. “It is huge for us. It is generating economic development opportunities. Departments give us ideas for podcasts all of the time. We definitely plan to keep producing video podcasts.”

“It has helped our promotional efforts overall,” said Muriel Clark from the North Platte/Lincoln County Convention and Visitors Bureau.

“It has been a great tool to provide information to students and teachers,” said Lance Swanson from South Sioux City Public Schools. We will continue to use podcasts to get information to staff and students. We plan to use it in the classroom more. One teacher is already creating videos showing how to solve math problems so students can refer to it at home if they get stuck on a homework problem.”

Lessons learned

- The program has generated a lot of enthusiasm.
- Podcasting is easier than many people think.
- Participants cited training as the most valuable aspect of the program.
- There are limited training opportunities to learn how to create podcasts or to utilize new technologies in Nebraska for those not involved in K-12 or higher education—especially in rural communities.
- Podcasts need to be incorporated into an organization’s overall marketing plan.
- It is important to include links to individual episodes from an organization’s Web site. An organization’s Web site is probably the most important vehicle for delivering podcasts.

- Participants marketed their podcasts in a variety of ways including :
 - Putting links to individual episodes from the organization's Web site.
 - Disseminating information about the podcasts to listservs.
 - Putting information on the podcasts in newsletters.
 - Playing the podcasts at meetings and giving demonstrations on Podcasting.
- Post-training technical support was critical to the success of the program. All participants had at least one question or request for assistance in troubleshooting a problem. Most of the issues were related to uploading files to the server and creating XML feeds.



Lieutenant Governor Rick Sheehy awards podcasting equipment to Lisa Cox.



Jessica Davies receives podcasting equipment from Lt. Governor Rick Sheehy.

Podcasts Created

As of August 24, 2007

- **South Sioux City CardinalCast**
 - Tourism
 - Economic Development
 - Spring Services
 - Mobile Communications Bus
 - National Night Out
 - Cardinal Virtual Building

- **South Sioux City Public Schools Digital Life Podcast**
 - Internet Safety
 - Middle School Introduction
 - Operation Care Bear
 - Welcome to South Sioux City: Tour of Middle and High School
 - Internet Safety Night Part 1
 - Internet Safety Night Part 2
 - High School News

- **North Platte/Lincoln Co. Convention and Visitors Bureau podcast**
 - Sandhill Cranes
 - Attractions and Events
 - Buffalo Bill State Historical Park
 - North Platte Canteen
 - Fishing in Lincoln County
 - Nebraskaland Days
 - Cottonwood Massacre

- **Panhandle Public Health District and Panhandle Podcasting Partners Podcast**
 - Alliance Walking Tour
 - West Nile Virus

- **Highway 14 Association Podcast**
 - Pop-In
 - Fullerton

- **Podcasting Across Nebraska**
 - Podcasting Across Nebraska Year 1 Report

Links to these podcasts can be found at <http://www.nitc.ne.gov/cc/podcasting/podcasting.html>.

HISPC

Health Information Security and Privacy Committee State of Nebraska

Security and Privacy Barriers to Health Information Interoperability

Recommendations and Summary:

Final Report for the state of Nebraska June 2007

A complete version of the Final Report is available upon request from the state of Nebraska Office of Rural Health (Phone: 402-471-0142) or as a downloadable PDF file from the Creighton Health Services Research Program at <http://chrp.creighton.edu>



Partial resources support from the Creighton Health Services Research Program (CHRP) and grant no. 1P20 HS015816 Building Research Infrastructure Capacity from the Agency for Healthcare Research and Quality (AHRQ); and the State Offices of Rural Health grant no. H95RH00119, Nebraska Health and Human Services System

HISPC

Health Information Security and Privacy Committee State of Nebraska

Security and Privacy Barriers to Health Information Interoperability

Executive Summary Final Report for the state of Nebraska

The United States is in the middle of a ten year plan to develop and implement a nationwide electronic health information infrastructure that will allow authorized health care professionals to securely access relevant patient data from any location in the country at any time. As envisioned, the National Health Information Initiative in the United States will be a “series of cross-jurisdictional interconnected regional health information exchanges or organizations”.¹ The Lieutenant Governor for the State of Nebraska formed the Health Information Security and Privacy Committee (HISPC) in 2006. The vision driving the state HISPC is to create the flexibility to electronically exchange patient authorized health care information, confidentially and securely between the patient/client and all appropriate persons involved in the health care process. Many issues have come to light nationwide as states begin to work on these linkages and collaborations. One core issue is how to appropriately protect the privacy and security of health information in an interconnected electronic health information system. The Nebraska HISPC has focused its energy on the issue of “privacy”, believing that security is an issue that lies outside of a single state’s ability.

The HISPC has reviewed key documents related to the state statutes that address, movement of personalized health information to assist in the treatment and care of a patient. We have also conducted surveys of three stakeholder groups in Nebraska: 1) health/licensure/certification and facilities oversight board managers, 2) health professions organizations leadership, and 3) consumers. These surveys assessed stakeholder security and privacy issues as they relate to stakeholder knowledge and perception about health information exchange, technology, and quality and safety of patient care. These state level findings are then presented in comparison to the nation when feasible, as determined through a review of national reports, publications and technical information from leading health information organizations and the government.

This final report reflects a benchmark about the progress toward health information exchange and overcoming security and privacy barriers in the state of Nebraska as compared to the nation. The HISPC committee has identified a fundamental need for a *sustainable* process of monitoring and facilitating the assurances of privacy and security as both the entities in the state and the state government continues to increase in capacity for health information exchange. Researchers must continue to play a key role in assisting us to gain new knowledge as we move forward. Our findings in the state were consistent with in the 33 state examination of security and privacy issues released in June of 2007, whose findings are summarized in our full report.²



Partial resources support from the Creighton Health Services Research Program (CHRP) and grant no. 1P20 HS015816 Building Research Infrastructure Capacity from the Agency for Healthcare Research and Quality (AHRQ); and the State Offices of Rural Health grant no. H95RH00119, Nebraska Health and Human Services System

¹ Substance Abuse and Mental Health Services Administration (SAMSHA): the Implementation of E-consent Mechanisms, Feb. 16, 2007

²Dimitropoulos, L.L. Interim assessment of variation: privacy and security solutions for interoperable health information exchange. December 29, 2006. RTI Project No. 0209825.000.004.002 RTI International, Chicago, Illinois.

Recommendations are provided. The magnitude, complexity, and dynamic nature of the developing health information exchange efforts in the state have guided these recommendations. These factors also influenced the committee to develop this report as an educational resource document that offers guidance to health and information technology (IT) professionals while also assisting consumers of health care with some basic understanding of terms and concepts about security, privacy and health information exchange.

The final findings and recommendations of the HISPC Committee are:

Finding 1: Facilitation of knowledge and understanding about health information exchange is essential for the Nebraska Health and Human Services Health Board managers and Facility Oversight Managers. This knowledge directly affects the management of security and privacy issues. Managers who are equipped with this understanding can assist the boards to address how current and future rules and regulations affect and are affected by the evolving landscape of health information exchange and interoperability.

Recommendation:

- **Nebraska Health and Human services develop a process for obtaining timely and up to date technical information on health information and interoperability and disseminating this to health/ licensure/ certification board managers and their members.**
- **Nebraska Health and Human services charge managers to facilitate the boards to address how current and future rules and regulations affect and are affected by the advancement of health information exchange and interoperability.**

Finding 2: Facilitation of knowledge and understanding of health professionals across the state is an important role that the health professions organizations can perform. These organizations vary in their engagement and understanding of the technical information about health information interoperability and the related security and privacy issues. The organizations would provide a great service in the process of informing their members about understanding health information exchange and interoperability, and the related security and privacy practices and issues.

Further, the unique knowledge and expertise of health care practitioners, facilities in which health care is provided, organizations involved with health issues at the societal level and educators of health professions students, is needed to address how current laws, rules and regulations related to their disciplines affect and are affected by the electronic exchange of health information. We encourage these associations to seek additional information about health information exchange and interoperability in other regions within the state, region, nationally and internationally.

Recommendation:

- **the e-Health Council engage all health professional associations involved in health care delivery and services to assist in present and future efforts to design, implement and educate key stakeholders in the health professions, health education and health organizations about the sharing of health information, and the related security and privacy issues as these processes unfold.**

Finding 3: The HISPC recognizes that state government, boards and health care providers need more knowledge about the Nebraska consumer. Consumer viewpoints are critical to this broader understanding of health information exchange and interoperability. A larger and broader representation of consumer viewpoints and needs will greatly improve our understanding of “what” consumers will participate in and “how” they will participate.

Similarly, consumers are in great need of information and education about health information exchange and interoperability. Consumers have concerns that must be addressed through knowledge dissemination. This will facilitate the best decision-making possible for the consumer. A dissemination process for essential and timely information related to progress of this initiative occurring at both the federal and state level to consumers is needed.

A variety of ways of consumer involvement are needed to assist in the design of the processes of education of all stakeholders and policy formulation as the macro system of sharing health information electronically unfolds over time. This is an essential step to facilitating citizens and providers to more easily establish a common understanding and agreed upon set of solutions to health information exchange as security and privacy issues are addressed.

Recommendation:

- **The e-Health Council engage consumers to assist in present and future efforts to design, implement and educate other consumers and key stakeholders in the health professions, health education and health organization about the sharing of health information, and the related security and privacy issues as these processes unfold.**

Finding 4: The complexity of the rules and regulations create confusion in the area of privacy. Because the HIPAA preemption rules are complex, individuals in a position to potentially disclose protected health information (PHI) sometimes are unsure if the PHI may be disclosed without written individual authorization. Health care providers and payers who are faced with potential civil and criminal HIPAA fines and penalties, state law causes of action for invasion of privacy, and reporting to licensure boards for breach of confidentiality, may often decide not to disclose PHI without written patient authorization, when it is otherwise permissible to disclose.

