MEETING AGENDA

Technical Panel
of the
Nebraska Information Technology Commission

Tuesday, February 14, 2012
9:00 a.m.
Varner Hall - Board Room
3835 Holdrege St., Lincoln, Nebraska

AGENDA

Meeting Documents (33 pages)

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

2. Public Comment

3. Approval of Minutes* - December 13, 2011

4. Enterprise Projects

   - Discussion and Recommendation - Enterprise Project Designation*
     - Workers Compensation Court - E-Filing Project - Glenn Morton and Randy Cecrle
   - Final Report
     - OCIO - Enterprise Content Management System - Kevin Keller
   - Project Status Dashboard - Skip Philson

5. Discussion: ESUCC Structures and Plans - Matt Blomstedt, Executive Director ESUCC

6. Standards and Guidelines

   - Set for 30-Day Comment Period*
     - NITC 5-101: Enterprise Content Management System for State Agencies (New)
     - NITC 7-301: Wireless Local Area Network Standard (Revised)
   - Approval of Revised Attachments*
     - NITC 1-204: IT Procurement Review Policy - Attachment A
     - NITC 5-204: Linking a Personal Portable Computing Device to the State Email System - Attachments A and B
   - Request for Waiver*
     - Kronos Steering Committee (NDCS/HHSS/OCIO) - Request for Waiver from requirements of NITC 8-301

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

   - Accessibility of Information Technology Work Group - Christy Horn
     - Discussion: Updating accessibility policies
   - Learning Management System Standards Work Group - Kirk Langer
   - Security Architecture Work Group - Brad Weakly
   - Intergovernmental Data Communications Work Group - Tim Cao

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 December 15, 2011. The agenda was posted to the NITC website on February 7, 2012.

Technical Panel
of the
Nebraska Information Technology Commission
Tuesday, December 13, 2011, 9:00 a.m.
Varner Hall - Board Room
3835 Holdrege St., Lincoln, Nebraska
MINUTES

MEMBERS PRESENT:
Walter Weir, CIO, University of Nebraska, Chair
Brenda Decker, CIO, State of Nebraska
Kirk Langer, Lincoln Public Schools
Michael Winkle, NET

MEMBERS PRESENT:
Christy Horn, University of Nebraska

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 November 21, 2011. The agenda was posted to the NITC website on December 7, 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 NOVEMBER 8, 2011 MINUTES

Mr. Winkle moved approval of the November 8, 2011 minutes as presented. Ms. Decker seconded. Roll call vote: Decker-Yes, Langer-Yes, Weir-Yes, and Winkle-Yes. Results: Yes-4, No-0, Abstained-0. Motion carried.

OTHER PROJECTS - NEBRASKA STATE PATROL - MESSAGE SWITCH REPLACEMENT PROJECT

Suzy Fredrickson, Information Technology; Tom Prevo, Security Officer; and Keta Wright, Project Manager

The project is being funded through CLEIN (Combined Law Enforcement Information Network) funds through the Office of the CIO. Agencies (federal, state and local) pay a monthly fee to the fund which can be used for information network projects. The primary function of the message switch is to administer and control the flow of data messages between various CJIS systems. Primary functions include message routing, distribution, and the exchange of binary objects (images, fingerprints, and other non-text objects) among local, state, and national criminal justice users and databases. The message switch replacement project kick off began August, 2011 and is expected to conclude April, 2012. Datamaxx won the bid for the project. Five of the ten milestones have been completed so far. Project milestones completed to this point include:

- Establishing a project schedule
- Development of design specifications
- Receipt of software licensing
- Serve installs
- Implementation of interfaces in testing and production environments

The only project risk at this point is not meeting project timelines. Technical Panel members had an opportunity to ask questions. Mr. Philson will be in touch with Ms. Fredrickson regarding future project reports to the Technical Panel

ENTERPRISE PROJECTS

PROJECT STATUS DASHBOARD - Skip Philson

The Link-Human Capital Management Project is going live in February for Benefits, Performance Review and Human Capital Management. This will cause a delay for the Procurement phase. Other projects are on schedule. The ECM (Enterprise Content Management) Project will give their final report at the February meeting.

Mr. Weir reported that the NeSIS project is still dealing with Oracle and ADA compliance. Jim Zempke is the Project Manager. The University if very concerned about ADA compliance. Ms. Horn's office will be involved determining the deficiencies as well as working on solutions.

Discussion occurred about the need to review and further define the NITC's Accessibility Standard. The standard must be clear regarding expectations and ADA Compliance. In addition, strategies should be developed for mobile technologies. State agencies and the legislature are dealing with the issue of captioning on the web. Captioning would also need appropriate standards and will have technical implications and impact on the state systems. The Office of the Blind and Visually Impaired have also visited with the Office of the CIO about website accessibility as well. Mr. Weir will speak to Ms. Horn about the work group's plan to update the accessibility standard. This will be an agenda item for the February meeting.

ELECTION - TECHNICAL PANEL CHAIR FOR 2012*

Ms. Decker moved to nominate Walter Weir to serve as the Chair for 2012. Mr. Winkle seconded. Roll call vote: Langer-Yes, Weir-Abstain, Winkle-Yes, and Decker-Yes. Results: Yes-3, No-0, Abstained-1. Motion carried.

REGULAR INFORMATIONAL ITEMS AND WORK GROUP UPDATES (as needed)

Accessibility of Information Technology Work Group - Christy Horn. Ms. Horn was not present to report

Learning Management System Standards Work Group - Kirk Langer. Mr. Langer provided an update to the Panel. Members discussed the Virtual High School and the use of various systems such as Blackboard and Sakai.

