Executive Memorandum No. 41

Policy on Research Data and Security

Scope and Reason for Policy

This policy applies to all personnel at the University of Nebraska who obtain, access, use, study, analyze, or generate research data. Research personnel required to comply with this policy include principal investigators, program/project directors, co-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.

All research data that is generated, collected, or acquired on or after the effective date of this policy is subject to these requirements regardless of funding source. Other research data in possession of the University of Nebraska and its research personnel that was generated prior to the effective policy date, however, shall be identified and categorized as provided in the procedures accompanying this policy.

The University of Nebraska is committed to the safeguarding of research data in accordance with all applicable federal, state, and University regulations. Those involved in research activities at the University of Nebraska have certain rights and responsibilities with respect to research data. All data from sponsored or non-sponsored research activities must be recorded, maintained, and made accessible in a reasonable and responsible manner by research personnel and in accordance with all applicable federal, state, and University requirements.

Definitions

- **Confidential Disclosure Agreements (CDAs)** – legal agreements between two or more parties which outline information the parties wish to share with one another for a specific purpose but wish to restrict from wider use and dissemination. Also referred to as nondisclosure agreements (NDAs) or secrecy agreements.

- **Cybersecurity Maturity Model Certification (CMMC)** – cybersecurity framework that aligns cybersecurity processes and practices with the type and sensitivity of information to be protected and the associated range of cybersecurity threats.

- **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.

- **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, 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.

- **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.

- **Metadata** – information describing the characteristics of data, including descriptions of data format, syntax, and semantics (structural metadata) and data describing contents such as security labels (descriptive metadata).

- **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.

- **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 health care.

- **Public Domain** – a work of authorship is in the public domain if it is no longer under copyright or if it failed to meet the requirements for copyright protection. Works in the public domain may be used freely without permission of the copyright owner. Information which is generally accessible or available to the public. For export control requirements, the definition of public domain and publicly available information should be referenced to International Traffic in Arms Regulations (ITAR) or Export Administration Regulation (EAR). The ITAR states that information in the public domain that is published and that is generally accessibly or available to the public is excluded from control as ITAR technical data.[1] The EAR excludes from its control publicly available technology and software, except software classified under ECCN

[1] ITAR paragraph 120.11

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 system, to assert ownership over research data for projects conducted at the University,

[2] EAR part 734.3(b)

under the auspices of the University, or with University resources. Although the University as the owner of research data, must meet the requirements of sponsors or other research regulatory requirements, good management practice and practical considerations necessitate that the University and research personnel act in partnership to fulfill these obligations.

Unless superseded by terms of sponsors, other agreements, or University policy (e.g. Copyright), the University owns all research data generated or acquired by University employees or non-University of Nebraska employees working in University controlled facilities, regardless of funding source. However, University of Nebraska students shall retain ownership of their research data except as noted below.

Students own research data that they generate or acquire in their academic work, unless the research data is:

- 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 Principal Investigator).

Principal Investigators (PIs) and other research personnel are stewards of research data. No matter how such responsibilities are delegated, the PI is ultimately responsible to the institution for the stewardship of research data, just as the institution is ultimately responsible to the research sponsor for compliance with applicable research regulatory requirements.

Research data shall be accessible to members of the University community, external collaborators, and others as appropriate (e.g., for patent applications or journal submissions). Where necessary, the University may take custody of research data to assure needed and appropriate access (e.g., auditing purposes or research misconduct investigations). Research personnel shall not enter into (sign) agreements that affect the control and use of data; such agreements must only be documented, approved, and signed by designated University official(s) granted such authority.

In addition, research personnel are required to use their University designated email address and appropriate security protocols when communicating or transmitting research data. Personal email shall not be used due to the many challenges it presents regarding the appropriate management, ownership, and security of research data.

Responsibilities of the University of Nebraska, its designated campus official(s), and research oversight bodies with respect to research data include, but are not limited to:

- Complying with the terms of sponsored project agreements;
- Ensuring the appropriate use of project resources (e.g., animals, human participants, recombinant DNA, biological agents, radioactive materials, export controls, conflicts of interest, and intellectual property);

- 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;
- Ensuring compliance with program requirements and terms of sponsored project agreements;
- Identifying the initial level of data classification and verifying, where appropriate, whether approval is necessary by the appropriate research oversight body (e.g., high risk data associated with human subjects or export-controlled research);
- Maintaining security and confidentiality of research data, where appropriate. PIs should consider implementing confidentiality agreements with their research teams depending on the type of data involved in the research;
- Complying with applicable federal, state, and local laws and regulations, and sponsor requirements as they related to research data;
- Educating all participants in the research project about their obligations regarding the research data and protecting the University's rights and ability to meet obligations related to the research data;

- 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

information. The more restrictive policy shall take precedence regarding any discrepancy between this policy and other University policies.

