Section: Information Technologies Policies
Policy Name: Data Governance Policy
Policy Owner: Office of the President
Responsible University Office: Vice President for Information Technologies
Origination Date: February 26, 2018
Revisions:

I. SCOPE OF POLICY

A. Data is an institutional asset and will be managed according to a University-wide data governance framework to facilitate the missions and activities of the University and minimize exposure to risk inherent in information management.
B. This policy creates, under the authority of the President, a data governance framework to support the consistent and appropriate management of University information.
C. This policy creates a framework for organizing the University into functional areas.
D. This policy sets forth a standard for management of University information and holds data trustees accountable for their functional area's compliance with data management requirements, including this policy.
E. This policy establishes the rules, roles, and responsibilities related to the management, including acquisition, utilization, maintenance, access, and protection, of University information.
F. This policy applies to all members of the University community and anyone with access to University information.

II. DEFINITIONS

A. "Availability" means ensuring timely and reliable access to and use of University information.
B. "Confidentiality" means preserving authorized restrictions on University information access and disclosure, including means for protecting personal privacy and proprietary information.
C. "Council for Data Governance (CDG)" is the University council responsible for overseeing the appointment and action of data trustees for each of the University's functional areas. It includes the Chief Information Officer, VP & General Counsel, and other members as appointed by the President and/or his or her delegates.
D. "Data custodian" is a University entity or employee with operational responsibility to manage a shared data repository on behalf of a data steward.
E. "Data governance" is the responsible oversight of the informational quality, effectiveness, usability, strategic value, and security of data throughout its lifecycle.

F. “Data management” is the responsible stewardship of data throughout its lifecycle, including acquisition, utilization, maintenance, access, and protection.
G. “Data Management Advisory Committee (DMAC)” is the University council responsible for coordinating data quality, effectiveness, usability, and strategy efforts and monitoring and recommending necessary data management actions to the University. It is chaired by the Associate Provost for Institutional Research and Effectiveness and includes delegates as may be appointed from time to time by data trustees and/or the chair.
H. “Data Security Advisory Committee (DSAC)” is the University council responsible for coordinating information security and risk management efforts and monitoring and recommending necessary security actions to the University. It is chaired by the director of IT Security and includes delegates as may be appointed from time to time by data trustees and/or the chair.
I. “Data set” is a collection of related University information that supports University missions or activities.
J. “Data steward” is an individual within the University who is the primary institutional authority for a particular data set and who is principally responsible for the management and security of that data set across the institution.
K. “Data stewardship” is the responsible oversight of a data set, including principal responsibility for the establishment of standards and guidelines for appropriately managing and securing that data across the institution.
L. “Data trustee” is an executive officer of the University who has the highest level of strategic and policy-setting authority and responsibility for his or her functional area.
M. “End user” is any individual who accesses and/or utilizes IT resources.
N. “Functional area” is one or more units that have primary responsibility for managing a core University mission or business function.
O. “Integrity” means guarding against improper modification or destruction of University information, and includes ensuring non-repudiation and authenticity.
P. “IT resources” are the full set of University owned or controlled information technology devices and data involved in the processing, storage, accessing, and transmission of information.
Q. “Legitimate interest” means a requirement to access University information commensurate with an end user’s conduct of official University activities.
R. “Quality” means accuracy, completeness, and timeliness; reflects the fitness of data for its intended University purposes.
S. “Shared data repository” is a collection of University information to which multiple individuals or entities have access.
T. “Unit” means a University department, school, institute, program, office, initiative, center, or other operating unit.
U. “Unit head” is a University official with the highest level of authority over the day-to-day management or oversight of a unit’s operation.

V. “University information” is defined as any information within the University’s purview, including information that the University may not own but that is governed by laws and regulations to which the University is held accountable. University information encompasses all data that pertains to or supports the administration and missions, including research, of the University.

III. POLICY STATEMENTS

A. The University, as an organization, owns all University information. The management of University information is subject to the general oversight of the Board of Trustees.
B. The President of the University—and his or her delegates, including the Provost and the Executive Vice President & University Treasurer—exercises the highest degree of authority over the University’s data governance model.
C. Individuals have particular roles and responsibilities for the appropriate management of University information. Roles are not exclusive. An individual fulfills any and all roles for which they meet the stated criteria.
D. This policy requires that University data governance practices, including management and security, comply with applicable laws, regulations, and other requirements. All individuals who have access to University information must manage it in a manner that is consistent with the University’s need for privacy, analysis of strategic initiatives, security, and reporting standards compliance.
E. Functional areas must develop, implement, and maintain clear and consistent procedures for managing University information as appropriate.

