VANDERBILT UNIVERSITY

Data Governance Framework

Approval Authority:	**Chancellor**	Originally issued: May 11, 2020
Responsible Administrator:	**Assistant Provost & Executive Director, Planning and Institutional Effectiveness (PIE)**	
Responsible Office:	**PIE**	Current version effective as of:
Contact:	**Assistant Provost & Executive Director, PIE**	May 11, 2020

REASON FOR FRAMEWORK

Vanderbilt's data is a high-value asset. It supports delivery of Vanderbilt's central mission of scholarly research, informed and creative teaching, and service to the community and society at large.

This document defines an institution-wide framework of principles and decision-making structures and roles for data governance. This framework will enable Vanderbilt to manage its data intentionally and consistently to deliver maximum value in support of its institutional mission.

Successful implementation of this framework will provide a measurable improvement in data security and data usability. It will also enhance the data awareness and capability of those creating, accessing, and using Vanderbilt data. The demands of information security and mitigating risk will be balanced with the demands of maximizing business value.

This framework is supported by related policies, standards, and guidelines. These may develop and evolve with the needs of the institution.

This framework will be periodically reviewed and updated to ensure it remains current.

FRAMEWORK SCOPE

This framework applies to all persons and entities who access the University's data or computing and network facilities. This group includes students, faculty, staff, researchers, contractors, visitors, and any others accessing the University's data or computing and network facilities. It applies in all locations where the University conducts its activities without geographical limits, subject to applicable local laws and regulations.

This framework applies to all data owned by the University, under the University's custody, or otherwise present in the University's network or computing environment. This data may be held on any of the University's premises or in any external or cloud-based IT infrastructure licensed, rented or contracted by the University or on the University's behalf. This framework also includes data held on personal devices on the University's behalf.

This framework applies to the governance of institutional data belonging to the University. It does not apply to research data. The principles and structure of research data governance will be defined in a separate document, developed with reference to this document. Oversight of research data governance will be led by the Vice Provost for Research.

DEFINITIONS

Data means information held in a structured, logical format, in files or in a database. Data may be held on local devices, on premises in managed IT infrastructure, or in the cloud.

Institutional data is all data maintained to support delivery of Vanderbilt's central mission of scholarly research, informed and creative teaching, and service to the community and society at large, *except research and teaching data.* It includes data to support the auxiliary services that Vanderbilt delivers.

Research data is data generated by research.

POLICY

A. Principles

Data governance is an institution-wide framework of principles and decision-making structures and roles. This framework will enable Vanderbilt to manage its data intentionally and consistently to deliver maximum value in support of the institutional mission.

This framework will uphold moving Vanderbilt toward complying with the following principles:

- Data is a valued asset.
  - Data has value as much as other assets such as buildings, vehicles, or money.
  - Institutional data does not "belong" to individuals or units – rather it is managed by them on behalf of the University.
- Data is managed.
  - Data shall be appropriately managed (i.e., collected, stored, protected and used) throughout its life cycle.
  - Data management shall be a core capability that is an integral part of the University's culture.
  - Named roles with specific responsibilities for the curation of data from data entry to archive or disposal should be defined, trained, and appropriately resourced.
  - The single, master source for each different type of data shall be identified and data systems and integrations structured to rely on that source.
- Data is fit for purpose.
  - Data shall be accurate and complete, at the appropriate quality for its primary purpose and all other known legitimate uses.
  - Data shall be monitored so it can be trusted. Data owners have the role of accountability and oversight to assure this trust, with decisions and actions recorded at an appropriate level of detail.
- Data is accessible, comparable and reusable.
  - Data shall be made available where and when required, subject to appropriate security constraints.
  - Standards will be consistently applied to encourage reuse, and promote a common understanding of context, meaning, and comparability.
  - Data shall be easy to find, quick to understand, and simple to compare.

    - Data shall be consistent and predictable, avoiding harm caused by conflicting versions.
- Data is secure and compliant with regulations.
    - Data shall be protected against unwanted, or unauthorized access. Appropriate confidentiality shall be maintained.
    - Data shall be acquired, used, stored and disposed of in compliance with the law and applicable standards, regulations and contractual obligations.
    - Data integrity protects the university from reputational, financial, and regulatory damage

B. Roles and Responsibilities

Data Governance Structure

The activities of data governance are applying policies, standards, guidelines, and tools to manage the institution's data. Responsibility for the activities of data governance is shared among the roles listed below. Descriptions of roles and responsibilities below provide the framework of how data governance should be implemented and maintained.

