MEETING AGENDA

Technical Panel
of the
Nebraska Information Technology Commission

Tuesday, May 10, 2011
9:00 a.m.
Varner Hall - Board Room
3835 Holdrege St., Lincoln, Nebraska

AGENDA

Meeting Documents: Click the links in the agenda
or click here for all documents (21 pages).

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

2. Public Comment

3. Approval of Minutes* - April 12, 2011

4. Enterprise Projects

   - Project Status Dashboard - Skip Philson

5. Standards and Guidelines

   - Set for 30-Day Comment Period*
     - NITC 4-205: Social Media Guidelines (Revised)
     - NITC 5-204: Linking a Personal Portable Computing Device to the State Email System - New form for data classified as "Confidential"

6. 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

7. Other Business

8. 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 April 18, 2011. The agenda was posted to the NITC website on May 6, 2011.

Technical Panel
of the
Nebraska Information Technology Commission
Tuesday, April 12, 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
Jayne Scofield, Alt. for Brenda Decker, CIO, State of Nebraska
Christy Horn, University of Nebraska
Kirk Langer, Lincoln Public Schools

MEMBERS ABSENT: Mike 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. Meeting notice was posted to the NITC website and Nebraska Public Meeting Calendar on February 17, 2011. The agenda was posted to the NITC website on April 8, 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 FEBRUARY 8, 2011 MINUTES

Ms. Horn moved to approve the February 8, 2011 meeting minutes as presented. Mr. Langer seconded. Roll call vote: Scofield-Yes, Horn-Yes, Langer-Yes, and Weir-Yes. Results: Yes-4, No-0, Abstained-0. Motion carried.

ENTERPRISE PROJECTS

Project Updates - Public Safety Wireless Project, Mike Jeffres
The project is going well and is currently working with Motorola regarding acceptance testing. Some utility companies and local agencies have expressed an interest in joining the system. Project staff and partner are developing user guidelines and determining participation fees. Project has had to adapt as it has been implemented and has learned to think ahead in regards to the users and agencies involved. Good partnerships have been developed with Motorola and NPPD. The project has gone through 4 phases. It is in its last phase and is working through tower, network, and frequency issues. There are still towers that need to be set up and there are operational type issues that are being discussed. It is anticipated to have complete beneficial use of the system by the end of this summer. Mr. Weir recommended that the project document best practices and to share this on the NITC website.

Project Updates - Public Safety Interoperable Project, Pete Peterson (telephone) and Bob Wilhelm
The project is in the process of putting microwave links at tower locations. There had been some difficulties with towers not meeting the structural requirements which have put the project a little behind schedule. The goal was to use local and state owned towers as much as possible but is has had to find other alternative. Final structural analysis on two towers is underway. It is anticipated that these will have equipment installed by the end of summer. Continued discussions will occur with public officials about the project. The Project is working with the Office of the CIO regarding network management. Mr. Weir stated that the University of Nebraska has certain spectrum available which may be useful to the project. Mr. Peterson was given Rick Golden's contact information for follow-up. NWIN and NCORE are working together to continue coordination and management of the projects.

Project Status Dashboard - Skip Philson. The ECM (Enterprise Content Management) project did not have a report for this month. There were two observations that Mr. Philson wanted to follow-up on from the last Technical Panel meeting:

- NeSIS and ADA compliance. Ms. Horn reported that the University has spoken to Oracle. It has been determined that that there is a feature that can be turned on but is dependent on the browser being used. The University informed them that the browser requirement must be flexible for users. The project will be doing more accessibility testing.
- Lessons learned and how do we share this information. Mr. Weir recommended that project complete an "After Action Report" to be posted it on the NITC website. It was also recommended to post well written RFP's, develop RFP templates, and to include a list of contacts (who are state experts in the area of networks, public safety, microwave connections, etc.).

Mr. Langer requested that the Online Assessment Testing project provide a report at an upcoming meeting.

