**AGENDA**
**TECHNICAL PANEL**
**Varner Hall - Board Room**
**3835 Holdrege Street**
**Lincoln, Nebraska**
**Tuesday, August 13, 2024**
**9:00 a.m. CT**

I. ROLL CALL; MEETING NOTICE; OPEN MEETINGS ACT INFORMATION

II. PUBLIC COMMENT

III. APPROVAL OF APRIL 9, 2024, MEETING MINUTES *** *(Attachment III)*

IV. REGULAR BUSINESS

A. PROJECTS

1. Enterprise project status dashboard report. Andy Weekly. *(Attachment IV-A-1)*
2. Biennial budget review timeline; October meeting date. *(Attachment IV-A-2)*

B. TECHNICAL STANDARDS AND GUIDELINES

1. Proposal 32. Amend the application code standard. [Motion to recommend approval.] *** *(Attachment IV-B-1)*
2. Proposal 35. Amend access control provisions of the Information Security Policy. [Motion to post for 30-day comment period.] *** *(Attachment IV-B-2)*
3. Proposal 36. Amend system security provisions of the Information Security Policy. [Motion to post for 30-day comment period.] *** *(Attachment IV-B-3)*
4. Proposal 37. Adopt a new section relating to Artificial Intelligence. [Motion to post for 30-day comment period.] *** *(Attachment IV-B-4)*
5. Temporary waivers granted by the state information security officer pursuant to section 1-103(3). Patrick Wright.

V. OTHER BUSINESS

VI. ADJOURN

*** Action item.

The Technical Panel will attempt to adhere to the sequence of the published agenda but reserves the right to adjust the order and timing of items and may elect to take action on any of the items listed. If you need interpreter services or other reasonable accommodations, please contact the Technical Panel at 402-471-3560 at least five days prior to the meeting to coordinate arrangements.

Meeting notice was posted to the NITC website and the Nebraska Public Meeting Calendar on July 29, 2024. The agenda was posted to the NITC website on August 9, 2024.

Nebraska Open Meetings Act | Technical Panel Meeting Documents

# Attachment III

**TECHNICAL PANEL**
Varner Hall - Board Room
3835 Holdrege Street Lincoln, Nebraska
Tuesday, April 9, 2024, 9:00 a.m. CT
**MINUTES**

**MEMBERS PRESENT:**
Kirk Langer, Chair, Lincoln Public Schools
Mark Neemann, Interim Chief Information Officer
Remy Sydik, University of Nebraska
Ling Ling Sun, Nebraska Public Media

**MEMBERS ABSENT:**
Heath Tuttle, University of Nebraska

**STAFF PRESENT:**
Rick Becker, NITC Administrative Manager and Legal Counsel
Lori Lopez Urdiales, Office Services Manager II
Andy Weekly, OCIO Project Management Office, IT Supervisor
Patrick Wright, State Information Security Officer

**ROLL CALL; MEETING NOTICE; OPEN MEETINGS ACT INFORMATION**

Mr. Langer called the meeting to order at 9:01 a.m. A quorum was present. The meeting notice was posted to the NITC website and the Nebraska Public Meeting Calendar on March 25, 2024. The agenda was posted to the NITC website on April 5, 2024. A copy of the Nebraska Open Meetings Act was in the meeting room and a link to the act was included with the agenda.

**PUBLIC COMMENT**

There was no public comment.

**APPROVAL OF FEBRUARY 13, 2024, MEETING MINUTES**

Mr. Langer had a correction to the minutes.

**Mx. Sydik moved to approve the February 13, 2024, minutes as corrected. Mr. Neemann seconded. Roll call vote: Neemann-Yes, Sydik-Yes, Langer-Yes, and Sun-Yes. Results: Yes-4, No-0, Abstained-0. Motion carried.**

**REGULAR BUSINESS**

**PROJECTS**

**Enterprise project status dashboard report.**

Mr. Weekly provided the report and entertained questions from the panel members.

**TECHNICAL STANDARDS AND GUIDELINES**

**Proposal 33. Amend the waiver policy.**

No comments were received during the 30-day comment period.

**Ms. Sun moved to recommend approval of Proposal 33. Mx. Sydik seconded. Roll call vote: Sun-Yes, Langer-Yes, Sydik-Yes, and Neemann-Yes. Results: Yes-4, No-0, Abstained-0. Motion carried.**

**Proposal 34. Adopt a new section relating to international travel.**

No comments were received during the 30-day comment period.

**Ms. Sun moved to recommend approval of Proposal 34. Mr. Neemann seconded. Roll call vote: Sun-Yes, Langer-Yes, Sydik-Yes, and Neemann-Yes. Results: Yes-4, No-0, Abstained-0. Motion carried.**

Ms. Sun complimented the work done by Mr. Wright regarding security issues.

Proposal 32 was discussed at the last meeting. The Security Architecture Workgroup has not had an opportunity to meet and discuss the standard. That proposal will be on the next meeting agenda.

## OTHER BUSINESS

Mx. Sydik reported that the U.S. Attorney General has signed off on new ADA accessibility standards. The NITC's accessibility standards will need to be reviewed for possible updates.

