UNIVERSITY OF SOUTH ALABAMA

**Responsible Office:** Office of Research and Economic Development

**Last Review Date: 7/2020**

**Next Required Review: 7/2025**

# Data Management Practices Policy

## 1. Purpose

This policy is guided by best practices for data management. University data, whether managed and residing on university information technology resources, stored on personal devices, managed by a third party, or outsourced to a service provider, is an important asset that must be governed, protected, and appropriately safeguarded. Members of the university community have the responsibility to appropriately use, maintain, and safeguard university data.

## 2. Applicability

This document is applicable to members of the University research community.

## 3. Definitions

Terms used herein are as defined in the *USA Data Management and Laboratory Notebook Ownership Policy*

**USANAS**: USA Network Access Storage is the university's computer system data storage network

## 4. Policy

This document supplements *the Data Management and Laboratory Notebook Ownership Policy*

## 5. Procedures

Managing data is an integral part of the research process. How you manage your data depends on the type of data, how the data is collected, and how the data is used throughout the life of the project. Effective data management helps ensure the integrity of your research and supports the published results of your research.

### 5.1 Collection of Research Data

Principal Investigators (PIs) must implement a classification system to organize Data. It is the responsibility of the PI to communicate the selected system to the PI's laboratory personnel and

ensure the methods and accuracy of Data collection and analysis are maintained. The Research records should entail adequate detail to allow examination for the purpose of replicating Research experiments, verifying authenticity of records, validating conclusions, and responding to allegations of Research misconduct.

For studies involving multiple University Affiliated Individuals or collaborators, it is recommended the PI of record retain a master log cataloging the experiments for the entire study. The PIs must also keep record as to locations of Laboratory Notebook, Data, and pertinent materials kept in other laboratories/locations.

The Laboratory Notebook is the most common method used to document experiments and field work. Recommended recordkeeping practices can be found in the University's "Laboratory Notebook: Best Principles and Standards" publication. Briefly, in addition to the study title, the University Affiliated Individual's name(s), and the study hypothesis, the experimental lab notebook should include detailed information on the materials used, sources of the materials, experimental methodology, statistical treatments, results and conclusions so as to enable replication of the experiments by others at any time. Data that cannot be entered directly in the Laboratory Notebook (e.g. glass microscope slides, fixed tissue samples, geological field samples, thumb drives, etc.) should be referenced in the Laboratory Notebook along with explicit instructions as to where the Data can be found.

## 5.2 Storage of Research Data

### 5.2.1 Digital Backups

The guiding principle behind digital backups is to ensure that at least two instances of the protected data exist on separate media. For example, the following would be considered "back-ups":

- Scanned images of paper documents, when both the scanned images and the original documents are retained.
- Data on USB keys or other media which have been copied to network storage or other digital media, and in which both instances are retained.
- Data located on a network storage system (for example, the University's "USANAS" system) which itself is also backed up on a regular basis.

The following would *not* be considered backups:

- Data which exists only on a Google Drive/Share. Although Google does provide back-up protection of the Drive items from failure of their system, it does not protect your data from *your* actions such as mistaken deletions.
- Data which exists on only a single USB key or CD copy.

Ideally data back-ups will be stored in separate locations. The USANAS system, for example, backs up data to storage facilities located in separate campus locations, as well as to a disaster

recovery node in Montgomery, Alabama. Your particular grant or research program may have specific requirements for appropriate backup procedures.

The University Computer Services Center and USA Health IT offices can provide further assistance in planning data storage and back up procedures.

#### 5.2.2 University Digital Storage options

The University Computer Services Center (CSC) can assist researchers in assessing storage options for digital data. Call 251-460-6161 or email the Academic Computing support desk at helpdesk@southalabama.edu to initiate contacts. The CSC manages several networked storage systems which may be applicable to your needs, including:

- USANAS, an on-premises, high availability storage system
- The University G Suite (Google) "cloud" system which includes Google Drive storage.