STANDARDS AND GUIDELINES

The Technical Panel must approve any revisions to the Project Status Form. Mr. Philson added the following items to the form, highlighted in yellow on the meeting document:

- Project Start Date: mm/dd/yyyy   Project End Date: mm/dd/yyyy
- Monthly Status Summary

Mr. Becker will also revise the task section so that the sample percentages adds up to 100%.

Mr. Langer moved to approve the proposed changes to the Project Status Form (Attachment A to NITC 1-203). Ms. Horn seconded. Roll call vote: Scofield-Yes, Horn-Yes, Langer-Yes, and Weir-Yes. Results: Yes-4, No-0, Abstained-0. Motion carried.

REGULAR INFORMATIONAL ITEMS AND WORK GROUP UPDATES (as needed)

Accessibility of Information Technology Work Group, Christy Horn. The work group has not met due to addressing accessibility issues with Distance Education and NeSIS projects.

Learning Management System Standards Work Group, Kirk Langer. Discussions have occurred regarding the Virtual High School and curriculum development.

Security Architecture Work Group - Brad Weakly. No report.

OTHER BUSINESS

There was no other business.

ADJOURN

Ms. Horn moved to adjourn the meeting. Ms. Scofield seconded. All were in favor. Motion carried.

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

Nebraska Information Technology Commission
Enterprise Project Status Dashboard – As of May, 2011

Project:	Access Nebraska			Contact:	Karen Heng	
Start Date	09/16/2008	Orig. Completion Date	06/30/2012	Revised Completion Date	n/a	
	May	April	February	January	December	November
Overall Status	🟢	🟢	🟢	🟢	🟢	🟢
Schedule	🟢	🟢	🟢	🟢	🟡	🟡
Budget	🟢	🟢	🟢	🟢	🟢	🟢
Scope	🟢	🟢	🟢	🟢	🟢	🟢
Comments:						

The project is operating completely in the “Green” we do not have any anticipated implementation delays at this time. The project is 65% implemented. All tasks related to the project concerning the rollout of the Customer Service Centers have been started.

The project budget remains on track. The budget expenditures have followed the allocated amounts. The expenditures are occurring at a later time than originally projected. It is the projected that actual total costs for the project will be match the estimated costs; no extra appropriation will be required.

Project:	Student Information System			Contact:	Walter Weir	
	May	April	February	January	December	November
Overall Status	⚪	⚪	🟢	🟢	🟢	🟢
Schedule	⚪	⚪	🟢	🟢	🟢	🟢
Budget	⚪	⚪	🟢	🟢	🟢	🟢
Scope	⚪	⚪	🟢	🟢	🟢	🟢
Comments						

No update for May.

ADA Compliance updates are only outstanding items.

Project:	**Talent Management System**		Contact:		**Dovi Mueller**	
Start Date	6/1/2009	Orig. Completion Date	7/1/2012	Revised Completion Date		n/a
	May	April	February	January	December	November
Overall Status	⚪	🟢	🟢	🟢	🟢	🟢
Schedule	⚪	🟢	🟢	🟢	🟢	🟢
Budget	⚪	🟢	🟢	🟢	🟢	🟢
Scope	⚪	🟢	🟢	🟢	🟢	🟢
Comments						

No update for May.

Employee Performance Management (Target: January, 2012)

- **Employee Performance Management (EPM) will be the next implementation. This will also be implemented by a statewide team made up of employees, managers, supervisors and HR representatives from the agencies. Our goal is to have one statewide Employee Performance Management solution that addresses the four pillars of performance which include: Performance Appraisals (the form), Goal Management, Competency Management and Development Planning. This team will officially kick-off implementation with a training event scheduled for the week of April 25.**

Project:	**Network Nebraska Education**		Contact:		**Tom Rolfes**	
Start Date	05/01/2006	Orig. Completion Date	06/30/2012	Revised Completion Date		n/a
	May	April	February	January	December	November
Overall Status	⚪	🟢	🟢	🟢	🟢	🟢
Schedule	⚪	🟡	🟡	🟡	🟡	🟡
Budget	⚪	🟢	🟢	🟢	🟢	🟢
Scope	⚪	🟢	🟢	🟢	🟢	🟡
Comments						