Recommendation:

- **The e-Health Council should study the issues identified and described in the background information of this report and recommend a sustainable action plan developed to facilitate progress in assuring privacy and security protections of the individual while progressing in health information exchange.**

Finding 5: Our HISPC study of security and privacy issues is consistent with the same concerns and areas of work needing to be addressed within our state and its’ communities as a most recent cross-sectional study of the nation revealed.¹ The issues are embedded in complexity and confusion associated with state and federal level inconsistencies, conflicting business practices, and varying

¹Dimitropoulos, L.L. Interim assessment of variation: privacy and security solutions for interoperable health information exchange. December 29, 2006. RTI Project No. 0209825.000.004.002. RTI International, Chicago, Illinois. (ref. 16)

consent policies and approaches. These issues must be untangled and addressed. This will require a sustained commitment to achieve.

Recommendation:

- **The e-Health Council should explore the development of a sustainable system for monitoring our progress in studying and addressing the security and privacy issues within the state of Nebraska.**
- **An in-depth study of existing laws and regulations, with guidance from representatives from health professions, health educators and health organizations is needed to develop solutions on how to overcome these barriers.**

Finding 6: Based on the three research reports from this committee and our discussions, we believe there is a need for further research needed about implications to consumers, health professionals, health systems, educators, private and public care providers, and payers. Examples of important research questions that the committee has thought about, but are not limited to include:

- How are consumer's health and safety outcomes affected by the sharing of health information?
- What processes are necessary for consumers to participate in the sharing of health information?
- How will consumers concerns about the risks they perceive with health information sharing be "stewarded" as the processes emerge, and who will "steward" them?
- How are small business health care providers, health systems and large healthcare organizations, affected by the impact of sharing health information: What is the impact on workload? What is the impact on workforce considerations?
- How will the educational needs of the young, middle age, young-old and old-old adults be met as these processes develop?
- What is the impact of a partial adoption of health information sharing on patient security and privacy?

Recommendation:

- **The NHHS should pursue further research in the area of how to obtain needed technical information and employ effective processes of applying this information to assist health boards and facility boards with the ongoing process of staying current in and facilitating adoption of future rules and regulations that advance secure, private health information and interoperability approaches.**
- **Further research should be conducted by professional organizations about the on-going impact of health information and exchange and interoperability on provider and patient security and privacy issues.**
- **Further research should be conducted to better understand consumer viewpoints and needs.**

HISPC Steering Committee:

- ◆ Lieutenant Governor Rick Sheehy
- ◆ Senator Pat Bourne (Past Member)
- ◆ Senator Jim Jensen (Past Member)
- ◆ Senator Philip Erdman
- ◆ Mark Adams, Corporate Security Officer, Blue Cross/Blue Shield of Nebraska
- ◆ Brenda Decker, Chief Information Officer, State of Nebraska
- ◆ David H. Filipi, M.D., Vice President, Medical Affairs, Physicians Clinic
- ◆ Kimberly Galt, Pharm.D., F.A.S.H.P., Associate Dean of Research, School of Pharmacy and Health Professions and Director, Creighton Health Services Research Program (CHRP)- Creighton University
- ◆ Steve Grandfield, Exec. Vice President, Blue Cross/Blue Shield of Nebraska (Past Member)
- ◆ Donna K. Hammack, Chief Development Officer, St. Elizabeth Foundation
- ◆ Steven H. Hinrichs, M.D., Professor/Director, UNMC – Dept. of Pathology/Microbiology
- ◆ Ron Hoffman, RHU, S5-Enterprise Privacy Office, Mutual of Omaha Insurance Company
- ◆ Dick Nelson, Director, NE HHSS – Dept. of Finance & Support (Past Member)
- ◆ Nancy Shank, Associate Director, University of Nebraska Public Policy Center
- ◆ September Stone, R.N., Nebraska Health Care Association
- ◆ Joni R. Cover, J.D., Executive Vice President, Nebraska Pharmacists Association
- ◆ Rick Zarek, R.P. (Past Member)

HISPC-RFP State of Nebraska Internal Project Team:

- ◆ Dennis Berens, Director, Nebraska Office of Rural Health NE HHSS – Dept of Regulation & Licensure (Facilitator)
- ◆ Joseph Acierno, M.D., J.D., Deputy Chief Medical Officer, NE HHSS – Dept of Regulation & Licensure
- ◆ Jacqueline Miller, DDS, Deputy Director, NE HHSS – Dept of Regulation & Licensure
- ◆ Roger Brink, J.D., Legal Counsel, NE HHSS – Dept of Finance & Support
- ◆ Harry Farley, Legal Services, NE HHSS – Dept of Finance & Support
- ◆ David Lawton, R.N. Ph.D., Health Surveillance Administrator, Public Health Assurance/Bioterrorism, NE HHSS – Dept of Regulation & Licensure
- ◆ Bob Leopold, Public Health Assurance/Bioterrorism, NE HHSS – Dept of Regulation & Licensure
- ◆ Dan Noble, M.D., Deputy Chief Medical Director, NE HHSS – Dept of Regulation & Licensure (Past Member)
- ◆ Jim Ohmberger, Administrator Information Systems & Technology Division, NE HHSS – Dept of Finance & Support
- ◆ Kathie Osterman, Administrator Communications & Legislative Services Division NE HHSS – Dept of Finance & Support
- ◆ Jane McGinnis, Managed Care Epidemiologist, Public Health Assurance/Bioterrorism, NE HHSS – Dept of Regulation & Licensure

Consultants:

- ◆ Sheila A. Wrobel, Chief Compliance Officer UNMC – Dept. of Pathology/Microbiology
- ◆ Pat Pankoke, Administrative Assistant, Public Health Assurance/Bioterrorism, NE HHSS – Dept of Regulation & Licensure (Past Member)
- ◆ Kevin Cueto, IT Consultant, Green Iris Technologies, Inc.
- ◆ John A. Glock, IT Project Coordinator, UNMC Public Health Laboratory
- ◆ Karen A. Paschal, P.T., D.P.T., Associate Professor of Physical Therapy, Creighton University
- ◆ Whitney Shipley, Program Coordinator UNMC – Center for Biopreparedness Education (Past Member)

Report Prepared by:

- ◆ Dennis Berens, Kimberly Galt, Pharm.D, F.A.S.H.P., and Karen A. Paschal, P.T., D.P.T. The assistance of Ms. Jamie Barbee of the Creighton University Health Services Research program with data collection and report preparation is acknowledged.



NEBRASKA TECHNOLOGY COMMISSION

STANDARDS AND GUIDELINES

Information Security Policy

Category	Security Architecture
Title	Information Security Policy
Number	

Applicability	<input checked="" type="checkbox"/> State Government Agencies <input type="checkbox"/> All.....Not Applicable <input checked="" type="checkbox"/> Excluding Higher Education institutionsStandard <input type="checkbox"/> State Funded Entities - All entities receiving state funding for matters covered by this document..... Not Applicable <input checked="" type="checkbox"/> 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 the NITC Technical Panel. Guideline - Adherence is mandatory.
---------------	---

Status	<input type="checkbox"/> Adopted <input type="checkbox"/> Draft <input checked="" type="checkbox"/> Other: <u>Reviewed</u>
Dates	Date: Date Adopted by NITC: Last Review Date:

TABLE OF CONTENTS



NEBRASKA TECHNOLOGY COMMISSION	1
STANDARDS AND GUIDELINES	1
TABLE OF CONTENTS	2
PURPOSE	4
SCOPE.....	4
APPLICABILITY	5
SECTION 1. OPERATIONAL ROLES AND FUNCTIONAL RESPONSIBILITIES	6
SECTION 2. STATE OF NEBRASKA INFORMATION	7
<i>Management of the Confidentiality, Integrity, and Availability of State Information.....</i>	7
<i>Sharing Non-public Information Outside the Agency.....</i>	7
SECTION 3. PERSONNEL ACCOUNTABILITY AND SECURITY AWARENESS.....	8
<i>Individual Accountability.....</i>	8
<i>Agency Accountability</i>	8
Including Security in Job Responsibilities	9
User Training	9
Separation of Duties	9
SECTION 4. COMPLIANCE.....	9
Managing Compliance.....	9
Monitoring.....	10
Incident Response.....	10
SECTION 5. PHYSICAL AND ENVIRONMENTAL SECURITY	10
Physical Security Perimeter.....	10
Asset Security	11
Secure Disposal or Re-use of Storage Media and Equipment.....	11
Clear Screen	11
SECTION 6. ASSET CLASSIFICATION.....	11
SECTION 7. ACCESS CONTROL	12
Logon Banner	12
User Account Management	12
Privileged Accounts Management.....	13
User Password Management	13
Network Access Control.....	13
User Authentication for External Connections (Remote Access Control)	13
Segregation of Networks	13
Operating System	14
Application Access Control.....	14
Monitoring System Access and Use.....	14
SECTION 8. OPERATIONAL MANAGEMENT.....	14
<i>Network Management.....</i>	14
Cooperation Between Organizations	15
Penetration Testing, Intrusion Testing, and Vulnerability Scanning.....	15
External Connections.....	16

Portable Devices.....	16
Server Hardening.....	17
System Planning.....	17
Protection against Malicious Code.....	17
Software Maintenance.....	17
Wireless Networks.....	17
<i>Communications</i>	18
Security of Electronic Mail.....	18
Telephones and Fax Equipment.....	18
Modem Usage.....	18
SECTION 9. SYSTEM DEVELOPMENT AND MAINTENANCE.....	18
System Acceptance.....	19
Separation of Development, Test and Production Environments.....	19
Risk Assessment.....	19
Input Data Validation.....	20
Control of Internal Processing.....	20
Message Integrity.....	20
Cryptographic Controls.....	20
Key Management.....	20
Protection of System Test Data.....	20
Protection of Source Code.....	21
Change Control Management.....	21
DOCUMENT CHANGE MANAGEMENT.....	21
CONTACT INFORMATION.....	21
REPEAL.....	21
DEFINITIONS.....	22
INDEX.....	28
ADDENDUM A.....	31
<i>Operational and Functional Responsibilities</i>	31
ADDENDUM B.....	33
<i>Role and Responsibilities of the Agency Information Security Officer</i>	33

PURPOSE

The purpose of this Information Security Policy is to provide a uniform set of reasonable and appropriate security safeguards for protection of the confidentiality, integrity, availability and privacy of State of Nebraska information collected, stored, and used to serve the citizens of the State of Nebraska. This Information Security Policy contains the minimum safeguards, responsibilities and acceptable behaviors required to establish and maintain a secure environment.

