MEETING AGENDA

Technical Panel
of the
Nebraska Information Technology Commission

Tuesday, June 14, 2011
9:00 a.m.
Varner Hall - Board Room
3835 Holdrege St., Lincoln, Nebraska

NOTE: Due to road construction on Holdrege Street please use these alternate directions to Varner Hall.

AGENDA

Meeting Documents: Click the links in the agenda
or click here for all documents (22 pages).

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

2. Public Comment

3. Approval of Minutes* - May 10, 2011

4. Enterprise Projects

   - Project Updates
     - Access Nebraska - Karen Heng
     - Talent Management System - Mike McCrory and Steve Sulek

5. Standards and Guidelines

   - Recommendations to the NITC*
     - NITC 4-205: Social Media Guidelines (Revised)
       - Comments Received (None)
       - State Government Council Recommendation: Approve
     - NITC 5-204: Linking a Personal Portable Computing Device to the State Email System (Revised)
       - Comments Received (None)

6. Lincoln Public Schools Disaster Recovery Efforts

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

   - Accessibility of Information Technology Work Group - Christy Horn
   - Learning Management System Standards Work Group - Kirk Langer
   - Security Architecture Work Group - Brad Weakly
   - Discussion: New Work Group for Intergovernmental Data Communications

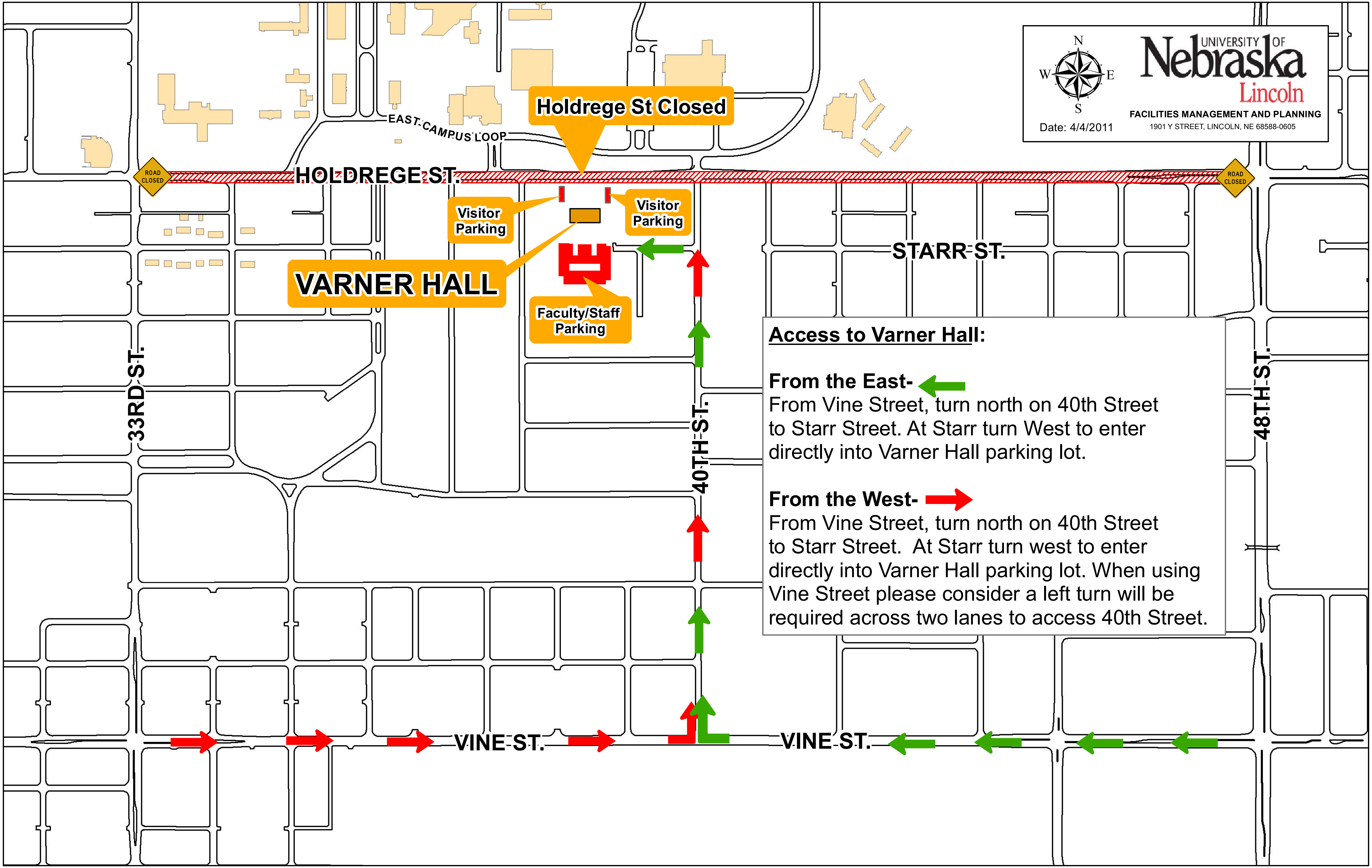
8. Other Business

9. Adjourn

* Denotes Action Item

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

NITC and Technical Panel websites: http://nitc.ne.gov/
Meeting notice was posted to the NITC website and Nebraska Public Meeting Calendar on May 13, 2011.
The agenda was posted to the NITC website on June 10, 2011.



University of Nebraska Lincoln
FACILITIES MANAGEMENT AND PLANNING
1901 Y STREET, LINCOLN, NE 68588-0605
Date: 4/4/2011

Access to Varner Hall:

From the East- ←

From Vine Street, turn north on 40th Street to Starr Street. At Starr turn West to enter directly into Varner Hall parking lot.

From the West- →

From Vine Street, turn north on 40th Street to Starr Street. At Starr turn west to enter directly into Varner Hall parking lot. When using Vine Street please consider a left turn will be required across two lanes to access 40th Street.

TECHNICAL PANEL
Nebraska Information Technology Commission
Tuesday, May 10, 2011, 9:00 a.m.
Varner Hall - Board Room
3835 Holdrege St., Lincoln, Nebraska
PROPOSED MINUTES

MEMBERS PRESENT:

Walter Weir, CIO, University of Nebraska, Chair
Brenda Decker, CIO, State of Nebraska
Christy Horn, University of Nebraska
Kirk Langer, Lincoln Public Schools
Michael Winkle, NET

ROLL CALL, MEETING NOTICE & OPEN MEETINGS ACT INFORMATION