## ADJOURNMENT

**Mr. Neemann moved to adjourn. Mx. Sydik seconded. All were in favor. Motion carried.**

Meeting minutes were taken by Ms. Lopez Urdiales and reviewed by Mr. Becker.

# Attachment IV-A-1

# Projects Status Dashboard

## August 2024

## Enterprise Projects - Current

| Project Name | Sponsoring Government Entity | Manager | NITC Designated | Total Estimated Costs | Actual Costs to Date | Estimate to Complete |
|---|---|---|---|---|---|---|
| Nebraska Regional Interoperability Network (NRIN) | 31 Nebraska Emergency Management Agency (NEMA) | Krogman, Sue | 3/15/2010 | $ 12,500,000.00 | $ 10,405,204.00 | $ 2,094,796.00 |
| iServe Nebraska | 25 Department of Health and Human Services | Leonard, Anthony | 11/12/2020 | $ 33,524,476.00 | $ 26,207,464.00 | $ 7,317,012.00 |
| NDOT Financial System Modernization (WO 275056) | 27 Department of Transportation | Lusero, Cody | 7/8/2021 | $ 5,945,871.00 | $ 1,328,765.55 | $ 4,617,105.45 |
| OPS Retirement Plan Management Transfer | 85 Public Employees Retirement Systems | Deshpande, Jaydeep | 11/4/2021 | $ 5,300,826.00 | $ 5,152,152.77 | $ 148,673.23 |
| SONAR - State of Nebraska Appropriation Request | 65 Department of Administrative Services | Bush, Gary | 11/10/2022 | $ 1,209,574.00 | $ 546,228.04 | $ 663,345.96 |
| Kronos Transition to UKG Dimensions | 65 Office of the CIO | Beer, Joe | 7/14/2023 | $ 1,340,000.00 | $ 1,054,129.25 | $ 285,870.75 |
| Message Switching System (MSS) Modernization Project | 64 State Patrol | Neukirch, Chris | 7/14/2023 | $ 1,628,927.96 | $ 276,953.87 | $ 1,351,974.09 |
| Computer Aided Dispatch Project | 64 State Patrol | Neukirch, Chris | 7/14/2023 | $ - | $ - | $ - |

Note: Status is self-reported by the agency

## Nebraska Regional Interoperability Network (NRIN)

| Report Date | Project ID | Project Manager |
|---|---|---|
| Aug 8, 2024 | PROJ-00011 | Krogman, Sue |

Milestone Timeline

Start Oct 1, 2010

Finish Aug 31, 2026

| Overall Status | Schedule Status | Scope Status | Cost and Effort Status |
|---|---|---|---|
| → Needs Help | → Needs Help | → On Track | → On Track |

Status Report Update

UPDATE FOR AUGUST 2024 – The southeast and south-central electricity has been installed. The tower crew has come back and did their path alignments. The south-central region is complete to the Superior NPPD site. - We will run off of the fiber that NPPD has installed there all the way to Pauline NPPD site. The northeast equipment is prepped and ready to go. The alternative path is from Hubbard NPPD to Thurston WT. We have made several trips and visited with everyone involved. Installation has not yet started, but equipment is ready to go.

UPDATE FOR JUNE 2024 – Finished up all of the installations in the Southeast Region except for the connection from RC Sheriff's tower to dispatch. We will connect to the City's fiber for that. Waiting for the electricians to do all of the path alignments. Working in the South Central area now – have completed connections and installations for the Eastern most part – am waiting for approval from NPPD to connect thru the Doniphan NPPD site.

Key Accomplishments

Finished the electricity in the southeast and south-central regions

Prepped the equipment for the Hubbard NPPD tower to the Thurston water tower

Upcoming Activities

Once the installation crew is ready, will begin working on the installs for the Hubbard to Thurston path.

# iServe Nebraska

| Report Date | Project ID | Project Manager |
|---|---|---|
| Aug 8, 2024 | PROJ-03224 | Leonard, Anthony |

Milestone Timeline

Start **Apr 6, 2020**

Finish **Feb 25, 2027**

| Overall Status | Schedule Status | Scope Status | Cost and Effort Status |
|---|---|---|---|
| → On Track | → On Track | → On Track | → On Track |

Status Report Update

Status Report Update:
1. Iterative development work continues for upcoming iServe Portal releases. Multiple releases have been incrementally deployed since Launch 1 (April 2022) delivered the foundation of the iServe Portal. They are:
a. January 27, 2023, production deployment of the Explore Benefits functionality for all portal users.
b. July 10, 2023, production deployment of the integrated Medicaid and Economic Assistance online application to a select group of Community Partners in Pilot mode (Launch 2).
c. October 16, 2023, production deployment of the integrated and Economic Assistance online application to all Community Partners and Nebraskans as well as USPS standardized address prompts when completing an online application (Launch 3).
d. January 11, 2024, production deployment of the Benefits Applications to all Community Partners and Nebraskans, and the beginning of a standard cadence of releases for the delivery team.
e. April 29, 2024, production deployment – Secure Kisok Deployment; EA Re-certification; PIN Validation to support existing benefit recipient account access for new features; Text Vendor Updates to reference iServe URL; Social Media Links to reference iServe URL; PDF Updates from Operations; "Notification of Expiration" Correspondence to support online recertifications for EA.
f. July 11, 2024 production deployment of Client Benefit Inquiry Dashboard to support Medicaid, and EA program information for participants; Client Preferences updates to correspondence delivery preferences by participants; Economic Assistance Online EA Recertification application 'Save Draft' function; Recertification Support and Enhancements from prior feature rollout.

