OLD DOMINION UNIVERSITY

Policy #

DATA GOVERNANCE POLICY

Responsible Oversight Executive: Executive Vice President for Enrollment, Transformation, & Technology

Date of Current Revision or Creation: XXXXXX

A. PURPOSE

The purpose of this Policy is to establish the University's enterprise Data Governance Program, including the governance framework, principles, roles, responsibilities, and decision-making processes necessary to manage Institutional Data as a strategic University asset. The Policy promotes consistent stewardship, protection, quality, accessibility, and appropriate use of Institutional Data in support of the University's academic, research, administrative, and operational missions while supporting compliance with applicable legal, regulatory, and contractual requirements.

B. AUTHORITY

Code of Virginia Section 23.1-1301, as amended, grants authority to the Board of Visitors to make rules and policies concerning the institution. Section 6.01(a)(6) of the Board of Visitors Bylaws grants authority to the President to implement the policies and procedures of the Board relating to University operations.

Restructured Higher Education Financial and Administrative Operations Act, Code of Virginia Section 23.1-1000 et seq., as amended

C. DEFINITIONS

Affiliated Entities - Affiliated Entities (each, an Affiliated Entity) are legally separate organizations that maintain a formal relationship with the University through an operating, governance, contractual, or similar agreement and exist, in whole or in part, to support or advance the University's mission. These entities include, but are not limited to, foundations, alumni associations, research organizations, or other related entities that operate under legally separate and distinct governance, legal ownership, and fiduciary responsibilities.

Affiliated Individuals - Affiliated Individuals are individuals formally associated with the University who have access to Institutional Data and are authorized to perform work or activities in support of University operations, including contractors, consultants, volunteers, visiting scholars, and individuals engaged through contractual or other formal agreements.

Data Domain/Data Subdomain - The grouping of data, or subset of such data that is organized around, and assigned to, a major business or functional area of the University, such as Finance, Academic Affairs, Athletics, Talent Management and Culture, Research, Administration, Health Sciences, and other major functional areas.

Institutional Data – Institutional Data refers to information, in any form, that is owned by the University and that is collected, created, maintained, processed, recorded, or transmitted, by the University, its staff and agents working on its behalf, in support of its academic, administrative, operational, or regulatory functions.

University Information Systems - University Information Systems refers to the collection of hardware, software, networks, applications, and processes that manage, control, store, and disseminate data across the University's functional areas. These systems are owned, operated, or managed by the University or by third-party service providers, and they support the University's academic, research, and administrative missions by enabling secure, organized, and appropriate access to Institutional Data.

D. SCOPE

This policy applies to all employees (faculty, staff, and residents), students, visiting faculty, researchers, and Affiliated Individuals who create, access, manage, share, or otherwise interact with Institutional Data as part of University operations or employee responsibilities. It applies regardless of the format, medium, or location in which Institutional Data is created, maintained, processed, stored, transmitted, or otherwise managed.

This policy applies to Affiliated Entities as set forth in Section K.

E. POLICY STATEMENT

Institutional Data is a strategic University asset that shall be governed through shared accountability, clearly defined roles, and coordinated stewardship across the University. It is the policy of the University that the protection, integrity, accessibility, and appropriate use of Institutional Data are shared responsibilities of the University community and shall be governed through the Data Governance Program established by this Policy.

This Policy establishes the University's enterprise governance framework for Institutional Data and serves as the foundation for University policies, standards, procedures, and guidance relating to data governance, including data administration, classification, access, sharing, quality, privacy, security, and related governance activities. Where a conflict exists among University data governance documents, this Policy shall prevail unless superseded by applicable law or a more specific University policy expressly approved under this framework.

F. DATA GOVERNANCE PROGRAM

This Policy establishes the University's Data Governance Program as the enterprise-wide framework for the governance of Institutional Data. The Program establishes the principles, governance structure, roles, responsibilities, and decision-making processes necessary to manage Institutional Data as a strategic University asset for the development and implementation of related data governance policies, standards, procedures, and guidance. While this Policy establishes governance and accountability for Institutional Data, it does not replace existing responsibilities for the design, operation, or management of University

Information Systems or the operational, technical, and procedural requirements established through applicable University policies, standards, and procedures.

