

VU Data Governance Policy

STATEMENT OF PURPOSE

University data are institutional assets maintained to support VU's central mission of teaching and service. "University data" refers to collections of data elements relevant to the operations, planning, or management of any unit at VU or data that are reported or used in official administrative University reports.

To support effective and innovative management, University data must be accessible, must correctly represent the information intended, and must be easily integrated across VU's information systems. The purpose of data governance is to develop University-wide policies and procedures that ensure that University data meet these criteria within and across VU's administrative data systems, particularly the student, financial, and human resource systems.

Data governance at VU was established at the direction of the President in Spring of 2023. The purpose of the current Data Governance Policy is to achieve the following:

- Establish appropriate responsibility for the management of University data as an institutional asset.
- Improve ease of access and ensure that once data are located, users have enough information about the data to interpret them correctly and consistently.
- Improve the security of the data, including confidentiality and protection from loss.
- Improve the integrity of the data, resulting in greater accuracy, timeliness, and quality of information for decision-making.

The Data Governance Policy addresses data governance structure and includes policies on data access, data usage, data integrity, and integration.

ENTITIES AFFECTED BY THIS POLICY

Anyone at VU who creates, manages, or relies on data for decision making and planning.

WHO SHOULD READ THIS POLICY

Data governance executive sponsors, data stewards, and all other VU employees who use data, regardless of the form of storage or presentation.

POLICY

Table of Contents

1. Data Governance Structure
2. Data Access Policy
3. Data Usage Policy
4. Data Integrity and Integration Policy

A. Data Governance Structure

Data Governance is the practice of making strategic and effective decisions regarding VU's information assets. It assumes a philosophy of freedom of access to University data by all members of the community coupled with the responsibility to adhere to all policies and legal constraints that govern that use.

In the interest of attaining effective data governance, the University applies formal guidelines to manage the University's information assets and assigns staff to implement them. While the University data Governance

Committee is assigned a leadership role and oversight for the activities of data governance, this function is shared among the executive sponsors, data stewards, data administrators, and data users.

Executive sponsors will appoint data stewards, and through the establishment of data policies and institutional priorities, provide direction to them and data administrators. The University's data stewards comprise the Data Governance Committee, a body that meets regularly to address a variety of data issues and concerns.

Overview of Roles for Governing University data

The following are general descriptions of the primary roles and responsibilities within Data Governance.

Executive Sponsors

Executive sponsors are senior University officials who have planning and policy responsibility and accountability for major administrative data systems (e.g., student, human resources, and financial) within their functional areas. By understanding the planning needs of the institution, they are able to anticipate how data will be used to meet institutional needs. Executive sponsors may include the following administrative personnel currently in place at VU: President, Provost, VP Finance, VP for Government and Legal Affairs, Chief Information Officer, Director of Admissions, Director of Foundation, VP Workforce Development, Director External Relations, Director of Athletics and Sr. Director Institutional Effectiveness and Research.

Chair of Data Governance Committee

The Chair of the Data Governance Committee works with the campus community to define a campus wide structure of data stewardship by making explicit the roles and responsibilities associated with data governance and compliance monitoring. This individual is responsible for coordinating data policies and procedures in the three primary enterprise data systems - student, finance, and human resources - ensuring representation of the interests of data stewards, managers, and key users. The Chair of the Data Governance Committee coordinates the meetings and agendas for the Data Governance Committee and provides support to related data management efforts. This individual is also responsible for developing a university culture that supports data governance in areas with critical peripheral databases that exist beyond the major administrative systems.

The Chair of the Data Governance Committee works to ensure that all University data are represented accurately and managed appropriately that serve as source data for all data sources and models. When questions regarding data quality or use arise, they work to address the concerns. They do so by being informed by the Data Governance Committee, led by the Chair of the Data Governance Committee (Sr. Director of Institutional Effectiveness and Research). This body is responsible for monitoring of VU data sources and reporting with corresponding data structures and domains. They recommend policy and process changes to the President and Executive Committee to improve data quality and data operations within the VU system.

Data Stewards

Data stewards are appointed by executive sponsors to implement established data policies and general administrative data security policies. Data stewards, who comprise the Data Governance Council, are responsible for safeguarding data from unauthorized access and abuse through established procedures and educational programs. They authorize the use of data within their functional areas and monitor this use to verify appropriate data access. They support access by providing appropriate documentation and training to support University data users. Included among data stewards are the following administrative personnel currently in place at VU: Registrar, AVP of Finance Controller, Director of Institutional Research, Director of Assessment, Budget Director, Director of Admissions, Director of Student Financial Services, Director of Human Resources, and Assistant Provost for Student Affairs.

Data Administrators

Data administrators are University employees who most often report to data stewards and whose duties provide them with an intricate understanding of the data in their area. They work with the data stewards to establish procedures for the responsible management of data, including data entry and reporting. Some data administrators may work in a technology unit outside of the functional unit, but have responsibilities for implementing the decisions of the stewards. Technical data administrators may be responsible for implementing backup and retention plans, or ensuring proper performance of database software and hardware.