2. Incremental delivery will continue with upcoming releases, approximately every 14 weeks, as teams continue to complete Program Increment (PI) planning, requirement refinement, development, and testing for the remainder of 2024.

Key Accomplishments

1. Program Increment 9 – Deployed July 2024
a. Delivered Customer Features:
i. Client Benefit Inquiry Dashboard of Medicaid, and EA program information for participants
ii. Client Preferences updates to correspondence delivery preferences by participants
iii. Economic Assistance Online EA Recertification application 'Save Draft' function
iv. Recertification Support and Enhancement
b. Delivered Enhancements:
i. Expedited SNAP Logic updates for initial and recertification applications
ii. CMS SPA updates
iii. EA Rights and Responsibilities disclosure updates for initial and recertification applications
iv. Support of the split of RRP to RCA and RMA benefits
v. Production Support (Explore Benefits, Integrated Initial application, Online EA Recertification)
vi. Ongoing Platform Maintenance and Support

2. Delivered Program Increment (PI) 8 in April 2024
a. Delivered Customer Features:

Upcoming Activities

Actively Working Program Increment 10 – Target Oct 2024
Customer Features Under Development:
1. Client Preferences – adding email validation function
2. Online Recovery of Account Activation PIN

Committed Enhancements Under Development:
1. Client Benefit Inquiry (CBI) - Post release enhancements and defect support
2. Ongoing Production Support (Explore Benefits, Integrated Initial application, Online EA Recertification, CBI Dashboard)
3. Ongoing Platform Maintenance and Support

Design Work Underway
1. CBI Dashboard – Inbound Correspondence Design
2. Multi-language for Login embedded Microsoft B2C function Design
3. Online Medicaid Renewals Screen and Data Prefill Designs

## OPS Retirement Plan Management Transfer

| Report Date | Project ID | Project Manager |
|---|---|---|
| Aug 8, 2024 | PROJ-00912 | Deshpande, Jaydeep |

Milestone Timeline

Start Oct 1, 2021

Finish Sep 2, 2024

| Overall Status | Schedule Status | Scope Status | Cost and Effort Status |
|---|---|---|---|
| → On Track | → On Track | → On Track | → On Track |

Key Accomplishments

Key Accomplishments:-

1. UAT for the project started

Status Report Update

1. Completed in July

• Updated and loaded critical data loaded for data levels 1 – 6 in testing environments.
• Continued data validation and submission of bugs for data and system configuration.
• Continued UAT testing.
• For Development and Conversion identified the list of things that need to be done post deployment.
• Continued testing for converted data.
• Enhancements to DQCP scripts for targeted data quality.
• Began parallel testing with OPS and NPERS focused on Retiree Payroll.
• Ran the first pass as retirement and refunds parallel.
• Reran the updated payroll parallel for month of May

2. Coming up in August

• Regular conversation on critical path and contingency planning including reporting at detailed level on bugs and blocked items.
• Finalize updates for the NPERS Web Portals.
• Continue testing test cases and bugs for Sprints 1 – 4, testing of resolved bugs and re-testing of failed test cases.
• Execute dry run of system cutover and do a mock deployment run of the complete deployment.
• Continue review and subsequent data cleanup for DQCP's.
• Complete mapping and migration for additional identified objects for DL5&6(Related to Outgoing Payment) and purchase of service and refund buybacks.
• Continue Parallel Testing (including resolution of issues/data fixes).
• Communication news letter for the new OSERS members
• Sign off UAT
• Production deployment

3. Scanning project

• 112 boxes have been picked up from OSERS and 107 sent to Secretary of state till date
• This includes over 255,549 pages & 59,544 docs scanned.

4. Implementation of the Multifactor Authentication for the NPERS Self service option

• UAT signoff achieved
• Deployment of code scheduled for Saturday 8/3

Upcoming Activities

# NDOT Financial System Modernization (WO 275056)

| Report Date | Project ID | Project Manager |
|---|---|---|
| Aug 8, 2024 | PROJ-00826 | Lusero, Cody |

Milestone Timeline

Start Mar 28, 2022

Finish Aug 1, 2026

| Overall Status | Schedule Status | Scope Status | Cost and Effort Status |
|---|---|---|---|
| → On Track | | | |

Key Accomplishments

Status Report Update

NDOT has no updates. We are in a holding pattern waiting for meeting with Epiphany group.