IV. POLICY STANDARDS AND PROCEDURES

A. Data governance is a cooperative effort; the success of data governance efforts depends on collaboration between key University stakeholders, who provide critical expertise and perspectives related to specific aspects of data management and security.
    1. Data trustees provide a strategic perspective on data governance. They direct institutional data initiatives and ensure that data is used in support of the University’s missions and strategic goals.
    2. Data stewards provide an operational perspective on data governance. They oversee efforts to ensure and improve the informational quality, effectiveness, usability, strategic value, and security of data. They also understand how their data is managed and used across the institution.
    3. Data custodians provide a technical perspective on data governance. They manage information systems and shared data repositories on behalf of data trustees and

data stewards. They also understand the underlying infrastructure that supports the management and security of data across the institution.

B. The President and/or his or her delegates will establish and oversee the Council for Data Governance (CDG).
    1. The CDG facilitates the identification of the University's functional areas and their data trustees.
    2. The CDG will include
        a. The Chief Information Officer
        b. The VP & General Counsel
        c. Other University executives knowledgeable about the University's missions, strategy, administration, and operations.

C. This policy establishes an institutional data governance model.
    1. The University is organized into functional areas according to common strategic and operational objectives between units.
        a. The functional areas are identified by the CDG.
        b. Each functional area is assigned a data trustee by the CDG.
    2. Each functional area has governance responsibilities for University information.
        a. Ultimate accountability—including strategic oversight and authority—for a data set is entrusted to its data trustee.
            (1) An individual is the data trustee for a particular data set if he or she is primarily accountable for the strategic value and use of that data across the institution.
            (2) Each data trustee is responsible for overseeing University-wide data use in a manner consistent with the University's missions and strategic goals.
        b. Stewardship—including operational oversight and authority—for a data set is the responsibility of its data steward.
            (1) An individual is the data steward for a particular data set if he or she is the primary authority for the management and security of that data across the institution.
            (2) Each data steward is responsible for establishing University-wide standards and guidelines for the management, including acquisition, utilization, maintenance, access, and protection, of the University information within his or her stewardship.
            (3) Data stewards are identified by data trustees based on their operational knowledge of a given data set and their understanding of its management and security needs.
    3. Each functional area encompasses one or more units.
        a. Each unit has an assigned unit head who is responsible for ensuring that his or her unit's management of University information complies with the

policies, standards, and guidelines established by the appropriate data trustees and data stewards.

4. All University employees who use University information in any form or location are end users.
    a. Every end user of University information is responsible for complying with policies and procedures for the management and security of University information to which they have access.
5. Any University entity or employee with operational responsibility to manage a shared data repository is a data custodian.

D. Data trustees and their functional areas are identified in the Data Trustees and Functional Areas Table.

E. This policy creates two operational committees to assist with data governance.
    1. Data Management Advisory Committee (DMAC)
        a. The DMAC facilitates the coordination of data management efforts to assure the informational quality, effectiveness, usability, and strategic value of data across the University.
        b. The DMAC includes:
            (1) The Associate Provost for Institutional Research & Effectiveness (chair)
            (2) Other members as appointed by data trustees and/or the chair
                i. The chair may invite data trustees to appoint delegates to represent their functional areas in the DMAC. Delegates must be knowledgeable about their functional area's missions, strategy, administration, operations, and data management practices.
    2. Data Security Advisory Committee (DSAC)
        a. The DSAC facilitates the coordination of data security efforts across the University.
        b. The DSAC includes:
            (1) The director of IT Security (chair)
            (2) Other members as appointed by data trustees and/or the chair
                i. The chair may invite data trustees to appoint delegates to represent their functional areas in the DSAC. Delegates must be knowledgeable about their functional area's missions, strategy, administration, operations, and data management practices.

