Executive Memorandum No.

Office of the President
Varner Hall | 3835 Holdrege Street | Lincoln, NE 68583-0745 | 402.472.8636 | nebraska.edu/president

publication and sharing of research results in accordance with federal, state, and University regulations.

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

¶ **Information Technology Systems** – Endpoints, computers, networks (wired and wireless video, voice, data, and security devices), servers, systems (including software,

5D002 on the Commerce Control List (certain encryption software), that are already published or will be published.[2] Campus research offices must be contacted when dealing with data subject to ITAR or EAR.

¶ **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 of Nebraska 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 Steward** – any University of Nebraska campus or system personnel with day-to-day responsibilities for managing research data, processes, and security.

¶ **Research Oversight Bodies** – a committee, council, office, or other unit that has responsibility for research activities.

¶ **Research Personnel** – principal investigators, program/project directors, investigators, co-directors, research associates, visiting scientists, postdoctoral fellows, technicians, graduate students, undergraduate students, or any other person involved in the design, conduct, or reporting of research.

¶ **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.

Policy Statements

1. Data Ownership and Responsibility

It is the policy of the University of Nebraska, as a state and federally funded University

Protecting the rights of research personnel, including, but not limited to, their rights to access data from research in which they participate, where appropriate;
Securing intellectual property rights;
Facilitating the investigation of charges such as noncompliance or research misconduct;
Working with research oversight bodies to identify security risks and ensuring appropriate staffing levels in order to accomplish these requirements;
Working with research personnel to promote training and foster awareness and understanding of this policy;
Ensuring compliance with this policy;
Reviewing and updating this policy as necessary and at least on a an annual basis;
Overseeing the security and confidentiality of research data;
Complying with applicable federal, state, University, and sponsor laws and regulations as they relate to research data;
Denying the acceptance or approval of grants and contracts if the University cannot meet data management requirements; and
Denying the acceptance of data if the University cannot meet data management requirements.

Responsibilities of the PI and other Research Personnel with respect to research data include, but are not limited to:

Ensuring proper management and retention of research data in accordance with all applicable federal, state, University, and sponsor requirements;
Establishing and maintaining appropriate procedures for the protection of research data and other essential records;
Ensuring those responsible for de-identification of data (e.g., human subjects research data) have the knowledge and expertise to ensure that deductive re-identification cannot occur and the risk of re-identification has been appropriately evaluated and accounted for prior to release prior to sharing data or making it public;

Taking either joint responsibility for complying with this policy or delegating responsibilities to different members of the group when the research project involves collaboration (of groups or teams). These responsibilities should be documented in writing and maintained as part of the research record; and
Consulting with applicable University officials prior to starting any project to ensure the resources and capabilities are available to meet the obligations outlined in this policy.

Responsibilities of NU ITS (UNL, UNO, UNK, and UNCA) or UNMC-ITS (UNMC) with respect to research data include, but are not limited to:

Assisting research personnel and research oversight bodies with the implementation of appropriate security controls in accordance with the assigned level(s);
Training ITS personnel commensurate with the type of data being stored;
Maintaining, and if requested providing in a timely and reasonable manner to appropriate PIs/designated research officials:

- Auditing and other records required to document that the assigned CMMC security level has. Been obtained and maintained;
- Annual logs and reports documenting data access, use, incidents, breaches, and destruction-status/certification specific to each data set stored;
- Confidentiality agreements with ITS personnel commensurate with the type of data being stored; and
- Identification of ITS personnel, their country(ies) of citizenship, and management of access through screenings and notification to the applicable regulatory oversight body for data that is export-controlled and has foreign national restrictions.

Immediately reporting to the PI and designated University officials any incident with the data (e.g., security breaches or inappropriate access by ITS or other staff);
Provision of information and controls in order to sequester or take custody of information as deemed necessary by the University of Nebraska, the campus Senior Research Administrator(s), or the campus Research Integrity Officer (RIO);
Providing an annual report to the campus Senior Research Administrator and the Office of the Executive Vice President and Provost regarding the number of cyber incidents or attacks specific to research data being stored in a NU or UNMC ITS designated unit;
Identifying the resources and controls required to maintain the security and confidentiality of research data, where appropriate;
Complying with applicable federal, state, University, and sponsor laws and regulations; and
As applicable, ensuring compliance with other NU policies regarding appropriate data security and stewardship (e.g., HIPAA covered data that does not involve research). Please reference Executive Memorandum No. 26 for further

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 risk of 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

4. The loss of confidentiality, integrity, or availability could have a ***significant*** adverse impact on organizational mission, operation, assets, or reputation or on individuals.

Security controls applied to high risk data and IT systems classified as high risk must conform to the provisions of Executive Memorandum No. 42: Data Classification and Minimum Security Standards and, if required, practices and processes associated with CMMC Level 3.

Examples: government issued identification numbers (e.g., SSN, Driver's license or state ID card numbers, passport numbers), credit card numbers, financial account numbers, Protected Health Information (PHI), ITAR controlled information, Federal Controlled Unclassified Information (CUI), identifiable human subject research data containing high risk data elements, servers or applications handling high risk data, servers managing access to high risk systems.

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.

It is also important to note that University of Nebraska campuses are:

1. Not cleared facilities and are not authorized to receive classified research or

The campus-based research office should be contacted to coordinate the sharing or transfer of data to or from another institution via a DUA, DTA, or MTA.

8. Data Breaches: Theft, Loss, or Unauthorized Use

A data security breach occurs when there is a loss, theft, or other unauthorized access to information that could result in the potential compromise of the security, confidentiality, or integrity of data.

Any research personnel, faculty, staff, or student who knows of or suspects a research data breach has occurred must promptly notify both campus-based Research Compliance Services and NU or UNMC ITS as the first points of contact for reporting. Incidents, including cases where absolute certainty and full details are not yet available, must be reported within two hours of discovery of the event or notification of the event. The situation can initially be reported via phone, email, or in-person disclosure. Documentation of a data security breach must be done under the direction of the University of Nebraska Office of the Vice President and General Counsel.

Incidents involving data security breaches will be referred to and investigated by the applicable research oversight body and NU or UNMC ITS. Incidents that also involve physical security, personnel action, student conduct, or other areas of concern will be handled in accordance with established University protocols and procedures.

9. Training

Training is a vital component of ensuring understanding and adherence to appropriate research data controls. Therefore, all research personnel must complete information security training prior to their access, generation, processing, storage, transmission, or use of medium and high risk research data and annually therefore, regardless of the project's funding status.

All research personnel are subject to these training requirements on or after the effective date of this policy. 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.

In addition to the completion of training, all research personnel are expected to be familiar with this policy, their applicable research oversight body's policies regarding research data and data security, and University-wide policies relating to research and data security.

10. Verification and Risk Reduction

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.

Procedures

¶ **Data Classification** – all research data that is generated, collected, or acquired on or after the effective date of this policy is immediately subject to the requirements outlined in this policy regardless of funding source. As such, this data should be assigned an appropriate risk classification and arrangements 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 data has been classified, appropriate security controls must be applied to high risk data within the next 60 days, to data classified as medium risk within the next 180 days, and to data classified as low risk within the next 360 days.

¶ **Data Repositories** – University of Nebraska campus libraries should be contacted for assistance with locating appropriate data repositories for public dissemination of data.

¶ **Policy Enforcement** – failure of research personnelpria/F5 12 Tf1 0 qc0 1 2y /4MCID 8>5000 0 P0.00000

Executive Memorandum No. 41