The Information Security Policy is based upon the ISO 27002 standard framework and is designed to comply with applicable laws and regulations; including the Records Management Act (Neb. Rev. Stat. § 84-1201 - 1227), however, if there is a conflict, applicable laws and regulations take precedence.

This Information Security Policy sets the direction, gives guidance, and defines requirements for information security processes and actions across agencies. This policy documents many of the security practices already in place in some agencies.

The primary objectives are to:

- effectively manage the risk of exposure or compromise to State resources;
- communicate the responsibilities for the protection of information;
- establish a secure, resilient processing environment;
- provide security controls for internally developed software to protect unauthorized access, tampering, or programming errors;
- provide a formal incident management processes; and
- promote and increase the awareness of information security.

SCOPE

This policy is applicable to State of Nebraska full time and temporary employees, third party contractors and consultants, volunteers and other agency workers (hereafter referred to as “Staff”). The Nebraska Information Technology Commission (hereafter referred to as the “NITC”) is fully committed to information security and agrees that all staff or any other person working on behalf of the State of Nebraska have important responsibilities to continuously maintain the security and privacy of agency data.

This policy applies to all State Agencies, Boards and Commissions (hereafter referred to as “Agency”). Any agency may enact stronger security safeguard requirements, as necessary, to meet their individual business needs, State or Federal regulations. Where conflicts exist between this policy and an agency’s policy, the more restrictive policy shall take precedence.

This Information Security Policy encompasses all systems, automated and manual, for which the State has administrative responsibility, including systems managed or hosted by third parties on behalf of an agency. This policy, subject to the provisions of the Records Management Act, applies to information in all forms, including but not limited to paper, microfilm, and electronic formats, created or used in support of business activities of the agency. This policy must be communicated to all staff that have access to or manage agency information.

Guidelines and standards, published by the NITC, which are associated with this policy, provide specific details for compliance with this mandatory Information Security Policy. Published guidelines and standards reflect current practices and will be periodically reviewed and updated as necessary to meet changes in business needs, State or Federal regulations, or changes in technology implemented or supported by the State of Nebraska.

APPLICABILITY

The NITC has statutory responsibility to adopt minimum standards and guidelines for acceptable and cost-effective use of information technology, and to provide strategic direction for State agencies and educational institutions for information technology. This Information Security Policy will be implemented to ensure uniformity of information protection and security management across the different technologies deployed within an agency.

The Secretary of State (State Records Administrator) has statutory responsibility to establish standards, procedures, and techniques to assist agencies in identifying essential records, and guide them in the establishment of schedules for the creation, preservation, and disposal of such records.

POLICY

The components of this Information Security Policy encompass: 1) Operational Roles and Functional Responsibilities, 2) Management of the confidentiality, integrity and availability of State of Nebraska Information, 3) Personnel Accountability and Security Awareness, 4) Compliance, 5) Physical and Environmental Security, 6) Asset Classification, 7) Access Control, 8) Operational Management, and 9) System Development and Maintenance.

Section 1. Operational Roles and Functional Responsibilities

Agencies that create, use or maintain information systems for the State of Nebraska must create and maintain an internal information security infrastructure that ensures the confidentiality, availability, and integrity of the State's information assets.

State Agencies: Management will ensure that an information security organization structure is in place to:

- appoint, designate or hire an Information Security Officer to serve as the primary agency point of contact to the State Information Security Officer;
- implement information security policies, procedures and standards as necessary to meet security requirements imposed on the agency by federal, state or local regulations and as promulgated by the NITC;
- assign information security responsibilities;
- implement a security awareness program;
- monitor exposure and implement appropriate safeguards of information assets;
- monitor and implement changes to meet legal or regulatory requirements;
- respond to security incidents; and
- develop a process to measure compliance with this policy.

As required by this policy, an Agency Information Security Officer must be designated to oversee all security-related events and information. Depending on the agency's size and complexity, this role may be a fulltime position. The Agency Information Security Officer may report to the Agency Management.

Office of Chief Information Officer: The Chief Information Officer is the executor of this Information Security Policy, which establishes and monitors the effectiveness of information security, standards and controls within the State of Nebraska. The State Information Security Officer, operating through the Office of the Chief Information Officer, performs as a security consultant to agencies and Agency Information Security Officers. The Office of the CIO may also perform periodic reviews of agency security for compliance with this and other security policies and standards.

Nebraska Information Technology Commission (NITC): The NITC is the owner of this policy with statutory responsibility to promote information security through adoption of policies, standards, and guidelines. The NITC develops strategies for implementing and evaluating the effectiveness of information security.

The **NITC Technical Panel**, with advice from the Security Work Group, has responsibility for recommending security policies and guidelines and making available best practices to operational entities.

For additional roles and responsibilities that an agency may adopt, see [Addendum A](#).

Section 2. State of Nebraska Information

State information is a valuable asset and must be protected from unauthorized disclosure, modification, or destruction. Prudent information security policies, standards, and practices must be implemented to ensure the confidentiality, integrity, and availability of State information is not compromised.

Management of the Confidentiality, Integrity, and Availability of State Information

The confidentiality, integrity, and availability of State of Nebraska information is critical to support an agency's business activities. Security controls provide the necessary physical, logical and procedural safeguards to protect State resources.

All information, regardless of the form or format, which is created, acquired or used in support of State of Nebraska's business activities, must be used for official business only. Agency information is an asset and must be protected from its creation through its useful life, and to its authorized disposal in accordance with the Records Management Act and your agency's retention schedule. State information must be maintained in a secure, accurate, and reliable manner and be readily available for authorized use. Information must be classified and protected based on its importance to business activities, risks, and security best practices. (See [NITC Data Security Standard](#).)

Sharing Non-public Information Outside the Agency

For information to be released outside an agency or shared between agencies, a process must be established that, at a minimum:

- evaluates and documents the sensitivity of the information to be released or shared;
- identifies the responsibilities of each party for protecting the information;
- defines the minimum controls required to transmit and use the information;
- records the measures that each party has in place to protect the information;
- defines a method for compliance measurement;
- provides a signoff procedure for each party to accept responsibilities;
- establishes a schedule and procedure for reviewing the controls (Refer to [Section 6. Asset Classification](#)).

Non-public State information must not be made available through a public network without appropriate safeguards approved by the data owner(s). The agency must implement safeguards to ensure access control, and data protection measures are adequately protecting State information and logs are collected and protected against unauthorized access. Non-public information includes, but is not limited to:

- critical infrastructure assets which are so vital that their infiltration, incapacitation, destruction or misuse could have a debilitating impact on health, welfare or economic security of the citizens and businesses of the State of Nebraska
- data that identifies specific structural, operational, or technical information, such as: mechanical or architectural drawings, floor plans, operational plans or procedures, or other detailed information relating to electric, natural gas, steam, water supplies, nuclear or telecommunications systems or infrastructure, including associated facilities;
- personal identifying information as defined under Neb. Rev. Stat. § 87-802.

Section 3. Personnel Accountability and Security Awareness

The State of Nebraska provides information technology resources to authorized Users to facilitate the efficient and effective performance of their duties. The use of such resources imposes certain responsibilities and obligations subject to state government policies and applicable state and federal laws. It is the responsibility of all staff to protect information resources and ensure that such resources are not misused.

Individual Accountability

Each user must understand his/her role and responsibilities regarding information security issues and protecting state information. Access to agency computer(s), computer systems, and networks where the data owner(s) has authorized access, based upon the “Principle of Least Privilege”, must be provided through the use of individually assigned unique computer identifiers, known as UserIDs, or other technologies including biometrics, token cards, etc. Each individual is responsible for reasonably protecting against unauthorized activities performed with their UserID.

Associated with each UserID is an authentication token, such as a password or pin, which must be used to authenticate the person accessing the data, system or network. These authentication tokens or similar technology must be treated as confidential information, and must not be shared or disclosed. ([Refer to Section 7. Access Control](#) and, [NITC Individual Use Policy](#)).

Agency Accountability

All agency information must be protected from unauthorized access to help ensure the information’s confidentiality and maintain its integrity. As with other assets, not all information has the same use or value, and therefore information requires different levels of protection. Each agency will follow established data classification processes in accordance with the NITC Security Officer’s Handbook, best practices, State directives, and legal and regulatory requirements, as determined by the appropriate levels of protection and classification of that information. All information will be classified and managed based on its confidentiality, integrity, and availability characteristics as defined in the [NITC Security Officer Handbook](#).

To ensure interruptions to normal agency business operations are minimized and critical agency business applications and processes are protected from the effects of major failures, each agency, in cooperation with the Chief Information Officer, must develop disaster recovery and business continuity plans that meet the recovery requirements defined by the agency. Preservation of critical data and software must be performed regularly and stored properly. Appropriate processes

will be defined in the agency's recovery plan to ensure the reasonable and timely recovery of all information, applications, systems and security regardless of platform or physical form or format, should that information become corrupted, destroyed, or unavailable for a defined period. ([Refer to NITC Information Technology Disaster Recovery Plan Standard](#))

To provide accountability regarding physical computing assets, each agency must maintain an up-to-date inventory of all State hardware and software, in accordance with DAS or agency fixed asset guidelines.

Including Security in Job Responsibilities

Specific security roles and responsibilities for those individuals responsible for information security must be documented. ([See Addendum A](#) and [Addendum B](#) for specific roles and responsibilities).

User Training

An information security awareness program must be developed, implemented, documented, and maintained that addresses the security education needs of the State. To ensure staff is knowledgeable of security procedures, their role and responsibilities regarding the protection of agency information and the proper use of information processing to minimize security risks, all staff with access to agency information must receive security awareness training, which must be reinforced at least annually. ([See NITC Individual Use Standard](#)). Technical staff must be trained to a level of competence in information security that matches their duties and responsibilities. ([See NITC Education, Training & Awareness Policy](#))

Separation of Duties

To reduce the risk of accidental or deliberate system misuse, separation of duties must be implemented where practical.

Whenever separation of duties is impractical, other compensatory controls such as monitoring of activities, audit trails and management supervision must be implemented. At a minimum the audit of security must remain independent and segregated from the security function.