F. Data governance roles and responsibilities
    1. The President
        a. Understand the need for a comprehensive data governance model.
        b. Authorize the creation of a University-wide data governance framework.

    c. Establish and appoint members to the CDG.
2. The Council for Data Governance (CDG)
    a. Monitor and manage this policy and the University's data governance framework.
    b. Identify the University's functional areas and their data trustees.
    c. Ensure that data trustees fulfill their data governance responsibilities according to policy.
        (1) Ensure that data trustees remain accountable for, engaged in, and committed to data quality, effectiveness, usability, strategy, and security.
    d. Resolve disputes of responsibility where data overlaps the functional areas of multiple data trustees.
    e. Oversee the formation and operation of the DMAC and DSAC.
3. Data trustees
    a. Appoint a data steward for each data set entrusted to their care.
    b. Oversee data stewardship efforts for University information entrusted to their care.
    c. Are ultimately accountable for their functional area's compliance with policies, laws, regulations, standards, and guidelines for the appropriate management of University information.
    d. Coordinate the use of University information entrusted to their care in a manner commensurate with the University's missions and strategic goals.
    e. Launch and support initiatives to improve the confidentiality, integrity, availability, and effectiveness of University information across the University and its units.
    f. Appoint delegates to participate in the DMAC and DSAC.
4. Data stewards
    a. Oversee the informational quality, effectiveness, usability, strategic value, and security of the University information within their stewardship.
    b. Establish definitions of the data sets within their stewardship.
    c. Develop and promulgate data management standards and guidelines to ensure the confidentiality, integrity, availability, and usefulness of University information within their stewardship.
    d. Ensure that University information within their stewardship is managed according to legitimate interests and operational requirements and in a manner that ensures the privacy and security of that University information.
    e. Develop and publish standards and guidelines for access to University information within their stewardship.

    f. Review and approve uses or proposed uses of University information within their stewardship.
    g. Authorize the creation of shared data repositories containing University information within their stewardship and assign custodianship responsibilities for those shared data repositories.
    h. Authorize the access of individual end users to University information within their stewardship.
    i. Audit at least annually the authorized access to University information within their stewardship.
5. The Data Management Advisory Committee (DMAC)
    a. Assist the CDG and data stewards in the implementation of the data management aspects of this policy.
    b. Assist data stewards in coordinating initiatives to improve the informational quality, effectiveness, usability, and strategic value of University information across the University and its units.
    c. Aid in the development of standards and guidelines concerning the management of data by the University and its units.
    d. Report to the CDG relevant data management initiatives and recommendations as appropriate.
6. The Data Security Advisory Committee (DSAC)
    a. Assist the CDG and data stewards in the implementation of the risk management aspects of this policy.
    b. Assist data stewards in coordinating initiatives to improve the confidentiality, integrity, and availability of University information across the University and its units.
    c. Aid in the development of standards and guidelines concerning the management of information security and risk by the University and its units.
    d. Report to the CDG relevant security initiatives and recommendations as appropriate.
7. Data custodians
    a. Are assigned management responsibility for the shared data repositories they maintain.
    b. In compliance with data stewards' standards and guidelines, grant and manage end user access to the shared data repositories for which they are responsible.
8. Unit heads
    a. Assume primary policy compliance responsibility for their units.
    b. Thoroughly understand the policies, laws, and regulations impacting University information used within their units.

c. Implement procedures to comply with data trustees' and data stewards' policies, standards, and guidelines for the University information to which their units have access.
d. Report to data trustees the unit's compliance with data management requirements at least annually.
e. Request end user access to University information only in compliance with data stewards' standards and guidelines and only for end users who have a legitimate interest in access.
f. Ensure that end users are aware of and understand their responsibilities for University information.

9. End users
    a. Understand and adhere to policies, standards, and guidelines for data management.
    b. Recognize the consequences of improper management of University information.
    c. Acknowledge annually through the Secure UD End User Acknowledgement their responsibility to appropriately manage the IT resources in their care.

G. This policy requires adherence to ethical, legal, and professional standards for data management including, but not limited to:
    1. Manage University information in accordance with institutional need only.
    2. Access and use University information only for legitimate University activities and only according to your authorization to use that information (i.e., no "administrative voyeurism").
    3. Disclose University information only in compliance with federal, state, and local laws, University policies, and data stewardship and management rules.
    4. Do not facilitate the violation of administrative policies or the circumvention of technical or physical safeguards by others.