No update for May

High points for 2011: Internet Access demand for K-12 has increased by 16% over 2010-11 amounts driven by an all-time low of $6.00/Mbps/month; three new colleges and one public library will join in Summer 2011; Network Nebraska-Education Advisory Group is embracing their advisory role to the CIO; Education Council's Network Nebraska Marketing Survey is finishing their 2011 Report and that is providing very good data upon which to make decisions and set strategic directions. Neb. Rev. Stat. 86-5, 100 Detailed Financial Reporting was completed on November 15, 2010; Neb. Rev. Stat. 86-520.01 Equipment Notification website was finished on 3/1/2011.

The Legislative deadline of the CIO providing access to every public education entity "no later than July 1, 2012" is rapidly approaching, which explains the yellow stop light for 'Schedule'. There are approximately 40 of the 60 remaining K-12 entities that have expressed interest in joining Network Nebraska for July 1, 2011. Otherwise, all but one public college and several nonpublic colleges are members of the Network. Overall Project Status, Budget, Scope and Quality are all green.

Nebraska Information Technology Commission
Enterprise Project Status Dashboard – As of May, 2011

Project:	**Public Safety Wireless**		Contact:	**Mike Jeffres**		
	May	April	February	January	December	November
Overall Status	⚪	🟢	🟢	🟢	🟢	🟢
Schedule	⚪	🟢	🟢	🟢	🟢	🟢
Budget	⚪	🟢	🟢	🟢	🟢	🟢
Scope	⚪	🟢	🟢	🟢	🟢	🟢

Comments

At the April meeting, the Tech Panel decided to continue to track this project.

No update for May.

Project:	**Fusion Center**		Contact:	**Kevin Knorr**		
Start Date	04/13/2010	Orig. Completion Date	06/11/2011	Revised Completion Date		n/a
	May	April	February	January	December	November
Overall Status		🟢	🟡	🟡	🟡	🟡
Schedule		🟢	🟡	🟡	🟡	🟡
Budget		🟢	🟢	🟢	🟢	🟢
Scope		🟢	🟢	🟢	🟢	🟢

Comments

No update for May

Project Synopsis

Over the last 20-25 days, noticeable progress has been made on the Data integration side and a rapid action plan to start testing the Intel system in the Production/Test environment by mid-April to go live with Intel and few data integrations by end of May 2011.

On the integration front, Memex and NCJIS had a several meetings to iron out the initial approach to access NCJIS from Memex system.

Significant Accomplishments during Reporting Period

- **Memex continued to work on bugs/changes and have identify all the change requests for Intel system**
- **Had a great meeting with Omaha PD Gang department on March 3rd and shown the demo of OPD Gang Data from Legacy system to Memex, testing will be starting soon and expecting a sign off by end of March 2011**
- **VPN connectivity between RISS and NSP has been established successfully and a meeting has been scheduled to work out the TEST schedule and expecting a sign off from Customer by end of March 2011.**
- **A significant progress has been made on NSP CAD data and it is available for NSP to test. CAD data was refreshed again for further testing.**
- **Security on Intel/Data integration systems has been revamped and will be ready for testing by March 28, 2011**
- **Continued testing of NSP RMS and CAD data for correctness and consistency.**
- **Memex-NCJIS front end was presented to NIAC for an initial pass**
- **Several meetings took place for NCJIS integration and Memex is making a good headway to access NCJIS from Memex Patriarch.**

Nebraska Information Technology Commission
Enterprise Project Status Dashboard – As of May, 2011

Project:	**Online Assessment**			Contact:	**John Moon**	
Start Date	07/01/2010	Orig. Completion Date	06/30/2011	Revised Completion Date		n/a
	May	April	February	January	December	November
Overall Status	🟢	🟢	🟢	🟢	🟢	🟢
Schedule	🟢	🟢	🟢	🟢	🟢	🟢
Budget	🟢	🟢	🟢	🟢	🟢	🟢
Scope	🟢	🟢	🟢	🟢	🟢	🟢
Comments						

We have administered over 250,000 assessments online including 88,000 math, 121,000 reading and 42,000 science assessments. At this time we do not have the ratio of paper/pencil and online assessments. The last day for the testing window is May 6th.