Section 4. Compliance

Managing Compliance

Compliance with this policy is mandatory. Any compromise or suspected compromise of this policy must be reported as soon as reasonably possible to appropriate agency management and the State Information Security Officer. The failure to comply with this or any other security policy that may or may not result in the compromise of State information confidentiality, integrity, privacy, and/or availability may result in action as permitted by law, rule, regulation or negotiated agreement. Each agency will take appropriate steps necessary, including legal and administrative measures, to protect its assets and monitor compliance with this policy.

An agency review to ensure compliance with this policy must be conducted at least annually and each Agency management will certify and report the agency's level of compliance with this policy in accordance with the [NITC Data Security Standard](#).

The State Information Security Officer may periodically review Agency compliance with this policy. Such reviews may include, but are not limited to, reviews of the technical and business analyses required to be developed pursuant to this policy, and other project documentation, technologies or systems which are the subject of the published policy or standard.

Monitoring

Consistent with applicable law, employee contracts, and agency policies, the Chief Information Officer reserves the right to monitor, inspect, and/or search at any time all State of Nebraska information systems. Since agency computers and networks are provided for business purposes, staff shall have no expectation of privacy of the information stored in or sent through these information systems. The Chief Information Officer additionally retains the right to remove from agency information systems any unauthorized material.

Only individuals with proper authorization from the Office of the Chief Information Officer will be permitted to use "sniffers" or similar technology on the network to monitor operational data and security events on the State network. Network connection ports should be monitored for unknown devices and un-authorized connections.

Incident Response

Agencies must identify incident response procedures to promote effective response of security incidents, including procedures for information system failure, denial of service, disclosure of confidential information and compromised systems, according to the [NITC Incident Response and Reporting Procedure for State Government](#).

To ensure quick, orderly, and effective responses to security incidents, all users of agency systems must be made aware of the procedure for reporting security incidents, threats or malfunctions that may have an impact on the security of State information. ***Users must not attempt to prove a suspected weakness unless specifically authorized by the agency to do so.***

Note: Access authorization for user accounts involved in a compromise may be suspended during the time when a suspected violation is under investigation.

Section 5. Physical and Environmental Security

Physical Security Perimeter

Agencies will perform a periodic threat and risk assessment to determine the security risks to facilities that contain State information, and implement reasonable and appropriate hardening measures to prevent and detect unauthorized access, theft, damage or interference.

Based on the threat and risk assessment, a multi-layered physical security perimeter must be established in agency environments where information or information assets are stored or where operational data centers, network wiring closets, or telephony connection equipment exists, or where printers that print confidential or sensitive information may be printed, and any other location where information may be in use or stored, such as file cabinets, microfiche storage areas, etc. The security layers create a security perimeter that would require multiple methods of access control to gain entry. These layers could be in the form of an entry point with card key access, a staffed reception area, a locked cabinet or office, or other physical barrier.

To detect and prevent unauthorized access attempts in areas within facilities that house sensitive or confidential information, where possible, agencies must utilize physical access controls designed to permit access by authorized users only that identify, authenticate and monitor all access attempts to restricted areas within agency facilities.

Asset Security

Computer assets must be physically protected from physical and environmental hazards to reduce the risk of unauthorized access to information and to protect against loss or damage. Special controls may be necessary for electrical supply and uninterruptible power, fire protection and suppression, air and humidity controls, and cabling infrastructure in data centers, wiring closets, server rooms, and storage facilities where computers and computer peripherals are stored.

Secure Disposal or Re-use of Storage Media and Equipment

Disclosure of sensitive information through careless disposal or re-use of equipment presents a risk to the State of Nebraska. Formal procedures must be established to minimize this risk. Storage devices such as hard disk drives, paper or other storage media (e.g. tape, diskette, CDs, DVDs, USB drives, cell phones, memory sticks, digital copiers/printers/scanners with data storage capabilities) regardless of physical form or format containing sensitive information (Refer to [Section 6 Asset Classification](#)) must be physically destroyed or securely overwritten when the data contained on the device is no longer required under the provisions of the Records Management Act.

Clear Screen

To prevent unauthorized access to information, agencies will implement automated techniques or controls to require authentication or re-authentication after a predetermined period of inactivity for desktops, laptops, PDA's and any other computer systems where authentication is required. These controls may include such techniques as password protected screen savers, automated logoff processes, or re-authentication after a set time out period.

Section 6. Asset Classification

Data is a critical asset of the State of Nebraska. All staff have a responsibility to protect the confidentiality, integrity, and availability of data generated, accessed, modified, transmitted, stored or used by the State of Nebraska, irrespective of the medium on which the data resides and regardless of format (such as in electronic, paper or other physical form).

Agencies are responsible for establishing and implementing appropriate managerial, operational, physical, and technical controls for access to, use of, handling of, transmission of, and disposal of State data in compliance with this policy and the agency Records Retention schedule. The agency data owner should carefully evaluate and determine the appropriate data sensitivity or classification category for their information. Assigning classifications determines day-to-day practices with information: how it is handled, who handles it, how it is transported, stored, who has access, where it can go, etc.

Data owned, used, created or maintained by the State is classified into the following four categories:

- Public
- Internal Use Only
- Confidential
- Highly Restricted

(See [NITC Security Officer Handbook](#))

Section 7. Access Control

To preserve the confidentiality, integrity and availability, state information assets must be protected by logical and physical access control mechanisms.

Logon Banner

Logon banners must be implemented on all workstations, servers and laptops to inform users that the system is for official agency use, or other approved use consistent with agency policy, and that user activities may be monitored, and the user should have no expectation of privacy. Logon banners are usually presented during the authentication process.

User Account Management

A user account management process will be established and documented to identify all functions of user account management, to include the creation, distribution, modification and deletion of user accounts. Data owner(s) are responsible for determining who should have access to information and the appropriate access privileges (read, write, delete, etc.). The “Principle of Least Privilege” should be used to ensure that only authorized individuals have access to applications and information and that these users only have access to the resources required for the normal performance of their job responsibilities. (See [NITC Identity and Access Management Standard](#) and [NITC Acceptable Use Policy State Data Communication Network](#))

Agencies or data owner(s) should perform annual user reviews of access and appropriate privileges.

Privileged Accounts Management

The issuance and use of privileged accounts will be restricted and controlled. Processes must be developed to ensure that users of privileged accounts are monitored, and any suspected misuse is promptly investigated.

All individuals requiring special privileges (programmers, database administrators, network and security administrators, etc.) will have a unique privileged account (UserID) so activities can be traced to the responsible user. UserIDs must not give any indication of the user's privilege level, e.g., supervisor, manager, administrator, etc. (See [NITC Remote Administration of Internal Devices Standard](#)).

User Password Management

Passwords are a common means of authenticating a user's identity to access information systems or services. Passwords must be implemented to ensure all authorized individuals accessing agency resources follow the [NITC Password Standard](#).

Password management controls should be implemented, where technically or operationally feasible, to provide a reliable, effective method of ensuring the use of strong passwords.

Network Access Control

Access to an agency's trusted internal network must require all authorized users to authenticate themselves through the use of an individually assigned User ID and an authentication mechanism (e.g., password, token, smart card, etc.). Network controls must be developed and implemented that ensure authorized users can access only those network resources and services necessary to perform assigned job responsibilities.

User Authentication for External Connections (Remote Access Control)

In the special case where software, servers, storage devices or other computer equipment has the capability to automatically connect to a vendor (e.g. to report problems or suspected problems), the Agency Information Security Officer or designee must conduct a risk assessment prior to establishing access to ensure that connectivity does not compromise the state or other third party connections.

(See also [Section 8. Operational Management, External Connections](#) and [NITC Remote Access Standard](#))

Segregation of Networks

When the state network is connected to another network, or becomes a segment on a larger network, controls must be in place to prevent users from other connected networks access to the agency's private network. Routers or other technologies must be implemented to control access to secured resources on the trusted state network.

Detailed maps of agency physical and logical network connections should be available to the State Information Security Officer.

Operating System

Access to operating system code, services and commands must be restricted to only those individuals necessary in the normal performance of their job responsibilities.

In certain circumstances, where there is a clear business requirement or system limitation, the use of a shared UserID/password for a group of users or a specific job can be used. Approval by Agency Information Security Officer or designee must be documented in these cases. The approval process must include the State Information Security Officer. Additional compensatory controls must be implemented to ensure confidentiality and accountability is maintained (*See Section 3. Personnel Accountability and Security Awareness, Individual Accountability*).

Where technically feasible, default administrator accounts must be renamed, removed or disabled. The default passwords for these accounts must be changed if the account is retained, even if the account is renamed or disabled.

Application Access Control

Access to systems and business applications must be restricted to those individuals who have a business need to access those resources in the performance of their job responsibilities.

Monitoring System Access and Use

Activities of information systems and services must be monitored and events logged to provide a historical account of security related events. Agencies will implement appropriate audit logs to record events, exceptions and other security-relevant events. The Agency Information Security Officer or designee will regularly review logs for abuses and anomalies. Logs will be kept consistent with Record Retention schedules developed in cooperation with the State Records Administrator and agency requirements to assist in investigations and access control monitoring.

Section 8. Operational Management

All information processing facilities must have detailed documented operating instructions, management processes and formal incident management procedures authorized by agency management and protected from unauthorized access. Where an agency provides a server, application or network services to another agency, operational and management responsibilities must be coordinated by both agencies.

Network Management

The Office of the Chief Information Officer and agencies will implement a range of network controls to ensure the integrity of the data flowing across its trusted, internal network, and ensure the protection of connected services and networks. If there is a business need, additional measures to ensure the confidentiality of the data will also be implemented. The Office of the Chief Information Officer will ensure that measures are in place to mitigate any new security risks created by connecting the state network to a third party network. All direct connections to the

State network and direct connections between agencies must be authorized by the Office of the Chief Information Officer.

Where an agency has outsourced a server or application to a third party service (such as a web application), the agency must perform or have performed a security review of the outsourced environment to ensure the confidentiality, integrity, and availability of the state's information and application is maintained. For applications hosted by Nebraska.gov, the Nebraska State Records Board or designee will perform the security review on behalf of all Agencies.

