AGENDA
TECHNICAL PANEL
Varner Hall - Board Room
3835 Holdrege Street
Lincoln, Nebraska
Monday, October 28, 2024
1:00 p.m. CT

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

II. PUBLIC COMMENT

III. APPROVAL OF SEPTEMBER 6, 2024, MEETING MINUTES *** *(Attachment III)*

IV. REGULAR BUSINESS

A. PROJECTS

1. Enterprise project status dashboard report. Andy Weekly. *(Attachment IV-A-1)*
2. Recommend closure of the following enterprise projects: (1) SONAR - State of Nebraska Appropriation Request and (2) OPS Retirement Plan Management Transfer. ***

B. TECHNICAL STANDARDS AND GUIDELINES

1. Proposal 35. Amend access control provisions of the Information Security Policy. [Motion to recommend approval.] *** *(Attachment IV-B-1)*
2. Proposal 36. Amend system security provisions of the Information Security Policy. [Motion to recommend approval.] *** *(Attachment IV-B-2)*
3. Proposal 37. Adopt a new section relating to artificial intelligence. [Motion to recommend approval.] *** *(Attachment IV-B-3)*

V. INITIAL DRAFT RULES AND REGULATIONS RELATING TO CYBERSECURITY RECORDS (*Attachment V)*

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 October 1, 2024. The agenda was posted to the NITC website on October 23, 2024.

Nebraska Open Meetings Act | Technical Panel Meeting Documents

Attachment III

TECHNICAL PANEL
Varner Hall - Board Room
3835 Holdrege Street Lincoln, Nebraska
Friday, September 6, 2024, 9:00 a.m. CT
MINUTES

MEMBERS PRESENT:
Kirk Langer, Chair, Lincoln Public Schools
Dr. Matthew McCarville, Chief Information Officer, State of Nebraska
Ling Ling Sun, Nebraska Public Media
Remy Sydik, University of Nebraska
Rick Haugerud, University of Nebraska

MEMBERS ABSENT:
None

STAFF PRESENT:
Rick Becker, NITC Executive Administrator and Legal Counsel
Patrick Wright, State Chief Information Security & Privacy Officer

ROLL CALL; MEETING NOTICE; OPEN MEETINGS ACT INFORMATION

Mr. Langer called the meeting to order at 9:00 a.m. A quorum was present. The meeting notice was posted to the NITC website and the Nebraska Public Meeting Calendar on August 23, 2024. The agenda was posted to the NITC website on September 4, 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 AUGUST 13, 2024, MEETING MINUTES

Ms. Sun moved to approve the August 13, 2024, minutes as presented. Dr. McCarville seconded. Roll call vote: McCarville-Yes, Sydik-Yes, Langer-Yes, Haugerud-Yes, and Sun-Yes. Results: Yes-5, No-0, Abstained-0. Motion carried.

REGULAR BUSINESS

TECHNICAL STANDARDS AND GUIDELINES

Proposal 37. Adopt a new section relating to artificial intelligence.

This proposal was previously discussed at the August meeting. A revised version was included in the meeting documents.

Members discussed the revised proposal and made the following changes by consensus:

1. On page 1, line 3, after “systems” insert “capable of generating output” and on line 4, strike “simulate” and insert “simulates”;
2. On page 1, line 12, after “(b)” insert “agencies must conduct” and on line 13, strike “must be conducted”;
3. On page 1, line 4, strike “technologies are” and insert “is” and on line 10, strike “technologies”;
4. On page 1, line 16, strike “technology services for” and insert “with”;
5. On page 1, line 18, strike “technologies” and on page 2, lines 3, 5, and 21, strike “technologies”;
6. On page 1, beginning in line 17, strike “, which is publicly available,”;