Security Architecture Work Group - Brad Weakly. After meeting with the Department of Agriculture, it was determined that their system is a stand-alone system. Users do not use any personal identification to log-on. The agency does weekly scans using Qualys. The front end of the system is located at the OCIO. The back end is at the Department of Agriculture but they are considering moving it to the OCIO. The agency's waiver request was reasonable and appropriate. Mr. Weir asked that a written report of his finding be on file.

For discussion at the next Technical Panel meeting, Mr. Weakly presented revisions to Attachments A and B to NITC 5-204. Some wording has been changed so that both documents read the same. The signature block will include a place to print the name as well for easier identification.

The work group has drafted a policy for external hosting and is now working on gathering background information. FedRAMP released the federal government policy for cloud computing. The work group has also been discussing mobile device management.

Intergovernmental Data Communications Work Group - Tim Cao, Mr. Cao was not present to report.

OTHER BUSINESS

Ms. Decker announced that the Network Nebraska RFP bids were opened on Friday, December 9 and are currently being reviewed. The intent to award is scheduled for December 28. This is the largest bid that Network Nebraska has released.

Ms. Decker introduced Nathan Watermeier, new GIS Administrative Manager. He will be replacing Larry Zink who is retiring at the end of December.

ADJOURNMENT

With no further business, Mr. Weir adjourned the meeting. The meeting was adjourned at 9:50 a.m.

Project Status Form

General Information			
Project Name			Date
Adjudication Re-engineering - Project 1a - Release of Liability E-Filing			2/3/2012
Sponsoring Agency			
Nebraska Workers' Compensation			
Contact	Phone	Email	Employer
Randy Cecrle	402-471-2976	Randy.cecrle@nebraska.gov	WCC
Project Manager	Phone	Email	Employer
Randy Cecrle	402-471-2976	Randy.cecrle@nebraska.gov	WCC

Project Start Date	09/01/2011	**Project End Date**	Open	Revised End Date	n/a

Key Questions		Explanation (if Yes)
1. Has the project scope of work changed?	□ Yes □ No	
2. Will upcoming target dates be missed?	□ Yes □ No	
3. Does the project team have resource constraints?	□ Yes □ No	
4. Are there problems or concerns that require stakeholder or top management attention?	□ Yes □ No	

Summary Project Status
Any item classified as red or yellow requires an explanation in the Status box that follows this section. Additional priority items can be added to the list for status reporting.

Select one color in each of the Reporting Period columns to indicate your best assessment of:	Last Reporting Period [MM/DD/YYYY]			This Reporting Period [02/03/2012]		
1. Overall Project Status	□ Red	□ Yellow	□ Green	□ Red	□ Yellow	☒ Green
2. Schedule	□ Red	□ Yellow	□ Green	□ Red	□ Yellow	☒ Green
3. Budget (capital, overall project hours)	□ Red	□ Yellow	□ Green	□ Red	□ Yellow	☒ Green
4. Scope	□ Red	□ Yellow	□ Green	□ Red	□ Yellow	☒ Green
5. Quality	□ Red	□ Yellow	□ Green	□ Red	□ Yellow	☒ Green

Color Legend	
🟥	***Project has significant risk to baseline cost, schedule, or deliverables. Requires immediate escalation and management involvement.***
🟨	***Project has a current or potential risk to baseline cost, schedule, or deliverables. PM will manage based on risk mitigation planning.***
🟩	***Project has no significant risk to baseline cost, schedule, or project deliverables.***

Monthly Status Summary
Provide a summary of the project status since the last reporting period. (This summary will become part of the monthly NITC Dashboard.)

This is the initial report of the project.

Adjudication Re-engineering is a multi-phase project that will span a number of years to incorporate e-filing, electronic docket files, public web access to docket status, e-documents creation and judges e-signing of decisions and orders, and other performance improvement changes.

Project 1a - Release of Liability E-Filing is focusing on the development of one pleading type to complete the full end-to-end set of e-filing functions and limited changes to Clerks Review to process the submitted e-documents in the same manner as performed today with paper.

Project 1b - Semi-automated Docket / RFJA Setup, Electronic Docket File, and possibly Centralized Scanning will follow up immediately after 1a is completed. A rough time frame for completion is first half of calendar year 2013.

Because of the tight integration of judicial data and functions with non-judicial data and functions, (such as Vocational Rehabilitation), WCC systems, including e-filing are separate from the rest of the courts in the state.

Because of the court’s limited jurisdiction, our e-filing system is being designed to provide web-based drafting of pleading documents that utilizes internal WCC electronic docket information. PDFs are generated for printing and “wet signatures” and the submittal with the “/s/” signature format as is the current rule and practice by the other courts in the state.

Tentatively, Project 2 will focus adding the remainder of the pleading types to e-filing with a rough target completion date end-of-calendar year 2013.

Other adjudication functions to be addressed following Project 2 include:

- Scheduling and Calendar management,
- Public access to case status and case documents,
- Judge’s Decisions and Orders management,
- Automated notification to other sections of the court of court case changes,
- Electronic transmission of documents to the Court of Appeals,
- Electronic Exhibit management.

There has not been any identification of additional out-of-pocket costs other than the knowledge that electronic storage costs will grow as more e-documents are added to the Electronic Docket Files.

Significant Milestones (Met, Not Met, Scheduled) Insert additional lines as necessary.

