AGENDA

State Government Council
of the
Nebraska Information Technology Commission

Thursday, June 23, 2011
1:30 p.m. - 2:30 p.m.
Executive Building - Lower Level Conference Room
521 S 14th Street
Lincoln, Nebraska

AGENDA

Meeting Documents: Click the links in the agenda
or click here for all documents (27 pages).

1. Roll Call, Meeting Notice & Open Meetings Act Information

2. Public Comment

3. Approval of Minutes* - April 21, 2011

4. Revised SGC Charter*

5. Standards and Guidelines*

   - NITC 5-204: Linking a Personal Portable Computing Device to the State Email System (Revised)

6. Updates and Other Reports (as needed)

   - Microsoft
   - Hardware Support Work Group
   - Nebraska Cyber Security Conference - July 26 (Website | Brochure)
   - OCIO Lotus Notes Environment

7. Other Business

8. Agency Reports

9. Adjourn

* Denotes Action Item

(The Council 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.)

Meeting notice was posted to the NITC website and the Nebraska Public Meeting Calendar on June 2, 2011. The agenda was posted to the NITC website on June 21, 2011.

STATE GOVERNMENT COUNCIL
of the
Nebraska Information Technology Commission
Thursday, April 21, 2011, 2:30-3:30 p.m.
Executive Building - Lower Level Conference Room
521 S 14th Street, Lincoln, Nebraska
PROPOSED MINUTES

MEMBERS PRESENT:
Brenda Decker, Chief Information Officer, Chair
Beverlee Bornemeier, OCIO-Enterprise Computing Services
Glen Morton, Workers' Compensation Court
Josh Daws, Secretary of State's Office
Pat Flanagan, Private Sector
Suzy Fredrickson, Nebraska State Patrol
Lori Henkenius, Nebraska Department of Education
Eric Henrichsen, Department of Health and Human Services
Joe Kellner, Department of Roads
Mike McCrory, Alt. for Carlos Castillo, Administrative Services
Bill Miller, State Court Administrator's Office
Bob Shanahan, Department of Correctional Services
Jayne Scofield, OCIO-Network Services
Terri Slone, Department of Labor
Len Sloup, Department of Revenue
Rod Wagner, Library Commission

MEMBERS ABSENT: Dennis Burling, Dept. of Environmental Quality; Dick Clark, Policy Research Office; Mike Calvert, Legislative Fiscal Office; Keith Dey, Department of Motor Vehicles; Rex Gittins Department of Natural Resources; Dorest Harvey, Private Sector; Kelly Lammers, Department of Banking; Gerry Oligmueller, Budget Office; and Mike Overton, Crime Commission

ROLL CALL, MEETING NOTICE & OPEN MEETINGS ACT INFORMATION

Brenda Decker called the meeting to order at 2:30 p.m. There were 15 members present. A quorum existed to conduct official business. The meeting notice was posted to the NITC website and the Nebraska Public Meeting Calendar on March 28, 2011. The agenda was posted to the NITC website on April 18, 2011. The Open Meetings Act was located on the podium at the front of the room.

PUBLIC COMMENT

There was no public comment.

APPROVAL OF JANUARY 13, 2011 MINUTES

Mr. Sloup moved to approve the January 13, 2011 meeting minutes as presented. Ms. Henkenius seconded. Roll call vote: Decker-Yes, Bornemeier-Yes, Morton-Yes, Daws-Yes, Flanagan-Yes, Henkenius-Yes, Henrichsen-Yes, Kellner-Yes, McCrory-Abstained, Miller-Yes, Shanahan-Yes, Scofield-Yes, Slone-Yes, Sloup-Yes, and Wagner-Yes. Results: Yes-14, No-0, Abstained-1. Motion carried.

NASCIO STATE I.T. RECOGNITION AWARDS 2011 (external link)

NASCIO (National Association of State Chief Information Officers) annually presents awards for successful information technology initiatives and projects in state governments. This year's awards program has a submission deadline of June 1. More information is available on the link to the agenda. Members were asked to coordinate any agency submission with Rick Becker.

Ms. Fredrickson arrived to the meeting.

NITC 4-205: SOCIAL MEDIA GUIDELINES (REVISED)

After the NITC adopted the Standard & Guideline NITC 4-205: Social Media Guidelines, there was an issue about deleting posts that were considered "inappropriate". The revision is attempting to provide agencies more guidance on this issue. The proposed revised language for Item #5 under 2.8 would be read as follows:

5. *If comments are allowed on a Social Media site, it is a limited forum and comments must be related to the subject matter of the Social Media posting. Comments may be monitored and the following forms of content will not be allowed:*
    - *Comments not related to the subject matter of the particular Social Media article being commented upon;*
    - *Comments campaigning for or against the nomination or election of a candidate or the qualification, passage, or defeat of a ballot question;*
    - *Profane language or content;*
    - *Content that promotes, fosters, or perpetuates discrimination on the basis of race, creed, color, age, religion, gender, marital status, national origin, physical or mental disability or sexual orientation;*
    - *Sexual content or links to sexual content;*
    - *Solicitations of commerce;*
    - *Conduct or encouragement of illegal activity;*
    - *Information that may tend to compromise the safety or security of the public or public systems; or*
    - *Content that violates a legal ownership interest of any other party.*

    A copy of the content which is removed will be maintained in accordance with records retention policies.

The Webmasters has reviewed the standard and have endorsed the revision. If the State Government Council approves the revision today, this will go to the Technical Panel for review and recommendation to NITC for final approval.