The Data Governance Program promotes consistent stewardship, quality, accessibility, protection, sharing, retention, and appropriate use of Institutional Data while supporting compliance with applicable laws, regulations, contractual obligations, and University policies. The Program establishes governance requirements for data classification, administration, privacy, security, records management, analytics, artificial intelligence, and other activities involving Institutional Data. It is implemented through the DGC and the University's governance structure, including designated Data Governance Committees, Data Trustees, Data Stewards, Data Custodians, and Data Users, each with defined data governance responsibilities.

G. GUIDING PRINCIPLES

The Data Governance Program is guided by the following principles:

1. Accountability: Accuracy, integrity, and appropriate use of Institutional Data are supported through clearly defined stewardship and shared responsibility across the University.
2. Transparency: Clarity, shared understanding, and data literacy are supported through documented and accessible data definitions and governance standards across the University.
3. Consistency: Consistent interpretation and use of Institutional Data are supported through shared definitions, governance standards, and coordinated data governance practices across units, systems, and reporting environments, while recognizing varying operational contexts across the University.
4. Security and Privacy: Confidentiality, integrity, and availability of Institutional Data are protected through management practices that align with applicable laws, regulations, and University policies.
5. Appropriate Access: Access to Institutional Data shall be granted in accordance with the University's Access Determination and Control Standard. Institutional Data shall be shared only for authorized University purposes and in accordance with applicable laws, regulations, contractual obligations, and University policies and standards.

H. DATA GOVERNANCE COUNCIL

The Data Governance Council (DGC) oversees implementation of the University's Data Governance Program and serves as the University's enterprise governance body for Institutional Data. The DGC approves data-related policies, standards, and procedures, and provides oversight to ensure that data management practices are consistent, compliant, and aligned with institutional objectives. The DGC operates in coordination with designated Data Trustees, who are accountable for the governance, appropriate use, and protection of data within their respective Data Domain/Data Subdomains.

1. Composition. The core members and their roles are as follows:
    i. Chief Data & Analytics Officer (CDAO) - The CDAO is the Chair of the DGC and serves as the liaison between the DGC and Data Trustees/Data Stewards. The CDAO provides executive leadership and strategic oversight

for the Data Governance Program to include data governance, data management, and analytics programs.

ii. Chief Information Officer (CIO) - The CIO advises the Data Governance Council on enterprise information technology strategy, data architecture, system integration, and technology capabilities that support the governance, management, and use of Institutional Data. The CIO provides guidance on the technical feasibility and implementation of enterprise data governance initiatives.

iii. Chief Information Security Officer (CISO) – The CISO advises the Data Governance Council on information security, cybersecurity risk, technical safeguards, and regulatory security requirements affecting Institutional Data. The CISO provides recommendations to help ensure that data governance policies, standards, and initiatives appropriately protect the confidentiality, integrity, and availability of Institutional Data.

iv. One or more Data Stewards from the major Institutional Data domains to provide operational expertise regarding the management, quality, definition, and use of Institutional Data.

v. Liaisons from Data Governance Committees.

The DGC may invite ad hoc members to participate in its meetings and activities as necessary to provide subject matter expertise or support for specific issues. Ad hoc members may include, but are not limited to:

i. University Counsel to provide legal and regulatory interpretation, contract review litigation guidance.

ii. University Privacy Officer to provide advice on guidance when privacy, HIPAA, FERPA, GDPR or other data protection issues are implicated.

iii. Risk Management to provide advice on enterprise data risks and coordinate response on significant data incidents.

iv. Procurement to provide guidance on considerations related to the acquisition of information technology, vendor due diligence, contractual data governance requirements and issues, and the integration of enterprise data governance requirements into procurement and contracting processes.

2. Meetings. The DGC shall meet as needed to provide enterprise oversight of the University's Data Governance Program. Special meetings may be called by the Chair as necessary to address time-sensitive matters or emerging risks. The Chair may also establish standing or ad hoc subcommittees, task forces, or working groups as necessary to study specific issues, develop recommendations, draft policies or standards, conduct assessments, or carry out other activities within the scope of the Data Governance Program. The Council shall define the purpose, scope, membership, and expected deliverables of each subcommittee or working group. Unless expressly delegated by the Council, subcommittees and working groups serve in an advisory capacity and shall report their findings and recommendations to the DGC for review and appropriate action.