Additions or changes to network configurations, including through the use of third party service providers, must be reviewed and approved through the Office of the Chief Information Officer's change management process.

Cooperation Between Organizations

The Agency Information Security Officer should maintain contact lists of both internal and external contacts and service providers. These lists should be organized to quickly facilitate security-related events and investigations and should detail the agency management staff authorized to make decisions regarding security-related events.

Membership in security-related organizations may provide valuable insight into the ongoing practices of security administration; however, the release of information regarding State security events and issues is strictly prohibited without Office of the Chief Information Officer prior approval.

Penetration Testing, Intrusion Testing, and Vulnerability Scanning

Systems that provide information through a public network, either directly or through another service that provide information externally (such as the World Wide Web), will be subjected to agency penetration testing, intrusion testing, and vulnerability scanning.

- All servers will be scanned for vulnerabilities and weaknesses by the Office of the Chief Information Officer before being installed on the State network. For both internal and external systems, scans will be performed at least annually or after any major software or configuration changes have been made, to ensure that no major vulnerabilities have been introduced. The frequency of additional scans will be determined by the agency and the data owner(s), depending on the criticality and sensitivity of the information on the system.
- All web-based applications will be scanned for vulnerabilities and weaknesses before being promoted to a production environment or after any major upgrades or changes have occurred.
- Penetration and intrusion testing will be conducted at the request of the agency or data owner(s) to determine if unauthorized access and or changes to an application can be made.

The results of the penetration and intrusion testing, and vulnerability scans will be reviewed in a timely manner by the State Information Security Officer. Any vulnerability detected

will be evaluated for risk by the agency and a mitigation plan will be created and forwarded to the State Information Security Officer. The tools used to perform these tasks will be updated periodically to ensure that recently discovered vulnerabilities are included.

Where an agency has outsourced a server, application or network services to another entity, responsibility for penetration and intrusion testing and vulnerability scanning must be coordinated by both entities.

Any penetration or intrusion testing or vulnerability scanning, other than that performed by State Information Security Officer must be conducted by individuals who are authorized by the State Information Security Officer and who have requested and received written consent from the Office of the Chief Information Officer at least 24 hours prior to any testing or scanning. Agencies authorized to perform penetration and intrusion testing or vulnerability scanning must have a process defined, tested and followed at all times to minimize the possibility of disruption. Any other attempts to perform tests or scans will be deemed an unauthorized access attempt.

External Connections

Direct connections between the State network and external networks must be implemented in accordance with the [NITC Remote Access Standard](#). Connections will be allowed only when external networks have been reviewed and found to have acceptable security controls and procedures, or appropriate security measures have been implemented to protect state resources. A risk analysis should be performed to ensure that the connection to the external network would not compromise the state's private network. Additional controls, such as the establishment of firewalls and a DMZ (demilitarized zone) may be implemented between any third party and the state. All external connections will be reviewed on an annual basis.

Third party network and/or workstation connection(s) to the state network must have an agency sponsor and a business need for the network connection. An agency non-disclosure agreement may be required to be signed by a legally authorized representative from the third party organization. In addition to the agreement, the third party's equipment must also conform to the state's security policies and standards, and be approved for connection by the Office of the Chief Information Officer.

Any connection between agency firewalls over public networks that involves sensitive information must use encryption to ensure the confidentiality and integrity of the data passing over the external network.

(See also [Section 7. Access Control, User Authentication for External Connections](#))

Portable Devices

All portable computing devices (notebooks, USB flash drives, PDA's, laptops and mobile phones) and information must be secured to prevent compromise of confidentiality or integrity. No device may store or transmit sensitive information without suitable protective measures that are approved by the agency data owner(s).

Special care must be taken to ensure that information stored on the device is not compromised. Appropriate safeguards must be in place for the physical protection, access

control, cryptographic technique, back up, virus protection, and properly connected to the State network.

Devices storing sensitive and/or critical information must not be left unattended and, where possible, must be physically locked away, or utilize special locks to secure the equipment.

Employees in the possession of portable devices must not check these devices in airline luggage systems. These devices must remain in the possession of the traveler as hand luggage unless restricted by Federal or State authorities.

Server Hardening

In order to protect State resources, agencies must remove all unnecessary software and disable services in accordance with [NITC Minimum Server Configuration Standard](#).

System Planning

Because system and data availability is a security concern, advance planning and preparation must be performed to ensure the availability of resources. Storage and memory capacity and other hardware requirements must be monitored and future requirements projected to ensure adequate processing and storage capabilities are available when needed. This information will be used to identify and avoid potential bottlenecks that might present a threat to system security or user services.

Protection against Malicious Code

Software and associated controls must be implemented across agency systems, and logs monitored, to detect and prevent the introduction of malicious code into the State environment. The introduction of malicious code such as a computer virus, worm or Trojan horse can cause serious damage to networks, workstations and state data. Users must be made aware of the dangers of malicious code. The types of controls and frequency of updating signature files, is dependent on the value and sensitivity of the information that could be potentially at risk. For workstations, virus signature files must be updated at least weekly. On host systems or servers, the signature files must be updated daily or when the virus software vendor's signature files are updated and published.

Software Maintenance

All installed software must be maintained at a vendor-supported level to ensure accuracy and integrity. Maintenance of agency-developed software must follow the State's change management process to ensure changes are authorized, tested and accepted by agency management. All known security patches must be reviewed, evaluated and appropriately applied in a timely manner as defined by the Agency.

Wireless Networks

Advances in wireless technology and pervasive devices create opportunities for new and innovative business solutions. However security risks, if not addressed correctly, could expose state information systems to a loss of service or compromise of sensitive information. Everything that is transmitted over the radio waves (wireless devices) can be

intercepted. This represents a potential security issue. Agencies shall take appropriate steps, including the implementation of encryption, user authentication, and virus protection measures, to mitigate risks to the security of State data and information systems associated with the use of wireless network access technologies in accordance with the [NITC Wireless Local Area Network Standard](#).

No wireless network or wireless access point will be installed without the written approval of the Office of the Chief Information Officer.

Communications

Security of Electronic Mail

Electronic mail provides an expedient method of creating and distributing messages both within the organization and outside of the organization. Users of the state E-mail system are a visible representative of the state and must use the system in a legal, professional and responsible manner. Users must comply with this policy, the Records Management Act, and be knowledgeable of their responsibilities as defined in [NITC Secure E-Mail for State Agencies](#).

Telephones and Fax Equipment

Communication outside the state telephone system for business reasons is sometimes necessary, but it can create security exposures. Employees should take care that they are not overheard when discussing sensitive or confidential matters; avoid use of any wireless or cellular phones when discussing sensitive or confidential information; and avoid leaving sensitive or confidential messages on voicemail systems. (See [Section 6. Asset Classification](#) and [NITC Use of Computer-based Fax Services by State Government Agencies](#))

Modem Usage

Connecting dial-up modems to computer systems on the state network is prohibited unless a risk assessment is performed, risks are appropriately mitigated, and the Office of the Chief Information Officer approves the request.

Section 9. System Development and Maintenance

To ensure that security is built into information systems, security requirements, including the need for rollback arrangements, must be identified during the requirements phase of a project and justified, agreed to, and documented as part of the overall business case for the system. To ensure this activity is performed, the Agency Information Security Officer or designee must be involved in all phases of the System Development Life Cycle from the requirements definition phase, through implementation and eventual application retirement.

Controls in systems and applications can be placed in many places and serve a variety of purposes. The specific control mechanisms must be documented at the application level, and included in the agency's security standards documents. The security measures that are

implemented must be based on the threat and risk assessments of the information being processed and cost/benefit analysis.

Agencies should follow the latest “best practices” in secure coding techniques as identified in NIST guidelines, OWASP principles, etc.

System Acceptance

The security requirements of new systems must be established, documented and tested prior to their acceptance and use. Agency Information Security Officer or designee will ensure that acceptance criteria are utilized for new information systems and upgrades. Acceptance testing will be performed to ensure security requirements are met prior to the system being migrated to the production environment.

Separation of Development, Test and Production Environments

Development software and testing tools can cause serious problems to the production environment if separation of these environments does not exist. Separation of the development, test and production environments is required, either on physically separate machines or separated by access controlled domains or directories. Processes must be documented and implemented to govern the transfer of software from the development environment to the production platform. Separation must also be implemented between development and test functions. Each agency must consider the use of a quality assurance environment where user acceptance testing can be conducted. The following controls must be considered:

- access to compilers, editors and other system utilities must be removed from production systems when not required; and
- logon procedures and environmental identification must be sufficiently unique for production testing and development.

Risk Assessment

Security requirements and controls must reflect the value of the information involved, and the potential damage that might result from a failure or absence of security measures. This is especially critical for Internet (Web) and other online applications. The framework for analyzing the security requirements and identifying controls to meet them is associated with a risk assessment, which must be performed by the data owner(s) and Agency management. A process must be established and implemented for each application to:

- address the business risks and develop a data classification profile to help to understand the risks;
- identify security measures based on the criticality and data sensitivity and protection requirements;
- identify and implement specific controls based on security requirements and technical architecture;
- implement a method to test the effectiveness of the security controls; and
- identify processes and standards to support changes, ongoing management and to measure compliance.

Input Data Validation

An application's input data must be validated to ensure it is correct and appropriate including the detection of data input errors. The checks that are performed on the client side must also be performed at the server to ensure data integrity. Checks will be performed on the input of business transactions, static data (names, addresses, employee numbers, etc.) and parameter tables. A process should be set up to verify and correct fields, characters, and completeness of data and range/volume limits.

Control of Internal Processing

Data that has been entered correctly can be corrupted by processing errors or through deliberate acts. Checks and balances must be incorporated into systems to prevent or stop an incorrect program from running. Application design must ensure that controls are implemented to minimize the risk of processing failures leading to a loss of data or system integrity.

Message Integrity

Message integrity must be considered for applications where there is a security requirement to protect the message or data content from unauthorized changes (e.g. electronic funds transfer, EDI transactions, etc.) Encryption techniques should be used as a means of implementing message integrity. *It should be noted that message integrity does not protect against unauthorized disclosure.*

Cryptographic Controls

Use of encryption for protection of high-risk information should be considered when other controls do not provide adequate protection. The decision to use encryption should be based on the level of risk of unauthorized access and the sensitivity of the data to be protected. Consideration must also be given to the regulations and national restrictions that may apply to the use of cryptographic techniques in different parts of the world.