Upcoming Activities

# Kronos Transition to UKG Dimensions

Report Date
Aug 8, 2024

Project ID
PROJ-01242

Project Manager
Beer, Joe

Milestone Timeline

Start Aug 29, 2022

Finish Mar 3, 2025

| Overall Status | Schedule Status | Scope Status | Cost and Effort Status |
|---|---|---|---|
| → Needs Help | → Needs Help | → Needs Help | → On Track |

Status Report Update

1. Resources:
New UKG Project Sponsor – Jonnathan Perez (Previously Elizabeth Barner)

2. Scheduling:
We have encountered delays regarding the schedule and go-live dates over the past several months. One item that has played a major factor in this delay is labor distribution calculations/reporting. This is a required and critical item for the Department of Agriculture, as well as the Department of Education, and thus is on the critical path. UKG was notified of this requirement on project inception, and again in late 2023, but is just now being addressed. A Statement of Work has been provided by UKG for Labor Distribution calculations and reporting, and is near acceptance by State of Nebraska. Current estimation of 12 weeks by UKG for completion of labor distribution portion (customer acceptance testing will follow).

3. Integration:
Continuing work on finalizing interface configurations as well as base testing. Payroll export will need to be revisited and tested once labor distribution solution is completed.

4. Telestaff:
Telestaff configuration for Non-production Environment for DCS/DHHS is nearly complete. Currently waiting for business structure and person imports from WFM to Telestaff from UKG solution consultant and telestaff consultants.

5. Testing:
Currently testing integration configurations and looking to move into sample payroll testing over the next several weeks.

Key Accomplishments

Upcoming Activities

Statement of Work - Labor Distribution
Interface/Integration testing
Telestaff environment testing

## SONAR - State of Nebraska Appropriation Request

| Report Date | Project ID | Project Manager |
|---|---|---|
| Aug 8, 2024 | PROJ-01324 | Bush, Gary |

Milestone Timeline

Start Feb 22, 2023

Finish Aug 31, 2024

| Overall Status | Schedule Status | Scope Status | Cost and Effort Status |
|---|---|---|---|
| → Needs Help | → Needs Help | → At Risk | → On Track |

Key Accomplishments

Work is ongoing to produce the reports.

Status Report Update

Work continues on the reporting functionality. The due date for an acceptable report to be produced is August 31, 2024. If an acceptable report is not produced, the project will be cancelled.

The reports are looking good, and expectations are that Allitix will complete the needed work.

Upcoming Activities

Completion of reports by Fluence and acceptance by State Budget Division by August 31, 2024.

# Message Switching System (MSS) Modernization Project

| Report Date | Project ID | Project Manager |
|---|---|---|
| Aug 8, 2024 | PROJ-01443 | Neukirch, Chris |

Milestone Timeline

Start Jun 1, 2023

Finish Jul 31, 2025

| Overall Status | Schedule Status | Scope Status | Cost and Effort Status |
|---|---|---|---|
| → On Track | → On Track | → On Track | → On Track |

Key Accomplishments

Datamaxx has begun the FAT (Factory Acceptance Testing) process.
The Comcast line is scheduled for install on 9/27/2024.

Status Report Update

System Testing
Datamaxx is progressing with the FAT.
Awaiting the final test plans for SAT and UAT.
UAT is scheduled to being 10/1/2024.
Batch processes have been created. Awaiting on permissions to folders to begin testing.

Comcast Connection
Datamaxx is working with Comcast and OCIO on the line into the OCIO Data Center.
Comcast install is scheduled for 9/27/2024.

Switch Connections
Test connections to external systems are in place for 1 of the 2 needed connections (NCIC - Yes, NLETS - No)

Documentation Deliverables
The TEAM (Test and Evaluation Master Plan) has been reviewed and approved.

CLEIN Network
Reviewing standdown and equipment procedures.
Discussing how AFIS will connect to the state network without the CLEIN Network available.

Upcoming Activities

Review the FAT outcomes and SAT and UAT test plans.
Testing the batch processes.
Creating the test plans for NSP and Statewide testing.
Identifying individual testers.

# Computer Aided Dispatch Project

| Report Date | Project ID | Project Manager |
|---|---|---|
| Aug 8, 2024 | PROJ-01444 | Neukirch, Chris |

Milestone Timeline

Start **Jul 31, 2023** Finish **Dec 20, 2026**

| Overall Status | Schedule Status | Scope Status | Cost and Effort Status |
|---|---|---|---|
| → On Track | → On Track | → On Track | → On Track |

Key Accomplishments

The RFP responses were reviewed.
Vendors were selected for in-person presentation

Status Report Update

RFP NSP7149 Z1 was released on 6/10/2024.

Bids were opened on 7/22/2024 and the evaluation started on 7/29/2024.

In August, select vendors will be giving in-person presentations to the evaluation team.

The groups is on track to have a vendor selected by 10/15/2024.

Upcoming Activities

The RFP review will begin on 7/29/2024 and continue through 10/15/2024.
In-person presentations will take place in August and September, 2024.

