
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 USANAS 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 laboratory personnel and

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 full 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 256-6161 or email the A

{ (/ o o P š] } v • Œ P Œ] v P Z • Œ Z Œ] • U • μ Z • Z • Œ Z u] • } v
 Data must be retained for a minimum of seven years as required by federal regulation, or until such changes 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:

- x Adhere to the guidelines set by a funding agencies and institutions that are sponsoring the research.
- x Templates for data management plans are based on specific requirements listed in funder policy documents. See [DMPTool](#) for a collection of public templates.
- x Complete your DMP early so that it will not be put aside at the start of data collection
- x 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 Controlled Unclassified Information \(CUI\) Policy](#) in receipt or development of CUI research. Those who submit grant applications for projects containing sensitive information should be aware of the following requirements: 72.9 (s)-i itivpm faps c c 0 Td3 (c)-9.9 es<>>B (iva)-17MCchmmumthmubmb3hsw

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 Index on the main University web server, or use the direct link <https://www.southalabama.edu/departments/csc/informationsecurity/>

USA Health employees may also