Executive Memorandum No. 42

Policy on Risk Classification and Minimum Security Standards
(f/k/a ITS-05: Data Classification and Storage Policy)

Scope and Reason for Policy

This policy applies to all University of Nebraska (NU) personnel including faculty, staff, students, contractors, consultants, affiliates, or others that obtain, access, use, study, analyze, generate, process, store, transmit, or use institutional or research data. In addition, this policy applies to:

- All institutional or research data, independent of location (physical or cloud);
- Any account, device, application, or system that is use to transmit, process, store, access, or control institutional or research data independent of ownership;
- All devices independent of this location or ownership when connected to a University network or cloud service and used to transmit, process, store, access, or control institutional or research data;
- All research projects performed under the auspices of the University; and
- All research or institutional data transfers to third parties.

All institutional or research data, generated or previously existing on or after the effective date of this policy is subject to these requirements. Other institutional and research data in possession of the University, its personnel, or affiliated parties generated prior to the effective policy date, however, shall be identified and categorized as provided in procedures accompanying this policy.

Institutional and research data, and IT systems, are key assets of the University. The University seeks to protect data integral to the University's mission of teaching, research, and public service while preserving academic freedom, encouraging research collaboration, and ensuring data availability in accordance with prevailing best practices. Fulfillment of our mission also requires the University to comply with multiple University, state, federal, international, and sponsor requirements. Proper classification of data and systems and application of appropriate security controls are essential to the protection of these assets and ensure compliance with all applicable regulations and accomplishment of mission-critical goals.

Definitions

- **Application** – a software program funding on a server that is remotely accessible, including mobile applications.

- **Controlled Unclassified Information (CUI)** – government created or owned information that requires safeguarding or dissemination controls pursuant to and

consistent with applicable law, regulations, and government-wide policies. CUI is not classified information and is not classified under Executive Order 13526 or the Atomic Energy Act, as amended. CUI is not corporate intellectual property unless created for or included in requirements related to a government contract.

- **Data Use/Data Transfer Agreements (DUAs/DTAs)** – contractual documents for the use of a portion of data or transfer of a portion or complete set of data where the data is nonpublic or is subject to some restrictions. Universities must ensure that DUA/DTA terms protect confidentiality and security when necessary but permit appropriate publication and sharing of research results in accordance with federal, state, and University regulations.

- **Directory Information** – Board of Regents' Policies define data elements designated as student public directory information in Regents' Policy 5.10; and faculty and staff public directory information in Regents' Policy 6.7.

- **Endpoint** – end-user machine such as, but not limited to, a workstation, laptop, desktop, tablets, printers, mobile device, or any other device capable of connecting to the University network.

- **Information Technology Services** – endpoints, computers, networks (wired and wireless video, voice, data, and security devices), servers, systems (including software, storage, licensed platforms, and cloud-based services), and other similar devices that are administered, owned, or operated by the University or for which the University is responsible.

- **Institutional Data** – information created, collected, maintained, transmitted, or recorded by or for the University to conduct University business. It includes data used for planning, managing, operating, controlling, or auditing University functions, operations, and mission. Institutional data includes, but is not limited to, information in paper, electronic, audio, and visual formats.

- **Institutional Data Classification Matrix** – defines the appropriate data classification levels for data elements and identifies which classifications of data are permitted for specific data user's activities.

- **Institutional Data Stewards** – subject matter experts and operational managers in a functional area with day-to-day responsibilities for managing business processes and establishing the business rules for that area and its related institutional data.

- **Institutional Data Classification, Use, and Policy Committee** – University-wide committee established in ID-01: Institutional Data Use Policy which is charged with establishing data definitions, risk classifications, and data standards for institutional data.

- **ITS** – University of Nebraska (NU) or University of Nebraska Medical Center (UNMC) Information Technology Services.

- **Material Transfer Agreements (MTAs)** – contractual documents used for the acquisition of various biological and research materials and occasionally data. Universities must ensure that MTAs protect confidentiality, security, and intellectual property when necessary, but permit appropriate publication and sharing of research results in accordance with federal, state, and University regulations.

- **Minimum Security Standards** – a set of standards that protect physical and electronic data and IT systems from intentional or accidental destruction, modification, access, or disclosure. Minimum security standards are applied using a range of techniques, including administrative controls, physical security, logical controls, organizational standards, and other safeguarding techniques that limit access to unauthorized or malicious users or processes.

- **Personal Data** – information created, collected, maintained, transmitted, or recorded by University-owned devices, media, or systems in accordance with Executive Memorandum No. 16 that is personal in nature and not related to University business.