# Attachment IV-A-2

### Nebraska Information Technology Commission

## 2025-2027 Biennial Budget Review Timeline

| | | |
|---|---|---|
| 1 | IT project proposals due with biennial budget requests | 9/15/2024 |
| 2 | Project reviewers assigned and notice sent to Technical Panel members | 9/20/2024 |
| 3 | Project review documents sent to reviewers | 9/23/2024 |
| 4 | Completed scoring due from reviewers | 10/4/2024 |
| 5 | Reviewer scores and comments sent to agencies for comment/response | 10/7/2024 |
| 6 | Agency response due seven days prior to Technical Panel (optional) | Tech Panel date minus 7 days |
| 7 | **Education Council** meeting (if needed) | 10/16/2024 |
| 8 | **Technical Panel** meeting | 10/23 - 10/31 |
| 9 | **Nebraska Information Technology Commission** meeting | 11/8/2024 |
| 10 | **Report submitted to Governor and Legislature** | 11/15/2024 |

## 1-202. Project reviews; information technology projects submitted as part of the state biennial budget process.

Neb. Rev. Stat. § 86-516 provides, in pertinent part:

> "The commission shall: …. (5) Adopt guidelines regarding project planning and management and administrative and technical review procedures involving state-owned or state-supported technology and infrastructure. Governmental entities, state agencies, and noneducation political subdivisions shall submit all projects which use any combination of general funds, federal funds, or cash funds for information technology purposes to the process established by sections 86-512 to 86-524. The commission may adopt policies that establish the format and minimum requirements for project submissions. The commission may monitor the progress of any such project and may require progress reports; …. (8) By November 15 of each even-numbered year, make recommendations on technology investments to the Governor and the Legislature, including a prioritized list of projects, reviewed by the technical panel pursuant to section 86-521. The recommendations submitted to the Legislature shall be submitted electronically; …."

This policy provides the format, minimum requirements, and review procedures for information technology projects submitted as part of the state biennial budget process. The requirements are as follows:

(1) Format. Budget requests for information technology projects that meet the minimum requirements set forth in subsection (2) must include a completed information technology project proposal form. The form provided in the Nebraska Budget Request and Reporting System is the approved format for information technology project proposals.

(2) Minimum Requirements for Project Submissions.

(a) Information technology projects that meet the following criteria are subject to the project review requirements of this section: (i) the estimated total project costs are more than $500,000, or (ii) the estimated total project costs are more than $50,000, and the project will have a significant effect on a core business function or multiple agencies.

(b) Exceptions. The following information technology projects are not subject to the project review requirements of this section and do not require the submission of a project proposal: (i) multi-year projects that have been reviewed as part of a previous budget submission; or (ii) projects utilizing the enterprise content management system managed by the Office of the CIO.

(3) Technical Review Procedures. The technical review of information technology projects submitted pursuant to this section will consist of the following steps:

(a) Individual Technical Reviewers. Each project will be reviewed and scored by three individual technical reviewers using review and scoring criteria approved by the Technical Panel. Qualified reviewers include: members of the Technical Panel, members and alternates of the advisory councils chartered by the commission, and such other individuals as approved by the Technical Panel.

Assignment of Reviewers. Individual technical reviewers will be assigned to projects as follows: (1) staff will assign three reviewers for each project based on the subject matter of the project; (2) staff will notify Technical Panel members by email of the initial assignment of reviewers; (3) members will have 24 hours to object to any of the reviewer assignments, objections to be made by email to the other members noting the specific assignment for which there is an objection and the reason(s) for the objection; (4) if there are objections, reassignments will be made and communicated in the same manner as the initial assignment, or the Technical Panel chairperson may call a special meeting of the Technical Panel to assign reviewers; (5) staff will provide the assigned reviewers with the project review documents; (6) in the event a reviewer is unable to complete an assigned review, a new reviewer will be assigned using the same process as the initial assignment; and (7) if for any reason less than three individual reviews are completed prior to the Technical Panel's review referenced in subsection (3)(d), the Technical Panel may complete the project review without regard to the requirements of this subsection.

(b) Agency Response. The requesting agency will be provided with the reviewer scores and comments. The agency may submit a written response to the reviewer scores and comments. The deadline for submitting a response will be one week prior to the Technical Panel review referenced in subsection (3)(d).

(c) Advisory Council Review. Depending on the subject matter of a project, one or more of the commission's advisory councils may review the project and provide recommendations to the Technical Panel and commission.

(d) Technical Panel Review. The Technical Panel will review each project including the reviewer scores and comments, any agency response, and any recommendations by the advisory councils. The Technical Panel will provide its analysis to the commission.

(e) Commission Review and Recommendations. The commission will review each project including any recommendations from the Technical Panel and advisory councils. The commission will make recommendations on each project for inclusion in its report to the Governor and the Legislature.

--

**History:** Adopted on June 18, 2008. Amended on June 16, 2010; August 15, 2012; August 14, 2014; July 14, 2016; July 12, 2018; and July 14, 2023.

**URL:** https://nitc.nebraska.gov/standards/1-202.pdf

# Attachment IV-B-1

## State of Nebraska
## Nebraska Information Technology Commission
## Technical Standards and Guidelines

## Proposal 32

A PROPOSAL relating to the application code standards; to amend section 8-602; and to repeal the original section.

