## 1. Purpose

1.1. Arizona State University (ASU) Knowledge Enterprise (KE) follows principles of data management to ensure the security, effective use, and appropriate access to research data generated at or under the auspices of the institution. This standard:

1.1.1. Governs Research Data Management at ASU, and

1.1.2. Supports the Office of Science and Technology Policy (OSTP) memorandum: Ensuring Free, Immediate, and Equitable Access to Federally Funded Research which directs all US federal agencies to make data, code, and other research outputs broadly available with the fewest possible restrictions, ensuring equitable delivery of federally-funded research results and data.

## 2. Definitions

2.1. **Data Manager** is the assigned employee (faculty or staff) who has responsibility and decision-making authority for the documentation, management, sharing, and security of the Research Data collected, stored and ultimately published as part of a research study.

2.2. **Principal Investigator (PI)** is an Investigator who has primary responsibility for a research project within the university for the design, conduct, and reporting of research.

2.3. **Research Data** is defined as any recorded material collected, retained, and applied by investigators in the course of a research project, regardless of funding source, that are also used to derive and validate research findings. Research Data include both derived data (e.g., statistics, findings, formulas, etc.) and primary physical and digital data (e.g., notebooks, protocols, images, case history records, etc.). Research data may be quantitative in the form of spatial and tabular files, remote sensing output; qualitative information such as documentation, interviews, and survey results; and supplementary information including images, digitized physical samples, audio of video recordings, computational models, or other relevant software/code.

2.4. **Researcher** is any faculty member, student, postdoctoral researcher, research associate or fellow, or other person involved in the design, conduct or reporting of research. See also “Investigator”.

## 3. Applicability

3.1. This standard applies to:

3.1.1. Any Researcher(s) overseeing or performing research conducted at, or under the auspices of, ASU when research data are collected or produced, or provided by a third party, regardless of the source of funding.

3.1.2. Any individual(s) who has been designated as Principal Investigators, Data Managers, and Researchers.

3.2. Unless the data are collected as part of a federal grant, this policy *does not apply* to students when the research data are collected or produced as part of:

3.2.1. credit-bearing coursework,

3.2.2. internships,

3.2.3. dissertations or theses.

## 4. Standard

Users of Knowledge Enterprise resources shall maintain good data stewardship and regulatory compliance through defined data security and retention, grant access to research data for the people of Arizona and the world, unless exempt from release per A.R.S. 15-1640, in alignment with public access mandates and support open access of scholarly articles.

## 5. Data Governance & Ownership

Research Data produced under the auspices of ASU is defined as Tangible Intellectual Property belonging to the Arizona Board of Regents (ABOR) unless ownership is altered under the exceptions specified in the ABOR Intellectual Property Policy.

## 6. Data Management

6.1. The Principal Investigator shall work with relevant supporting units to create a Data Management and Sharing Plan (DMSP) prior to beginning a research project if one of the following are true:

6.1.1. It is required by an external funder,

6.1.2. The research is being funded internally by ABOR or by an ABOR university, or

6.1.3. There is a significant legal or financial risk to the institution if the research data were to be lost or inadvertently released (e.g., data obtained via data use agreements, commercially licensed data, data subject to HIPAA, indigenous data, etc.).

## 7. Data Classification and Handling

7.1. Conducting research has legal and ethical implications with respect to the collection, storage, publication, and preservation of data. Therefore, ASU faculty, staff, students, and collaborators shall adhere to standards, processes, and guidelines in place for the proper handling of these data as required by applicable legal or regulatory requirements as outlined in:

7.1.1. The project-specific Data Management and Sharing Plan,

7.1.2. Procedures for the Review of Human Subjects Research,

7.1.3. ASU Data Handling Standard

7.2. Researchers must:

7.2.1. Use protocols to protect locations of sensitive environmental or archaeological data,

7.2.2. Not release Research Data if they contain confidential or proprietary information,

7.2.3. Properly de-identify or anonymize Research Data prior to sharing,

7.2.4. Not release Research Data if prohibited by contractual or license agreements,

7.2.5. Ensure that the applicable DMSP identifies the steps that will be taken to protect the data during the life of a research study and that planned measures are being followed.

7.2.6. Obtain the appropriate informed consent for information sharing from participants in human subjects Research Data as may be required prior to collecting and analyzing the data,

7.2.7. Choose a university-approved storage medium that satisfies security requirements for the data,

7.2.8. Ensure that anonymization and access to the data are appropriately controlled,

7.2.9. Be knowledgeable of contractual obligations required by third-party data sharing agreements,

7.2.10. Monitor and manage data security and legal and ethical obligations when working with sensitive data,

7.2.11. Appropriately assess which information can be published at study completion.

## 8. Data Access

### 8.1. Public Access

Public access to Research Data lowers the barrier to building on the research produced at ABOR institutions. This ensures ASU's

compliance with mandates from federal funders and are also recognized as major contributors to cutting edge research and innovation. Under this Policy:

8.1.1. Research Data shall be published no later than 2 years after the end of the applicable funded research project period unless a different period is mandated by the terms of the award or contract that applies to the Research Data. This requirement extends to Research Data produced under the auspices of ABOR universities regardless of funding source, where allowable based on privacy or security of the data or otherwise exempt.