Key Management

Protection of cryptographic keys is essential if cryptographic techniques are going to be used. Access to these keys must be tightly controlled to only those individuals who have a business need to access the keys. Loss of a cryptographic key would cause all information encrypted with that key to be considered at risk.

Protection of System Test Data

Test data is developed to test a comprehensive set of conditions and outcomes, including exception processing and error conditions to demonstrate accurate processing and handling of information and the stability of the software, system or application. Production data may not be used for testing unless all personally identifiable information is removed.

Once test data is developed, it must be protected and controlled for the life of the software, system or application. This protection mechanism is essential to ensuring a valid and controlled simulation with predictable outcomes.

Protection of Source Code

Access to source code libraries for both agency business applications and operating systems must be tightly controlled to ensure that only authorized individuals have access to these libraries and that access is logged to ensure all activity can be monitored.

Change Control Management

To protect information systems and services, a formal change management system must be established to enforce strict controls over changes to all information processing facilities, systems, software, or procedures. Agency management must formally authorize all changes before implementation and ensure that accurate documentation is maintained. These change control procedures will apply to agency business applications as well as systems software used to maintain operating systems, network software, hardware changes, etc.

DOCUMENT CHANGE MANAGEMENT

Requests for changes to this policy must be presented to the State Information Security Officer. If the State Information Security Officer agrees to the change, he or she will formally draft the change and have it reviewed and approved through the NITC normal policy approval process. Each Agency Information Security Officer will be responsible for communicating the approved changes to their organization.

This policy and supporting policies and standards will be reviewed at a minimum on an annual basis.

CONTACT INFORMATION

Questions concerning this policy may be directed to State Information Security Officer, or (402) 471-7031.

REPEAL

The Information Security Management Policy, Access Control Policy, Disaster Recovery Policy, and Network Security Policy, adopted on January 23, 2001, are repealed.
(http://nitc.ne.gov/tp/workgroups/security/security_policies.html.)

DEFINITIONS

Agency: State agencies, boards and commissions are collectively referred to as ‘agency’ throughout this document.

Authentication: The process to establish and prove the validity of a claimed identity.

Authenticity: This is the exchange of security information to verify the claimed identity of a communications partner.

Authorization: The granting of rights, which includes the granting of access based on an authenticated identity.

Availability: This is the ‘property’ of being operational, accessible, functional and usable upon demand by an authorized entity, e.g. a system or user

Biometrics: Refers to the use of electro-mechanical devices that measure some physical, electrical or audio characteristic of an individual and make use of that specific measurement to verify identity.

Business Risk: This is the combination of sensitivity, threat and vulnerability.

Change Management Process: A business process that ensures that no changes occur on a computing resource without having gone through a methodology to ensure that changes will perform as expected, with no unexpected repercussions.

Chief Information Officer: The Chief Information Officer is responsible for vision, strategy, direction, and oversight for Information Technology for State of Nebraska. The Chief Information Officer reports to the Governor, is a member of the Governor’s cabinet, and is a member of the Nebraska Information Technology Commission, which oversees and legislates IT standards and policy as empowered by law.

Classification: The designation given to information or a document from a defined category on the basis of its sensitivity.

Computer: All physical, electronic and other components, types and uses of computers, including but not limited to hardware, software, central processing units, electronic communications and systems, databases, memory, Internet service, information systems, laptops, Personal Digital Assistants and accompanying equipment used to support the use of computers, such as printers, fax machines and copiers, and any updates, revisions, upgrades or replacements thereto.

Confidentiality: The property that information is not made available or disclosed to unauthorized individuals, entities, or processes.

Controls: Countermeasures or safeguards that are the devices or mechanisms that are needed to meet the requirements of policy.

Critical: A condition, vulnerability or threat that could cause danger to data, a system, network, or a component thereof.

Data: Any information created, stored (in temporary or permanent form), filed, produced or reproduced, regardless of the form or media, including all records as defined by the Records Management Act.. Data may include, but is not limited to personally identifying information, reports, files, folders, memoranda, statements, examinations, transcripts, images, communications, electronic or hard copy.

Data Security: The protection of information assets from accidental or intentional but unauthorized disclosure, modification, or destruction, or the inability to process that information.

Data Owner: An individual or a group of individuals with responsibility for making classification and control decisions regarding use of information.

Denial of Service: An attack that takes up so much of the company's business resource that it results in degradation of performance or loss of access to the company's business services or resources.

Disaster: A condition in which information is unavailable, as a result of a natural or man-made occurrence, that is of sufficient duration to cause significant disruption in the accomplishment of the State of Nebraska's business objectives.

DMZ: Demilitarized zone; a semi-secured buffer or region between two networks such as between the public Internet and the trusted private State network.

Encryption: The cryptographic transformation of data to render it unintelligible through an algorithmic process using a cryptographic key.

Executive Management: The person or persons charged with the highest level of responsibility for an Agency (e.g. Agency Director, CEO, Executive Board, etc.).

External Network: The expanded use and logical connection of various local and wide area networks beyond their traditional Internet configuration that uses the standard Internet protocol, TCP/IP, to communicate and conduct E-commerce functions.

Family Educational Rights and Privacy Act (FERPA): Federal law regarding the privacy of educational information. For additional information visit: <http://www.ed.gov/policy/gen/guid/fpco/ferpa/index.html>

Firewall: A security mechanism that creates a barrier between an internal network and an external network.

Gramm-Leach-Bliley Act (GLB): Federal regulation requiring privacy standards and controls on personal information for financial institutions. For additional information visit: <http://www.ftc.gov/privacy/privacyinitiatives/glbact.html>

Guideline: An NITC document aims to streamline a particular process that Agency compliance is voluntary.

Health Insurance Portability Accountability Act (HIPAA): A Congressional act that addresses the security and privacy of health data. For additional information visit: <http://www.hhs.gov/ocr/hipaa/>

Host: A system or computer that contains business and/or operational software and/or data.

Incident: Any adverse event that threatens the confidentiality, integrity or accessibility of information resources.

Incident Response: The manual and automated procedures used to respond to reported network intrusions (real or suspected); network failures and errors; and other undesirable events.

Information: Information is defined as the representation of facts, concepts, or instructions in a formalized manner suitable for communication, interpretation, or processing by human or automated means.

Information Assets: (1) All categories of automated information, including but not limited to: records, files, and databases, and (2) information technology facilities, equipment (including microcomputer systems), and software owned or leased by the State.

Information Security: The concepts, techniques and measures used to protect information from accidental or intentional unauthorized access, modification, destruction, disclosure or temporary or permanent loss (See Availability).

Information Technology Resources: Hardware, software, and communications equipment, including, but not limited to, personal computers, mainframes, wide and local area networks, servers, mobile or portable computers, peripheral equipment, telephones, wireless communications, public safety radio services, facsimile machines, technology facilities including but not limited to, data centers, dedicated training facilities, and switching facilities, and other relevant hardware and software items as well as personnel tasked with the planning, implementation, and support of technology.

Integrity: The property that data has not been altered or destroyed from its intended form or content in an unintentional or an unauthorized manner.

Internet: A system of linked computer networks, international in scope, which facilitates data transmission and exchange, which all use the standard Internet protocol, TCP/IP, to communicate and share data with each other.

Internal Network: An internal (i.e., non-public) network that uses the same technology and protocols as the Internet.

Malicious Code: Malicious Code refers to code that is written intentionally to carry out annoying, harmful actions or use up the resources of a target computer. They sometimes masquerade as useful software or are embedded into useful programs, so that users are induced into activating them. Types of malicious code include Trojan horses and computer viruses.

Nebraska Information Technology Commission (NITC): The governing body, set forth by the State of Nebraska Legislature. See <http://www.nitc.state.ne.us/>

Penetration Testing: The portion of security testing in which evaluators attempt to exploit physical, network, system or application weaknesses to prove whether these weaknesses can be exploited by gaining extended, unauthorized or elevated privileged access to protected resources.

Personal Information: Personal information means any information concerning a person, which, because of name, number, personal mark or other identifier, can be used to identify such natural person.

Physical Security: The protection of information processing equipment from damage, destruction or theft; information processing facilities from damage, destruction or unauthorized entry; and personnel from potentially harmful situations.

Policy: An NITC document that establishes a set of consistent rules and the means of achieving them that support the business objectives for the State of Nebraska

Principle of Least Privilege: A framework that requires users be given no more access privileges (read, write, delete, update, etc.) to systems than necessary to perform their normal job functions, and those privileges be granted no longer than the time required to perform authorized tasks.

Privacy: The right of individuals and organizations to control the collection, storage, and dissemination of information about themselves.

Private Information: Private Information means personal information in combination with any one or more of the following data elements, when either the personal information or the data element is not encrypted or encrypted with an encryption key that has also been acquired:

- social security number; or
- driver's license number or non-driver identification card number; or
- account number, credit or debit card number, in combination with any required security code, access code, or password which would permit access to an individual's financial account

“Private information” does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

Privileged Account: The User ID or account of an individual whose job responsibilities require special system authorization, such as a network administrator, security administrator, etc. Special authorizations are allocated to this account such as RACF Administrator, auditor, Special, UNIX root or Microsoft Administrator, etc.

Procedures: Specific operational steps that individuals must take to achieve goals stated in this policy.

Records Officer: The agency representative from the management or professional level, as appointed by each agency head, who is responsible for the overall coordination of records management activities within the agency.

Records Management Act: The governing statute, set forth by the State of Nebraska Legislature. Neb. Rev. Stat. § 84-1201 through § 84-1228

Risk: The probability of suffering harm or loss. It refers to an action, event or a natural occurrence that could cause an undesirable outcome, resulting in a negative impact or consequence.

Risk Assessment: The process of identifying threats to information or information systems, determining the likelihood of occurrence of the threat, and identifying system vulnerabilities that could be exploited by the threat.

Risk Management: The process of taking actions to assess risks and avoid or reduce risk to acceptable levels.

