Executive Memorandum No. 48

Acceptable Use of Artificial Intelligence (AI) Systems

1. Purpose

The University of Nebraska supports the responsible use of Artificial Intelligence (AI) [a.k.a. Super Intelligence (SI)] technologies to advance instruction, research, University-operated clinical operations, administration, innovation, outreach, academic service, and all other University services. The purpose of this Executive Memorandum is to establish requirements for the secure, ethical, compliant, and responsible use of AI technologies by the University when accessing, creating, processing, transmitting, storing, or generating data and information used to conduct its business and educational functions, including but not limited to Institutional Data and Research Data as defined in Executive Memorandum 42, student responses to assignments, faculty and staff research, publications, and creative activities, collectively "University Information."

Nothing in this memorandum is intended to prescribe whether or how AI may be used for teaching, learning, curricular development, scholarship, research, creative activity, or assessment where such use otherwise complies with applicable law, University policy, data-protection requirements, and contractual obligations. Faculty members and academic units retain authority, consistent with applicable University policies, governance, and this Executive Memorandum, to establish expectations for the appropriate use, limitation, disclosure, or prohibition of AI within their courses, assignments, research, creative activities, and disciplines.

This memorandum supplements and shall be interpreted in conjunction with all University of Nebraska System policies, but of particular relevance:

- **Executive Memorandum 16 (Responsible Use of University Computers and Information Systems)**, which establishes requirements for the authorized and secure use of University information systems.
- **Executive Memorandum 41 (Policy on Research and Data Security)**, which establishes requirements for the ownership, classification, storage, retention, transfer, security, and breach reporting of research data.

- **Executive Memorandum 42 (Policy on Risk Classification and Minimum Security Standards)**, which classifies institutional and research data and establishes minimum security requirements for systems that access, process, transmit, or store such data.
- **Executive Memorandum 47 (Information and Communication Technology Accessibility Policy),** which establishes accessibility requirements for Information and Communication Technology, Web Content, and Mobile Applications procured, developed, maintained, or used by or for the University.

2. Scope

This memorandum applies to the use or handling of University Information by all University faculty, staff, students, contractors, consultants, affiliates, volunteers, visiting scholars, and other workforce members when using any AI technology, including but not limited to: generative AI platforms; large language models; AI coding tools; AI transcription and summarization tools; AI-powered research tools; AI-enabled analytics platforms; and autonomous AI agents and workflows.

Consistent with Executive Memorandum 42, this policy applies regardless of where data resides, including on-premises, cloud-hosted, third-party, and personally owned devices.

The University recognizes that there may be academic or research pursuits that require deviations from standard policies, standards, and procedures. Therefore, the University has developed an exception process that users may utilize to justify such deviations and document the associated risks. Exceptions and the exception process are defined in section 11 of this Executive Memorandum.

3. Policy Statement

3.1 Responsible Use

Within the framework established by this Executive Memorandum, University Approved AI Technology may be used to augment human work and decision-making. “University Approved AI Technology” means an AI technology that has been authorized through all applicable University technology, security, privacy, procurement, records retention, and governance processes for the relevant data classification and intended use. Responsibility for compliance with all University policies and the accuracy, appropriateness, legality, and compliance of AI-generated output remains with the individual using the technology.

3.2 Student Use in Academic Work

Use of AI in student academic work, including research and creative activities, is governed by the expectations established by the faculty member or academic unit responsible for the course or assignment. Faculty may permit, restrict, require disclosure of, or prohibit AI use as appropriate to the learning objectives and disciplinary context.

3.3 Faculty and Staff Use in University Business

Faculty and staff may use University Approved AI Technologies for University Business when such use is consistent with this memorandum, applicable unit policies, and the following:

1. Supports legitimate University business, research, creative, educational, or operational activities.
2. Complies with applicable laws, regulations, contracts, sponsor requirements, accreditation obligations, and University policies.
3. Protects the confidentiality, integrity, availability, ownership, and stewardship of University Information.
4. Utilizes University-Approved AI Technologies appropriate to the classification of the data being processed.
5. Ensures human accountability for decisions, actions, and outcomes influenced by AI.
6. Is approved for use by faculty/staff ultimately responsible for the assignment, research project, or work product.
7. Is undertaken only by users who have completed the information-security training required under Executive Memoranda 16, 41, and 42 for the applicable data classification and use and who have completed AI training.