Mr. Shanahan moved to recommend approval of the revisions to NITC 4-205: Social Media Guidelines. Ms. Slone seconded. Roll call vote: Decker-Yes, Bornemeier-Yes, Morton-Yes, Daws-Yes, Flanagan-Yes, Fredrickson-Yes, Henkenius-Yes, Henrichsen-Yes, Kellner-Yes, McCrory-Abstain, Miller-Yes, Shanahan-Yes, Scofield-Yes, Slone-Yes, Sloup-Yes, and Rod Wagner-Yes. Results: Yes-15, No-0, Abstained-1. Motion carried.

UPDATES (as needed)

Microsoft, Brenda Decker. On April 4, Microsoft opened the pilot production environment for cloud-based services called Office 365. The Office of the CIO is reviewing the State's options for moving to this environment. One issue that needs to be resolved is how to account for the first year of the three-year agreement for hosted email. The service was unavailable the first year, so Microsoft is looking at providing the State a credit for that year. The proposal is to extend the agreement for two additional years, and the State will get one half-year credit in Year 4 and one half-year credit in Year 5 for the Office 365 service. The two year extension also applies to the software enrollment for Office and Windows. However, for that part of the agreement, we are working on language that would allow each agency an option to not participate in either Year 4 or 5 if funding was not available. There were no questions.

Hardware Configuration Work Group, Steve Schafer. This work group was created to develop standard configurations for PCs and laptops in an effort to lower costs from vendors. The OCIO, working with State Purchasing, reviewed the existing PC and laptop contract used by WSCA (Western States Contracting Alliance). That contract provides similar configurations as we were considering. Nebraska subsequently signed on to this agreement and agencies can now purchase off of the WSCA contract. The State has not

committed to purchasing any specific amount. The configurations are regularly updated by WSCA and Nebraska will have input through a group that updates the configurations. Mr. Schafer provided a handout. The Office of the CIO would like to hear from agencies if the configurations don't meet their needs.

Hardware Support Work Group, Eric Henrichsen. The Work Group held their first meeting on January 18. Sirius (formerly MSI) has been assisting in gathering information from agencies to develop a list of recommendations. It is anticipated to have the recommendations available for a future council meeting.

OTHER BUSINESS

Request to Link a Personal Computing Device to the State Email System for Data Classified as "Confidential", Brad Weakly, State Information Security Officer. In March, the NITC approved the standard and guideline NITC 5-204 Linking Personal Portable Computing Device to the State Email System for Data Classified as "Internal Use Only or "Unclassified/Public". Agencies have been asking about a similar standard for data classified as "confidential." The Security Architecture Work Group is developing a standard that will be reviewed by the Council.

ActiveSync and IronPort, Brad Weakly. The Office of the CIO's next change management will include disabling ActiveSync for those users who have never used it. Only State devices and authorized personal devices will be allowed to connect through ActiveSync. Also, IronPort has been tested for identifying emails that contain Social Security numbers and credit card information. The test had a 0% false positive detection rate. When this functionality is activated, any attempt to send an email containing this information from the State system will be bounced. The sender will get an email indicating why it was bounced. It will be at least three more weeks before these features are implemented.

New State Government Council Member. Col. David Sankey has replaced Bryan Tuma at the Nebraska State Patrol and therefore is the newest member of the State Government Council. Suzi Fredrickson will continue to serve as the agency's alternate.

AGENCY REPORTS

Department of Revenue will be going through another Security Audit which will involve the Nebraska State Patrol, Health and Human Services, and the Office of the CIO. Mr. Sloup also reported that Nebraska has an electronic tax filing rate of 92% which is one of the highest rates in the country.

The Department of Health and Human Services has started their Windows 7 rollout.

Brent Hoffman reminded agencies that Nebraska.gov offers a service from GovDelivery for an automated email notification system. Price is based on the number of agencies who are part of the contract. If more agencies participate, the price will go down.

Douglas County has been added to the JUSTICE System.

The Nebraska State Patrol will be conducting periodic testing of CRISCOM (State Employee Automatic Notification System) throughout the upcoming months. The Nebraska State Patrol will receive data dumps containing employee location information from EnterpriseOne and hope to begin testing in the next two weeks. The Lincoln area facilities have been tested and proved to be very successful. The next test will occur in the Omaha area and surrounding counties. Tests will proceed throughout the remaining counties in a similar manner (Norfolk and surrounding counties, Grand Island and surrounding counties, North Platte and surrounding counties, Scottsbluff and surrounding counties). At the conclusion of all initial facility testing, periodic maintenance testing will be scheduled throughout the year.

ADJOURNMENT

Mr. Flanagan moved to adjourn. Mr. Sloup seconded. All were in favor. Motion carried.

The meeting was adjourned at 3:23 p.m.

The meeting minutes were taken by Lori Lopez Urdiales and reviewed by Rick Becker of the Office of the CIO.

Nebraska Information Technology Commission

--State Government Council Charter--

DRAFT REVISED

1. Introduction

The Nebraska Information Resources Cabinet ("IRC") was created in January 1996 by Executive Order 96-1. The IRC was re-established as the Government Council of the Nebraska Information Technology Commission (hereafter referred to as "Commission") through Executive Order 97-7 in November 1997. The Commission became a statutory body in Laws 1998, LB 924, and the Commission re-established the State Government Council (hereafter referred to as "Council").

2. Purpose

The purpose of this Charter is to clarify the role of the Council and its relationship with the Commission.