USA Health employees may wish to contact their IT support office for services specific to them.

Although organizationally separate, the CSC and USA Health IT support cooperate and consult on common issues such as these and will refer researchers to the appropriate support groups

## 5.3 Retention of Research Data

Retention of Research Data is based on state law, federal regulations, and sound management practices. Research Data should be archived for a minimum of seven years following the conclusion of the research project. If funding is provided from an outside organization, the policies of the grantee organization generally will prevail over the minimum standards set herein. There are state and federal regulations prescribing the length of time original Data must be retained, varying from three to seven years depending on the governmental organization. In addition, any of the following may warrant justification for longer periods of retention:

• Terms of a sponsored Research agreement administered by the University's Office of Sponsored Projects Administration; including clinical trial agreements;

- If a student is involved, data must be retained at least until the degree is awarded or it is clear that the student has abandoned the work;

• Research involving minors may need to be retained until the subjects reach the age of 21;

• Research Data must be retained as long as necessary to protect intellectual property resulting from the work. Data used to support a patent or copyright application must be archived for a minimum of twenty years or such other time as required by the University Office of Commercialization and Industry Collaboration;

• If allegations regarding Research arise, such as Research misconduct or conflict of interest, Data must be retained for a minimum of seven years as required by federal regulation, or until such charges are fully resolved.

Records of Research Data collection and retention should be retained by the PI in the department or unit where they originated. In any event where encryption is used to secure electronic records of Research Data, keys and recovery procedures should also be appropriately maintained by the PI to ensure data can be decrypted into a readable format.

## 5.4 Data Management Plan

Even if one is not required by your funding agency, developing a data management plan (DMP) at the beginning of a new project will inform good practice throughout the project life cycle. The following practices are fundamental to effective data management and can be applied to all disciplines:

***Data Management Plan:***

- Adhere to the guidelines set by any funding agencies and institutions that are sponsoring the research.
- Templates for data management plans are based on specific requirements listed in funder policy documents. See DMPTool for a collection of public templates.
- Complete your DMP early so that it will not be put aside at the start of data collection.
- The minimum expenses to include when calculating your data management costs are: data creation, processing, analysis, storage, sharing, and preservation. Remember that some Funding Agencies accept these costs in grant applications -- be sure to include these costs.

## 5.5 Security and Privacy

Password protect and/or encrypt sensitive files. Follow USA's Controlled Unclassified Information (CUI) Policy if in receipt or development of CUI research. PIs who submit grant applications for projects containing CUI or other access controlled research must engage the USA Director, Information Technology and Risk Compliance at the earliest possible moment to determine appropriate security protocols. PIs must not wait until the grant is actually awarded since these protocols can take months to implement and cause delay to the project.

Users of the University G Suite (Google) Drive and JagMail system will find guidance on security features by looking up ""JagMail Secure Messaging Features" in the A-Z index of the main University web server, or via the direct link
https://www.southalabama.edu/services/jagnet/securedata/

A key security feature, recommended for all users of the G Suite system, is two-factor authentication. This can be applied to protect both the email (JagMail) and Google Drive services. Please use the A-Z index on the main University Web Server to look up "JagMail 2 Factor Authentication", or use the direct link
https://www.southalabama.edu/services/jagnet/twofactor.html

The University Information Security Office provides substantial guidance on appropriate procedures for protecting computer systems and data whether working on premises or remotely. To access their web page, look up “Information Security” in the “A-Z Index” on the main University web server, or use the direct link https://www.southalabama.edu/departments/csc/informationsecurity/

USA Health employees may also receive guidance from USA Health Information Technology and Information Security offices. Please use your normal IT contact procedures for further information.

## 6. Enforcement

Concerns regarding data management is overseen by the Office of Research and Economic Development.

## 7. Related Documents

Controlled Unclassified Information (CUI) Policy
USA Data Management and Laboratory Notebook Ownership Policy
Laboratory Notebook: Best Principles and Standards