Milestone	Met	Not Met	Sche-duled	Original Date	Actual Date	Impact (if late)
Beta testing with limited external attorney offices	□	□	□	May 2012		No Impact
Initial production roll-out	□	□	□	May-June 2012		No Impact
	□	□	□			

Project Issues Insert additional lines as necessary.				
Description	**Impact on Project - (H,M,L)**	**Date Resolution is Needed**	**Issue Resolution Assigned to**	**Date Resolved**
Waiting on the judges need to make decisions on standardization of language on the Release of Liability pleading.	H	February 28, 2012	Barb Frank, Clerk of the Court	
Implementation by OCIO of Analytics Reporting Service (Oracle BI Publisher) in a production environment for the generation of PDFs.	H	April 2012	Kevin Keller - OCIO	

Impact: **H=High -** major impact on time, scope, cost. Issue must be resolved. **M= Medium**- moderate impact to time, scope, cost. **L=Low**- Issue will not impact project delivery

Project Risks Insert additional lines as necessary.			
Major Risk Events	High Medium Low	Risk Mitigation	Mitigation Responsible Party
Adoption by attorney offices of the court e-filing drafting system instead of their systems to produce the formatted pleadings for e-filing in place of uploading e-documents prepared on their systems.	Low	This approach was communicated in previous discussions with attorney offices during the last couple of years while we were working on the Application for Lump Sum Settlement e-filing drafting system. Select attorney offices were involved in testing until that project was put on hold. Select attorney offices will be involved in beta testing. Additional information will be released to external stakeholders and other communications will occur over the next couple of months.	Presiding Judge and Clerk of the Court

Decision Points Insert additional lines as necessary.
Use this section to document any major decisions that impact target dates, scope, cost, or budget.

Decision Point	Decision Due Date	Decision made by (name or names)	Decision's Impact on Project
Change requests from attorney offices during testing.	May 2012	Presiding Judge and Clerk of the Court	Delay the rollout of the system into production.

Comparison of Budgeted to Actual Expenditures
Use a chart like the following to show actual expenditures compared to planned levels. Break the costs into other categories as appropriate.

Fiscal Year [2012] – This is an internal development project utilizing WCC information technology staff and any application services provided by the OCIO. Limited cash expenditures have been made for PDF stamping software.

Budget Item	Actual Costs to Date	Estimate to Complete	Total Estimated Costs	Total Planned Budget
Salaries	Internal staff, not tracked			
Contract Services	$0	$0	$0	$0
Hardware	$0		$0	$0
Software	$6,759.14	$0	$6,759.14	$6,759.14
Training	$0	$0	$0	$0
Other Expenditures*	$0	$0	$0	$0
Total Costs	$6,759.14		$6,759.14	$6,759.14

Other Expenditures include supplies, materials, etc.

Additional Comments / Concerns Use this section to insert comments / concerns not included in any other section.

Nebraska Information Technology Commission
Enterprise Project Status Dashboard – As of February, 2012

Project:	**Access Nebraska (Q)**	Contact:	**Karen Heng**

Start Date	09/16/2008	Orig. Completion Date	06/30/2012	Revised Completion Date	n/a

	February	January	December	November	October	September
Overall Status	🟢	⚪	⚪	🟢	⚪	⚪
Schedule	🟢	⚪	⚪	🟢	⚪	⚪
Budget	🟢	⚪	⚪	🟢	⚪	⚪
Scope	🟢	⚪	⚪	🟢	⚪	⚪

Comments:

Now reporting Quarterly. No report required for December.

February update:
ACCESSNebraska transition is almost complete. On January 24, the Lexington Customer Service Center went on phones. We have less than 1000 cases to move to ACCESSNebraska Universal Case Management System. Initial hiring is complete, current hiring is to fill vacancies.

On the technology side, in December 2011 we added the ability to place email and other documents submitted to internal N-FOCUS users to be added to the Document Imaging System. An Automated Interview Scheduler was introduced on November 13. This schedules the customer interview and sends the customer a notice of interview date and time. In January an updated telephone dashboard was rolled out to staff on January 9, 2012. This new dashboard allows staff to see number of calls waiting for each queue, average wait time, number of calls answered today.

There are no major technology pieces still in development. We have a couple of enhancements. We are developing an electronic display board for the Customer Service Centers. We are also looking at adding an automated call back feature to the phone system. The next tool for web services will be a Partner Inquiry feature were agencies working on the same customer as DHHS can look up the DHHS case status and information around case status.

Project:	**Student Information System (Q)**	Contact:	**Walter Weir**

	February	January	December	November	October	September
Overall Status	⚪	⚪	⚪	⚪	⚪	⚪
Schedule	⚪	⚪	⚪	⚪	⚪	⚪
Budget	⚪	⚪	⚪	⚪	⚪	⚪
Scope	⚪	⚪	⚪	⚪	⚪	⚪

Comments

ADA Compliance updates are only outstanding items.

Project:	**Link – Human Capital Management (formerly Talent Management System)**		Contact:	**Dovi Mueller**	
Start Date	6/1/2009	Orig. Completion Date	7/1/2012	Revised Completion Date	n/a

	February	January	December	November	October	September
Overall Status	🟡	⚪	🟢	🟢	⚪	🟢
Schedule	🟢	⚪	🟢	🟢	⚪	🟢
Budget	🟢	⚪	🟢	🟢	⚪	🟢
Scope	🟢	⚪	🟢	🟢	⚪	🟡

Comments

Applicant Tracking (NEOGOV)

- The integration from NEOGOV to Workday has been completed and is being tested. Very few issues / changes have been necessary.