Additional approval is required where otherwise specified by University policy, the responsible unit, law, contract, sponsor requirements, or applicable data-protection requirements.

4. Data Protection Requirements

4.1 Institutional Data Protection

In accordance with Executive Memorandum 42, University institutional and research data must be classified and protected according to its risk classification.

Institutional and research data may only be entered, uploaded, processed, analyzed, generated, stored, or transmitted within University Approved AI Technologies.

4.2 Protected Technology Requirement

University institutional and research data shall be created, accessed, stored, processed, transmitted, and retained only through University Approved AI Technologies that have been acquired in compliance with all applicable University policies and processes such that the technologies provide appropriate contractual, security, privacy, and compliance protections.

Unless explicitly approved through the Exception Process, or such information is already in the public domain or classified as Low Risk, institutional and research data shall not be entered into, uploaded to, processed by, or retained within:

- An individual's personal AI subscription, personal cloud services, or personal cloud storage as defined in ITS-00: Information Technology Definitions Standard.
- AI technologies that claim ownership rights to institutional and research data.
- AI technologies that train models using institutional and research data.
- AI services lacking contractual protections sufficient to protect University interests in the institutional and research data.

Unless explicitly approved through the Exception Process, any AI service used to process institutional and research data must:

- Utilize University identity management and access management systems;
- Meet applicable security and privacy requirements, including those required by Executive Memorandum 42;
- Maintain appropriate contractual protections that have been reviewed and meet all necessary protections for technology, security, privacy, procurement, records retention, and governance implications; and
- Support compliance with applicable legal and regulatory obligations.

4.3 AI-Related Security Incidents

Users shall report known or suspected security or data incidents, including those that involve AI technologies, in accordance with applicable University incident-response procedures. With the use of AI technologies, these incidents also include data leakage, suspected model-training behavior, and use of non-University Approved AI Technology. When an incident involves research data, any research personnel, faculty member, staff member, or student who knows or suspects that a breach has occurred shall notify both campus Research Compliance Services and NU ITS or UNMC ITS within two hours of discovery, even when certainty or complete details are not yet available, as required by Executive Memorandum 41.

4.4 Inventory and Ongoing Security Review

AI technologies procured or developed with University resources shall be included in applicable University information system inventories and shall be subject to required security review and vulnerability management. AI technologies and services that access, process, transmit, or store Medium or High Risk Data (both as defined in Executive Memorandum 42) are subject to periodic verification by NU ITS or UNMC ITS and applicable University oversight bodies regarding data classification, security controls, and storage practices. Associated data and information-system classifications shall be reviewed at least annually in accordance with Executive Memorandum 42.

5. Data Classification Requirements

5.1 Medium- and High-Risk Data

Medium Risk Data that has been anonymized and deidentified is permitted in University Approved AI Technologies. Any medium risk data that cannot be anonymized or deidentified shall not be used with AI technologies unless such technologies or specific environments have been approved for such use through the Exception Process.

5.2 High Risk Data

High Risk Data shall not be used with AI technologies unless such technologies or specific environments have been approved for such use through the Exception Process.

5.3 Prohibited Uses

The following are prohibited without formal approval through the Exception Process:

- Processing University Information through personal AI subscriptions, personal cloud services, or personal cloud storage as defined in ITS-00: Information Technology Definitions Standard.
- Using AI technologies that claim ownership rights to University Information.
- Using AI technologies that train models using University Information.
- Uploading confidential information, legal documents, intellectual property, personally identifiable information, or institutional or research data into non-University Approved AI Technologies.