- **Protected Health Information (PHI)** – individually identifiable health information collected by covered entity or covered function of a hybrid entity that is related to an individual's past, present, or future physical or mental health or condition, provision of health care to the individual, or payments for provision of healthcare.

- **Records** – information of any kind and in any form including writings, drawings, graphs, charts, images, prints, photographs, microfilms, audio and video recordings, data and data compilations, and electronic media, including email.

- **Research Data** – all information in any physical or electronic form collected, obtained, and/or generated in the course of a research project conducted at the University, under the auspices of the University, or with University resources. This includes original and derivatives of research data, regardless of form or funding, physically housed at the University or stored remotely, including recordings of such data. Examples of research data include, but are not limited to:
    - Data, analytical programs, procedures, and records necessary for the reconstruction and evaluation of the results of research;
    - Laboratory notebooks;
    - Data collected using instrumentation or systems and stored in an electronic format; or
    - Source documentation and reporting forms for human participant research studies.

  Research data ***does not*** include data generated or acquired by students in their academic work, unless the research data are generated or acquired within the scope of their employment at the University, generated or acquired through use of substantial

University resources, or subject to other agreements that supersede this right (e.g., research data ownership agreements signed by the student and PI).

- **Research Oversight Bodies** – a committee, council, office, or other unit that has responsibility for research activities at each NU campus and central administration.

- **Research Data Stewards** – any NU campus or system personnel with day-to-day responsibilities for managing research data, processes, and security. Principal Investigators (PIs) are ultimately responsible to the University for decisions or actions in regard to research data.

- **Responsible Party** – individual or group of people that are responsible for a decision or action.

- **Server** – a system entity that provides a service in response to a request from a client.

- **Substantial University Resources** – resources provided by the University that go above and beyond what is customarily provided to University employees or students. These resources may vary by department/unit and context, but include resources provided from extramural sources, internal grants, startup funds, and targeted campus/University investments in a program or unit.

- **Verification** – an evaluation of an organization's information technology infrastructure, policies, and operations. Information technology reviews conducted to determine whether IT controls protect institutional assets, ensure data integrity, and are aligned with the goals and mission of the University.

Policy Statements

The University of Nebraska has an obligation to safeguard its institutional and research data in order to accomplish its mission, protect its assets, honor its legal and contractual responsibilities, provide continuity to business functions, and protect individuals. Security classifications for data and IT systems are established by taking into consideration both the potential impact on the University of Nebraska if data or IT systems are compromised (e.g., impacts to data integrity or availability of data) and potential impacts to individuals (including breaches of confidentiality or privacy). Increased levels of potential impact on the institution and individuals require increased levels of administrative, technical, and physical security controls to protect NU data.

1. Classification and Security Standards

There are three risk classification levels for NU data and IT systems. These levels (low, medium, and high) are commensurate with the risk associated to the University and individuals; as the level of risk increases, so do security requirements. The University of Nebraska's Minimum Security Standards for Low, Medium, and High Risk data are based on recognized national and governmental standards. Most institutional data will utilize Minimum Security Standards that are aligned to National Institute of Standards and Technology (NIST) frameworks (800-53, 800-171, Cybersecurity Framework).

While research data must be classified using the University's Minimum Security Standards, there may be additional specific compliance requirements associated with some research data or controlled unclassified information (CUI) that will be aligned with other frameworks like the Cybersecurity Maturity Model Certification (CMMC), Federal Information Security Management Act (FISMA), DoD Federal Acquisition Regulation Supplement (DFARS), International Traffic in Arms Regulations (ITAR), and NIST 800-171. The highest risk classification applicable to the data and associated IT systems or a classification required by agreement or regulation should be applied. Non-exhaustive examples of data or systems for each risk classification are provided for each category. Please contact NU ITS, UNMC ITS, or applicable campus research oversight bodies for assistance in appropriately classifying data, if necessary.

Low Risk Data

Data or IT systems are low risk if:

1. They are not considered to be Medium or High Risk;
2. The data can generally be made available to the public without harm to the University, entities with an affiliation to the University, or to individuals; and
3. The loss of confidentiality, integrity, or availability would have a limited adverse effect on organizational mission, operations, assets, regulation, or on individuals.

Security controls applied to low risk data and IT systems classified as low risk must conform to the provisions of this policy, the minimum security standards for Low Risk Data, and any additional compliance requirements for research data.

Examples: surveys of personal opinions about agricultural producer crop rotation; EAR 99 information; publicly available manuscripts and associated data; public directory information; personal data; University job postings; publicly available campus maps; University of Nebraska Human Resources Handbook for Policies.

Medium Risk Data

Data or IT systems are medium risk if they are not considered to be high risk, and:

1. The data is not legally available to the public; or
2. The loss of confidentiality, integrity, or availability could have a ***moderate*** adverse impact on organizational mission, operations, assets, reputation, or on individuals.