Learning Development & Performance (Cornerstone OnDemand)

- Finalizing the outbound CSoD integration and getting ready to run unit test

Benefits / Human Capital Management (Workday)

- Finalizing the integration from Workday to E1 is the focus. Initial testing has been completed; however, there are changes needed that will affect our next phase which is the first phase of payroll testing. This will cause the project to be extended by approximately 30 days. This is why the overall status is Yellow.
- During the month of January, HR contacts along with the State implementation team participated in two weeks of user acceptance testing. Code, non-code and constitutional agencies participated in testing.

- Training on Workday basics began on February 6, 2012. We expect to train 160 HR Partners and agency representatives by February 25, 2012. We conduct two courses a day and courses have been full. Agency HR Partners who completed the initial Workday HCM training are presenting this training along with the State Team. The next training phase will be geared toward HR Partners only and will include supervisory organizational structure, managing positions, E1 payroll and HR transactions, benefits enrollment and employee self service. This training will begin toward the end of February or early March.

Project:	**Link - Procurement**		Contact:	**Dovi Mueller**	
Start Date	6/1/2009	Orig. Completion Date	7/1/2012	Revised Completion Date	tbd

	February	January	December	November	October	September
Overall Status	⚪	⚪	🟢	🟢	⚪	🟢
Schedule	⚪	⚪	🟡	🟢	⚪	🟢
Budget	⚪	⚪	🟢	🟢	⚪	🟢
Scope	⚪	⚪	🟢	🟢	⚪	🟢

Comments

No Update for February.

December update:

Procurement

- Work on the Procurement phase of the Link project has been reduced due to the implementation priorities of the HCM phase.
- The Procurement team is working on establishing revised project dates.

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

RFP 3827 received 230 bids and 31 ‘No Bids’ or ‘No Awards’ that were rolled over to a second-round RFP 3886, which is due to open on Friday, February 17. Of the 230 successful awards, involving 10 companies, none of them have been posted as State contracts as of 2/9/2012. Once each contract is posted, the staff of the OCIO are prepared to rapidly disseminate purchase and E-rate filing information.

Budget numbers are NEW and inclusive of the UNCSN 2nd Qtr invoice report, presented for payment on 1/30/2012.

Actual Costs	Estimate to Complete	Total Planned Budget
$230,318	$331,173	$561,491

Issue:
State Purchasing is overdue on Terms and Conditions negotiations with 10 vendors on RFP 3827, which may require local school districts to hold emergency board meetings to approve purchases off of the State contracts. Resolution is needed by February 17, 2012.

Project:	Public Safety Wireless (Q)			Contact:	Mike Jeffres	
	February	January	December	November	October	September
Overall Status	⚪	⚪	⚪	🟢	⚪	🟢
Schedule	⚪	⚪	⚪	🟢	⚪	🟢
Budget	⚪	⚪	⚪	🟢	⚪	🟢
Scope	⚪	⚪	⚪	🟢	⚪	🟢
Comments						

Now reporting quarterly. No report for February.

November update:
System acceptance is pending coverage testing, which is on temporary hold.

We are currently in discussion with Motorola on developing the final check list any remaining open issues to complete the system acceptance plan.

Issue:
Coverage testing on hold – pending ongoing investigation of noise issue related to antenna used at towers, system remains in operation. Resolution is needed by Spring, 2012.

Nebraska Information Technology Commission
Enterprise Project Status Dashboard – As of February, 2012

Project:	**Fusion Center**		Contact:	**Kevin Knorr**	
Start Date	04/13/2010	Orig. Completion Date	06/11/2011	Revised Completion Date	12/15/2011

	February	January	December	November	October	September
Overall Status	🟢	⚪	🟢	🟢	⚪	🟢
Schedule	🟡	⚪	🟡	🟡	⚪	🟡
Budget	🟢	⚪	🟢	🟢	⚪	🟢
Scope	🟢	⚪	🟢	🟢	⚪	🟢

Comments

Development and training resources are on track to deploy the training plan on February 15, 2012 with an expected completion of the system training on March 15, 2012. System testing continues with minor issues being resolved by the Memex/SAS team. MOU's and Participation agreements have been or will be signed by February 15 in order to have the needed security protocols in place at "go live."

Project:	**Online Assessment**		Contact:	**John Moon**	
Start Date	07/01/2010	Orig. Completion Date	06/30/2011	Revised Completion Date	06/30/2012

	February	January	December	November	October	September
Overall Status	🟢	⚪	🟢	🟢	⚪	🟢
Schedule	🟢	⚪	🟢	🟢	⚪	🟢
Budget	🟢	⚪	🟢	🟢	⚪	🟢
Scope	🟢	⚪	🟢	🟢	⚪	🟢

Comments

February 3, 2012 Update _
Check 4 Learning Training has been completed and access to the assessment system was opened on January 23rd. Teachers/administrators have been developing classes along with student lists and assessments using the C4L items in the system. Some bugs have been noted and addressed by our vendor.

Online assessment of writing was initiated this year for grades 8 and 11. Feedback from districts on the online assessment of writing has been very positive with few disruptions. Student reactivations due to various reasons have been effective and timely. The test window for writing ends on February 10, 2012. Scoring will be completed by March 1. School/district reports along with individual student results will provided electronically through eDIRECT on May 21.