B. Data Access Policy

INTRODUCTION

Vincennes University (VU) shall manage access to Private and Sensitive Institutional Data in order to ensure that such access is authorized and based on the principles of least privilege and need to know, that its use is appropriate, and that authorized access complies with VU policies, standards and rules and relevant state and federal laws.

SCOPE

This policy outlines requirements for granting and revoking access to Confidential, Private and Sensitive Institutional Data. This policy applies to access to Confidential and Private Data maintained by the University or party(ies) acting on the behalf of the University.

Data that is classified as Public Directory can be accessed by and distributed to any entity by approved university parties.

Requests for records by the public are outside of the scope of this policy and shall be handled by approved university parties and facilitated by VU's Office of Government and Legal Affairs. This policy also does not apply to situations in which the University is legally compelled to provide access to information. Such requests shall be the responsibility of VU's Office of Government and Legal Affairs according to governmental policy.

POLICY STATEMENT

Data Stewards Approve Access to Confidential and Private Institutional Data

Access to Confidential and Private Institutional Data is approved by VU's designated Data Stewards, whose roles and responsibilities are defined by Section A of the Data Governance Administration and Access Policy.

- Data Stewards shall grant access in compliance with the VU Data Governance Administration and Access Policy and all relevant regulations (e.g. [FERPA](#), [HIPAA](#) and [GLBA](#)).
- Data Stewards shall grant access only to those employees, affiliates, and systems that need the access to perform their job duties or mission and have a legitimate need to know.
- In the event that a Data Steward is not designated, the data in question is owned by the dean, vice president, or head of the unit that creates/owns the data.

The President and Vice Presidents Retain the Right to Approve All Access to SSN Data

Per the VU Data Classification Guidelines, Social Security Numbers (SSNs) are classified as Confidential Data. Therefore, access to SSN data shall not be granted unless approval has been provided by a University President and/or Vice President or a Vice President's designee.

VU Primary Care Center and University Counseling Center Retain the Right to Approve All Access to HIPAA/PHI Data for their records respectively.

Appropriate access is provided/controlled according to established policies and procedures within VU HIPAA covered entities. Access shall be granted based on the need-to-know and the minimum necessary standards.

Data Stewards are Responsible for Procedures for Requesting, Approving, and Revoking Access

Data Stewards shall ensure that procedures for access to Confidential and Private Institutional Data are documented and implemented. Procedures may vary per Data Steward or Data Users group. However, all procedures shall include sufficient tracking for requests, approvals, and revocations, and such tracking must be auditable.

Only Authorized Users Shall Access Confidential and Private Institutional Data

All access by individuals to Confidential and Private Institutional Data shall be supervised, stored and controlled by reasonable measures to prevent access to and/or distribution of said data to unauthorized users.

Data Users Shall Use Confidential and Private Institutional Data Responsibly

Data Users must maintain the confidentiality and integrity of data in accordance with all applicable laws, the VU [Data/Information Confidentiality-Security-Retention Statement](#), and the Data Classification Guidelines.

Data Stewards May Delegate Approval Responsibilities to a Trusted Designee

A Data Steward may delegate the ability to approve access to Confidential and Private Institutional Data to individuals in designated roles. Approved documented procedures must exist that allow a trusted designee to grant access for employees that have certain pre-approved roles and responsibilities based on their job requirements and need to know. Data Stewards retain the responsibility for ensuring that all access to Confidential and Private Institutional Data is authorized, appropriate, and complies with relevant legal requirements and University policies, standards, and rules. The responsibility for owning and protecting the data does not transfer to designees.

External Third-Party Access to Confidential and Private Institutional Data Shall be Governed by Contractual Agreement

Individual contractual agreement or memoranda of understanding (MOU), if the third party is a governmental organization, shall govern access to Confidential and Private Institutional Data by external parties. Such contractual agreements shall be approved through the President (or Designee), CIO (or Designee), and Office of Government and Legal Affairs.

EXCEPTION

Exceptions may be granted in cases where security risks are mitigated by alternative methods, or in cases where security risks are at a low, acceptable level and compliance with minimum security requirements would interfere with legitimate academic or business needs. Security exceptions must be documented and approved by the President (or Designee) and/or Chief Information Officer.

NON-COMPLIANCE

Confirmed violations of this policy will result in consequences commensurate with the offense, up to and including termination of employment, appointment, student status, or other relationships with VU.

MAINTENANCE (Move to the end of the document)

This policy will be reviewed by VU's Data Governance Committee annually, or as deemed appropriate.

IMPLEMENTATION

The Data Governance Committee and Chief Information Officer are responsible for the oversight and implementation of this policy, including the overall procedures related to its implementation and management.