Faculty Handbook	**Standard E30 #1: Research Data Management**
Approved By: Faculty Senate Research Policy Committee	
Effective Date: Draft 8/2/2022	

Revisions to the remaining sections of this document may be amended with the approval of the Faculty Senate Research Policy Committee. Collaboration on revisions with relevant administration and other interested parties is expected.

This document provides standards and guidelines that assist in compliance with *Faculty Handbook* **Policy E30** "Research Data Management." This document is to be used in conjunction with **Policy E30** which delineates rights and responsibilities pertaining to ownership and management of data and associated materials for UNM research activities.

1. Roles and Responsibilities

1.1 Research Data Owners

To comply with the rights and responsibilities listed in **Policy E30**, it is critical that research data owners support UNM systems and services that enable researchers to maintain effective research data management. For example, research data owners should:

- Provide training and tools that streamline the definition and assessment of data management requirements as part of the proposal development (for sponsored research) and data management planning process (for both sponsored and unsponsored research).
- Develop and maintain a collection of data use and other user agreement templates that have been reviewed by University Council to provide a streamlined process for developing and executing such agreements.
- In the absence of existing agreements, include language in sub-award and/or other contractual agreements with collaborators and their institutions to define and ensure their compliance with UNM data sharing obligations.
- Coordinate with campus infrastructure and support service providers to ensure streamlined research data management throughout the data lifecycle: from planning; initial data creation/capture; through analysis and management; and ultimately deposit into long-term preservation, discovery, access, reuse, and retention systems.
- Support a base level of tiered infrastructure that meets defined levels of physical, network, and storage security requirements. Clearly define the limits of this base service level and provide mechanisms for researchers to build upon this base level of service through sponsor or other program funds.

1.2. Research Data Stewards

To comply with the rights and responsibilities listed in **Policy E30**, research data stewards should:

- Ensure all project participants are working in compliance with UNM data management, security, sharing, preservation, and retention policies.
- Make research data available to collaborators, including students.
- Ensure compliance with sponsoring agency (if applicable) and other requirements for data management, preservation, and sharing—and communicating to appropriate parties any deviations from or changes in planned activities in a timely manner.
- Work with the designated research data owner to ensure that research data and associated documentation are being placed in appropriate data sharing, preservation, and retention systems in compliance with all relevant requirements and written Data Management Plans (DMPs).
- Ensure that there are sufficient resources to fulfill data stewardship requirements.
- Clearly communicate data ownership and associated rights and responsibilities so they understood by all project participants.

1.3 Research Data Custodians

To comply with the rights and responsibilities listed in **Policy E30**, research data custodians should
support researchers, research data owners, research data stewards, and research data users in meeting their research data management obligations under **Policy E30**. For example, research data custodians should ensure that:

- Research data are stored in accordance with directions provided by the research data steward (or designee).
- Research data have and maintain associated system-level metadata (e.g., checksum) for integrity verification. Such metadata should be used as part of a regular audit process to ensure long-term and durable storage integrity.
- Research data are stored in a secure manner such that user and role-based protections are implemented to restrict access to only authorized personnel as defined by the research data steward or designee.
- Research data have near-line and offline redundancy in place for high-value products as determined by the research data steward.
- That the access and management processes of research data be recorded using audit and logging services to securely document associated activity.
- Data access services are continuously available.

1.4. Research Data Users

To comply with the rights and responsibilities listed in **Policy E30**, research data users should:

- Ensure the retention of original research data and research materials as required under UNM policies.
- Abide by any licenses, terms, or conditions set forth by third parties that retain ownership of data used in research.
- Maintain the confidentiality and ensure appropriate protection of research data; particularly human subject research data, student data, health data, personal financial

data, controlled unclassified information, and other protected data in accordance with established protocols, agreements, policies, and regulations.
- Ensure the appropriate use of data management systems that comply with all applicable data security, protection, or restriction requirements.
- Maintain and comply with procedures for the protection of restricted data and other essential data and records.
- Complete of any trainings required by UNM – for example compliance, information security, responsible conduct of research, and/or project management.

2. Data Stewardship

To assist with effective data stewardship, in addition to the responsibilities listed in **Policy E30**, the following standards and guidelines should be followed.

2.1 Data Management Planning

The research data steward working with the research data owner should develop a plan for effective management of the data for each research project for which they are appointed as research data steward. This planning typically includes the specification of and plans related to:

- The types of data to be managed.
- How data will be stored and secured.
- Derived data that will be produced.
- Documentation that will be produced, including reference to any appropriate documentation standards.
- Any limitations or requirements related to security and confidentiality.
- Plans for sharing and preservation.
- Timing of release of data for discovery and reuse.
- Designated repositories where the data and associated documentation will be placed.
- Strategy for meeting data retention requirements.
- Individuals responsible for monitoring and compliance with the data management plan.

In specific contexts this general recommendation for the development of a plan for research data management transitions into a requirement from a sponsor or other organization for a more formalized written Data Management Plan (DMP), where the DMP structure and content requirements are specific to a given funding proposal or other context.