Section 1. Section 8-602 is amended to read:

**8-602. Application code.**

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

(2) All application code must be on a vendor-supported version.

(3) All associated libraries, code, and software must be on a vendor-supported version.

(4) All application source code must be backed up and access restricted to authorized personnel only.

(5) Application changes are required to go through a software development life cycle process that ensures the confidentiality of information, and integrity and availability of source and executable code. Application changes must follow the change management process as defined in section 8-202.

Sec. 2. Original section 8-602 is repealed.

Sec. 3. This proposal takes effect when approved by the commission.

Attachment IV-B-2

**State of Nebraska**
**Nebraska Information Technology Commission**
**Technical Standards and Guidelines**

**Proposal 35**

A PROPOSAL to amend access control provisions of the Information Security Policy; to amend sections 8-302 and 8-303; and to repeal the original sections.

Section 1. Section 8-302 is amended to read:

**8-302. Passwords.**

(1) Minimum Password Requirements. The following are the minimum password requirements for state government passwords:

(a) Must contain a minimum of 12 characters;

(b) Must contain at least three of the following: (i) at least one uppercase character; (ii) at least one lowercase character; (iii) at least one numeric character; or (iv) at least one symbol (!@#$%^&);

(c) Must expire after 90 days;

(d) Must have a minimum password age of at least 15 days prior to changing;

(e) Must use multi-factor authentication;

(f) Must not repeat any of the passwords used during the previous 366 days;

(g) Accounts must automatically lock after three consecutive unsuccessful password attempts;

(h) Authentication and credentials must be transmitted over secure protocols; and

(i) Default passwords must be changed before a system is put into production.

(2) Restricted Account and Service Account Passwords. Non-expiring passwords may be used for restricted accounts (“RA”) where the end user is not given the password and service

accounts (“SA”) that are used only for machine-to-machine communications. These accounts are used for programmatic purposes only. For these use cases the following criteria apply:

(a) Must contain a minimum of 20 characters;

(b) Must only be used for a single purpose; and

(c) Must be approved by the state information security officer.

(3) System Equipment/Device Passwords. Agencies may use non-expiring passwords for 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 like 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 in which case the following requirements apply:

(a) Must contain a minimum of 20 characters; and

(b) Remote access and administration must use multi-factor authentication.

~~(1) Minimum Password Requirements. The following are the minimum password requirements for state government passwords:~~

~~(a) Must contain a minimum of eight characters;~~

~~(b) Must contain at least three of the following four: at least one uppercase character; at least one lowercase character; at least one numeric character; or, at least one symbol (!@#$%^&); and~~

~~(c) Cannot repeat any of the passwords used during the previous 365 days.~~

~~In addition to the minimum password complexity outlined above, additional password requirements are necessary for differing levels of data classification when authenticating users to networks or applications. The highest data classification level that a user has access to during an authenticated session will determine the additional password requirements. All~~

~~employees and contractors of the state shall use a password that follows at least a confidential level of authentication when logging into a state network or application.~~

~~(2) Additional Access Requirements for HIGH IMPACT Information. Information that is classified as HIGH IMPACT requires the highest level of security. This includes root/admin level system information accessed by privileged accounts. A password used to access HIGH IMPACT information must follow the password complexity rules outlined in subsection (1), and must contain the following additional requirements:~~

~~(a) Multi-factor authentication;~~

~~(b) Expire after 60 days;~~

~~(c) Minimum password age set to 15 days; and~~

~~(d) Accounts will automatically be disabled after three unsuccessful password attempts.~~

~~(3) Additional Access Requirements for MODERATE IMPACT Information. Information that is classified as MODERATE IMPACT requires a high level of security. A password used to access MODERATE IMPACT information must follow the password complexity rules outlined in subsection (1), and must contain the following additional requirements:~~

~~(a) Expire after 90 days; and~~

~~(b) Accounts will automatically lock after three consecutive unsuccessful password attempts.~~

~~(4) Password Requirements for LOW IMPACT Information. Information that is classified as LOW IMPACT requires minimal level of security and need not comply with subsection (1). Typically, this data would not include personal information but may carry special regulations related to its use or dissemination. LOW IMPACT data may also be data that is sold as a product or service to users that have subscribed to a service.~~

~~(5) Password Requirements for Accessing NO IMPACT Information. Information that is classified as NO IMPACT requires no additional password security and need not comply with subsection (1).~~

~~(6) Non-Expiring Passwords. Non-expiring passwords require a unique high level of security. Typically this information is confidential in nature and must follow the requirements in subsection (1). The additional requirements for access to HIGH IMPACT or MODERATE IMPACT data with a non-expiring password are:~~

~~(a) Extended password length to 10 characters;~~

~~(b) Independent remote identity proofing may be required;~~

~~(c) Personal security question may be asked;~~

~~(d) Multi-factor authentication; and~~

~~(e) Any feature not included on this list may also be utilized upon approval of the state information security officer.~~

~~(7) Automated System Accounts. Examples of automated system accounts include those that act as an intermediary between the public user and state systems, internal system to system interfaces, perform backups or run batch jobs. System account passwords shall expire after 365 days, unless mechanisms to restrict the use of those credentials to just the authorized service can be implemented and approval is granted by the state information security officer.~~