Mr. Weir called the meeting to order at 9:05 a.m. There were four members present at the time of roll call. A quorum existed to conduct official business. The meeting notice was posted to the NITC website and Nebraska Public Meeting Calendar on April 18, 2011. The agenda was posted to the NITC website on May 6, 2011. A copy of the Open Meetings Act was posted on the South wall of the meeting room.

PUBLIC COMMENT

There was no public comment.

APPROVAL OF APRIL 12, 2011 MINUTES

Mr. Winkle moved approval of the April 12, 2011 minutes as presented. Mr. Langer seconded. Roll call vote: Decker-Abstained, Langer-Yes, Weir-Yes, and Winkle-Yes. Results: Yes-3, No-0, Abstained-1. Motion carried.

ENTERPRISE PROJECTS

Project Status Dashboard - Skip Philson

The Fusion Project report was not submitted. All projects appear to be on schedule. There are some concerns from the Public Safety Interoperability Project but these are variables that are out of the project's control. Members discussed the status of the MMIS Project.

Christy Horn arrived to the meeting.

Mr. Philson has been receiving feedback from agencies that the 5-page report form is time consuming. He would like to propose that agencies complete the 5-page for the first initial report and to develop a shorter form for project updates. The Technical Panel asked that a draft of the proposed report form be an agenda item for the next meeting.

STANDARDS AND GUIDELINES (SET FOR 30-DAY COMMENT PERIOD), NITC 4-205: SOCIAL MEDIA GUIDELINES (REVISED)

> Purpose: The purpose of this document is to provide guidelines for the use of social media by state government agencies. Agencies may utilize these guidelines as a component of agency policy development for sanctioned participation using Social Media services, or simply as guidelines. State employees or contractors creating or contributing to blogs, microblogs, wikis, social networks, or any other kind of social media both on and off the Nebraska.gov domain need to be made aware of these guidelines or the guidelines of their agency. The State expects all who participate in social media on behalf of the State, to understand and to follow the appropriate

guidelines. These guidelines will evolve as new technologies and social networking tools emerge. The decision to utilize social media technology is a business decision, not a technology-based decision. It must be made at the appropriate level for each department or agency, considering its mission, objectives, capabilities, and potential benefits. Since these technologies are tools created by third parties, these guidelines are separate from state policies regarding privacy and cookies. Agencies may choose to author disclaimers to remind users that, at their own risk, they are leaving an official state website for one which is not hosted, created, or maintained by the State of Nebraska, and that privacy controls and the use of cookies becomes the jurisdiction of that third-party utility.