Responsibilities of the University of Nebraska Consortium of Libraries (UNCL) through its individual campus Deans of Libraries with respect to research data will evolve over time and include, but are not limited to:

- Support accessibility of research data through select curation activities, including those designed to ensure data are findable, accessible, interoperable, and reusable (FAIR); metadata creation and consulting services; data review, testing, and characterization support; education relating to federal and other funders' data retention and sharing requirements; services attached to libraries repositories, including minting identifiers and digital preservation services; and
- Broad educational and consultation services to train and support research personnel in the creation and implementation of data management plans and best practices, including strategies for securing consent and releasing data in a manner consistent with expectations of applicable research oversight bodies (e.g., human subjects research approval from IRBs, etc.). Includes education and consultation around long-term digital preservation practices and options.

2. Data Classification

In order to appropriately and effectively safeguard research data, University of Nebraska research personnel, research oversight bodies, and NU and UNMC ITS are responsible for understanding their roles and obligations with regard to the protection of data.

The University of Nebraska classifies all research data and associated IT systems based on varying degrees of institutional and individual risk according to Executive Memorandum No. 42 (formerly Policy ITS-05): Risk Classification and Minimum Security Standards. 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 upon recognized national and governmental standards. The applicable research oversight body holds final approval and decisional authority regarding the assignment of risk classification levels for research data. 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 research data and the appropriate security controls that will be applied to these systems in order to meet or exceed requirements set by the applicable research oversight body.

The level of risk assigned to human subjects research data under this policy may not always match the level of risk articulated by IRB approval categories (Exempt: less than minimal risk; Expedited: minimal risk; and Full Board: greater than minimal risk). This could also apply to other research regulatory areas besides the IRB (e.g., an IRB protocol may be certified as Exempt but still utilize HIPAA covered information, which would require a high risk classification).

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 adverse effect on organizational mission, operations, assets, reputation, or on individuals.

Security controls applied to low risk data and IT systems classified as low 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 1.

Examples: surveys of personal opinions about agricultural producer crop rotation, EAR 99 information, publicly available manuscripts and associated data, applications or servers used for research that do not contain moderate or high risk data.

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, operation, assets, or reputation or on individuals.

Security controls applied to medium risk data and IT systems classified as medium 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 2.

Examples: personally identifiable student information/records that do not contain high risk data, human subjects research data that do not contain high risk data, information that could fall under a dual use category as having both military and civilian application, servers or applications handling medium risk data.

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 data is inappropriately accessed; or

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 information on campuses. However, there are some University research personnel that travel to a secure/cleared location to review and/or work on classified information. In these cases, research personnel are not allowed to bring back, store, or access any classified information at the University or via University owned computers.
2. A hybrid entity per HIPAA regulations. This means that the University engages in both HIPAA covered and non-covered activities. Depending on the research area and research data, research personnel must understand when and if they are collecting, accessing, or generating protected health information.

3. <u>Security Control Variances</u>

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. These variances shall be documented in writing by the applicable research oversight body, NU or UNMC ITS, and the PI.

4. <u>Data Storage</u>

Unless details associated with the project dictate otherwise, research data classified as low risk shall 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 research data shall be retained within a NU or UNMC ITS

designated unit or cloud-based computing resource designed to secure medium or high risk data. Information technology systems used to store medium or high risk research data must be deemed and designated as appropriate by NU or UNMC ITS and the applicable campus research oversight body. Electronic storage of research data is not permitted on personal 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.

5. Data Retention

All research data must be retained for at least the minimum period required by applicable laws and regulations, sponsor and publisher requirements, other agreements, and University records retention schedules. While PIs may choose to retain the data beyond the minimum period, they should ensure adherence to the storage of data as it pertains to any laws, regulations, or agreements, including human subjects' consent or protocol information.

Research data must be maintained for a period of time that allows the University of Nebraska to meet its legal and academic obligations. Research data and records that contain protected health information (PHI) must be maintained and retained per HIPAA requirements for a minimum of seven years.

Research data must be maintained for a period as outlined below:

- Research data must be kept for as long as may be necessary to protect any intellectual property resulting from the work;
- If litigation or other dispute resolution, claims, financial management review, or audit related to the research is started before the expiration of the retention period, or commenced after the retention period but the relevant data and records have not been destroyed, the research data and other project records must be retained until all such litigation or other dispute resolution, claims, financial management review, or audit findings involving the records have been resolved and financial action taken;
- If any changes regarding the research arise, such as allegations of research misconduct, research data must be retained as specified by the University of Nebraska, the campus Senior Research Administrator(s), and/or the campus Research Integrity Officer (RIO);
- If a student thesis or dissertation is involved, research data must be retained at least until the student's degree is awarded (or the student otherwise withdraws or terminates their pursuit of a NU degree) and any resulting papers are published. University Libraries house electronic theses and dissertations and should be consulted regarding retention of this information;
- When research is funded by an award to or contract with the University of Nebraska at includes specific provision(s) of that agreement may supersede this policy;
- Research data and records from human participant research studies must be maintained consistent with University Institutional Review Board (IRB) policies.