7. On page 2, line 5, after the second “AI” insert “for use with HIGH IMPACT or MODERATE IMPACT data, or LOW IMPACT data that contains personal data elements”;
8. On page 2, beginning in line 5, strike subsection (ii) in its entirety and renumber the remaining subsections accordingly;
9. On page 2, beginning in line 6, strike “through the OCIO Cloud Review Board” and insert “by the Office of the CIO”;
10. On page 2, beginning in line 7, strike “can only be retrained on agency data, unless specifically intended for public use” and insert “may only be trained or retrained on agency data in combination with LOW IMPACT or NO IMPACT data”;
11. On page 2, line 9, after “AI” insert “generated output”, after “unbiased” insert “to support practices that neither discriminate nor negatively impact a specific group of people”, and strike the remainder of subsection (2);
12. On page 2, line 12, after “(a)” insert “Agencies use of”;
13. On page 2, beginning in line 18, strike subsections (a) and (b) and insert “(a) AI must be verifiably reliable and valid; (b) predictive AI must be identified as data supported projections; and (c) agencies shall verify the validity and reliability of AI;”;
14. On page 2, line 21, strike “and their” and insert “use and”;
15. On page 2, line 22, after “outputs,” insert “data set transformations and substitutions”;
16. On page 2, line 22, strike “disclosing” and insert “; (b) agencies shall disclose” and renumber the remaining subsection accordingly; and
17. On page 3, line 3, strike “monitored regularly” and insert “reviewed periodically”.

Dr. McCarville moved to post Proposal 37 as revised for the 30-day public comment period. Mx. Sydik seconded. Roll call vote: McCarville-Yes, Sydik-Yes, Langer-Yes, Haugerud-Yes, and Sun-Yes. Results: Yes-5, No-0, Abstained-0. Motion carried.

OTHER BUSINESS

There was no other business.

ADJOURNMENT

Dr. McCarville moved to adjourn. Mr. Langer seconded. All were in favor. Motion carried.

The meeting was adjourned at 10:55 a.m.

The meeting minutes were taken by Mr. Becker.

Attachment IV-A-1

Projects Status Dashboard

October 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
Oct 23, 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 OCTOBER 2024 – Work continues on the South Central area in and around Nuckolls County. The new tower for Nelson Dispatch has been ordered and should be delivered by the 1st of the year. Pre-work on the Dakota City to Tekamah path is complete and bids have gone out for tower crews. We are expecting as much of that build-out to be completed this year. The Governance Committee is considering hiring a second full-time person to work on all hardware equipment and be the POC for our vendors.

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.

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
Oct 15, 2024	PROJ-03224	Leonard, Anthony

Milestone Timeline

Start **Apr 6, 2020** — Finish **Feb 28, 2027**

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

Status Report Update

Overall Status: Green
Status Report Update:

Note -
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.
(Please Note The full history of the themes of "all the releases" has been emailed to Andy Weekly. Due to space limitations in this field I am only including historically the release themes from 2024 to current).
a.) 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.
b.) 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.
c.) 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.
d.) October 10th, 2024, production deployment Client Preferences email verification; Online Recovery of Account Activation PIN, Application Data API to facilitate automated Pend & Tie actions within Operations.

2.) Incremental delivery will continue with upcoming releases, approximately every 14 weeks, as teams continue to complete Program Increment (PI) planning of agency approved priorities, requirement refinement, development, and testing for the remainder of 2024 and into the first quarter of 2025.

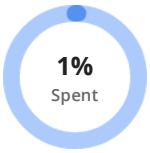
Key Accomplishments

Program Increment 10 – Deployed October 10th, 2024.
• Client Preferences – Email validation function.
• Online Recovery of Account Activation PIN
• Application Data API – support future automated pend and tie feature for operations.
• Revised income levels for Explore Benefit feature to be inline with benefit program updated thresholds

Upcoming Activities

Actively Working Program Increment 11 – Target Jan 2025
• Planned Customer Features:
o HCBS Online Application
o Medicaid Online Renewals
o High Priority Enhancements
o Change in Circumstance (Note: This effort is

Effort Metrics



Total Effort	42,765,964.74
Spent	284,857.75
Effort Balance	42,481,106.99

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			

Status Report Update

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

Key Accomplishments

Upcoming Activities

OPS Retirement Plan Management Transfer

Report Date	Project ID	Project Manager
Oct 1, 2024	PROJ-00912	Deshpande, Jaydeep

Milestone Timeline

Start **Oct 1, 2021** — Finish **Sep 30, 2024**

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

Status Report Update

Accomplishments

1. Go live achieved successfully.
2. Started with Daily backup on 8/30 and once the backup finished around 8 we were able to get the Data conversion started.
3. With all tasks and deployment of code completed Sunday 9/1 Morning a little ahead of schedule.
4. UAT was conducted in the afternoon of Sunday 9/1 and the system was confirmed successfully deployed by the UAT team around 4 PM.

Sincere vote of thanks to the OCIO SQL team during this long weekend time to be available and helpful late night and throughout the entire weekend. their support was an immense help in bringing this project to conclusion.