The student data file from NSSRS was sent to Data Recognition Corporation (DRC) on February 3, 2012. Districts were instructed to update student data in the NSSRS before February 1 to provide the most up-to-date information for our testing process. The assessment window for NeSA –Reading, NeSA-Math, and NeSA-Science (NeSA-RMS) is March 26, 2012 through May 4, 2012. Training on test administration for NeSA-RMS will be conducted through a WebEx with six sessions scheduled for Feb. 27 through Mar. 1, 2012. The online management tools will open on March 5 for districts to print tickets and edit student information.

Project:	**Interoperability Project**		Contact:	**Bob Wilhelm**	
Start Date	10/01/2010	Orig. Completion Date	06/01/2013	Revised Completion Date	09/30/2013
	February	January	December	November	October	September
Overall Status	🟡	⚪	🟡	🟡	⚪	🟡
Schedule	🟡	⚪	🟡	🟡	⚪	🟡
Budget	🟢	⚪	🟢	🟢	⚪	🟢
Scope	🟢	⚪	🟢	🟢	⚪	🟢

Comments

Construction of the Pilot Ring (Panhandle Region) began in September 2011 with completion, system testing and signoff planned to take place by March 31, 2012. In the Southwest region, all path studies, tower mapping, structural analyses and grounding tests have been completed and equipment will be ordered after the Pilot Region is tested and accepted (after March 31, 2012). Completion and signoff of the Pilot Region is a prerequisite for starting construction in the rest of the regions. In the South Central and Southeast regions, all path studies, tower mapping, structural analyses and grounding tests are ongoing. Equipment is anticipated to be ordered for South Central by June 2012. In the remaining regions (East Central, Northeast and Tri-County) pre-construction efforts have begun.

Although construction of the Pilot Region continues, the project has been impacted negatively by the inability to secure adequate tower sites. Alternate locations are being sought, reluctant tower hosts are being re-contacted and tower remediation options are being studied. The end result is that we do not anticipate testing or acceptance of the Pilot system prior to March 31, 2012. Lessons learned on the Pilot Ring will serve the project well as the project moves east.

Completing the Pilot Ring acquisition leases and permissions and tower remediation are critical to moving forward.

Project Risks Insert additional lines as necessary.

Major Risk Events	High Medium Low	Risk Mitigation	Mitigation Responsible Party
Finding adequate towers to locate the NRIN system on	H	Deal with facility owners to gain access to their towers, etc.	Sue Krogman & NCOR Representatives
MOUs and Lease Agreements	H	Deal with facility owners to gain access to their towers, etc.	Sue Krogman & NCOR Representatives

Project:	**Law Enforcement Message Switch Replacement (V)**		Contact:	**Suzy Fredrickson**	
Start Date	08/01/2011	Orig. Completion Date	04/13/2012	Revised Completion Date	n/a
	February	January	December	November	October	September
Overall Status	🟢	⚪	🟢	⚪	⚪	⚪
Schedule	🟢	⚪	🟢	⚪	⚪	⚪
Budget	🟢	⚪	🟢	⚪	⚪	⚪
Scope	🟢	⚪	🟢	⚪	⚪	⚪

Comments

Project milestones to this point include:

1. Establishing a Project Schedule
2. Development of Design Specifications
3. Receipt of Software Licensing
4. Server Installs
5. Implementation of Interfaces – Datamaxx developing interfaces for DMV, VTR, PO

Progress of Project Tasks within Milestone 6:
100 % - On-Site Configuration (All Systems)
78% - Data Conversion
74% - Solution Configuration & Factory Acceptance Testing
0 % - Datamaxx System Testing (on-site) – Functionality

Change Request:

Contracted with Datamaxx to write interfaces for DMV, VTR, PO on behalf of OCIO in order to stay on target with schedule.

Change order cost was $25,000.

Project:	**Adjudication Re-engineering (V)**			Contact:	**Randy Cecrle**	
Start Date	09/01/2011	Orig. Completion Date	Open	Revised Completion Date		n/a
	February	January	December	November	October	September
Overall Status	🟢	⚪	⚪	⚪	⚪	⚪
Schedule	🟢	⚪	⚪	⚪	⚪	⚪
Budget	🟢	⚪	⚪	⚪	⚪	⚪
Scope	🟢	⚪	⚪	⚪	⚪	⚪
Comments						

This is the initial report of the project.

Adjudication Re-engineering is a multi-phase project that will span a number of years to incorporate e-filing, electronic docket files, public web access to docket status, e-documents creation and judges e-signing of decisions and orders, and other performance improvement changes.

Project 1a - Release of Liability E-Filing is focusing on the development of one pleading type to complete the full end-to-end set of e-filing functions and limited changes to Clerks Review to process the submitted e-documents in the same manner as performed today with paper.

Project 1b - Semi-automated Docket / RFJA Setup, Electronic Docket File, and possibly Centralized Scanning will follow up immediately after 1a is completed. A rough time frame for completion is first half of calendar year 2013.

Because of the tight integration of judicial data and functions with non-judicial data and functions, (such as Vocational Rehabilitation), WCC systems, including e-filing are separate from the rest of the courts in the state.

Because of the court’s limited jurisdiction, our e-filing system is being designed to provide web-based drafting of pleading documents that utilizes internal WCC electronic docket information. PDFs are generated for printing and “wet signatures” and the submittal with the “/s/” signature format as is the current rule and practice by the other courts in the state.

Tentatively, Project 2 will focus adding the remainder of the pleading types to e-filing with a rough target completion date end-of-calendar year 2013.