Security Management: The responsibility and actions required to manage the security environment including the security policies and mechanisms.

Security Policy: The set of criteria for the provision of security services based on global rules imposed for all users. These rules usually rely on a comparison of the sensitivity of the resources being accessed and the possession of corresponding attributes of users, a group of users, or entities acting on behalf of users.

Separation of Duties: A concept that no individual should have control over two or more phases of an operation or areas of conflicting responsibility.

Sensitive Information: Disclosure or modification of this data would be in violation of law, or could harm an individual, business, or the reputation of the agency.

Sensitivity: The measurable, harmful impact resulting from disclosure, modification, or destruction of information.

Sniffer: Monitoring network traffic.

Staff: Any State of Nebraska full time and temporary employees, third party contractors and consultants who operate as employees, volunteers and other agency workers.

Standard: Sets of rules for implementing policy. Standards make specific mention of technologies, methodologies, implementation procedures and other detail factors.

State: The State of Nebraska.

State Information Security Officer: The Information Security Officer appointed by the Chief Information Officer to lead the NITC Security Architecture Workgroup. Responsibilities include creating and maintaining policies for the State of Nebraska, conducting vulnerability / penetration tests at an enterprise level, and to assist Agency Information Security Officer's.

State Network: The State of Nebraska's internal, private network, e.g. the State's 10.x.x.x address space.

State Records Administrator: The Secretary of State is the State Records Administrator. The Secretary of State establishes and administers the records management program for all state agencies.

System(s): An interconnected set of information resources under the same direct management control that shares common functionality. A system may include hardware, software, information, data, applications or communications infrastructure.

System Development Life Cycle: A software development process that includes defining the system requirements, the design specifications, the software development, installation and training, maintenance, and disposal.

Third Party: Any non-agency contractor, vendor, consultant, or external entity, etc.

Threat: A force, organization or person, which seeks to gain access to, or compromise, information. A threat can be assessed in terms of the probability of an attack. Looking at the nature of the threat, its capability and resources, one can assess it, and then determine the likelihood of occurrence, as in risk assessment.

Token: A device that operates much like a smart card but is in a physical shape that makes its use easier to manage.

Trojan Horse: Illegal code hidden in a legitimate program that when executed performs some unauthorized activity or function.

Unauthorized Access Or Privileges: Insider or outsider who gains access to network or computer resources without permission.

User: Any agency (ies), federal government entity (ies), political subdivision(s), their employees or third party contractor(s) or business associates, or any other individual(s) who are authorized by such entities to access a System for a legitimate government purpose.

Virus: A program that replicates itself on computer systems by incorporating itself into other programs that are shared among computer systems. Once in the new host, a virus may damage data in the host's memory, display unwanted messages, crash the host or, in some cases, simply lie dormant until a specified event occurs (e.g., the birth date of a historical figure).

Vulnerability: A weakness of a system or facility holding information that can be exploited to gain access or violate system integrity. Vulnerability can be assessed in terms of the means by which the attack would be successful.

Vulnerability Scanning: The portion of security testing in which evaluators attempt to identify physical, network, system or application weaknesses to discover whether these weaknesses may be exploited by persons or machines seeking to gain either unauthorized or elevated privileged access to otherwise protected resources.

World Wide Web (WWW): A hypertext-based system designed to allow access to information in such a way that the information may physically reside on locally or geographically different servers. This access was greatly improved through the introduction of a graphical interface to the World Wide Web called a web browser. Netscape and Internet Explorer are two of the most popular web browsers.

Worm: A program similar to a virus that can consume large quantities of network bandwidth and spread from one network to another.

INDEX

A

Access Control	8, 11, 12, 14, 15, 18
Accountability	8, 15
Agency Information Security Officer	6, 14, 15, 16, 20, 23, 34, 35, 36
Authentication	8, 12, 13, 14, 19
Availability	4, 6, 7, 9, 10, 12, 16, 18
Awareness	4, 34, 36

C

Change Control.....	22
CIO	9, 24
Classification	12
Clear Screen	12
Compliance.....	7
Computer Virus	See Malicious Code
Confidential	12
Confidentiality	4, 6, 7, 8, 9, 10, 12, 15, 16, 18, 24, 26
Consultants	See Staff, See Staff
Contractors	See Staff
Cryptographic Controls	22

D

Data Custodian	34
Data Owner.....	8, 12, 13, 16, 17, 18, 21, 34
Data Validation.....	21
Development Software	20
Disaster Recovery.....	36
Disposal.....	11, 12

E

Electronic Mail.....	19
Employees	See Staff, See Staff
Equipment	11
External Connections.....	17

H

Highly Restricted.....	12
------------------------	----

I

Incident Response.....	10
Information Security Policy.....	4, 5, 6, 34, 35
Integrity	4, 6, 7, 8, 9, 10, 12, 16, 18, 19, 21, 26
Internal Use Only	12
Intrusion Testing.....	16
ISO 27002	4

J

Job Responsibilities	9, 13, 14, 15
----------------------------	---------------

K

Key Management 22

L

Logon Banner 13

M

Malicious Code..... 18

Managing Compliance..... 10

Message Integrity 22

Modem Usage..... 20

Monitor Events..... 15

Monitoring.....6, 10

N

Nebraska Information Technology Commission..... See NITC

Network Management 16

NITC.....4, 5, 6, 7, 14, 23, 35

O

Objectives.....See Security Objectives

Operating System Access Control..... 15

Other Agency Workers.....See Staff, See Staff

P

Password Management..... 14

Penetration Testing..... 16

Physical Security Perimeter..... 11

Portable Devices..... 18

Principle of Least Privilege 13

Privacy.....4, 10, 13

Privilege Account Management 14

Production Environment..... 20

Public..... 12

Public Network.....8, See Internet

S

Security Administrators..... 34

Security Awareness6, 9, 36

Segregation of Networks 14

Sensitivity..... 12

Separation of Development 20

Separation of Duties 9

Sharing Information..... 7

Software Testing Tools..... 20

Source Code 22

Staff 4

State Information Security Officer6, 10, 15, 17, 23, 36

Storage Media..... 11

System Planning and Acceptance..... 20

T

Temporary Employees.....See Staff, See Staff

Test Data 22

Third Party.....5, 14, 16, 17, 36, 37
Trojan Horse.....*See* Malicious Code

U

Unauthorized Access4, 8, 11, 12, 17
Unauthorized Disclosure 22
User Account Management 13
User Training..... 9

V

Volunteers*See* Staff, *See* Staff
Vulnerability Scanning..... 16

W

Wireless.....19, 20
Wireless Access Point 19
World Wide Web..... 16
Worm.....*See* Malicious Code

ADDENDUM A

Operational and Functional Responsibilities

Data Owner: An individual or a group of individuals designated by an agency that represents the agency concerning the data the agency owns and tools the agency uses on the data. Data owners are responsible for determining who should have access to protected resources within their jurisdiction, and what those access privileges should be (read, update, etc.). Data owners also communicate to the Agency Information Security Officer the legal requirements for access and disclosure of their data. Data owners must be identified for all agency information assets and assigned responsibility for the maintenance of appropriate security measures such as assigning and maintaining asset classification and controls, managing user access to their resources, etc. Responsibility for implementing security measures may be delegated, though accountability remains with the identified owner of the asset.

Data Custodian: An individual or a group of individuals designated by the Data owner who will be responsible for maintaining and protecting the data. This role is typically filled by the IT department, and the duties include performing regular backups of the data, periodic validating the integrity of the data, restoring data from backup media, retaining records of activity, and fulfilling the requirements specified in this Security Policy and NITC standards and guidelines that pertain to information security and data protection.

Agency Information Security Officer: The Agency Information Security Officer has overall responsibility for ensuring the implementation, enhancement, monitoring and enforcement of the information security policies and standards. The Agency Information Security Officer is responsible for providing direction and leadership to the agency through the recommendation of security policies, standards, processes and education and awareness programs to ensure that appropriate safeguards are implemented, and to facilitate compliance with those policies, standards and processes. The Agency Information Security Officer is responsible for investigating all alleged information security violations. In this role, the Agency Information Security Officer will follow agency procedures for referring the investigation to other investigatory entities, including law enforcement. The agency Information Security Officer will coordinate and oversee security program activities and reporting processes in support of this policy and other security initiatives. (*For more detail, see [Addendum B, Role and Responsibilities of the Agency Information Security Officer.](#)*)

Security Administrators: When such an individual or individuals exist, the individual or individuals will work closely with the Agency Information Security Officer and support staff. Security Administrators are the staff normally responsible for administering security tools, reviewing security practices, identifying and analyzing security threats and solutions, and responding to security violations. This individual or individuals has administrative responsibility over all UserIDs and passwords and the associated processes for reviewing, logging, implementing access rights, emergency privileges, exception handling, and reporting requirements. Where a formal Security Administration function does not exist, the organization or staff responsible for the security administration functions described above will adhere to this policy.

Information Technology (IT) Management: IT management has responsibility for the data processing infrastructure and computing network which support the data owners. It is the

responsibility of IT management to support the Information Security Policy and provide resources needed to enhance and maintain a level of information security control consistent with the agency's Information Security Policy.

IT management has the following responsibilities in relation to the security of information:

- ensuring processes, policies and requirements are identified and implemented relative to security requirements defined by the agency's business;
- ensuring the proper controls of information are implemented for which the agency's business have assigned ownership responsibility, based on the agency's classification designations;
- ensuring the participation of the Agency Information Security Officer and technical staff in identifying and selecting appropriate and cost-effective security controls and procedures, and in protecting information assets;
- ensuring that appropriate security requirements for user access to automated information are defined for files, databases, and physical devices assigned to their areas of responsibility;
- ensuring that critical data and recovery plans are backed up and kept at a secured off-site storage facility and that recovery of backed-up media will work if and when needed.

NITC Technical Panel: The NITC Technical Panel, with advice from the Security Work Group, has responsibility for recommending security policies and guidelines and making available best practices to operational entities.