The standard was revised to provide more guidance to agencies on the handling of social media comments. The Webmasters group has reviewed the document.

Mr. Langer moved to approve revised NITC 4-205: Social Media Guidelines for the 30-day public comment period. Ms. Decker seconded. Roll call vote: Horn-Yes, Langer-Yes, Weir-Yes, Winkle-Yes, and Decker-Yes. Results: Yes-5, No-0, Abstained-0. Motion carried.

STANDARDS AND GUIDELINES (SET FOR 30-DAY COMMENT PERIOD), NITC 5-204: LINKING A PERSONAL PORTABLE COMPUTING DEVICE TO THE STATE EMAIL SYSTEM & NEW FORM FOR DATA CLASSIFIED AS "CONFIDENTIAL".

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.

The current standard is for unclassified/public data. Although the Office of the CIO has recommended to agencies that confidential data not be accessible on mobile devices, there are agencies requesting this. The security policy has four security classification levels: Highly Restricted (not allowed on personal devices), Confidential (will use new form), Internal Use Only (will use Attachment A), and Unclassified/Public (will use Attachment A). Mr. Weakly will revise this version to include confidential data as well as a new form request for confidential data. Panel members requested the document be sent to them for review when it is posted.

Ms. Horn moved to approve NITC 5-204: Linking a Personal Portable Computing Device to the State Email System – New Form for data classified as "Confidential" with the revisions discussed for the 30-day comment period. Mr. Langer seconded. Roll call vote: Winkle-Yes, Weir-Yes, Langer-Yes, Horn-Yes, and Decker-Yes. Results: Yes-5, No-0, Abstained-0. Motion carried.

REGULAR INFORMATIONAL ITEMS AND WORK GROUP UPDATES (AS NEEDED)

Accessibility of Information Technology Work Group, Christy Horn. The final regulations have not been released yet. Educational Testing Services (ETS) was at UNL campus and they brought CAL along with them. This is the company that is doing the State Department of Education’s online assessment. When Ms. Horn spoke to them about the online assessment not being accessible to students, they were surprised and stated the state was not implementing the testing correctly. Ms. Horn assured them that the state was implementing the test correctly. ETS provided a contact person to follow up with regarding accessibility. ETS is very aware and involved with mobile device accessibility. The current Technology Access clause was adopted about 10 years ago and needs to be updated. State Purchasing provides this to vendors in a template with a link. The link takes them to the NITC Standards & Guidelines website which has three documents - the accessibility clause, the policy and the checklist. Ms. Horn will take this back to the work group for updating.

Learning Management System Standards Work Group, Kirk Langer. Mr. Langer had no new items to report. Mr. Rolfes reported that there will be an update presentation at the Education Council this afternoon on the Virtual School white paper. Mr. Weir reported that he and Ms. Decker were asked to meet with Dr. Breed but were instructed to wait until the white paper was released. No one from the Technical Panel has reviewed the white paper. Discussion topics included: Should the Virtual School be classified as an enterprise project? Should there be state oversight? and Are the right persons involved with its development?.

