

Memo To: All UH-Downtown/PS Holders
From: Dr. Loren J. Blanchard, President
Subject: Data Governance Policy

UH-Downtown/PS 08.A.08
Issue No. 1
Effective Date: 7/21/2025
Page 1 of 6

1. PURPOSE

- 1.1. The Data Governance Program will support the business objectives of the University of Houston-Downtown (UHD), addressing data ownership, stewardship, integrity, access, privacy, privacy classification, and reporting for all UHD data including, but not limited to, student, faculty, human resources, finance, facilities, alumni, and donor data elements, wherever they reside. Research data is managed under Policy 08.A.07 Data Management and Sharing.
- 1.2. This policy applies to all individuals whose affiliation with UHD requires or permits access to University data, without regard to the manner, form, duration, or location of access.

2. DEFINITIONS

- 2.1. Co-Chairs: individuals who serve as the leads for the Data Governance Council.
- 2.2. Chief Data Management Officer: is a senior executive responsible for overseeing UHD's data strategy, governance, and management.
- 2.3. Data Access and Security: ensures the protection of sensitive information from unauthorized access, breaches, and misuse.
- 2.4. Data Asset: an object comprised of data elements, which could be logical or physical.
- 2.5. Data Dictionary: a set of information describing and defining the contents, format, and structure of a database, and the relationship among its elements.
- 2.6. Data Element: any defined unit of data within a system or dataset.
- 2.7. Data Governance Program: a set of guidelines to manage University data effectively, efficiently, and ethically in support of the University's mission.
- 2.8. Data Management: the people, processes, and technology required to create consistent and proper handling of data and understanding of information across the organization, irrespective of the boundaries created by organizational structures.

- 2.9. Data Management Officer: an employee who is responsible for overseeing the creation and implementation of Data Management strategies and policies.
- 2.10. Data Owner: the individual responsible for the business use of a collection of data, information, or the business function.
- 2.11. Data Steward: an Information Custodian responsible for managing, sourcing, documenting, and maintaining data assets.
- 2.12. Data Stewardship: the management and oversight of the University's data assets to ensure quality, integrity, security, accessibility, and reportability.
- 2.13. Data User: an authorized user, as defined by [PS-08.A.04 - Computer Access, Security and Use Policy](#) who accesses University data in performance of their assigned duties.
- 2.14. Executive Sponsor: an individual who provides oversight of the Data Governance Program and Council.
- 2.15. Functional Area: a department that represents and serves a particular subset of University data.
- 2.16. Information Custodian: a person (or department/unit) providing operational support for an information resource.
- 2.17. Lead Functional Data Stewards: individuals recommended by the Co-Chairs and appointed by the Executive Sponsor and appointed for a one-year term.
- 2.18. Metadata: describes how and when a particular set of data was collected and how the data are formatted. Metadata is necessary for understanding how data are stored in data warehouses.
- 2.19. Stakeholder: an employee who affects, or would be affected by, data policy or procedural change. Stakeholders request data, initiate requests for changes to University data, and identify problems with University data that are impeding normal daily operations. They provide input or feedback that assists with the process of satisfying any change request.
- 2.20. Subject Matter Expert (SME): any employee with extensive knowledge of given functional, technical, reporting, or security-related data issues.
- 2.21. University Data: any data element stored or used in the management and operation of UHD.

