Memorandum of Administrative Policy
Data Management and Sharing Policy

Area: **Academic Affairs**

Section: **Faculty Research**

Number: **06.A.02 AP**

Purpose and Scope

Data Management is the process of controlling and appropriately handling the information generated while conducting research, scholarly, or creative activities, including the storage, access and preservation of data throughout the research life cycle and beyond. In accordance with SAM 07.A.08 - Data Classification and Protection, research data includes mission-critical information and requires consistency in the handling and maintenance of the data. All research, scholarly, and creative works projects involve some level of data management; the outcome of the project often depends in part on how well this data is managed. Data sharing and open access to data is at times required by, or at a minimum, encouraged by, governmental and other funding agencies to reinforce open scientific inquiry, encourage diversity of analysis and opinion, and to permit the creation of new data sets when data from multiple sources are combined.

The purpose of this policy is to:

1. Ensure consistency in the appropriate handling, storage, and dissemination of research, scholarly, and creative works data; and

2. Protect the university and research teams by meeting the requirements of funding agencies; and

3. Provide adequate oversight by the Office of Research and Sponsored Programs (ORSP) to monitor the protection of research data and investigate related concerns.

Definitions

Data: Recorded factual material commonly accepted in the scientific or scholarly community as necessary to validate research findings or support the creation of creative works, excluding preliminary analyses, drafts of scholarly or scientific work, plans for future research, peer reviews, communications with colleagues and physical objects (e.g., laboratory samples). Research data includes any information needed for the university for purposes of research to conduct university business regardless of storage medium.

Mission-critical information (Level 1 data): Defined in SAM 07.A.08, Data Classification and Protection

Principal Investigator (PI): the individual with primary stewardship of data on behalf of the University. The PI is responsible for data collection, recording, storage, access, and retention in keeping with this policy and best practice of the PI's discipline.

Policy

1. Data Management Roles and Responsibilities

    a. **University of Houston-Clear Lake:** The primary owner of data generated by projects performed at or under the auspices of the University regardless of funding sources, unless expressly stated in contractual arrangements. NOTE: This may also apply to students who generate data as part of their employment by UHCL and/or whose data collection is supported by an external award. Data related to human subjects research must be retained by UHCL in accordance with federal and IRB

requirements. The University retains the right to access to data performed at the University, supported with University administered funds, or carried out by using University facilities. The University's entitlement to retain access to data shall remain irrespective of the PI. The University also has the right to refuse data coming into the institution, or leaving the institution, on a project-by-project basis.

b. **Principal Investigator (PI):** The primary steward of the data. The PI is responsible for:

   i. Identifying an individual as information custodian as defined in SAM 07.A.08, Data Classification and Protection to provide operational support during the project. Operational support for PIs at UHCL will be provided by the Office of Institutional Technology;

   ii. Identifying the individual from the college/university serving as the Information Security Officer for the research project with responsibilities for data protection and compliance. The Information Security Officer for PIs at UHCL will be the UH System Information Security Office;

   iii. Developing a written data management plan that adheres to university requirements and any applicable contracts. For example, in the case of funded research, the plan should include procedures for retaining and sharing data according to sponsor requirements. Data management plans will be developed in collaboration with the Office of Research and Sponsored Programs to ensure compliance with requirements and contracts;

   iv. Reviewing the data management plan with the Office of Research and Sponsored Programs at least annually to ensure it remains current;

v. Enacting processes necessary to confirm compliance with the plan with guidance from the Office of Research and Sponsored Programs, including data security per sponsor and regulatory requirements;

vi. Working closely with the College, the Office of Research and Sponsored Programs, and collaborating institutions upon leaving UHCL to ensure the appropriate transfer and ownership of data and IP; and

vii. Producing the plan and associated documentation upon request by the UHCL Office of Research and Sponsored Programs and/or applicable funding agencies.

c. **Colleges/Departments/Institutes/Centers** The College, Department, Institute, and/or Center is responsible for:

i. Providing the necessary resources for data management, addressing related information security issues and ensuring investigator compliance with data management requirements and university policy, such as SAM 07.A.08, Data Classification and Protection;

ii. Working with the PI upon their leaving UHCL to ensure appropriate transfer and ownership of research data.

d. **Office of Research and Sponsored Programs (ORSP)** ORSP is responsible for:

i. The development of a campus-wide policy for data management and review of compliance concerns related to data management, particularly with regard to compliance with federal grant requirements and sponsored project agreements, and data use agreements relating to data received from third

parties

ii. Maintaining the right to refuse an award if the University is unable to meet data requirements

iii. Sequestering/taking custody of data as necessary for investigations of noncompliance and/or research misconduct;

iv. Upon request, working with the College upon a PI leaving UHCL to ensure appropriate transfer and ownership of research data.

e. **Office of Information Technology (OIT)** OIT is responsible for:

i. The oversight of enterprise level software and systems related to data management;

ii. Ensuring that designated Information Security Officers (ISO's) are appropriately trained.