Security Architecture Work Group, Brad Weakly. The Work Group has been working on the mobile device policies. Plans and keynote speakers are being finalized for the 2011 Cyber Security Conference to be held on July 26th. Last year the OCIO has had enough sponsors to pay for the conference expenses so that state employees could attend free of charge. This year may be questionable. Mr. Weakly has recently been working on a project with MS-ISAC (Multi-State Information Sharing and Analysis Center). MS-ISAC is organizing a group buy with SANS Institute for an 18 module online security human awareness training at a cost of $1.15/person. The state will need to commit by July. Agencies have received the information to see if there is interest and if they feel it would be valuable. Mr. Weir suggested putting this information on the Network Nebraska website. PCI compliance is due June 1st for the State Treasurer's Office. Qualys vulnerability scans have been conducted for state agencies. IRS audits are coming up in June and July. This is done every three years and will involve the Office of the CIO, Department of Revenue, Health and Human Services, and the Department of Labor.   The Work Group has been discussing standards and guidelines for cloud computing security regarding third parties handling of data. There is a Cloud Computing Alliance which is focusing on auditing and accountability rather than on technological aspects of cloud computing. The Work Group discussed possibly developing a "security" clause that would be included in all RFP. Mr. Weir asked Mr. Weakly if he would be willing to work with Joshua Mauk on a Security Management RFP for the University of Nebraska.

OTHER BUSINESS

For a future meeting, it was suggested to have a discussion regarding IPv6. The Technical Panel needs to make sure we are operating in a coordinated fashion towards implementation of this new protocol.

ADJOURN

Ms. Decker moved to adjourn. Mr. Langer seconded. All were in favor. Motion carried.

The meeting was adjourned at 10:20 a.m.

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

Technical Panel
of the
Nebraska Information Technology Commission

Standards and Guidelines

Draft Document
30-Day Comment Period

Title: Social Media Guidelines (Revised)

Notes to Readers:

1. The following document is a draft document under review by the Technical Panel of the Nebraska Information Technology Commission (NITC). This document is posted at http://nitc.ne.gov/standards/comment/.
2. If you have comments on this document, you can submit them by email to rick.becker@nebraska.gov, or call 402-471-7984 for more information on submitting comments.
3. The comment period for this document ends on June 12, 2011.
4. The Technical Panel will consider this document and any comments received at a public meeting following the comment period, currently scheduled for June 14, 2011. Information about this meeting will be posted on the NITC website at http://nitc.ne.gov/.

DRAFT

State of Nebraska
Nebraska Information Technology Commission
Standards and Guidelines

NITC 4-205

Title	Social Media Guidelines
Category	E-Government Architecture
Applicability	Applies to all state government agencies, excluding higher education

1. Purpose

The purpose of this document is to provide guidelines for the use of social media by state government agencies. Agencies may utilize these guidelines as a component of agency policy development for sanctioned participation using Social Media services, or simply as guidelines. State employees or contractors creating or contributing to blogs, microblogs, wikis, social networks, or any other kind of social media both on and off the Nebraska.gov domain need to be made aware of these guidelines or the guidelines of their agency. The State expects all who participate in social media on behalf of the State, to understand and to follow the appropriate guidelines. These guidelines will evolve as new technologies and social networking tools emerge.

The decision to utilize social media technology is a business decision, not a technology-based decision. It must be made at the appropriate level for each department or agency, considering its mission, objectives, capabilities, and potential benefits.

Since these technologies are tools created by third parties, these guidelines are separate from state policies regarding privacy and cookies. Agencies may choose to author disclaimers to remind users that, at their own risk, they are leaving an official state website for one which is not hosted, created, or maintained by the State of Nebraska, and that privacy controls and the use of cookies becomes the jurisdiction of that third-party utility.

2. Guidelines

2.1 These guidelines apply to all Social Media and Web tools. See definitions below.

2.2 The decision to utilize Social Media and Web tools is an organizational decision, not a technology-based decision. It must be made at the appropriate level for each department or agency, considering its mission, objectives, capabilities, and potential benefits.

2.3 All state agencies will email the webmaster of the State of Nebraska website (ne-support@nicusa.com) to have their Social Media pages initially linked or updated on the state website.

2.4 Branding of the Social Media pages

2.4.1 All Social Media pages will be branded with the words “Official Nebraska Government Page” either in the bio or profile/information section.

2.4.2 List your official agency name and provide a link back to your agency website.

2.5 Retention Policy (Schedule 124 – State Agencies General Records, Item Numbers 124-1-41, 124-1-49, and 124-7: http://www.sos.ne.gov/records-management/retention_schedules.html)

2.6 It is the agency's responsibility to assure that more than one staff member can access the agency logon, and edit the website/social media. This is a backup in case of staff turnover. For example: An agency may set up one nebraska.gov email account through the OCIO and have several email address aliases created. This will accommodate the requirement of unique email addresses on your Social Media accounts, yet keep all of the emails from all of the accounts going into one email inbox.