~~(8) Multi-User Computers. Multi-user computers include those computers in kiosks or training labs, where users have limited or restricted access to state resources. Agencies may use non-expiring passwords on multi-user computers. In these cases, mechanisms to ensure the user account with non-expiring passwords is unable to access HIGH IMPACT or MODERATE IMPACT information.~~

~~System Equipment/Devices. Agencies may use non-expiring passwords for 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 like 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.~~

Sec. 2. Section 8-303 is amended to read:

**8-303. Identification and authorization.**

(1) All employees and other persons performing work on behalf of the state, authorized to access any state information or IT resources, that have the potential to process, store, or access non-public information, must be assigned a unique identifier which resides in a State of Nebraska identity management system with the minimum necessary access required to perform their duties to align with the least privilege methodology.

(2) Staff are required to secure their user IDs from unauthorized use.

(3) Sharing user IDs is prohibited.

(4) To reduce the risk of accidental or deliberate system misuse, separation of duties must be implemented where practical. Whenever separation of duties is impractical, other compensatory controls such as monitoring of activities, increased auditing and management supervision must be implemented. At a minimum, the audit of security must remain independent and segregated from the security function.

(5) State credentials and email addresses may only be used for the conduct of state business, state government sponsored activities, and such other uses allowed by law.

Sec. 3. Original sections 8-302 and 8-303 are repealed.

Sec. 4. This proposal takes effect when approved by the commission.

# Attachment IV-B-3

**State of Nebraska**
**Nebraska Information Technology Commission**
**Technical Standards and Guidelines**

**Proposal 36**

A PROPOSAL to amend system security provisions of the Information Security Policy; to amend sections 8-504; to adopt a new section relating to kiosks and public access workstations; and to repeal the original section.

Section 1. Section 8-504 is amended to read:

**8-504. Minimum workstation configuration.**

Improperly configured workstations are at risk to be compromised. Without proper adherence to these workstation security standards, the state is at increased risk to have data lost, stolen, or destroyed. This standard is necessary to protect the state from unauthorized data or activity residing or occurring on state equipment. It is also necessary to reduce the likelihood of malicious activity propagating throughout the state networks or launching other attacks. All managed workstations that connect to the state's network are required to meet these standards. The Office of the CIO is responsible for maintaining these standards and for configuring and managing the hardware, software, and imaging processes for all managed workstations. Workstation standards should be securely maintained and stored in a centralized documentation library. The degree of protection of the workstation should be commensurate with the data classification of the resources stored, accessed, or processed from this computer. The following are minimum workstation configuration standards:

(1) OCIO-approved endpoint security (anti-virus) software~~,~~ must be installed and enabled;

(2) The host-based firewall must be enabled;

(3) The operating system must be configured to receive automated updates;

(4) The system must be configured to enforce password complexity standards on accounts;

(5) Application software should only be installed if there is an expectation that it will be used for state business purposes. Application software not in use should be uninstalled;

(6) All application software must have security updates applied as defined by patch management standards and be of a vendor supported version;

(7) Web browsers settings should be selected or disabled as appropriate to increase security and limit vulnerability to intrusion;

(8) CIS Level 1 Controls should be maintained on all state managed workstations, where technically feasible;

(9) Shared login accounts are prohibited unless approved in advance and configured by IT. Shared login accounts are only acceptable if approved through the policy exception process and alternate mechanisms or access layers exist to ensure the ability to individually identify personnel accessing non-public information;

(10) Shared login accounts are forbidden~~ on multi-user systems where the manipulation and storage of HIGH IMPACT or MODERATE IMPACT information takes place~~;

(11) Users need to lock their desktops when not in use. The system must automatically lock a workstation after ~~5~~ 10 minutes of inactivity;

(12) Users are required to store all HIGH IMPACT or MODERATE IMPACT information on IT managed servers, and not the local hard drive of the computer. Local storage may only be used for temporary purposes when the data stored is not sensitive, and where loss of the information will not have any detrimental impact on the state;

(13) All workstations must be re-imaged with standard load images prior to reassignment; and

(14) Equipment scheduled for disposal or recycling must be cleansed following agency media disposal guidelines.

Sec. 2. The following new section is adopted:

**8-508. Kiosks and public access workstations.**

The purpose of this section is to provide standards and guidelines for kiosks and public access workstations (“kiosks”).

(1) Physical Security. (a) All publicly accessible kiosks must be physically secured to prevent theft, tampering, or unauthorized access; (b) kiosks must be installed in well-lit, high-traffic areas to minimize the risk of vandalism, unauthorized access, or tampering; and (c) where feasible, kiosks should be monitored with security cameras.

(2) Access Control. (a) Access to the kiosks' administrative functions and settings must be restricted to authorized personnel only and never granted to the public user; (b) all administrative passwords and access credentials must be securely stored and regularly updated; (c) users should only be granted access to features and functions necessary for their intended use of the kiosk; (d) the kiosks must not be able to access HIGH IMPACT data; and (e) kiosks must be segregated from other state resources by network segmentation or other means.