Recommend closing for Enterprise Status Reporting

Key Accomplishments

Key Accomplishments:-
1. Project Go live completed successfully.

Upcoming Activities

Project Support

SONAR - State of Nebraska Appropriation Request

Report Date	Project ID	Project Manager
Oct 22, 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	↓ At Risk	→ At Risk	→ On Track

Status Report Update

Final reports were provided by the deadline and were not acceptable. Decision has been made to terminate the project.

Key Accomplishments

None

Upcoming Activities

Termination of the Project.

Kronos Transition to UKG Dimensions

Report Date	Project ID	Project Manager
Oct 23, 2024	PROJ-01242	Beer, Joe

Milestone Timeline

Start **Aug 29, 2022** — Finish **May 30, 2025**

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

Status Report Update

1. Updates:
Labor Distribution Kickoff Meeting held on 10/17.
2. Scheduling: We have encountered delays regarding the schedule and go-live dates over the past six 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. Current estimation of 12 weeks by UKG for completion with a current planned date of completion on 2/7/25 (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 will move into payroll testing once Labor Distribution portion is complete.

Key Accomplishments

Upcoming Activities

Labor Distribution Solution (10/17/25 to 2/7/25)

Message Switching System (MSS) Modernization Project

Report Date	Project ID	Project Manager
Oct 1, 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

Status Report Update

System Testing
Datamaxx has completed FAT and NSP is reviewing the documentation.

Awaiting the final test plans for SAT and UAT.
UAT is scheduled to being 10/28/2024. - This is a slight but acceptable delay.

Comcast Connection
Datamaxx is working with Comcast and OCIO on the line into the OCIO Data Center.
Install was worked on 9/27/2024.

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

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

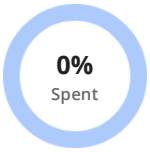
Key Accomplishments

NSP has prepared their UAT testing procedures. Several agencies have agreed to assist with testing.

Upcoming Activities

Complete UAT test plan process.
UAT Testing of the three areas, user, admin and batch/interface processes.

Effort Metrics



Total Effort	4,450.00
Spent	0.00
Effort Balance	4,450.00

Computer Aided Dispatch Project

Report Date	Project ID	Project Manager
Oct 1, 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

Continued review of the proposals to select the best solution for NSP.

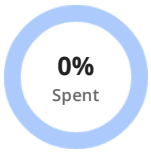
Status Report Update

The Evaluation Team is working through their final evaluations to determine the selection of the vendor.

Upcoming Activities

Reviewing scores and making a final decision on the selected vendor.

Effort Metrics



Total Effort	1,732.00
Spent	0.00
Effort Balance	1,732.00

Attachment IV-B-1

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-2

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 activity 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 by the state information security officer ~~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)~~(10) Users need to lock their desktops when not in use. The system must automatically lock a workstation after ~~5~~ 10 minutes of inactivity;

~~(12)~~(11) 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)~~(12) All workstations must be re-imaged with standard load images prior to reassignment; and

~~(14)~~(13) 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-3

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 capable of generating output that simulates functions commonly associated with human intelligence. AI is available in a variety of types and categories, including standalone systems (e.g., OpenAI – ChatGPT, and DALL-E), integrated as features within search engines (e.g., Microsoft Bing 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) Security and Risk Management. (a) Agencies utilizing AI shall consult with Office of the CIO's Security Risk Mitigation and Compliance team ("RMC") regarding system development and operations; (b) agencies must conduct privacy impact assessments, third-party and security risk assessments 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 residents; (c) agencies shall not utilize public AI with data classified as HIGH IMPACT or MODERATE IMPACT, nor LOW IMPACT data that contains personal data elements. LOW IMPACT or NO IMPACT data is permitted for use with public AI; (d) the Office of the CIO shall establish appropriate controls and risk mitigations to identify and

mitigate risks and ensure the use of AI does not compromise the safety or integrity of agency data and systems; (e) the Office of the CIO shall provide general AI training; (f) agencies shall provide role-based training to team members for specific and unique AI used for their business purposes in advance of production implementation; and (g) the following are approval requirements for the use of AI: (i) the Office of the CIO must review and approve all AI for use with HIGH IMPACT or MODERATE IMPACT data, or LOW IMPACT data that contains personal data elements; (ii) agencies may request an evaluation of new AI by the Office of the CIO; and (iii) AI used by agencies may only be trained or retrained on agency data in combination with LOW IMPACT or NO IMPACT data;