3. Authority

The Nebraska Information Technology Commission shall: "Establish ad hoc technical advisory groups to study and make recommendations on specific topics, including workgroups to establish, coordinate, and prioritize needs for education, local communities, intergovernmental data communications, and state agencies[.]" Neb. Rev. Stat. § 86-516(7).

"Information technology means computing and telecommunications systems, their supporting infrastructure, and interconnectivity used to acquire, transport, process, analyze, store, and disseminate information electronically." Neb. Rev. Stat. § 86-507

4. Commission Mission and Responsibilities

4.1 Commission Mission

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

4.2 Commission Responsibilities ~~(Neb. Rev. Stat. § 86-516)~~

~~4.2.1 Annually by July 1, adopt policies and procedures used to develop, review, and annually update a statewide technology plan;~~

~~4.2.2 Create an information technology 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 which directly utilize state-appropriated funds for information technology purposes to the process established by sections 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 workgroups to establish, coordinate, and prioritize needs for education, local communities, and state agencies;~~

~~4.2.8 By November 15 of each even-numbered year, 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;~~

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

~~4.2.11 Assist the Chief Information Officer in developing and maintaining Network Nebraska pursuant to section 86-5,100.~~

The responsibilities and duties of the Commission are codified at Neb. Rev. Stat. § 86-516.

5. Council Mission and Responsibilities

5.1 Council Mission

To provide direction and oversight for state government information technology vision, goals and policy.

5.2 Council Responsibilities

5.2.1 Establish, coordinate, and prioritize technology needs for state agencies;

5.2.2 Review and make recommendations to the Commission on requests for funds from the Government Technology Collaboration Fund;

5.2.3 Review and make recommendations to the Commission on agency technology projects requesting ~~new or additional~~ funding as part of the state budget process;

5.2.4 Assist the Commission in developing, reviewing and updating the statewide technology plan;

5.2.5 Recommend planning and project management procedures for state information technology investments;

5.2.6 Evaluate and act upon opportunities to more efficiently and effectively deliver government services through the use of information technology;

5.2.7 Recommend policies, guidelines, and standards for information technology within state government; and

5.2.8 Such other responsibilities as directed by the Commission.

6. Membership

6.1 Number of Members

The Council shall have 25 Members.

6.2 Representation

6.2.1 The agency director or his or her designee from the following agencies:

6.2.1.1 Administrative Services, Department of

6.2.1.2 Banking and Finance, Department of

6.2.1.3 Correctional Services, Department of

6.2.1.4 Crime Commission

6.2.1.5 Environmental Quality, Department of

6.2.1.6 Governor's Policy Research Office

6.2.1.7 Health and Human Services, Department of - Finance and Support

6.2.1.8 Labor, Department of

6.2.1.9 Motor Vehicles, Department of

6.2.1.10 Natural Resources, Department of

6.2.1.11 Revenue, Department of

6.2.1.12 Roads, Department of

6.2.1.13 State Patrol, Nebraska

6.2.2 Other Members

6.2.2.1 Chief Information Officer

6.2.2.2 Office of the CIO - IT Administrator, Enterprise Computing Services

6.2.2.3 Office of the CIO - IT Administator, Network Services

6.2.2.4 Education, Department of - Administrator for Education Support Services

6.2.2.5 Secretary of State

6.2.2.6 State Budget Administrator

6.2.2.7 State Court Administrator

6.2.2.8 Workers' Compensation Court Administrator

6.2.2.9 One additional representative of Non-Code state agencies, to be appointed by the Commission

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

6.2.3 Other Members - Nonvoting

6.2.3.1 Legislative Fiscal Office, Director

6.3 Alternates

Each member of the Council may designate one (1) official voting alternate. This official voting alternate shall be registered with the Office of the Chief Information Officer and, in the absence of the official member, have all the privileges as the official member on items of discussion and voting.

6.4 Member Responsibilities

A member with a potential conflict of interest in any action of the Council shall recuse himself or herself and not participate in such action. A member has a potential conflict of interest if he or she is faced with taking an official action which could result in a financial benefit or detriment to the member, an immediate family member, or a business or other private sector organization with which he or she is associated.

7. Meeting Procedures

7.1 Chair

The Chief Information Officer shall serve as the Chair of the Council.

7.2 Quorum

A quorum consists of at least 50% of the voting membership.

7.3 Voting

Issues shall be decided by a majority vote of the voting members present.

7.4 Non-Member Agencies

Attendance and input by non-member state government agencies is encouraged. The director of a non-member agency may submit to the Council the name of a contact person within his or her agency to receive notification of Council meetings.

7.5 Meeting Frequency

The Council shall meet not less than four times per year.

7.6 Notice of Meetings

~~7.6.1~~ Notice of the time and place of each meeting of the Council shall be made at least seven (7) calendar days prior to the meeting. Notice shall be published on the Council's website at http://www.nitc.~~state.ne.us~~ne.gov/.

~~7.6.2 The notice shall contain an agenda of subjects known at the time of the publicized notice or a statement that the agenda shall be readily available for public inspection at the Office of the Chief Information Officer, 501 S. 14th Street, 4th Floor, Lincoln, NE, during normal business hours by appointment.~~

7.7 Subcommittees

7.7.1 Subcommittees will be designated by vote of the Council to address specific topics.

7.7.2 Pursuant to provisions of Neb. Rev. Stat. § 84-1409(1), subcommittees of the Council shall not be required to provide notice of meetings.

Approved by the Nebraska Information Technology Commission on June 29, 1999. Amendments approved by the NITC on June 13, 2001; September 16, 2002; February 22, 2007, and June 27, 2007.