(3) Software Security. (a) Kiosks must meet the requirements of section 8-504; and (b) access to external devices such as USB and other mass storage devices must be disabled to prevent the introduction of malware or unauthorized software.

(4) Data Protection. (a) Any personally identifiable information (“PII”) collected by kiosks must be stored and transmitted using secure protocols; (b) encryption must be used to protect sensitive data both in transit and at rest; and (c) data collected by kiosks must be limited to what is necessary for the intended purpose and must not be retained longer than necessary.

(5) Monitoring and Compliance. (a) Regular audits and monitoring should be conducted to ensure compliance with this policy; and (b) any security incidents or breaches involving kiosks must be promptly reported to the Office of the CIO and investigated.

Sec. 3. Original section 8-504 is repealed.

Sec. 4. This proposal takes effect when approved by the commission.

Attachment IV-B-4

**State of Nebraska**
**Nebraska Information Technology Commission**
**Technical Standards and Guidelines**

**Proposal 37**

A PROPOSAL to adopt a new section relating to artificial intelligence.

Section 1. The following new section is adopted:

**8-609. Artificial intelligence policy.**

Artificial Intelligence ("AI") is the development of information processing systems that perform functions commonly associated with human intelligence, such as reasoning, learning, decision-making, language translation, and self-improvement. AI systems are available in a variety of types and categories, including: standalone systems (e.g., OpenAI – Enterprise ChatGPT, and DALL-E); integrated as features within search engines (e.g., Microsoft Bing chat and Google Gemini); and embedded in other software tools. (e.g., Adobe AI Assistant and Microsoft Copilot).

For AI systems owned, used, or managed by the State of Nebraska the following standards and guidelines apply:

(1) Valid and Reliable. (a) AI technologies must be reliable and consistently valid or accurate in its responses and output; and (b) agencies shall confirm the validity and reliability of output produced by AI technologies.

(2) Transparency. (a) Increased transparency fosters trust in AI technology and systems. AI technology transparency, combined with a risk management strategy, can minimize the impact of risks and adverse outcomes; (b) transparency on the use of AI must be clearly explained, communicated, and understandable; (c) agencies shall be transparent about AI technologies and their outputs, disclosing where constituents are interacting with AI, the outcome and/or

impact, if applicable, and the business purposes where AI is used; and (d) when using LOW IMPACT data, agencies shall ensure all systems and processes employing AI for decision-making or output generation are clearly marked to enhance transparency and accountability.

(3) Accountability. (a) Agencies must ensure AI used within systems is securely developed, assessed for risk, and monitored regularly; (b) agencies must ensure AI is used responsibly, operating correctly, and compliant with applicable laws, regulations, policies, procedures, standards, guidelines, and best practices; and (c) agencies must ensure that MODERATE IMPACT or HIGH IMPACT data is not used within AI systems or processes or part of a generated outcome from AI systems.

(4) Security and Risk Management. (a) Agencies utilizing AI system technologies shall incorporate OCIO's Security Risk Mitigation and Compliance ("RMC") into system development and operations when applicable; (b) privacy impact assessments, third-party and security risk assessments must be conducted regularly to ensure that security, safety, confidentiality, civil liberties, civil rights, and privacy are protected while continuing to promote and empower the use of AI to benefit the State of Nebraska and its citizens; (c) agencies shall not input any content into public AI technology services that contains MODERATE IMPACT or HIGH IMPACT data. LOW IMPACT data, which is publicly available data, is permitted for use with AI technologies; (d) the Office of the CIO shall establish appropriate controls and risk mitigation to mitigate identified risks and ensure the use of AI does not compromise the safety, soundness, or integrity of the entity's data and systems; (e) the Office of the CIO shall provide AI training through the cybersecurity education and awareness platform; (f) agencies shall provide role-based training to team members for specific and unique AI technologies used for their business purposes; and (g) the following are approval requirements for the use of AI: (i) the Office of the CIO must review and approve all AI technologies, including free software services; (ii) the Office of the CIO must maintain a list of approved AI technology; (iii) agencies shall only use OCIO-

approved AI technologies; and (iv) agencies may request an evaluation of new technologies through the OCIO Cloud Review Board.

(5) Privacy. (a) AI systems must comply with all applicable data protection and privacy laws, regulations, and guidelines; (b) agency, constituent, and regulated data must be collected, stored, processed, and shared in a secure and confidential manner, with explicit consent obtained where required; (c) agencies shall design and implement data privacy procedures for specific AI technologies being used; and (d) agencies shall evaluate the accuracy and compliance of AI technologies on a regular basis.

(6) Ethics, Fairness, and Bias. (a) AI technologies must be ethical, fair, and unbiased in a manner that is not discriminatory and negatively affects a specific group of people; (b) human rights, civil liberties, and dignity must be protected while making the selection of AI technologies and using their output; and (c) agencies shall ensure that AI technologies utilize an ethical and fair representation of culture, economics, and society within their data sets and that benefits are accessible to all citizens.

Sec. 2. This proposal takes effect when approved by the commission.