Data Governance Oversight

Oversight of data governance (DG) will be at the Vice Chancellor level. Vice Chancellors are accountable for ensuring that DG is practiced in their areas, including identifying Data Owners.

G2 or another designated committee or group at VC-level will provide oversight of the activities of the Data Governance Committee (DGC). This VC-level group will sign off policy, support appropriate cultural and behavioral change, and allocate appropriate resources to DG activities. The DGC will report periodically to this VC-level group on how it is delivering value to support institutional priorities, commensurate with its resourcing.

Data Governance Committee

Vanderbilt University's Data Governance Committee (DGC) is the body responsible for developing and leading the implementation of policy and practices for administrative data governance.

The DGC will develop tools, guidelines, principles, and policies as required on topics such as data classification, data access, data usage, data integrity, data retention, and data integration. The DGC is responsible for prioritizing data governance initiatives and supporting data management for institutional initiatives. The DGC is also responsible for cultivating a data management culture that provides value to the institution.

The DGC is chaired by the Assistant Provost and Executive Director of Planning and Institutional Effectiveness. The work of the committee is coordinated by the Director of Data Governance. The DGC membership will include representation from Information Security, Audit, Risk and Compliance, Office of General Counsel, Office of the Vice Provost for Research, and Data Owners and Stewards. Membership will include at least two members of the faculty. Changes to the DGC membership must be approved by the DGC Chair.

Director of Data Governance

The Director of Data Governance is responsible for the day-to-day operation of the Data Governance Program at Vanderbilt. They will convene the DGC on a regular basis and will work with the committee and the Data Owners and Stewards to resolve data governance related issues. This position reports to the Executive Director of Planning and Institutional Effectiveness.

Additional responsibilities include:

- Communication of Data Governance Committee outcomes.
- Decisions on day-to-day matters of data governance and directing decision making to the appropriate stakeholders when appropriate.
- Serves as a point of expertise on data governance and recommending data governance solutions, working with key stakeholders as appropriate.
- Maintains the Data Governance Committee agenda and convenes meetings.
- Identifies and includes key decision makers in matters as appropriate.
- Develops and maintains a central repository for data governance policies, guiding principles, and decisions.
- Oversees the maintenance of records and documentation about data governance, including the data inventory, working with VUIT, OGC, Internal Audit, and other groups as required.

Data Owners

Data Owners are appointed by the Vice Chancellors to be accountable for the implementation of data governance policy in their data domains. (A data domain is a coherent set of related data.) A Data Owner for institutional data will normally be a senior leader or administrator. Data Owners assign Data Stewards to administer and implement applicable data governance policies for the data domains in which they are accountable.

In addition, Data Owners also:

- Foster a culture that is aware of the data governance principles
- Sponsor, secure, and/or influence resources for managing data
- Set expectations for managing data in their Data Domain, such as Data Classification and Data Retention.
- Making decisions about their data domain where standard guidelines are ambiguous or do not apply.

Data Stewards

Data Stewards are appointed by Data Owners. There may be multiple Data Stewards within a data domain. They have day-to-day responsibility for implementing data governance in their data system or operational area. Data Stewards are often subject matter experts in a system or process and can make decisions on to be apply data governance policy and principles in different situations.

Key responsibilities of Data Stewards include:

- Developing standard operating procedures to comply with data governance policy and principles.
- Communicate and train personnel on data governance policies and procedures and the implications for their activities.
- Identify data integrity and data quality issues and develop plans to address.
- Review data access and usage agreements to ensure appropriate access is maintained.

RELATED POLICIES/DOCUMENTS

Vanderbilt Policies

- Electronic Communications and Information Technology Resources
  - Policy #HR-025 (http://hr.vanderbilt.edu/policies/HR-025.php)
- Vanderbilt Computing Privileges and Responsibilities – Acceptable Use Policy
  - http://www.vanderbilt.edu/info/computing-aup/
- Vanderbilt Data Classification Policy (in draft)

HISTORY

Issued: **05/11/2020**

Reviewed: **Approved by Interim Chancellor and Provost Susan R. Wente, 05/11/2020**
Comment

Amended:
Comment

***Disclaimer**: Vanderbilt reserves the right to modify its policies and practices, in whole or in part, at any time. Revisions to existing policies and procedures, and the development of new policies and procedures, will be made from time to time at the discretion of the University. When new policies are implemented or existing policies are revised, the University will notify members of the University community as soon as practicable. However, where differences occur, the most recent policy as reviewed and approved by the University will take precedence.*

Procedures Website

FAQ Website