8.1.2. For Research Data supporting peer-reviewed publications, such Research Data will be made available at the time of publication or according to the journal's requirements.

8.1.3. Public access compliance is achieved when materials are included with a peer reviewed publication as supplementary information and/or are deposited in an institutional or third-party data repository intended for long-term data availability. Placing materials solely on personal or professional websites or on platforms not intended for or unable to support long-term access is not sufficient to comply with this requirement.

8.1.4. Researchers who give collaborators access to Research Data under their responsibility, must inform them, in writing where appropriate, of any limitations or restrictions on the use or dissemination of the Research Data. Examples of how this may be achieved include but are not limited to the use of established licenses (Creative Commons, GNU, MIT) or data use agreements.

8.1.5. These public access requirements will not apply if they are superseded by specific provisions in contracts and awards, to any materials not subject to this Research Data Policy, or materials that cannot be made publicly available due to their specific nature.

## 8.2. Administrative Access and Availability

8.2.1. Researchers must retain access to Research Data resulting from research projects they themselves have initiated, and to Research Data acquired by processes for which they were primarily responsible.

8.2.2. Research Data are to be accessible to members of the University community, external collaborators, and others as appropriate (e.g., for patent applications or journal submissions), unless otherwise specified as not allowed by specific award or contract provisions. Where necessary to assure needed and appropriate access (e.g., for research misconduct investigations), the University may take custody of Research Data in a manner specified by the Vice President for Research or their delegate.

## 9. Data Archiving

In addition to Federal requirements for research records retention, this policy additionally requires that the Research Data, associated Metadata, and any other relevant documentation (e.g., readme files, wikis, or any other information that aids in understanding and using the information) be retained. In determining the retention period, certain requirements take precedence over others. The following is a list, ordered from highest to lowest precedence: Legal/regulatory, funder, journal/publisher, institutional, and disciplinary norms. In the absence of specific requirements at one level, the requirements of the next lower level apply. DMSPs should explicitly state the Research Data retention period.

## 10. Ethics in Data Use & Reuse

Principal Investigators are responsible for considering ethical implications of Research Data collection and use. Considerations include, but are not limited to: reviewing policies related to the data (e.g., human subjects research); in cases where no laws or policies apply, considering the potential harms of collecting, using, or sharing the data (e.g., data about indigenous people, lands, or custom; endangered species locations; potential for data misuse), clearly communicating to research subjects and potential data users any restrictions on data reuse (e.g., via licenses, data use agreements, consent forms).

## 11. Researcher Departure from ASU

11.1. Researchers separating from the institution are expected to meet with their respective research administration service provider to take steps to ensure continuity of projects, transfer any grants to their new institution, appoint an alternate Principal Investigator, appoint an alternate Research Data Manager or change investigator to take ownership of research dataset management, and share responsibilities as appropriate to their project and agreements.

11.1.1. If a Principal Investigator leaves, data ownership may be transferred to another institution with the approval of the applicable academic or research unit which shall determine who will take stewardship (see definitions) in consultation with the Vice President for Research (or their delegate).

11.1.2. After approval, the Principal Investigator may take copies of research data for projects on which they have worked. The purposes for which such data may be used are subject to relevant confidentiality restrictions and compliance regulations, or as formally agreed-upon beforehand in a data use agreement. The researcher's department is responsible for retaining the original or primary Research Data in and appropriate repository at the university unless the transfer of ownership is explicitly authorized.

11.1.3. Ownership of the data may be transferred with the approval of a delegate authorized by the originating institution, and with written agreement from the new institution that guarantees:

11.1.3.1. its acceptance of custodial responsibilities for the data,

11.1.3.2. University access to the data, should that become necessary, and

11.1.3.3. relevant confidentiality restrictions, where appropriate.

11.1.3.4. If a student or researcher leaves the institution, the Principal Investigator shall determine who will take stewardship (in consultation with Assoc. VP for Academic Programs, if a student).

## 12. Incident Response

In the event of a security incident, a correct, complete, and consistent response is essential to ensure the protection of critical information and systems as well as University compliance with applicable laws, rules, and regulations. Timely and relevant communication with the appropriate parties, including any contractually required communications, is necessary to ensure the quality of the response, support legal action if necessary, and maintain public confidence. Complete, accurate documentation and subsequent debriefing are important to prevent the recurrence of similar incidents. Researchers shall follow the processes outlined in the Information Security Incident Response Standard and contact the Research Technology Office at RTSHelp@asu.edu.

## 13. Violations and Enforcement

Enforcement may include removal of systems or access privileges to ASU resources until requirements are met. Violations of this Policy may lead to disciplinary actions or contract termination as applicable.

## 14. Resources

14.1. Office of Science and Technology Policy (OSTP) memorandum
14.2. ABOR Intellectual Property Policy
14.3. ASU IT Policies and Standards
14.4. Procedures for the Review of Human Subjects Research,
14.5. ASU Data Handling Standard
14.6. Research Data Storage Selector

## 15. Policy Revision

The Director of Research Computing will review this policy in consultation with other relevant local stakeholders at an interval no more than three (3) years.

| Date of Change | Responsible Party | Summary of Change(s) |
|---|---|---|
| 09/12/2024 | Kathryn Claypool | Initial Version Established |