Required data and records include, but are not limited to, the approved protocol, informed consent form(s), and IRB-PI communication;

- Research data and records involving export-controlled activities must be maintained consistent with University of Nebraska Export Control Compliance Program (ECCP) policies. Required data and records include, but are not limited to, the approved Technology Control Plans (TCPs), export control determinations, international travel and shipments, and ECCP-PI communication;
- Research data and records involving the Office of Sponsored Programs, Institutional Animal Care and Use Committee, Environmental Health and Safety, Institutional Biosafety Committee, and University-affiliated entities must be maintained consistent with their policies or requirements;
- Research data and records that contain information covered by the European Union's General Data Protection Regulation (GDPR) must be maintained and retained per GDPR requirements; and
- If other regulations, federal oversight, sponsor policies or guidelines, journal publication guidelines, or other University policies require longer retention, all applicable sources must be reviewed and the research data must be kept for the longest period of time applicable. At an absolute minimum, research data must be maintained for a minimum of three years after the financial report for the project period has been submitted or, for non-sponsored projects, after the project has ended and the budget reconciled (if applicable).

6. <u>Data Destruction</u>

When specific projects or regulatory requirements necessitate data destruction, the PI is responsible for the destruction of research data and the destruction must follow applicable federal regulations, University of Nebraska policies on records retention and data disposal, sponsor requirements, NU or UNMC ITS requirements, and any other applicable guidelines.

NU or UNMC ITS should be consulted when research data destruction is necessary. Secure disposal procedures approved by NU or UNMC ITS should be used based on best practices available and commensurate with the classification of that information and its related risk. For example, with increased risk associated with loss of the data, the data media should be physically destroyed and/or the cloud-based storage provider should be consulted regarding permanent data destruction procedures. If the data classification or sensitivity is unknown, the PI should consider the data classification to be high risk.

When destroying research data, the PI or research personnel should plan to retain documentation of the destruction for audit purposes in order to record that the data was destroyed appropriately and in compliance with all regulations, agreements, or policies. Destruction of research data documentation shall be retained by the unit in accordance with University of Nebraska records retention policies.

The applicable research oversight body and Institutional Official reserve the right to determine and carry out appropriate data destruction if they deem the PI is unable or that it would be inappropriate for the PI to take responsibility in this regard (e.g., research misconduct, non-compliance).

7. Data Sharing or Transfer

All research data and/or materials transferred to or from the University shall be shared or transferred in accordance with all applicable 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 Agreement (MTA) to protect intellectual property rights. Sharing or transferring research data does not refer to the common practice of sharing de-identified research data or their products with collaborators, journals, or other researchers as part of the normal scientific or scholarly process of conducting and publishing research.

The following scenarios, including but not limited to those below, require an agreement:

- A PI or other research personnel leaves or joins a University of Nebraska campus;
- A project is moved to or from another institution or University of Nebraska campus; or
- Confidential or sensitive research data will be shared with collaborators during or after the performance of the research.

In most cases, original research data that was generated at a University of Nebraska campus shall be maintained by that campus. If the researcher leaves the University of Nebraska and a project is to be moved to another institution, copies of the data may be shared or transferred from the University of Nebraska to the new institution upon request from the PI, subject to:

- Notification to the applicable research oversight body at each institution;
- Written approval of the sponsor(s) in order to move applicable funding or data;
- Written agreement from the PI's new institution that guarantees:
  - Acceptance of ongoing custodial responsibilities for the data;
  - The University of Nebraska retaining or having access to the original data, should such access become necessary for any reason; and
  - Relevant confidentiality, security, or intellectual property restrictions, where appropriate.
- In addition, the appropriate sharing or transfer of data in the following scenarios shall be decided on a case-by-case basis:
  - Requests for transfer of original data;
  - If a researcher leaves a University of Nebraska and has not identified a new institution; or
  - The researcher, upon leaving the University of Nebraska, will be affiliated with a non-research entity.

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 personnel to comply with all research data security policies will be referred to the applicable 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 applicable research sponsors and various local, state, and federal agencies.

  The University may decline or withhold funding in all cases in which research personnel do not comply with this policy. In general, applicable institutional official and research oversight body actions or consequences may including, but are not limited to:
  - Required implementation of a corrective action plan;
  - Required in-person or online training completion;
  - Required amendments to the data security level or plan;
  - Transfer of responsibility to another PI or required oversight from another PI;
  - A letter of reprimand placed within the research personnel's employee or student file;
  - Removal of research personnel from some or all work on a project;
  - Suspension or termination of some or all of the involved research in which noncompliant research data security activity has been identified; or

- Corrective action may also result up to and including referral for termination of employment in accordance with University of Nebraska Board of Regents Bylaws and/or Policies.

Research personnel have the right to appeal research data security determinations made under this policy. Any disagreement regarding the enforcement of this policy, assigned risk classification levels, or applicable security controls must be submitted in writing to the applicable campus research officer within 10 business days of receipt of the requirements for any given project. The appeal shall be referred to the applicable research oversight body and this body shall consult with NU or UNMC ITS regarding disputes related to applicable security controls. The applicable institutional official holds final authority regarding any appeal(s) by research personnel.

- **Review** – this policy will be reviewed annually by NU and UNMC ITS and campus research oversight bodies.

Reference: Adopted February 11, 2021