2.7 If the Social Media page is intended for pushing information only, indicate the proper channel for contacting the agency.

2.8 Below are some recommended key points to address in a Social Media webpage disclaimer/disclosure notice. Each agency may create their own or Link to this Guideline from their Social Media web page:

- General statement of the intent/purpose of agency Social Media tool.

  Example: The Library Commission uses Social Media as an outlet to show the Library community how they can interact with their public.

- Notice to users of the following:
  1. Communication of a personal or private nature in relation to agency business, as well as official state business interactions, should continue to be made via the traditional agency offices and communications channels and not via the public comment areas of the Social Media tool.
  2. The agency is not responsible for any webpage author’s personal content outside the work place.
  3. The agency is not responsible for any 3rd party content of any kind.
  4. All interactive communications made on this Social Media tool are

subject to the state public records disclosure requirements (http://www.nebraska.gov/privacypol.html).

5. ~~Material deemed inappropriate will be monitored and possibly removed by the agency. Inappropriate content will be maintained in accordance with records retention policies.~~ 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.

2.9 Best Practices. Suggestions on how best to use and maintain social networking at work:

2.9.1 Ensure that your agency sanctions official participation and representation on Social Media sites. Stick to your area of expertise and provide unique, individual perspectives on what is going on at the State and in other larger contexts. All statements must be true and not misleading, and all claims must be substantiated and approved.

2.9.2 Post meaningful, respectful comments, no spam, and no remarks that are off-topic or offensive. When disagreeing with others' opinions, keep it appropriate and polite.

2.9.3 Pause and think before posting. Reply to comments in a timely manner when a response is appropriate unless you have posted a disclaimer that this is not official two-way communication.

2.9.4 Be smart about protecting yourself, your privacy, your agency, and any restricted, confidential, or sensitive information. What is published is widely accessible, not easily retractable, and will be around for a long time (even if you remove it), so consider the content carefully. Respect proprietary information, content, and confidentiality.

2.9.5 If you are under a generic name (see Section 2.6 above) consider using some form of tagging so staff and users can find out who this is.

2.9.6 Email or login names should lead the user back to a “state id”, such as an official state email address or make a user name that indicates you are a state employee.

3. Definitions

3.1 Social Media and Web tools

Social Media and Web tools are umbrella terms that encompass various online activities that integrate the use of hardware/software to facilitate social interaction and collaborative content creation. Social Media authoring uses many forms of technology applications such as Twitter, Facebook, YouTube, Flickr, blogs, wikis, photo and video sharing, podcasts, social networking, and multiuser virtual environments.

4. Related Documents

4.1 Acceptable Use Policy. (NITC 7-101 http://nitc.ne.gov/standards/7-101.html)

4.2 Schedule 124 – State Agencies General Records, Item Numbers 124-1-41, 124-1-49, and 124-7. (http://www.sos.ne.gov/records-management/retention_schedules.html)

4.3 Personnel Rules. Classified System Personnel Rules and Regulations , Chapter 14, Section 003.15 (http://www.das.state.ne.us/personnel/classncomp/classifiedrules.htm). NAPE/AFSCME Labor Contract, Section 10.2 (http://www.das.state.ne.us/emprel/publications.htm)

HISTORY: Adopted on November 9, 2010. Draft revisions – March 31, 2011.
PDF FORMAT: http://nitc.ne.gov/standards/4-205.pdf

Technical Panel
of the
Nebraska Information Technology Commission

Standards and Guidelines

Draft Document
30-Day Comment Period

Title: Linking a Personal Portable Computing Device to the State Email System (Revised)

Notes to Readers:

1. The following document is a draft document under review by the Technical Panel of the Nebraska Information Technology Commission (NITC). This document is posted at http://nitc.ne.gov/standards/comment/.
2. If you have comments on this document, you can submit them by email to rick.becker@nebraska.gov, or call 402-471-7984 for more information on submitting comments.
3. The comment period for this document ends on June 12, 2011.
4. The Technical Panel will consider this document and any comments received at a public meeting following the comment period, currently scheduled for June 14, 2011. Information about this meeting will be posted on the NITC website at http://nitc.ne.gov/.

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:

NITC 5-204 Rev 1
Attachment A - Draft

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