Security controls applicable to data and IT systems classified as medium risk must conform to the provisions of this policy, minimum security standards for Medium Risk Data, and any additional compliance requirements for research data.

Examples: personally identifiable student, faculty, and staff information/records that do not contain high risk data; engineering, design, and operational information regarding the University's physical or technical infrastructure; human subjects research data that does not contain high risk data; information that could fall under a dual use category as having both military and civilian application.

High Risk Data

Data or IT systems are high risk if:

1. Data is confidential, restricted, or sensitive;
2. Protection of the data is required by law, regulation, or sponsor requirements;
3. The University is required to self-report to the government and/or provide notice to the individual if the date is inappropriately accesses; or
4. The loss of confidentiality, integrity, or availability could have a ***significant*** adverse impact on organizational mission, operations, assets, reputation, or on individuals.

Security controls applicable to data and IT systems classified as high risk must conform to the provisions of this policy, the minimum security standards for High Risk Data, and any additional compliance requirements for research data.

Examples: government issued identification numbers (e.g., SSN, driver's license, or state ID card numbers, passport and visa numbers); credit card numbers; financial account numbers; Protected Health Information (PHI); ITAR information; Federally Controlled Unclassified Information (CUI); identifiable human subject research data containing high risk data elements.

Some types of high risk data may require the application of processes and practices contained in Levels 4 and 5 of the CMMC. If law, regulation, contractual, or sponsor requirements specify a particular level of CMMC practices and processes apply to a data source, that specification shall control the CMMC process and practices applied.

NOTE: Data belonging to any classification level may be subject to Nebraska public records laws. Please contact the campus records officer or the Office of the Vice President and General Counsel immediately upon receipt of a public records request.

2. Security Control Variances

The applicable research oversight body and NU or UNMC ITS may apply commensurate or compensating security controls for the assigned research data risk classification level if certain controls mandated under the defined security level are deemed to be unfeasible or ineffective. Those variances shall be documented in writing by the applicable research oversight body, NU or UNMC ITS, and the PI. NU or UNMC ITS may apply such commensurate or compensating security controls to institutional data and shall retain a written record of such controls applied to institutional data.

Data classified at any level may be subject to Nebraska public records laws. Please contact the campus records officer and the Office of the Vice President and General Counsel immediately upon receipt of a public records request.

3. Data Storage

Unless details associated with the project dictate otherwise, low risk institutional and research data will be maintained by the unit in which they are produced using information technology systems designated by NU or UNMC ITS as being appropriate for such data.

Medium or high risk institutional or research data shall be stored within a NU or UNMC ITS designated unit or cloud-based computing resource designed to secure medium or high risk data. NU or UNMC ITS shall have final approval and decisional authority regarding the classification level associated with information technology systems used to store institutional and research data. Electronic storage of institutional or research data is not permitted on personal storage devices or personal cloud storage unless data has been classified as low risk and storage of the data on a personal device or in personal cloud storage has been approved by the applicable campus research oversight body (research data) or NU or UNMC ITS (institutional data).

4. **Approved Services**
   Not all University of Nebraska IT services are appropriate for all classifications of data. Please contact NU or UNMC ITS for assistance in determining which IT services can be used with each data classification level.

5. **Data Disposal**
   All parties wishing to dispose of medium or high risk data should contact NU or UNMC ITS for assistance with this task.

6. **Data Sharing**
   Individuals wishing to share institutional medium or high risk data with third party service providers or release data required by law (e.g., financial aid and payroll data) should have prior authorization from NU or UNMC ITS and have completed a formal data sharing agreement. Such an addendum or agreement will be reviewed by the Office of the Vice President and General Counsel; and templates are available from the same office.

   All research data and/or materials transferred to or from the University shall be shared or transferred in accordance with all applicable international, federal, state, University, or sponsor requirements. Transferring, moving, or sharing research data requires agreements such as the Data Use/Data Transfer Agreement (DUA/DTA) for confidential or sensitive research data or Material Transfer Agreements (MTAs) to protect intellectual property rights. Campus-based research oversight bodies should be contacted to coordinate the sharing or transfer of data to or from another institution via a DUA, DTA, or MTA.

7. **Verification and Risk Reduction**
   Medium and high risk data and information technology systems and services are subject to periodic review by NU or UNMC ITS to verify implementation of proper classification, security controls, and storage practices. Institutional data and information technology systems are subject to review as necessary, with or without prior notification.

   Campus research oversight bodies, in conjunction with NU or UNMC ITS, retain the right to verify implementation of proper classification, security controls, and storage practices related to research data, research-related federal contract information (FCI), research-related controlled unclassified information (CUI), research-related grants and

contract requirements, human subjects research, and export control. Research data and information technology systems are subject to review as necessary, with or without prior notification.