Other adjudication functions to be addressed following Project 2 include:

- Scheduling and Calendar management,
- Public access to case status and case documents,
- Judge’s Decisions and Orders management,

- Automated notification to other sections of the court of court case changes,
- Electronic transmission of documents to the Court of Appeals,
- Electronic Exhibit management.

There has not been any identification of additional out-of-pocket costs other than the knowledge that electronic storage costs will grow as more e-documents are added to the Electronic Docket Files.

Project:	**MMIS**		Contact:		
Start Date	n/a	Orig. Completion Date	n/a	Revised Completion Date	n/a

	February	January	December	November	October	September
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	09/30/2011

	February	January	December	November	October	September
Overall Status	🟢	⚪	⚪	🟢	⚪	🟢
Schedule	🟢	⚪	⚪	🟢	⚪	🟢
Budget	🟢	⚪	⚪	🟢	⚪	🟢
Scope	🟢	⚪	⚪	🟢	⚪	🟢

Comments

The project is complete.

Closeout presentation scheduled for February.

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.**

NITC 5-101

State of Nebraska
Nebraska Information Technology Commission
Standards and Guidelines

NITC 5-101 (DRAFT)

Title	Enterprise Content Management System for State Agencies
Category	Groupware Architecture
Applicability	Standard for all State government agencies, excluding higher education

1. Standard

1.1 State agencies managing content and creating workflow as described in Section 2 shall use the Enterprise Content Management System (ECM) that is provided through the Office of Chief Information Officer (OCIO).

1.2 Agencies must consider, through consultation with the OCIO, using the ECM's E-Forms software for any new electronic forms applications.

2. Managing content and creating workflow includes the following:

- Capturing paper documents through the use of scanners and storing them in electronic form;
- Capturing all type of content (audio, video, e-faxes, emails, MS Office documents, etc) and storing them in electronic form;
- Electronic searching and retrieval of captured content;
- Automating records retention and archiving;
- Automating business processes through workflow;
- Reducing and/or eliminating paper document storage.

3. Purpose

The purpose of this standard is to provide, to the extent possible, a single technical solution for State agencies:

- Capturing all types of content and storing content electronically;
- Converting and minimizing the number of paper documents the State maintains;
- Facilitate searching and retrieval of electronic documents;
- Retain and dispose of electronic documents based on established document retention policies;
- Improve efficiency and accuracy of exchanging information; and
- Unify document management in a single system to take advantage of economies of scale.

4. Exception

This standard does not apply to systems already in use by an agency, unless:

- The agency intends to buy significant upgrades;
- The agency intends to buy a significant amount of new modules; or
- The agency intends to do a significant amount of custom development

For guidance on these points, contact the OCIO.

5. Definitions

5.1 Documents – The State currently utilizes a great deal of paper-based documents. These documents are generated internally from both manual and automated processes. Paper documents also come from external businesses and citizens. Additionally, each paper document is read by a person to determine its purpose, what information it contains, what it is associated with and what should be done with it.

Indexing is a process of extracting the key content of the document and storing that information with the electronic version of the document. The purpose of the index information is to facilitate searching and retrieval of the document and facilitate automating processes using workflow in an agency. The index information can also be used for securing the document as well as to associate multiple documents together.

The ECM will consume paper documents by either using scanners and/or electronic document uploads. The documents can be indexed by automated means using Optical Character Recognition (OCR), Intelligent Character Recognition (ICR) and/or bar codes. The ECM facilitates both automated and manual indexing.

5.2 Processes (Workflow) –For those paper documents that are processed manually, (i.e. from one desk to another, one agency to another, and are dependent on individual organizational skill sets to insure documents are not lost, processed timely, processed accurately and filed correctly) can be greatly improved with automated workflow. Even automated processes that were previous built with little or no integration to other processes can be improved and enhanced as well.

The ECM supplies a framework to allow agencies to easily create flexible automated workflows that can utilize documents or work as independent processes. These automated workflows readily integrate with existing processes.

VERSION DATE: Draft - December 1, 2011
HISTORY:
PDF FORMAT: (to be added)

NITC 7-301

State of Nebraska
Nebraska Information Technology Commission
Standards and Guidelines

NITC 7-301 (DRAFT REVISED)

Title	Wireless Local Area Network Standard
Category	Network Architecture
Applicability	Applies to all state agencies, boards, and commissions, excluding higher education

1. Standard

This standard applies to state agencies which deploy a Wireless Local Area Network (WLAN). This standard is in replacement of previous requirements and is retroactive in perpetuity in the pursuit of remaining current with the constantly changing security needs of wireless connectivity.

1.1. Registration of Wireless Devices

State agencies must register WLANs, including each Access Point (AP) that connects to the State of Nebraska’s private network, with the Office of the CIO (OCIO).

1.1.1. Registration

The registration process will identify: contact information; WLAN device information, including the manufacturer, model, and physical location; the security/firewall technologies being deployed; and, where logging information is to be stored. Registration information should be submitted to the CIO Help Desk at [URL to be added]. **Registration must occur prior to deployment** to prevent the access point from being declared as rogue.

1.1.2. Review and Approval

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

1.1.3. Naming Convention

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

1.1.4. Unregistered (Rogue) and Unsecured Devices

Only approved WLANs and access points will be deployed within state agencies. **Unregistered (rogue) devices will be removed from service.** Network managers for the OCIO will incorporate procedures for scanning for unregistered (rogue) wireless devices and access points. This requires a full understanding of the topology of the network. It also requires performing periodic security testing and assessment, including randomly timed security audits to monitor and track wireless and handheld devices. **OCIO reserves the right to disable network access for a device, server or LAN if inadequate security is found or improper procedures are discovered.**

1.1.5. Internet Only Wireless

If the use of the wireless access is only for internet, then the requesting agency must provide a written method showing how they plan on keeping traffic separate.