State Records Administrator: The State Records Administrator establishes and administers, within and for state and local agencies, (1) a records management program which will apply efficient and economical methods to the creation, utilization, maintenance, retention, preservation, and disposal of state and local records, (2) a program for the selection and preservation of essential state and local records, (3) establish and maintain a depository for the storage and service of state records, and advise, assist, and govern by rules and regulations the establishment of similar programs in local political subdivisions in the state, and (4) establish and maintain a central microfilm agency for state records and advise, assist, and govern by rules and regulations the establishment of similar programs in state agencies and local political subdivisions in the State of Nebraska. Neb. Rev. State § 84-1203

ADDENDUM B

Role and Responsibilities of the Agency Information Security Officer

The Agency Information Security Officer is responsible for performing, at a minimum, the following tasks:

- coordinate the development and implementation of information security policies, standards, procedures, and other control processes that meet the business needs of the agency;
- provide consultation on the various agency computing platforms;
- work closely with security administration or those serving in that function to ensure security measures are implemented that meet policy requirements;
- evaluate new security threats and counter measures that could affect the agency and make appropriate recommendations to the State Information Security Officer and other appropriate management to mitigate the risks;
- review and approve all external network connections to the agency's network;
- provide consultation to the agency management with regard to all information security;
- investigate and report to appropriate agency management and the State Information Security Officer according to the [NITC Incident Reporting Policy](#);
- ensure that appropriate follow-up to security violations is conducted;
- ensure appropriate information security awareness and education to all agency staff, and where appropriate third party individuals;
- be aware of laws and regulations that could affect the security controls and classification requirements of the agency's information;

The mission of the Information Security Function is to:

- develop, deploy and maintain an information security architecture that will provide security policies, mechanisms, processes, standards and procedures that meet current and future business needs of the agency;
- provide information security recommendations to the agency regarding security threats that could affect the agency's computing and business operations, and make recommendations to mitigate the risks associated with these threats;
- assist management in the implementation of security measures that meet the business needs of the agency;
- develop and implement security training and awareness programs that educate agency employees, contractors and vendors with regard to the agency's information security requirements;
- investigate and report to management breaches of security controls, and implement additional compensating controls when necessary to help ensure security safeguards are maintained;
- participate in the development, implementation and maintenance of disaster recovery processes and techniques to ensure the continuity of the agency's business and the security controls, in the event of an extended period of computing resource unavailability;

- although information security roles & responsibilities may be outsourced to third parties, it is the overall responsibility of each agency to maintain control of the security of the information that it owns.



Nebraska Information Technology Commission

STANDARDS AND GUIDELINES

Data Security Standard

Category	Security Architecture
Title	Data Security Standard
Number	

Applicability	<input checked="" type="checkbox"/> State Government Agencies <input type="checkbox"/> All.....Not Applicable <input checked="" type="checkbox"/> Excluding higher education institutionsStandard <input type="checkbox"/> State Funded Entities - All entities receiving state funding for matters covered by this documentNot Applicable <input checked="" type="checkbox"/> Other: All Public EntitiesGuideline Definitions: Standard - Adherence is required. Certain exceptions and conditions may appear in this document, all other deviations from the standard require prior approval (see Section 3.2). Guideline - Adherence is voluntary.
---------------	--

Status	<input type="checkbox"/> Adopted <input type="checkbox"/> Draft <input type="checkbox"/> Other: _____
Dates	Date: 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

It is the responsibility of all State of Nebraska agencies to protect all information stored in electronic form against unauthorized access.

2.0 Purpose and Objectives

In the normal course of business operations information is gathered, stored and transmitted in electronic form. This information is normally required to provide public services or to carry out other state business responsibilities. Information collected may be of a nature deemed confidential to the business process being carried out and as such not open to sharing with any other entity. Certain types of data may also be deemed personal information. It is the objective of this policy to provide safeguards to protect that information.

Common methods of protecting information include, but are not limited to:

- Staff education
- Restricted data access and usage
- Administrative policies and procedures
- Data encryption
- Network encryption
- Account authorization
- Strong passwords
- Biometric authentication
- Physical security
- Network Firewalls
- Server hardening

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.

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 (Office of the NITC, 501 S 14th Street, Lincoln, NE 68509). The NITC Technical Panel will consider the request and grant or deny the exemption. A denial of an exemption by the 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 ensuring that all information stored in an electronic manner is protected with appropriate safeguards in a manner consistent with this standard and any other applicable security policies.

Each state agency will designate a data owner for each application or system who will be responsible for assigning the data classification according to the sensitivity and criticality of the information in accordance with the NITC Security Officer Handbook, and making all decisions regarding controls, access privileges, and information management.

Each state agency is responsible for filing a Data Security Compliance Report with the Office of the CIO by October 31 of each year.

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 Data Security Compliance Report – See appendix A

5.4 NITC Data Classification Standard (<http://www.nitc.state.ne.us/standards/index.html>)

6.0 References

6.1 State of Nebraska Records Management Act (Neb. Rev. Stat. § 84-1201-1227)

6.2 National Institute Standards and Technology (NIST) Special Publication, 800-53, revision 1, "Recommended Security Controls for Federal Information Systems".

(<http://csrc.nist.gov/publications/drafts/800-53-rev1-clean-sz.pdf>).

6.3 NSA (INFOSEC) Assessment Methodology (IAM) (<http://www.iatrp.com/certclass.cfm>)

Appendix A

Data Security Standard Compliance Report for _____,
(hereafter referred to as 'Agency').

I affirm that the Agency has performed an inventory of all Agency data, classified the data in accordance with the NITC Security Officer Handbook, and have implemented appropriate safeguards to protect the data from unauthorized access or disclosure.

Agency Director

Date

Submit by October 31, 2008 to:

Office of the CIO
Attn: Steve Hartman
501 South 14th Street
Lincoln, NE 68509



Nebraska Information Technology Commission

STANDARDS AND GUIDELINES

Password Standard

Category	Security Architecture
Title	Password Standard
Number	

Applicability	<input checked="" type="checkbox"/> State Government Agencies <input type="checkbox"/> All..... Not Applicable <input checked="" type="checkbox"/> Excluding higher education institutions 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: All Public Entities Guideline Definitions: Standard - Adherence is required. Certain exceptions and conditions may appear in this document, all other deviations from the standard require prior approval (see Section 3.2) Guideline - Adherence is voluntary.
---------------	---

Status	<input type="checkbox"/> Adopted <input type="checkbox"/> Draft <input type="checkbox"/> Other: _____
Dates	Date: 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

Passwords are a primary means to control access to systems; therefore all users must select, use, and manage passwords to protect against unauthorized discovery or usage.

1.1 Password Construction

The following are the minimum password requirements for State of Nebraska passwords:

- Must contain at least eight (8) characters
 - Must not repeat any character sequentially more than two (2) times
- Must contain at least three (3) of the following four (4):
 - At least one (1) uppercase character
 - At least one (1) lowercase character
 - At least one (1) numeric character
 - At least one (1) symbol
- Must change at least every 90 days
- Can not repeat any of the passwords used during the previous 365 days.

1.2 Non-Expiring Passwords

Agencies may use non-expiring passwords for automated system accounts (e.g. backups and batch jobs) after submitting the form found in Appendix A. All non-expiring passwords should exceed the character requirements listed in Section 1.1.

2.0 Purpose and Objectives

Passwords are used to authenticate a unique User ID to a variety of State of Nebraska resources. Some of the more common uses include: user accounts, web accounts, email accounts.

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.

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; system limitation, or financial hardship. Requests may be submitted to the Office of the NITC via e-mail or letter (Office of the NITC, 501 S 14th Street, Lincoln, NE 68509). The NITC Technical Panel will consider the request and grant or deny the exemption. A denial of an exemption by the 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 ensuring that any application or system requiring the use of a password adheres to this standard.

5.0 Related Documents

5.1 NITC Information Security Policy (<http://www.nitc.state.ne.us/standards/index.html>)

5.2 Non-expiring Password Agreement (Appendix A)

Appendix A

Non-Expiring Password Agreement

This agreement describes the agreed upon policy exception and/or level of security provided by the Office of the CIO for the application known as:

To the limits dictated by the State of Nebraska and Federal laws, agency data and system owners are responsible for determining how critical and sensitive information is for their applications to insure integrity, availability, and confidentiality.

Security Classification Levels

The NITC Data Security Standard recognizes four basic levels of security classifications that are associated with varying degrees of known risks. (See NITC Security Officer Handbook for more details). They can be summarized as follows:

HIGHLY RESTRICTED is for the most sensitive information intended strictly for use within your organization and controlled by special rules to specific personnel. It is highly critical and demands the highest possible security.

CONFIDENTIAL is for less sensitive information intended for use within your organization, yet still requires a high level of security. It may be regulated for privacy considerations. (e.g. HIPAA)

INTERNAL USE ONLY is for non-sensitive information intended for use within your organization. The security is controlled, but not highly protected.

UNCLASSIFIED/ PUBLIC is for information that requires minimal security and can be handled in the public domain.

Agency Justification

The undersigned agency representative has been authorized to request a **non-expiring password** for the application and data named above with a **security classification level** of _____ and includes the following criteria as supporting justification:

* * * * *

Office of the CIO Justification

The Office of the CIO recommends **no policy exceptions** with the following justification:

Agency Representative

Date

Office of the CIO Representative

Date

NEBRASKA INFORMATION TECHNOLOGY COMMISSION STANDARDS AND GUIDELINES

DRAFT (September 6, 2007)

NITC Standards and Guidelines 04-01

Title	Email Policy for State Government Agencies
Category	Groupware
Applicability	Policy for all state government agencies, excluding higher education.

1. Policy

All state government agencies will use the email service provided by the Office of the CIO for their workers.

2. Purpose

The purpose of this policy is to provide a single email system for all state government agency workers.

3. Exemptions

An exemption to this policy may be granted by the Technical Panel of the NITC upon request by an agency.

3.1 Exemption Process

Any agency may request an exemption to this policy by submitting a "Request for Exemption" to the Technical Panel of the NITC. 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 (Office of the NITC, 501 S 14th Street, Lincoln, NE 68509). The 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.

Document Information

DRAFT VERSION DATE: September 6, 2007

HISTORY: Adopted on November 17, 1997 (by the Information Resources Cabinet). Amendments approved by the NITC on June 3, 2004 and June 14, 2005.

URL: (To be added)