NU and UNMC ITS frequently scan data and revie traffic on the University network and endpoints to help reduce the risk of data breaches and material harm to the University. Access to reports generated by NU ITS or UNMC Cybersecurity Offices are limited to authorized personnel and internal or external auditors only in compliance with Executive Memoranda Nos. 16 and 26.

8. **Training**

All faculty, staff, students, contractors, consultants, affiliates, or others are subject to information security training requirements on or after the effective date of this policy. Information security training will be required for all parties prior to their access, generation, processing, storage, transmission, or use of medium or high risk institutional data. New faculty, staff, students, contractors, consultants, affiliates, or others interacting with medium or high risk institutional data shall complete information security training within thirty (30) days of initial hire and annually thereafter. Current faculty, staff, students, contractors, consultants, affiliates, or others interacting with medium or high risk institutional data shall be identified and required to complete training on an annual basis.

New research personnel are required to complete information security training within thirty (30) days of hire and shall not be added to a research protocol prior to completion of the training. Previously completed trainings from other institutions outside the University of Nebraska will not be accepted. Research personnel already participating in research prior to the policy's effective date shall be identified and required to complete training as deemed appropriate or upon submission of any new research projects on or after the effective date of this policy.

Procedures

- **Data Classification** – institutional data stewards are responsible for initial classification of institutional data and affiliated information technology systems. Initial classifications by data stewards shall be documented in the Institutional Data Classification Matrix or other approved documentation maintained by NU or UNMC ITS. All data classifications will be reviewed and are subject to final approval by the Institutional Data Classification, Use, and Policy Committee. NU or UNMC ITS shall have final approval and decisional authority regarding both the classification level associated with information technology systems that generate, process, transmit, or store institutional data, and the appropriate security controls that will be applied to these systems in order to meet or exceed requirements. Institutional data and information technology systems classifications will be reviewed annually by institutional data stewards, NU and UNMC ITS, campus research oversight bodies, and the Institutional Data Classification, Use, and Policy Committee.

Research personnel are responsible for the initial classification of research data and affiliated information technology systems and verifying, when appropriate, when approval is necessary from the appropriate research oversight body (e.g., high risk data associated with human subjects or export controlled research). Classification of research data will be reviewed and is subject to final approval by the appropriate campus research oversight body. The applicable research oversight body holds final approval and decisional authority regarding the assignment of risk classification levels for research data.

All research data that is generated, collected, or acquired on or after the effective date of Executive Memorandum No. 41 is immediately subject to the requirements outlined in this policy, Executive Memorandum No. 42, regardless of funding source. Such data shall be assigned an appropriate risk classification and arrangement should be made to apply the appropriate security controls for the risk level indicated immediately upon data generation, collection, or acquisition of said data.

Research data in possession of the University of Nebraska, its personnel, or affiliated parties generated, collected, or acquired prior to the effective policy date shall be identified and assigned a risk classification within 180 days of the effective date of this policy. Once existing research data has been classified, appropriate security controls must be applied to high risk data within the next 60 days, to medium risk data within the next 180 days, and to low risk data within the next 360 days.

All institutional data currently in the possession of the University of Nebraska must be appropriately classified (by data type) within 180 days of the effective date of this policy and such classification documented in accordance with NU or UNMC ITS approved procedures. Once existing institutional data has been classified, appropriate security controls must be applied to high risk data within 60 days, to medium risk data within 180 days, and to low risk data within 360 days.

All new institutional data generated, collected, or acquired subsequent to the effective date of this policy that has not previously been classified should be assigned an appropriate risk classification. Arrangements should be made to apply the appropriate security controls for the risk level indicated immediately upon data generation, collection, or acquisition of said date.

- **Policy Enforcement** – this policy is enforced by NU or UNMC ITS and applicable campus research oversight bodies. Failure to comply with University IT policies may result in sanctions related to the individual's use of IT resources or other appropriate sanctions according to policies applicable to University faculty and staff or student conduct policies.

  Failure of research personnel to comply with all research data security policies will be referred to the appliable institutional official, empowered official, research oversight body, and/or the department head/chair for non-compliance review and resolution within the appropriate policies. Failure to comply may require reporting to the applicable

research sponsors and various local, state, and federal agencies. Applicable sanctions for violation of NU research policies by research personnel are outlined in Executive Memorandum No. 41.

- **Review** – this policy will be reviewed annually by NU and UNMC ITS, campus research oversight bodies, and the Institutional Data Classification, use, and Policy Committee.

Reference: Adopted February 11, 2021