3. POLICY

3.1. Roles and Responsibilities

3.1.1. Data Governance Council (“Council”) - oversees management of the data governance program and directs activities in support of the University mission; consists of a leadership team and ex officio members determined by positions held within the University, as well as divisional representatives appointed by the Vice President for each division. The council will be led by Co-chairs, Lead Technical Data Steward, and a Lead Functional Data Steward, whose roles are defined. Collectively, the Council is responsible for:

- 3.1.1.A. Developing data governance policies and procedures addressing data privacy and classification, ownership, stewardship, integrity, access, change management, and reporting;
- 3.1.1.B. Ensuring compliance with state and federal laws as well as UHD and University of Houston System (UHS) policies related to data management including:
 - i. Implementing best practices for managing and securing data in accordance with all applicable laws, policies and data privacy classifications;
 - ii. Ensuring the University's records management programs apply to all types of data storage media;
 - iii. Increasing awareness of and outreach for the University's records management programs within UHD; and
 - iv. Conducting a data maturity assessment of the University's Data Governance Program.
- 3.1.1.C. Ensuring adherence to Data Management policies and procedures;
- 3.1.1.D. Identifying and resolving cross-functional data issues, and when necessary, arbitrating escalated data issues;
- 3.1.1.E. Directing shared Data Management activities across the University through guidance of Data Management sub-committees and working groups;

- 3.1.1.F. Coordinating training and support programs for Data Users;
- 3.1.1.G. Developing, maintaining, and documenting data and reporting standards; and
- 3.1.1.H. Informing Stakeholders of important data and reporting issues.
- 3.1.2. Co-Chairs are responsible for:
 - 3.1.2.A. Leading the Data Governance Council to ensure the duties and responsibilities of the Council are met;
 - 3.1.2.B. Providing annual reports to the Executive Sponsor and University leadership;
 - 3.1.2.C. Leading the Council to review and approve changes and updates to policies, business processes and ownership changes associated with University data;
 - 3.1.2.D. Consulting with appropriate parties to ensure state requirements for Data Governance and Management are met; and
 - 3.1.2.E. Appointing divisional Data Management Committees.
- 3.1.3. The Lead Functional Data Stewards are responsible for:
 - 3.1.3.A. Assisting with oversight of the Data Governance Program and Data Governance Council;
 - 3.1.3.B. Helping ensure the duties and responsibilities of the Data Governance Council are met;
 - 3.1.3.C. Serving as an alternate on the state data management advisory board in the event the Data Management Officer is unable to attend; and
 - 3.1.3.D. Performing other required duties in the absence of the Chief Data Management Officer to ensure compliance with the [Texas Government Code 2054](#).
 - 3.1.3.E. Functional Data Stewards are required to be knowledgeable regarding data assets in relation to business processes. Technical Data Stewards are expected to be knowledgeable about the underlying structure and administration of Data Assets. It is possible that a Data Steward could have both functional and technical knowledge.

- 3.1.4. A Data User is expected to be familiar with and abide by all data governance and data security policies and procedures. [SAM 07.A.08: Data Classification and Protection](#), [SAM 07.A.10: Information Security Program](#), [SAM 07.A.11: Information Security Incident Reporting and Investigation](#), [SAM 03.H.01: Record Retention](#).
- 3.1.5. All divisions are to appoint one divisional representative to the Data Governance Council. Divisional representatives will serve for a one-year term running from September 1 to August 31 and can be re-appointed for consecutive terms. Divisional representatives will function as the lead Data Steward for their area.

4. PROCEDURES

- 4.1. All data governance procedures are developed by the Data Governance Council and are housed on the www.uhd.edu/data-governance. These procedures are reviewed every two years for best practices.

5. REVIEW PROCESS

Responsible Party (Reviewer): Associate Vice President for Information Technology & CIO (or equivalent position)

Review Period: Every five years on or before September 1 and as necessary.

Signed original on file.

President

6. POLICY HISTORY

Issue #1: 07/21/25 (Current issue)

7. REFERENCES

[SAM 07.A.08: Data Classification and Protection](#)
[SAM 07.A.10: Information Security Program](#)

[SAM 07.A.11: Information Security Incident Reporting and Investigation](#)

[SAM 03.H.01: Records Retention](#)

[PS-08.A.04 - Computer Access, Security and Use Policy](#)

[UHD Data Governance](#)

[Texas Government Code 2054](#)

8. EXHIBITS

There are no exhibits associated with this PS.