Some districts have reported issues with connectivity and freezing. Our vendors have addressed these issues in a timely and efficient manner.

NDE has negotiated a contract for the 2011-2012 year of Reading/Math/Science assessment. Negotiation with our vendors for the writing contract (Year 2) has been initiated.

Plans are underway to display NeSA assessment results in the State of the Schools Report in the fall.

Project:	**Interoperability Project**			Contact:	**Rod Hutt / Pete Peterson**	
Start Date	10/01/2010	Orig. Completion Date	06/01/2013	Revised Completion Date		n/a
	May	April	February	January	December	November
Overall Status	🟡	🟡	🟢	🟢	🟢	🟢
Schedule	🟡	🟡	🟡	🟢	🟢	🟢
Budget	🟢	🟢	🟢	🟢	🟢	🟢
Scope	🟡	🟡	🟢	🟢	🟢	🟢
Comments						

Pre-design meetings with all regions were completed in April. Surveys, Tower Maping, Structural Engineering of towers will take place in May.
Approval and acceptance of the final Panhandle design is expected in May.

COMMENTS ON SUMMARY PROJECT STATUS: **The project is being challenged by many issues; inadequate tower and communications infrastructure, failing structure analysis reports, time allocation to locate new towers and adequate resources/infrastructure, availability of time necessary for local leadership or involvement in securing adequate resources/infrastructure and the fact that final cost will be impacted by all of the above.**

Nebraska Information Technology Commission
Enterprise Project Status Dashboard – As of May, 2011

Project:	MMIS			Contact:		
Start Date	n/a	Orig. Completion Date	n/a	Revised Completion Date	n/a	
	May	April	February	January	December	November
Overall Status	⚪	⚪	⚪	⚪	⚪	⚪
Schedule	⚪	⚪	⚪	⚪	⚪	⚪
Budget	⚪	⚪	⚪	⚪	⚪	⚪
Scope	⚪	⚪	⚪	⚪	⚪	⚪

Comments

Project On Hold until renewed

Project:	Enterprise Content Management			Contact:	Kevin Keller	
Start Date	10/15/2010	Orig. Completion Date	05/31/2011	Revised Completion Date		
	May	April	February	January	December	November
Overall Status	🟢	⚪	🟢	🟢	🟢	⚪
Schedule	🟢	⚪	🟢	🟢	🟢	⚪
Budget	🟢	⚪	🟢	🟢	🟢	⚪
Scope	🟢	⚪	🟢	🟢	🟢	⚪

Comments

Project is 98% complete.

The remaining issue that needs to be resolved is the Active Directory Security access across agencies for external users.

Color Legend		
🔴	Red	**Project has significant risk to baseline cost, schedule, or project deliverables.** **Current status requires immediate escalation and management involvement.** Probable that item will **NOT** meet dates with acceptable quality without changes to schedule, resources, and/or scope.
🟡	Yellow	**Project has a current or potential risk to baseline cost, schedule, or project deliverables.** **Project Manager will manage risks based on risk mitigation planning.** Good probability item will meet dates and acceptable quality. Schedule, resource, or scope changes may be needed.
🟢	Green	**Project has no significant risk to baseline cost, schedule, or project deliverables.** Strong probability project will meet dates and acceptable quality.
⚪	Gray	**No report for the reporting period or the project has not yet been activated.**

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

NITC 5-204

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. 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 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 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 **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).

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.

Attachment A: Request Form (Word Document)

HISTORY: Adopted on March 1, 2011.
PDF FORMAT: http://nitc.ne.gov/standards/5-204.pdf

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). 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.

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 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 ("OCIO"). 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 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.

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:

- 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

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 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 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.

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, 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).

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. **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.

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.

Requirements:

- All information must be protected to the extent required based on applicable State and Federal regulations.
- No "jail broken" or devices modified beyond manufactures expectations will be used to process or store sensitive information.

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