DRAFT

State of Nebraska
Nebraska Information Technology Commission
Standards and Guidelines

NITC 5-204

Title	Linking a Personal Portable Computing Device to the State Email System ~~for Data Classified as "Internal Use Only" or "Unclassified/Public"~~
Category	Groupware Architecture
Applicability	Applies to all state government agencies, excluding higher education

1. Purpose

This standard provides for the requirements to connect a personal Portable Computing Device ("PCD") to the State's email system. This standard does not apply to PCDs provided by the agency.

2. Standard

2.1 Procedures for Requesting Authority to Connect a Personal PCD to the State's Email System

2.1.1 Prior to connecting any personal PCD to the State's email system, a request must be submitted to the State Information Security Officer ("SISO") for review. ~~Attachment A is the form to be used to submit a request.~~ Attachment A is the request form to be used for data classified as “Internal Use” or “Unclassified/Public” and Attachment B is the request form to be used for data classified as “Confidential”. Completed forms should be emailed to the SISO at siso@nebraska.gov.

2.1.2 The SISO will review each request. The SISO will either approve or deny a request and communicate the decision to the requesting agency within 14 days.

2.2 Requirements

2.2.1 **Only the Native Microsoft Exchange active-sync method will be used as the syncing method for devices accessing the State email system**.2.2.2 **Password protection**: Personal smart devices must use a device password for access to the devices functionality. During the process of configuring the device for syncing to the

State's email system, the password protection setting will be automatically enabled on the device. Other security controls may be enabled by the State email system at any time.

2.2.3 **Storage of confidential information**: Appropriate safeguards must be utilized when processing or storing sensitive information. At no time shall confidential information received be transferred or stored in a system not meeting required safeguards for information control and storage.

~~**Storage of sensitive information**: Personal devices cannot be used to process or store sensitive State related information.~~

2.2.4 **Physical safeguards**: Appropriate physical security measures should be taken to prevent theft of portable devices and media. Unattended portable computing devices and media must be physically secured.

2.2.5 **Theft or Loss**:

2.2.5.1 **Reporting**: Theft or loss of portable computing devices assumed to contain sensitive information must be reported immediately to the Office of the CIO ("OCIO"). Please call the OCIO help desk at 402-471-4636 or 800-982-2468.
2.2.5.2 **Remote data delete**: All devices that are capable of native syncing to the State's email system support the remote data wipe feature. The user is required to take steps to safeguard data which should include initiating the remote wiping process in the case of theft or loss. Mobile email devices can be removed from email access or wiped using the "options/Mobile Devices" selection after logging into your Exchange email account using Outlook Web Access (OWA) at https://mail.nebraska.gov

2.2.6 **Disposal, Removal of data and Reuse**: Personal PCD users must follow the State Data Disposal and Reuse policy to properly remove data and software from the PCD before its disposal and any State and Agency policies that may be implemented must be followed. All State information contained on a device must be removed on request by the Agency Director or State Information Security Officer. Section 5 of NITC Standard 8-101 identifies base requirements for disposal and re-use. The removal of confidential information must be validated. The device may be "wiped" or cleared of all information remotely by the State without recourse and without compensation for personal data loss or the loss of service availability (including but not limited to the loss of personal contacts, music, messages, information and configuration).

~~**Disposal and Reuse**: Personal smart device users must follow the Data Disposal and Reuse policy to properly remove data and software from the PCD before its disposal or reuse.~~

2.2.7 **Support**: Personal device use is not supported by the OCIO. No State system will be reconfigured in order to make a particular device work and there is no guarantee that

a specific device will or will not work with the current system configuration. There is no obligation on the part of the State or Agency to support any personal device.

2.2.8 ~~2.2.8~~ **Liability**: The owner of the PCD is potentially liable for all criminal and civil penalties due to loss, theft or misuse of the confidential information accessed and stored on the personal device. The owner of the PCD may also be held liable for cost incurred by the State due to loss, theft, or misuse of confidential information accessed and stored on the personal device.**~~Removal of Data~~**: ~~All State information contained on a device must be removed on request by the Agency Director or State Information Security Officer. The device may be "wiped" or cleared of all information remotely by the State without recourse and without compensation for personal data loss (including but not limited to loss of personal contacts, music, messages and service unavailability).~~

2.2.9 **Encryption**: All reasonable attempts must be made to encrypt all confidential information stored on the device. Encryption must be enabled for primary and secondary storage of confidential data if the device includes that functionality.

2.2.10 All information must be protected to the extent required based on applicable State and Federal laws and regulations, and agency policies.

2.2.11 No "jail broken" or devices modified beyond manufacturers expectations will be used to process or store sensitive information.

3. Definitions

3.1 Portable Computing Device (PCD) includes but is not limited to notebook computers; tablet PCs; handheld devices such as Portable Digital Assistants (PDAs), Palm Pilots, Microsoft Pocket PCs, RIM (Blackberry); smart phones; and converged devices.