2.2 Data Sharing

Increasingly, academic societies, publishers, funders, and communities of practice are requiring research data be published in trustworthy (e.g., compliant with the TRUST principles) public repositories, along with the metadata, protocols, and code that underly such data, using FAIR (Findable, Accessible, Interoperable, and Reproducible) and other principles. Moreover, research data and associated artifacts should be cited in manuscripts and other scientific publications using common resolvable persistent identifiers, such as Digital Object Identifiers (DOI), to facilitate discovery, access, and citation.

As such, research data should be archived and published in a UNM recommended repository that meets both funding agency requirements and community needs. These typically include placement of well-structured data and associated metadata (documentation) in an appropriate long-term repository that provides a standardized persistent identifier (e.g., Digital Object Identifier (DOI)) for the deposited data. UNM encourages the responsible sharing of research data in accordance with its mission and in furtherance of its commitment to transparency, accountability, and reproducibility in research. Research data protection and sharing activities include (but are not limited to):

- When sharing research data, researchers should follow best practices established within their research disciplines and must follow applicable UNM policies and procedures. UNM recommends that researchers submit research data and metadata to a trustworthy long-term digital archive or repository whenever possible. Although personal or lab websites, electronic lab notebooks, wikis, local servers, and similar tools may be sufficient for meeting short-term data sharing needs and providing value added services based on research data, UNM does not recommend them as long-term data preservation or sharing solutions if they don't meet the requirements outlined above regarding support for well-structured data and metadata, persistent identifiers, and support long-term discovery, access, and reuse following the end of the research project.
- UNM recommends that all publicly shared research data and associated artifacts be accompanied with an appropriate open access license or data use agreement that places minimal restrictions (e.g., public domain, or open access with attribution) on data and associated artifacts while also maintaining compliance with applicable restrictions that may be associated with the data (e.g., human subjects' consent, data provider license agreements).
- Consistent with current practices among research sponsors and publishers, UNM recognizes there are circumstances under which an investigator can share only aggregate or deidentified data, as well as circumstances when publicly sharing data is prohibited. Researchers are encouraged to consult with UNM research support services such as the Libraries' Research Data Services program, the Center for Advanced Research Computing, or staff in the Offices of the Main Campus and Health Sciences Center Vice Presidents for Research, to develop strategies for meeting multiple or conflicting sharing requirements/restrictions.
- Ensuring that their plans for data retention and sharing as outlined in proposals to sponsors are actionable and executed. Researchers are discouraged from using boilerplate or language from previous proposals in any required DMP, as funder requirements and institutional capacity and services are subject to change.

2.3 Data Preservation

The deposit of research data into a digital preservation system that employs best practices and guidelines[1] related to long-term preservation is a necessary complement to placing data into a public- or limited-access repository in support of data sharing. Although long-term preservation of digital content is often a feature of these repositories, explicit digital preservation capabilities should be identified before assuming these repositories provide long-term preservation. When long-term preservation is not included in the services provided by a selected repository, placement of research data in a separate digital preservation system needs to be performed to

[1] e.g. the Federal Agencies Digital Guidelines Initiative

ensure long-term preservation in accordance with Sections 1 and 2 of this policy. Maintenance of backup copies of research data **is not** considered an alternative to placing research data into an appropriate preservation system.

Effective data preservation activities include:

- Placement of well-structured data and associated metadata (documentation) in an appropriate long-term data preservation system that provides digital preservation capabilities aligned with the Open Archival Information System (OAIS) reference model.
- Periodic review of preservation system content to identify material for which continued preservation is no longer required.

2.4 Data Protection

Researchers are required to adhere to all classification (including UNM's data classification) and protections relating to the data with which they work, and to comply with all requirements and regulations applicable to the protection of those data.

- **Protection of data based on classification**. All researchers must appropriately maintain the security of media and systems that store or transmit UNM data based on the classification of those data. UNM research data is understood to hold a minimum classification of "confidential" until such time that it is authorized by the research data steward for external access, review, or publication and meets all other required approvals and regulatory requirements.
- **Access to research data.** Protection measures for research data access must be aligned with the current classification of those data and reflect needs for providing controlled access to research collaborators, colleagues, students, and open access to the public.
- **Reporting information security incidents.** Researchers must report suspected or known compromises of information resources, including contamination of resources by computer viruses, to UNM's Information Security and Privacy Office (ISPO) immediately upon discovery.
- **Stewardship of research data.** Principal investigators serve as the stewards of their research data and are responsible for the confidentiality, integrity, handling, and protection of their data in accordance with UNM data security standards, related data management plans, applicable data use agreements, and applicable policies and regulations.
- **Research information security.** Researchers are responsible for adhering to the standards and guidelines for workstation maintenance and security as outlined in **UAP Policy 2500** "Acceptable Computer Use" and **UAP Policy 2520** "Computer Security Controls and Access to Sensitive and Protected Information Policy."