1.2. Management and Security of the access point

1.2.1. Physical Security

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

1.2.2. Configuration Management

All wireless access points must be secured using a strong password. Passwords will be changed at least every six months. Administrators must ensure all vendor default user names and passwords are removed from the device.

1.3. Security of the wireless network

1.3.1. Logging

All access to the wireless network must be logged with records kept for a minimum of one (1) year. Records must include the time of access, the IP and MAC addresses of the device, and the username.

1.3.2. Access to State Network

If access is to the states network:

1.3.2.1. Access to the wireless network requires a username and password combination that is unique to each user; and

1.3.2.2. The SSID must use a minimum of WPA2 with the use of a FIPS 140-2 validated AES encryption module

1.3.3. Wireless Intrusion Detection Systems

All wireless networks require the use of wireless intrusion detection systems (WIDS), capable of location detection of both authorized and unauthorized wireless devices. All systems will provide 24/7 continuous scanning and monitoring. WIDS logs and documented actions will be maintained for a minimum of (1) year.

1.4. Management of Airspace

All conflicts regarding wireless connectivity are resolved by the OCIO. Review of airspace requirements and changes will be addressed with notification of compliance.

2. Purpose

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

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

The purpose of this standard is to ensure that only properly secured and managed WLANs are deployed by agencies.

VERSION DATE: DRAFT - February 9, 2012.
REPEALER: Original NITC 7-301 is repealed.
HISTORY: Adopted on September 30, 2003. Revised on August 4, 2006.
PDF FORMAT: (to be added)

NITC 1-204
Attachment A

State of Nebraska
Office of the CIO

List of Preapproved Items for Purchase

For the purpose of procurement reviews conducted pursuant to NEB. REV. STAT. §§ 81-1117, 81-1120.17 and 81-1120.20, the following items are preapproved for purchase by agencies, if the cost of the item is less than $500.00:

1. Functionally equivalent parts needed to repair existing equipment
2. Cables for connecting computer components
3. Power Cords / Adapters
4. Extender Cables for Keyboards / Mice
5. KVM (Keyboard - Video - Mouse) Switches
6. USB / PS2 Connectors
7. Memory Chips
8. Laptop Batteries
9. Laptop Docking Stations
10. UPS (Uninterruptible Power Supply) Units, and replacement batteries
11. Keyboards, including those for tablet computers
12. Mice

~~12.~~13. Microphones
~~13.~~14. Speakers
~~14.~~15. Monitors that are ordered without a system
~~15.~~16. Hard Drives
~~16.~~17. CD/DVD/Blu-ray Drives and Players
~~17.~~18. Video Cards
~~18.~~19. Network Cards
~~19.~~20. Barcode Pens and Readers
~~20.~~21. Card Readers
~~21.~~22. Smart Board Overlays
~~22.~~23. Projectors and Projector Lamps
~~23.~~24. Desktop Printers
~~24.~~25. Printer Toner and Ink
~~25.~~26. Desktop Scanners
~~26.~~27. Small Label Printers
~~27.~~28. Blank CDs ~~or~~, DVDs or Blu-ray Discs
~~28.~~29. Blank Tapes
~~29.~~30. Digital Voice Recorders
~~30.~~31. Flash Drives
~~31.~~32. Software Books
~~32.~~33. Training CDs ~~or~~, DVDs or Blu-ray Discs
~~33.~~34. Logic boards and computers that are integral parts of equipment that serves a primary purpose other than information management, including digital cameras, lab equipment, and motor vehicles. (Items covered here are not subject to the $500.00 limit.)
~~34.~~35. The Office of CIO may provide documented preapproval for the purchase of certain other items by an agency.

Document History: Adopted on March 4, 2008, revised on May 13, 2008 and November 30, 2009.
[Current version posted at: http://nitc.ne.gov/standards/1-204-Attachment-A.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 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. HIPAA)~~ (e.g. PII, FISMA, NIST 800-53). All information must be protected to the standards required. Do not use this form. 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

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

Formatted: Tab stops: 6", Right + Not at 6.5"

Formatted: Font: (Default) Times New Roman, Italic 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 enabled on devices
- Approved wireless transmission protocols and encryption must be used when transmitting *sensitive* information. ~~S~~*Confidential and 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.
- All State and Agency policies governing the use of internal use/public 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.

Formatted: Tab stops: 6", Right + Not at 6.5"

Formatted: Font: (Default) Times New Roman, Italic

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:

____

____

I understand that in the event of litigation, or potential litigation, my personal device may be subject to discovery requirements up to and including impoundment of the device.

________________________________ __________

~~Individual~~ ~~Date~~

________________________________ ________________________________ __________

Individual (printed name) Individual (signature) Date

Formatted: Indent: Left: -0.25", Right: -0.06"

________________________________ __________

~~Agency Director~~ ~~Date~~

________________________________ ________________________________ __________

Agency Director (printed name) Agency Director (signature) Date

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

_____ Approved _____ Denied

Formatted: Tab stops: 6", Right + Not at 6.5"

Formatted: Font: (Default) Times New Roman, Italic

State Information Security Officer ________________________________ Date ______________

Formatted: Tab stops: 6", Right + Not at 6.5"

Formatted: Font: (Default) Times New Roman, Italic

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~~the device should employ a data delete function to ~~delete~~ wipe information ~~on a device that detects a password attack~~ from the device after multiple incorrect passwords/PINs have been entered.
- ~~If available, arrange for a remote data deletion service which can remotely delete sensitive information if the device is lost or stolen~~

Formatted: Font: 8 pt, Italic

Formatted: Font: 8 pt, Italic, English (U.S.)