4. Related Documents

4.1 Acceptable Use Policy (NITC 7-101)

4.2 Information Security Policy (NITC 8-101) (See Secure Disposal or Re-use of Storage Media and Equipment, Section 5; and Asset Classification, Section 6)

4.3 Data Security Standard (NITC 8-102)

Attachment A: FORM: Request to Link a Personal Portable Computing Device to the State Email System for Data Classified as "Internal Use Only" or "Unclassified/Public" ~~Request Form~~ (Word Document)

Attachment B: FORM: Request to Link a Personal Portable Computing Device to the State Email System for Data Classified as "Confidential" (Word Document)

HISTORY: Adopted on March 1, 2011. DRAFT REVISED on May 13, 2011.
PDF FORMAT:

FORM: Request to Link a Personal Portable Computing Device to the State Email System for Data Classified as "Internal Use Only" or "Unclassified/Public"

This is a request to use a personal portable computing device for the purpose of linking the device to the State's email system. The following State exchange email account will be used in conjunction with the access:

Exchange Account: _____

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 8-RD-01: NITC Security Officer Instruction Guide http://nitc.ne.gov/standards/security/so_guide.pdf). 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. Not allowed on personal devices.

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) Do not use this form. ~~Contact the State Information Security Officer.~~Use Attachment B NITC Standard 5-204

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

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

Standards:
All devices irrespective of device ownership that are syncing information with the State's email system must follow the standards listed in NITC Standard 5-204: http://nitc.ne.gov/standards/5-204.html~~these standards:~~

~~1. **Only the Native Microsoft Exchange active-sync method will be used as the syncing method for devices accessing the State email system.**~~

~~2. **Password protection:** Personal smart devices must use a device password for access to the devices functionality. During the process of configuring the device for syncing to the State's email system, the password protection setting will be automatically enabled on the device. Other security controls may be enabled by the State email system at any time.~~

~~3. **Storage of sensitive information**: Personal devices cannot be used to process or store sensitive State related information.~~

~~4. **Physical safeguards**: Appropriate physical security measures should be taken to prevent theft of portable devices and media. Unattended portable computing devices and media must be~~

physically secured.

5. **Theft or Loss:**
   a. **Reporting:** Theft or loss of *portable computing devices* assumed to contain *sensitive* information must be reported immediately to the Office of the CIO. Please call the OCIO help desk at 402-471-4636 or 800-982-2468.
   b. **Remote data delete:** All devices that are capable of native syncing to the State's email system support the remote data wipe feature. The user is required to take steps to safeguard data which should include initiating the remote wiping process in the case of theft or loss. Mobile email devices can be removed from email access or wiped using the "options/Mobile Devices" selection after logging into your Exchange email account using Outlook Web Access (OWA) at https://mail.nebraska.gov

6. **Disposal and Reuse**: Personal smart device users must follow the Data Disposal and Reuse policy to properly remove data and software from the device before its disposal or reuse. Section 5 of NITC standard 8-101 identifies requirements for disposal and re-use.

7. **Support**: Personal device use is not supported by the State help desk or email team. No State system will be reconfigured in order to make a particular device work and there is no guarantee that a specific device will or will not work with the current system configuration. There is no obligation on the part of the State or Agency to support any personal device.

8. **Removal of Data**: All State information contained on a device must be removed on request by the Agency Director or State Information Security Officer. The device may be "wiped" or cleared of all information remotely by the State without recourse and without compensation for personal data loss (including but not limited to loss of personal contacts, music, messages and service unavailability).

Recommendations:

- Federal and commercial privacy and security safeguards may not allow personal devices to contain certain types of information.
- Periodically delete unnecessary data and email
- If available, the device should employ a data delete function to wipe information from the device after multiple incorrect passwords/PINs have been entered.
- If available, enable device encryption functionality to encrypt local storage.
- Turn off Bluetooth and Wi-Fi connectivity when not specifically in use.
- Limit the use of 3rd party device applications. Unsigned third-party applications pose a significant risk to information contained on the device.
- Store devices in a secure location or keep physical possession at all times
- Carry devices as hand luggage when traveling
- It is recommended that remote tracking capabilities are enable on devices
- Approved wireless transmission protocols and encryption must be used when transmitting *sensitive* information. *Sensitive* data traveling to and from the device must be encrypted during transmission. For browser based access, SSL encryption meets State standards.
- Approved remote access services and protocols must be used when connecting to State equipment. See Remote Access Standard: http://nitc.state.ne.us/standards/security/Remote_Access_Standard_v4_20070222.pdf.

Identified NITC policies that apply to use, access and protecting information:

7-101 Acceptable Use Policy http://nitc.ne.gov/standards/7-101.html

8-101 Information Security Policy http://nitc.ne.gov/standards/security/8-101.pdf

- Data Disposal and re-use: Section 5 page 11.

- Asset Classification: Section 6.

8-102 Data Security Standard Policy

http://nitc.ne.gov/standards/security/Data_Security_Standard_20070918.pdf

As a reminder: All employees are obligated to protect the data they have access to. The use of the device must conform to all State and Agency use policies.

Violations of policy can result in disciplinary action, up to and including termination.

Individual Justification

The undersigned State representative is requesting to use a personal device for the purpose of accessing and/or storing data with a **security classification level** of UNCLASSIFIED/PUBLIC or INTERNAL USE ONLY and includes the following as supporting justification:

_____

_____

_____ _____

Individual Date

_____ _____

Agency Director Date

Send completed form to the State Information Security Officer at siso@nebraska.gov.

_____ Approved _____ Denied

_____ _____

State Information Security Officer Date

FORM: Request to Link a Personal Portable Computing Device to the State Email System for Data Classified as "Confidential"

This is a request to use a personal portable computing device ("PCD") for the purpose of linking the device to the State's email system. The following State exchange email account will be used in conjunction with the access:

Exchange Account: _____

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 8-RD-01: NITC Security Officer Instruction Guide http://nitc.ne.gov/standards/security/so_guide.pdf). 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 (e.g. PHI, FTI). Not allowed on personal devices.