(2) Ethics, Fairness, and Bias. (a) AI generated output must be ethical, fair, and unbiased to support practices that neither discriminate nor negatively impact a specific group of people;

(3) Privacy. (a) Agencies use of AI must comply with applicable data protection and privacy laws, regulations, and guidelines; (b) agency, constituent, and regulated data must be collected, stored, used, and distributed securely and confidentially, with explicit consent obtained where required; (c) in consultation with the Office of the CIO agencies shall design and implement data privacy procedures for specific AI being used; and (d) agencies shall evaluate privacy compliance of AI periodically where appropriate;

(4) Validity and Reliability. (a) AI must be verifiably reliable and valid; (b) predictive AI must be identified as data supported projections; and (c) agencies shall verify the validity and reliability of AI;

(5) Transparency. (a) Agencies shall be transparent about AI use and error rates, biases, outputs, data set transformations and substitutions; (b) agencies shall disclose where constituents are interacting with AI, the outcome and impact, if applicable, and the business purposes where AI is used; and (c) agencies shall ensure all systems and processes employing AI for decision-making or output generation are clearly marked to enhance transparency and accountability; and

(6) Accountability. (a) Agencies must ensure AI used within systems is securely developed in accordance with NITC standards and guidelines, assessed for risk and biases, as well as reviewed periodically; (b) agencies must ensure AI is used responsibly, operating as intended, and compliant with applicable laws, regulations, policies, procedures, standards, guidelines, and best practices.

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

Attachment V

Neb. Rev. Stat. § 84-712.05 provides, in pertinent part:

> "The following records, unless publicly disclosed in an open court, open administrative proceeding, or open meeting or disclosed by a public entity pursuant to its duties, may be withheld from the public by the lawful custodian of the records:
>
> …
>
> (26) Records relating to the nature, location, or function of cybersecurity by the State of Nebraska or any of its political subdivisions or any other public entity subject to sections 84-712 to 84-712.09, including, but not limited to, devices, programs, or systems designed to protect computer, information technology, or communications systems against terrorist or other attacks. The Nebraska Information Technology Commission shall adopt and promulgate rules and regulations to implement this subdivision;…."

https://nebraskalegislature.gov/laws/statutes.php?statute=84-712.05

For purposes of Neb. Rev. Stat. § 84-712.05(26), records relating to the nature, location, or function of cybersecurity include but are not limited to the following items, provided that a reasonable person, knowledgeable of cybersecurity best practices, would conclude that public disclosure of such items would create a substantial likelihood of endangering the security of the public entity's information technology infrastructure:

(1) Personnel. (a) The identity of personnel responsible for configuring or maintaining cybersecurity systems and assets; and (b) the identity of personnel in leadership roles who have direct responsibility or oversight of cybersecurity system and assets.

(2) Risk Management. (a) Risk assessment reports; (b) vulnerability assessments; and (c) penetration testing reports.

(3) Compliance and Legal Documentation. (a) Contract language that describes or defines cybersecurity related services and capabilities; (b) regulatory compliance documentation; and (c) technology audit reports.

(4) Technical Controls and Configurations. (a) Firewall configurations; (b) network segmentation plans; (b) access control policies; (c) encryption and key management policies; and (d) endpoint security settings and controls.

(5) Monitoring and Logging. (a) Log management plans; (b) SIEM (Security Information and Event Management) reports or data; (c) intrusion detection/prevention system (IDS/IPS) logs; (d) vulnerability scanning logs; (e) endpoint defense logs; and (f) firewall logs.

(6) Incident Response and Forensics. (a) Incident handling documentation; (b) incident response plans; (c) forensics analysis reports; and (d) evidence collection procedures.

(7) Employee Awareness and Training. (a) Security awareness training materials; (b) phishing simulation reports; and (c) training attendance records.

(8) Software and Patch Management. (a) Software inventory; (b) patch management records; and (c) configuration management documentation.

(9) Access Control and Authentication. (a) Identity and access management policies; (b) password policies; and (c) multi-factor authentication (MFA) policies.

(10) Data Protection Documentation. (a) Backup and recovery plans (BC/DR Plans); (b) data loss prevention (DLP) policies; (b) data loss prevention configurations and documentation; and (c) secure data storage and disposal documentation.

(11) Third-Party and Vendor Management. (a) Third-party security assessments; and (b) vendor risk management documentation.