- 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 ~~PCDs~~ devices 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~~devices as hand luggage when traveling
- ~~Tracking:~~ It is recommended that ~~devices use~~ remote tracking capabilities are enabled on devices.
- Approved wireless transmission protocols and encryption must be used when transmitting *sensitive* information. *Confidential and Sensitive* data traveling to and from the device~~PCD~~ must be encrypted during transmission. For browser based access, SSL encryption meets State standards.
- 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.

Formatted: Font: 8 pt, Italic

Formatted: Font: 8 pt, Italic, English (U.S.)

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. I understand that in the event of litigation, or potential litigation, my personal device may be subject to discovery requirements up to and including impoundment of the device.

~~Individual Date~~

______________________ ______________________ __________

Individual (printed name) Individual (signature) 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~~

______________________ ______________________ __________

Agency Director (printed name) Agency Director (signature) Date

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

_____ Approved _____ Denied

Formatted: English (U.S.)

Formatted: Justified

Formatted: English (U.S.)

Formatted: Font: 8 pt, Italic

Formatted: Font: 8 pt, Italic, English (U.S.)

State Information Security Officer	Date

State CIO	Date

Formatted: Font: 8 pt, Italic

Formatted: Font: 8 pt, Italic, English (U.S.)

The Kronos System is an electronic time keeping system, utilized as a time clock system, by the Department of Health and Human Services and the Department of Correctional Services. The Kronos System is supported by the Office of the CIO. The Kronos Steering Committee is comprised of authorized representatives of each agency, who are empowered to make policy and operational decisions as it relates to use and support of the Kronos tools.

- **Agency name** - Kronos Steering Committee (NDCS/HHSS/OCIO)
- **Name, title, and contact information for the agency contact person regarding the request -** Robert Shanahan, IT Manager, NDCS 402-489-5809
- **Title of the NITC Standards and Guidelines document at issue - ** Standard 8-301 *Password Policy*
- **Description of the problem or issue** – Kronos is currently out of compliance with the NITC Password Policy (and has been so since its inception) in the following areas;
  - Sequential character limitation – none
  - Contains three of four character types – not required
  - Case sensitive characters – not recognized
- **Description of the agency's preferred solution, including a listing of the specific requirement(s) for which a waiver is requested**
  - The Kronos Coordinating Committee with support of OCIO has implemented all aspects of the NITC 8-301 password standard for the Kronos Timekeeping System which are supported natively by the AS/400 operating system. (The AS/400 platform hosts the Kronos Timekeeping System). The Kronos Steering committee requests a waiver from the NITC 8-301 password standard, specifically;
    - NITC waives Standard 8-301 for the Kronos System, contingent on continued enforcement of the following minimum requirements for Kronos;
      - Passwords must contain at least 8 characters
      - Passwords must contain;
        - At least one (1) alphabetic character
        - At least one (1) numeric character
      - Passwords must change at least every 90 days
      - Passwords cannot be the same as any of the previous 32 passwords
- **Any additional information and justification showing good cause for the requested waiver**
  - Although Standard 8-301 includes no requirement that a system must be able to enforce the password criteria, the Auditor of Public Accounts says "it has been our office's position that we cannot verify that users are properly utilizing passwords that meet the criteria without an agency enforcing the criteria through password settings." Consequently, non-compliance with 8-301 has been a finding of recent Kronos audits.

- Approval of this waiver appears to be the only way to satisfy the Auditor, based on the position outlined above. (The alternative is to accept the expense of writing and maintaining custom code in order to achieve full compliance.)
- The Kronos system is not accessible outside of the state network – all users must first authenticate (using fully compliant passwords) to the network before gaining access to the Kronos system
- Kronos access control is reasonable and sufficient, and the additional security to be gained from custom coding is not cost justified.

NITC 8-301

State of Nebraska
Nebraska Information Technology Commission
Standards and Guidelines

NITC 8-301

Title	Password Standard
Category	Security Architecture
Applicability	Applies to all state agencies, boards, and commissions, excluding higher education

1. Purpose

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

2. Standard

2.1 Password Construction

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

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

2.2 Non-Expiring Passwords

An agency may request a non-expiring password by submitting the form found in Appendix A. All non-expiring passwords should meet the character requirements listed in Section 2.1.

2.2.1 Automated System Accounts. Agencies may use non-expiring passwords for automated system accounts. Examples of automated system accounts include those that perform backups or run batch jobs.

2.2.2 Multi-user Computers. Agencies may use non-expiring passwords on multi-user computers. Examples of multi-user computers include those computers in kiosks or training labs, where users have limited or restricted access to state resources.

2.2.3 System Equipment/Devices. It is common for many devices (e.g. IP cameras, HVAC controls) in today's IT environment to utilize login capabilities to protect the device from unauthorized access. While many of these devices make use of a user ID and password in a manner similar to those found while authenticating a user, the distinction to be made is that the User ID is used to authenticate the device itself to the system and not a person.

Attachment A: Non-Expiring Password Request (Word Document)

HISTORY: Adopted on September 18, 2007. Amended on November 12, 2008.
PDF FORMAT: http://nitc.ne.gov/standards/8-301.pdf