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. PII, FISMA, NIST 800-53). All information must be protected to the standards required. Use this form.

INTERNAL USE ONLY is for non-sensitive information intended for use within your organization. The security is controlled, but not highly protected. Use Attachment A NITC Standard 5-204.

UNCLASSIFIED/ PUBLIC is for information that requires minimal security and can be handled in the public domain. Use Attachment A NITC Standard 5-204.

Standards:
All devices irrespective of device ownership that are syncing information with the State's email system must follow the standards listed in NITC Standard 5-204: http://nitc.ne.gov/standards/5-204.html

Recommendations:

- The Office of the CIO does not recommend using personal devices to process and store sensitive information.
- Federal and commercial privacy and security safeguards may not allow personal devices to contain certain types of information.
- Periodically delete unnecessary data and email
- If available, PCD users should employ a data delete function to delete information on a device that detects a password attack
- If available, arrange for a remote data deletion service which can remotely delete sensitive information if the device is lost or stolen
- Store PCDs in a secure location or keep physical possession at all times

- Be alert and report unauthorized or suspicious activity to the Nebraska State Patrol immediately
- Do not leave equipment and media taken off the premises unattended in public places.
- Carry PCDs as hand luggage when traveling
- Tracking**:** It is recommended that devices use remote tracking capabilities
- Approved wireless transmission protocols and encryption must be used when transmitting *sensitive* information. *Confidential* data traveling to and from the PCD must be encrypted during transmission.
- Approved remote access services and protocols must be used when transmitting *sensitive* information. See Remote Access Standard: http://nitc.state.ne.us/standards/security/Remote_Access_Standard_v4_20070222.pdf.
- All State and Agency policies governing the use of confidential data are required to be followed.

Identified NITC policies that apply to use, access and protecting information:

7-101 Acceptable Use Policy http://nitc.ne.gov/standards/7-101.html

8-101 Information Security Policy http://nitc.ne.gov/standards/security/8-101.pdf

- Data Disposal and re-use: Section 5 page 11.
- Asset Classification: Section 6.

8-102 Data Security Standard Policy

http://nitc.ne.gov/standards/security/Data_Security_Standard_20070918.pdf

As a reminder: All employees are obligated to protect the data they have access to. The use of the device must conform to all State and Agency use policies.

Violations of policy can result in disciplinary action, up to and including termination.

Individual Justification

The undersigned State representative is requesting to use a personal device for the purpose of accessing and/or storing data with a **security classification level** of CONFIDENTIAL USE ONLY and includes the following as supporting justification:

_____

_____

_____

My signature below identifies I have read and understand the policy requirements and agree to abide by policy to protect the data contained or accessed by the personal device. I acknowledge the risk and accept responsibility for safeguarding the State and the Agency information that is accessed and stored by the personal device.

_____ _____

Individual Date

Agency Director's initials required: _____

This is a high-risk activity not recommended by the State with potential civil and criminal liability and penalties. The State does not endorse the use of personal devices for the processing or storage of confidential information. Allowing this activity significantly increases the possibility of unwanted information disclosure. I acknowledge the risk and accept responsibility for safeguarding the State and the Agency information that is accessed and stored by the personal device.

The Agency Director's signature below identifies the acceptance of increased risk to the agency due to the use of the personal device while also acknowledging possible civil or criminal penalties against the agency or individual from confidential information disclosure.

_____ _____

Agency Director Date

Send completed form to the State Information Security Officer at siso@nebraska.gov.

_____ Approved _____ Denied

_____ _____

State Information Security Officer Date

_____ _____

State CIO Date

Continuing Education

SUMMER 2011

NEBRASKA CYBER SECURITY CONFERENCE

Tuesday, July 26, 2011

SCC Continuing Education Center
301 S. 68th St. Place
Lincoln, NE

The Nebraska Cyber Security Conference is for security administrators and IT professionals including:

- Network Administrators
- System Administrators
- Information Security Professionals

This conference is a partnership between
Southeast Community College and the state of Nebraska.

NEBRASKA
CYBER SECURITY CONFERENCE

In today's world, we rely on technology and the Internet for a variety of transactions, communication and information – at home, in school and at the work place. While we are familiar with the myriad of conveniences provided through Internet use, it is difficult to stay abreast of all the changes and the potential risks presented by the Internet. We are all "virtual neighbors" in cyberspace, and what we do – or don't do – can affect many others.

The Nebraska Cyber Security Conference will assist in raising our awareness of cyber security and help in protecting all of us in cyberspace. If we do our part individually, we can have a tremendous positive impact collectively on our state's cyber security.

This will be valuable time learning from skilled industry experts, including keynote presenter David Hemsath. The day will be filled with a variety of breakout sessions that will encompass different areas of information security and technology.

For more information:
its.ne.gov/cybersecurity/conference

Tuesday, July 26, 2011

SCC Continuing Education Center
301 S. 68th St. Place • Lincoln, NE

8 a.m. - 4 p.m. • $99

Space is limited. • Registration deadline: July 18, 2011

CONFERENCE AGENDA

8 a.m. ....Check-in

8:30 a.m. ....Welcome
Brenda Decker
Chief Information Officer
State of Nebraska

9 a.m. ....Current Attack Vectors Workshop (9-11:30 a.m.) & 1st Breakout Session

10 a.m. ....Break

10:30 a.m. ....2nd Breakout Session

11:30 a.m. ....Lunch

12:30 p.m. ....Keynote
David Hemsath
IBM Security Tiger Team
Cyber Security for Executives

1:30 p.m. ....Wireless & Mobile Attack Vectors Workshop (1:30-4 p.m.) & 3rd Breakout Session

2:30 p.m. ....Break

3 p.m. ....4th Breakout Session

Southeast community college

BREAKOUT SESSIONS

1ST SESSION - 9 A.M.