Protection of research data throughout the research lifecycle involves explicit planning and activities, including:

- Documented access control methods that ensure only authorized users are allowed access to research data and that their access level (e.g., read-only, edit, etc.) is appropriate for their needs.
- On- and off-site backups of research data are maintained, with the access controls and protections associated with those backups (e.g., encryption) consistent with the security requirements of the original data.
- That strategies for data sharing and use ensure consistency and integrity of shared files for all authorized users.

2.5 Data Retention

A variety of retention requirements exist for research data independent of the data sharing and preservation requirements outlined above, with specific retention times depending upon the nature of the research data. Ultimately, the period of data retention must be consistent with institutional, state, federal, sponsor, and other relevant requirements. At a minimum, research data must be retained for a period of (5) years following the end of the activity (e.g., final report for a sponsored project, research outcome publication date) that produced the research products. Data must be retained within a UNM approved data retention system for secure non-public storage for the required period of retention. In cases where funders or other stakeholders establish different and/or conflicting periods of data retention, researchers should consult with UNM research support services and the Office of the Vice President for Research (VPR) or the Office of the Health Science Center Vice President for Research (HSCVPR) to develop strategies for meeting combined retention commitments while minimizing liabilities.

Beyond the period of retention specified here, continued storage and/or destruction of the research record is at the discretion of the Principle Investigator and their delegated successors. The destruction of any research data should be documented by the responsible party.

If the retention requirements specified in other statutes or external agency regulations are longer (such as in the case of retention of technical information in support of an active patent or in the event of an investigation), those extended requirements will apply. During the retention period and under the appropriate circumstances (e.g., audit compliance, infraction of regulation(s), etc.), allegations of compliance violations including research misconduct, academic misconduct, etc., requested research data must be immediately provided to relevant administrators upon request.

The following examples provide common circumstances that may require a modified period of retention or removal relative to the minimum period specified in the procedures section above:

- Research data must be kept as long as necessary to preserve and protect any intellectual property resulting from the work and to abide by all applicable retention obligations.
- If any charge, audit, claim, or litigation regarding the research arises, such as allegations of scientific misconduct or other compliance violations, data must be retained and made available for a period consistent with the requirements applicable to those processes.
- If a student is involved, absent any applicable data retention requirements based on the nature of the data itself, data must be retained at least until the degree is awarded to the student or it has been determined that the student has abandoned the work.
- If a data use agreement or other agreement governing source data acquired by UNM from an outside party specifies retention or destruction requirements, those source data must be retained and/or destroyed in accordance with the terms of the governing agreement.

3. References

3.1 Research Lifecycle

The NIST Data Framework (RDaF, https://doi.org/10.6028/NIST.SP.1500-18) provides a reference framework defining the phases of the research data lifecycle, consisting of:

- Envision
- Plan
- Generate and Acquire
- Process and Analyze
- Share, Use, and Reuse
- Preserve and Discard

3.2 NIST Data Security Standards

NIST *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations* publication (SP 800-171 Rev. 2 - https://csrc.nist.gov/publications/detail/sp/800-171/rev-2/final)

3.3 US National Archives - Controlled Unclassified Information (CUI) Registry

https://www.archives.gov/cui

3.4 Reference Principles

- FAIR - GoFAIR FAIR Principles website / *The FAIR Guiding Principles for Scientific Data Management and Stewardship* (https://doi.org/10.1038/sdata.2016.18)
- TRUST - *The TRUST Principles for Digital Repositories* (https://doi.org/10.1038/s41597-020-0486-7)
- CARE - *CARE Principles for Indigenous Data Governance* (https://www.gida-global.org/care)

3.5 NCURA Research Data Tutorial for Research Administrators

https://ori.hhs.gov/education/products/rcradmin/topics/data/open.shtml

3.6 Digital Preservation Coalition - Standards and Best Practice

https://www.dpconline.org/handbook/institutional-strategies/standards-and-best-practice

3.7 Digital Preservation at the Library of Congress

https://www.loc.gov/preservation/digital/index.html

3.8 Open Archival Information System (OAIS) Reference Model

Consultative Committee for Space Data Systems. *Reference Model for an Open Archival Information System (OAIS). Recommended Practice CCSDS 650.0-M-2.* Consultative Committee for Space Data Systems, https://public.ccsds.org/Pubs/650x0m2.pdf (2012)

4.____Research Data Support Resources

- Information about available research support services - Research Service Catalog - https://researchit.unm.edu
- University Libraries Research Data Services - https://libguides.unm.edu/data, rds@unm.edu
- Health Sciences Library and Informatics Center Research Support Services – Data Sharing Research Guide - https://libguides.health.unm.edu/c.php?g=1016541&p=7539721

5. Designated UNM Research Data Stewards

- http://data.unm.edu/data-stewards.html

6. Points of Contact for Questions Related to this Standard and Related Faculty Handbook Policy E30.

- Overall policy:
- Regulatory, legal, and compliance issues:
- Data ownership