2. **Data Management Plan**

a. To ensure the appropriate identification and protection for information, all university research projects require a formalized, written data management plan. The Office of Research and Sponsored Programs will be responsible for ensuring that all projects requiring a data management plan have completed a plan that complies with all requirements.

i. When a project is being submitted for external funding, the PI and Office of Research and Sponsored Programs should determine if the funding agency for a particular research project has specific requirements for a data

management plan and ensure a plan meeting those requirements is submitted to the funding agency as applicable.

ii. If there are no formal requirements, a data management plan including, at a minimum, the following information must be documented and shared with all key personnel involved with the project:

1. Type of data being collected and stored (e.g., survey, computational, financial, educational). This should include designation of any data with specific compliance requirements, such as Health Insurance Portability and Accountability Act (HIPAA), Family Education Rights and Privacy Act (FERPA), Federal Information Security Management Act (FISMA), or any project requiring compliance with National Institute of Standards and Technology (NIST) standards;

2. Description of the appropriate platform for data storage, including security components;

3. Responsibility for the data from an ownership perspective;

4. Responsibility for the data from an IT support perspective;

5. Responsibility for the data from an information security perspective, including the identification of the ISO for UHCL;

6. Location where the data will be stored (e.g., standalone computer, department share). All data should be stored in accordance with SAM 07.A.08;

7. How and by whom logical access to the data will be controlled;

8. How physical access to the system containing the data will be controlled;

9. Type of anti-virus controls the system containing the data will have;

10. Process for digital data backups for recovery purposes, including the media that will be used for backups, how often the backups will occur and how often backups will be restored for testing; and

11. Process for securely storing non-digital data (e.g., lab books, consent/data collection forms).

3. **Data Storage and Archiving**

a. Data must be archived in a controlled, secure environment in a way that safeguards the data (primary, secondary and metadata), observations, or recordings in accordance with SAM 07.A.08.

b. The archive must be accessible by scholars analyzing the data, and available to collaborators or others who have rights of access as allowed or required by the sponsor.

c. Research data should be stored securely for sufficient time following publication, analysis, or termination of the project. Research data includes not only the primary information produced through the conduct of the research, but also the corresponding metadata. Research data must be retained in accordance with all applicable sponsor and federal regulatory data retention requirements and profession-specific ethical guidelines/timelines.

d. If sponsor requirements indicate that data must be destroyed at a given time point,

the PI, in collaboration with the Office of Research and Sponsored Programs, information custodian, and Information Security Officers, is responsible for ensuring destruction per these requirements.

4. **Data Sharing**

   a. Investigators are expected to share with other researchers data created or gathered in the course of funded research within a reasonable time frame. These requirements may vary, based on funding agency, but in general require that research data be made available to the scientific community for subsequent analysis. In most cases, the PI has the right to first analysis, unless other requirements are in place to warrant immediate release. It is the PI's responsibility, in collaboration with the Office of Research and Sponsored Programs, information custodian, and Information Security Officers, to ensure that data sharing plans are developed and provided to the granting agency as required, and to ensure that the plan is executed.

   b. Methods of sharing data may include, but are not limited to, publications, placing data in public archives, and sharing directly with other researchers.

   c. PI's are responsible for working with ORSP to ensure that the intellectual property of the University is protected throughout any data sharing arrangement.

   d. Any data shared must meet all requirements for compliance including privacy and data protection. It is the PI's responsibility, in collaboration with the Office of Research and Sponsored Programs, information custodian, and Information Security Officers, to ensure that all compliance requirements for the data are properly identified and satisfied through any data sharing arrangement. This includes

requirements identified through IRB and other compliance processes.

Revision Log

Revision Number: 1

- Approval Date: 05/28/2025
- Description of changes: Clarifying definitions of data and individuals/offices involved in data management

Approval

Approved by:

/Dr. Christopher Maynard/

Senior Vice President of Academic Affairs and Provost

/Dr. Richard Walker/

President

May 28, 2025

Date