Please note on registration form which session you would like to attend.
NOTE: Morning breakout sessions last one hour; workshop lasts 2½ hours.

- ***Migrating to IPv6 - Allen Kluender, Cisco***
  An overview of IPv6 and strategies for migrating to IPv6 in the campus.

- ***How the SANS 20 Critical Security Controls Can Help Your Organization - Brandon Harms, Infogressive***
  Who are the attackers, what are they attacking, and what can I do to stop them? Checking the box for compliance with regulatory mandates looks great on paper, but lacks the thoroughness to detect, respond, and ultimately prevent real-world cyber attacks. This prioritized baseline of information security measures and controls created by federal and civilian experts for our national security should be the highest priority for information security decision makers in any environment.

- ***Current Attack Vectors: More Mobile Than Ever... - Ernest Staats***
  (9-11:30 a.m. workshop)
  Target Audience: Basic to Intermediate Security Experience
  A practical look at some of the recently identified threats IT Security Professionals and typical users face on a daily basis. We will take an "everyman's" approach in discussing some of the recent attack vectors along with a demo of some current attack vectors. We will be specifically looking at mobile devices.

2ND SESSION - 10:30 A.M.

Please note on registration form which session you would like to attend.

- ***Best Practices for Mobile Device Security & Management - Bob Beken & Jill Klein, Sirius***
  Mobile device usage in the enterprise is exploding, and more organizations than ever before are facing the challenge of how to manage and secure mobile devices in their corporate environments. The demands of end users and the needs of protecting networks and data often seem insurmountable – where do you begin? We'll discuss the Best Practices and potential solutions to better support the increasing number of mobile workers and applications, yet ensure the security and compliance that your business requires.

- ***Security in a Virtual World – John McCreary & Dave Lipowsky, Juniper***
  Learn about the unique aspects of securing virtual networks, including ways to take advantage of the lower operating and management costs of the new virtualized data center without sacrificing security, performance, or availability.

3RD SESSION - 1:30 P.M.

Please note on registration form which session you would like to attend.
NOTE: Afternoon breakout sessions last one hour; workshop lasts 2½ hours.

- ***Identity and Access Assurance Solution - David Hemsath, IBM***
  Identity and Access Assurance provides identity management, access management, and user activity auditing. It centralizes and automates the management of users, identification and authentication, authorization and audit. As part of a holistic set of testable, repeatable and automated controls, this solution helps organizations to:
  - Know who is coming into their systems,
  - Know what they are doing, and
  - Be able to prove it to their internal auditors and external regulators.

- ***Botnets: Modern Malware Madness - Tristan Lawson, Infogressive***
  A technical breakdown of how modern botnets gain access to your organization, how they spread and what you can do about it.

- ***Wireless and Mobile Attack Vectors - Ernest Staats***
  (1:30-4 p.m. workshop)
  Target Audience: Basic to Intermediate Security Experience
  Prerequisites/Requirements: Participants need to have an understanding of Network Administration, TCP/IP, and a willingness to use command line utilities.
  A laptop/netbook that can boot to USB or DVD is required.
  The hands-on security workshop will focus on some of the current attack vectors. We will specifically focus on wireless and mobile security vulnerabilities. We will be looking at how information can be stolen through wireless connections and what can be done with mobile devices on the network. We will be using open source or free products to scan and test our systems. We also will go over some ways to fix the security issues that can be fixed.

4TH SESSION - 3 P.M.

Please note on registration form which session you would like to attend.

- ***Securing the Mobile Workforce - Joshua Foltz, Fishnet***
  We will discuss Mobile Device Management and Protection in the mobile workforce, threats to organizations introduced by mobile technologies focusing on challenges and provide steps for securing a mobile environment.

- ***Overview of Network Security - Art Martinez, Cisco***
  This session will focus on the fundamental aspects of computer security and present aspects of perimeter security, secure connectivity and intrusion detection.

KEYNOTE PRESENTATION

Cyber Security for Executives

The world is becoming more instrumented, interconnected and intelligent. This is enabling tremendous efficiency and innovation, but it also is raising security and privacy concerns within the public and private sectors. Organizations care about two things with respect to security: ensuring the continuity of their operations and protecting their sensitive/critical assets. IBM Senior Technical Staff Member, Dave Hemsath, a security and privacy architect in IBM Security Solutions, will:

- Discuss external and internal threats,
- Introduce a security framework rooted in best practices and standards, and
- Discuss developing testable, repeatable and automated controls to assess, mitigate and manage risks.

Presenter: Dave Hemsath joined IBM in 1979 after receiving a Bachelor of Science degree in Computer Engineering from the University of Nebraska-Lincoln.

He has held a variety of technical and management positions in IBM, including z/VM development, Document Imaging and Management Solutions, Distributed Computing Environment for mainframes, Kerberos systems manager, security architecture, security standards and security strategy. He was IBM's representative to The Open Group's Security Program Group, the IETF Kerberos Working Group and led the initial security work in the Continua Health Alliance.

He is a security and privacy architect in IBM's Security Tiger Team, focusing on the health care and energy and utilities sectors. He is a Certified Information Systems Security Professional and an Information Systems Security Architecture Professional. He's also a Certified Professional for Healthcare and Information Management Systems. He is a Senior Member of the Association for Computing Machines, a Senior Member of the Institute for Electrical and Electronic Engineers, and a member of the Information Systems Security Association.