6. Human Oversight and Accountability

Users remain responsible for:

- Reviewing AI-generated output with a thoroughness proportionate to the risk and consequences associated with the use of AI for the generation of such output.
- Verifying factual accuracy.
- Validating references, citations, calculations, and recommendations.
- Preventing the dissemination of inaccurate or misleading information.
- Ensuring compliance with applicable laws and policies, including class syllabi.

AI-generated content must not be represented as independently drafted or verified without appropriate human review. Therefore, faculty, staff, students, contractors, consultants, affiliates, volunteers, visiting scholars, and other workforce members are expected to disclose material uses of AI that substantially contribute to content, analysis, interpretation, findings, or decisions. Routine spelling, grammar, and formatting assistance that preserves the author's intended meaning generally does not require disclosure. To support transparency, accountability, and human oversight, disclosures should identify the AI tool, describe its contribution, and indicate how the resulting work was reviewed or verified. Individuals remain responsible for the accuracy and integrity of the final work, protection of sensitive information, and appropriate consideration of bias and limitations. Academic and administrative units may establish discipline-specific guidance on material use and proportionate disclosure requirements.

University personnel remain accountable for all decisions, analyses, recommendations, communications, and actions derived from AI technologies.

7. Ethical and Responsible Use

Users shall not use AI technologies to:

- Violate privacy rights.
- Circumvent University security controls.
- Create fraudulent, deceptive, or misleading content.
- Conduct discriminatory or unlawful activities.
- Generate content that violates University policies or applicable law.
- Make employment, academic, admissions, disciplinary, or research determinations without appropriate human review.
- Submit academic assignments, research data/products, or creative works without approval of the faculty/staff making such assignments.

AI use should align with principles of:

- Fairness

- Transparency
- Accountability
- Privacy
- Security
- Academic integrity
- Research integrity

8. Accessibility

AI technologies and AI-generated digital content procured, developed, maintained, or used by or for the University to support teaching, working, learning, research, or University programs, services, activities, or communications shall comply with Executive Memorandum 47 and all applicable accessibility requirements. Accessibility shall be considered in the selection, procurement, development, implementation, and use of such systems and content. Any exemption from Executive Memorandum 47 shall be requested and approved under Executive Memorandum 47 and shall not eliminate the obligation to provide persons with disabilities access to University benefits and services to the maximum extent possible.

9. Software Development and AI Coding Tools

Absent an approved exception, only University Approved AI Technology may be used for AI-assisted software development and coding. Faculty, staff, students, contractors, consultants, affiliates, volunteers, visiting scholars, and other workforce members utilizing AI-assisted software development and AI coding tools must:

- Review AI-generated code before deployment.
- Validate security controls and ensure compliance with University policies.
- Assess licensing implications.
- Ensure no unauthorized disclosure of University source code, architecture, credentials, or sensitive information occurs.
- Comply with University secure software development standards.

10. Research Use

AI use in research and creative activity must comply with:

- Sponsor requirements

- Institutional Review Board requirements
- Human subject protections
- Export control requirements
- Data use agreements
- Research security requirements
- All existing University policies, including but not limited to Executive Memorandum 16, 41, and 42
- Academic, publication, and discipline-specific norms and requirements

11. Exceptions

Exceptions to this memorandum may be granted only through the "Exception Process" defined and managed by the AI Governance Committee.

12. Violations

Violations of this memorandum may result in:

- Removal of access to all University information technology systems;
- Revocation of AI tool access;
- Corrective action;
- Disciplinary action up to and including termination;
- Student conduct action;
- Contract termination; or
- Civil or criminal penalties where applicable.

Violations of AI policies shall be adjudicated in accordance with all applicable administrative unit policies and bylaws, including student conduct policies and those of the Board of Regents of the University of Nebraska.

Dated this 1st day of November 2026.

/s/

Jeffrey P. Gold, M.D., President

Reference: August 18, 2026
Rev. November 1, 2026

Generative AI tools, including ChatGPT, were used to support the development and wording of this policy. All AI-assisted content was critically reviewed and verified by University officials.