REGISTRATION DEADLINE

Space is limited. Please submit your registration by **5 p.m. July 18.**

LODGING INFORMATION

Lincoln Convention and Visitors Bureau
(402) 434-5348 • (800) 423-8212
www.lincoln.org/visiting/lodging

ADDITIONAL INFORMATION

WIFI is available.

** **Cancellation/Refund Policy:** You must call the Continuing Education office at 402-437-2700 or 800-828-0072 the day before the workshop begins to receive 100% refund. If you call the day of the workshop or after it has started, no refund will be issued.

MORE INFORMATION

Marguerite Himmelberg
Southeast Community College
Continuing Education
(402) 323-3388
(800) 828-0072, ext. 3388
mhimmelberg@southeast.edu
or
Brad Weakly
Office of the CIO
(402) 471-3677
brad.weakly@nebraska.gov

How to Register

1. Complete the non-credit registration form contained in this brochure. **Please print or type information on the registration form.**

NOTE for State of Nebraska Employees: Please register at CyberCon.Nebraska.gov

2. SEND the form with payment: **Check** payable to SCC, or **credit card** number (Mastercard, American Express, Discover or Visa) or a **letter of authorization on company letterhead** if your employer is paying the tuition.

MAIL TO:
SCC-Continuing Education Center
301 S. 68th Street Place
Lincoln, NE 68510

FAX TO: 402-437-2703

Confirmations are not mailed.

REGISTRATION FORM - NON-CREDIT COURSE

Southeast community college

Complete this form and send with payment to: **SCC, Continuing Education Center, 301 S. 68th Street Place, Lincoln, NE 68510 or FAX completed form to (402) 437-2703**. *Include payment or Letter of Authorization (required for third-party billing).*

The College requires a student's Social Security number as a condition for enrollment. A student's Social Security number information constitutes an "educational record" under the Family Educational Rights and Privacy Act (FERPA). The College will be privileged to redisclose that information only with the consent of the student or in those very limited circumstances when consent is not required by FERPA.

PLEASE PRINT

2011 QUARTER
__X__summer____winter
____fall ____spring

Social Security Number	Name: Last First Middle Initial			E-mail address	
Residence Mailing Address		City	State	Zip	County #
Race: (Used for statistical purposes only) ❑ Asian ❑ Other _____ ❑ White, Non-Hispanic ❑ Hispanic/Latino(a) ❑ Hawaiian/Pacific Islander ❑ Black/African-American, Non-Hispanic ❑ American/Alaska Native	❑ Resident of Nebraska ❑ Non-Resident of Nebraska Veteran or Dependent Utilizing Military Benefits ❑ Yes ❑ No	Birth Date / / Gender: ❑ Male ❑ Female	Business Phone Employer	Home Phone	Cell Phone

Nebraska Cyber Security Conference

Tuesday, July 26, 2011
Southeast Community College
Continuing Education Center
301 S. 68th St. Place
Lincoln, NE
8 a.m. - 4 p.m. • $99
INFO-6240-CEUA

CHECK ONE TOPIC IN EACH SESSION YOU WANT TO ATTEND

❑ I would like a vegetarian entree for lunch.

Break-out Session #1 • 9 a.m.
- ❑ Migrating to IPv6
- ❑ How the SANS 20 Critical Security Controls Can Help Your Organization
- ❑ **Current Attack Vectors: More Mobile Than Ever.. 9-11:30 a.m.**

Break-out Session #2 • 10:30 a.m.
- ❑ Best Practices for Mobile Devices Security & Management
- ❑ Security in a Virtual World

Break-out Session #3 • 1:30 p.m.
- ❑ Identity & Access Assurance Solution
- ❑ Botnets: Modern Malware Madness
- ❑ **Wireless & Mobile Attack Vectors • 1:30-4 p.m.**
  - Limited to 35 participants
  - Laptop/netbook that can boot to USB or DVD required

Break-out Session #4 • 3 p.m.
- ❑ Securing the Mobile Workforce
- ❑ Overview of Network Security

Signature _____

❑Check ❑Cash ❑Mastercard ❑AMEX ❑Discover ❑VISA V Code _____

Name as it appears on card: _____

Exp.Date _____ Credit card # _____

Billing agency (*INCLUDE LETTER OF AUTHORIZATION ON COMPANY LETTERHEAD*)

TOTAL DUE

For Office Use Only:

DE _____ ID# _____

Submission of this form indicates that I understand: 1) that my registration is complete and that I am accountable for the tuition and fees and subject to a grade in the courses listed; 2) that should I officially drop, cancel, or withdraw, any refund in tuition will be determined by the date I submit my request to Continuing Education; 3) that failure to attend a course does not constitute an official drop/withdrawal; 4) the personal information contained herein is correct as shown; and 5) any changes in SSN, legal name, address, residency, etc. must follow the College procedures in the Student Handbook and College Catalog. It is the policy of SCC to provide equal opportunity and nondiscrimination in all admission, attendance, and employment matters to all persons without regard to race, color, religion, sex, age, marital status, national origin, ethnicity, veteran status, sexual orientation, disability, or other factors prohibited by law or College policy. Inquiries concerning the application of SCC's policies on equal opportunity and nondiscrimination should be directed to the Vice President for Access/Equity/Diversity, SCC Area Office, 301 S. 68th Street Place, Lincoln,NE 68510, 402-323-3412, FAX 402-323-3420, or jsoto@southeast.edu.

MH