3. Authority and Responsibilities. The DGC has the following authority and responsibilities:

i. Provide strategic oversight of the University's Data Governance Program

ii. Approve enterprise-wide data governance policies, standards, guidance, and related requirements, and direct their development or revision through applicable University processes.

iii. Promote compliance with applicable legal, regulatory, contractual, privacy, security, records management, and data protection requirements governing Institutional Data.

iv. Establish Data Governance Committees and approve their charters, charges, and any material amendments to ensure alignment with the Data Governance Program.

v. Establish enterprise standards for common data definitions, metadata, data quality, classification, access, sharing, quality, reference data, analytics, artificial intelligence, and other practices necessary for the consistent management and use of Institutional Data.

vi. Review and provide recommendations regarding significant enterprise initiatives involving Institutional Data, including data integration, sharing, analytics, and artificial intelligence.

vii. Resolve cross-domain data governance issues that cannot be resolved at the Data Steward or Data Governance Committee level and elevate significant matters to the President or other executive leadership, as appropriate.

viii. Require corrective action plans for significant deficiencies and request information, reports, or other documentation necessary to carry out its responsibilities.

ix. Promote collaboration, data literacy, data stewardship, data quality, and continuous improvement in data management across the University.

I. DATA GOVERNANCE SUBCOMMITTEES

1. The DGC may authorize the establishment of Data Governance Subcommittees to provide governance, oversight, and decision-making authority for Institutional Data within specific functional areas, administrative units, or Data Domains/Data Subdomains where specialized expertise or operational needs warrant a dedicated governance structure.
2. Each Data Governance Subcommittee shall operate under an applicable University policy, written charter, or charge approved by the DGC, that defines its purpose, scope, membership, authority, responsibilities, and reporting relationships. Subcommittee charters, and any material amendments thereto, shall be reviewed and approved by the DGC to ensure consistency with the University's enterprise data governance framework, related policies, and governance objectives.
3. Data Governance Subcommittees shall have the following responsibilities within their assigned functional areas or Data Domains/Data Subdomains:
    i. Implementing the University's Data Governance Program
    ii. Establishing and maintaining data definitions, business rules, standards, and governance practices for data
    iii. Making decisions regarding data quality, stewardship, access, use, sharing, and lifecycle management

iv. Resolving data governance issues that do not require enterprise-level review

v. Recommending policies, standards, and governance improvements to the DGC

4. Each Data Governance Subcommittee shall appoint a member to serve as liaison to the DGC and shall report significant governance decisions, recommendations, and enterprise-wide issues to the DGC for oversight and coordination and shall seek DGC input when questions regarding interpretation of this Policy arise.

J. DATA GOVERNANCE ROLES

1. Data Trustees. Data Trustees are senior-level leaders appointed by the President, who are responsible for establishing governance expectations and providing oversight for data within their oversight areas. Data Trustees are responsible for the governance and stewardship of data within their Data Domains/Data Subdomains and ensure that data is managed, shared, and utilized in accordance with University policies, standards, and applicable laws and regulations. Data Trustees determine the acceptable level of business risk for data within their assigned domains and, where authorized, approve policy exceptions or risk acceptance decisions consistent with University policy and established exception management processes. Data Trustees may delegate operational responsibilities to Data Stewards and technical responsibilities to Data Custodians but remain accountable for data governance decisions.

2. Data Stewards. Data Stewards are identified and appointed by Data Trustees and are responsible for the operational management of data within their Data Domains/Data Subdomains. They establish and implement standards, procedures, and access controls within their assigned domains, approve access to data under their stewardship, and ensure that data are defined, maintained, and used consistently across the institution. Data Stewards may delegate operational responsibilities to appropriate personnel but remain accountable to the Data Trustee for the effective management and quality of data within their assigned domains.

3. Data Custodians. Data Custodians are identified and appointed by Data Stewards and are responsible for the technical implementation, administration, and management of information systems that store, process, transmit, or maintain data. Data Custodians are responsible for implementing and maintaining the technical controls necessary to protect and manage data within their assigned systems. Data Custodians also play a critical role in ensuring compliance with institutional policies and regulatory requirements. Data Custodians may delegate technical responsibilities to appropriate personnel but remain accountable for the effective technical management and protection of data within their assigned systems.

4. Data Users. Data Users are members of the University community and Affiliated Individuals who are authorized to create, collect, enter, modify, access, view, share, or otherwise use Institutional Data in the performance of authorized University activities. Data Users are responsible for using Institutional Data accurately, appropriately, and only as necessary to perform their authorized responsibilities. Data Users are responsible for safeguarding their credentials, completing required training, promptly reporting suspected unauthorized access, misuse, or security incidents, and exercising reasonable care to ensure the accuracy and appropriate use of Institutional Data.

K. AFFILIATED ENTITIES

1. To the extent data owned or controlled by an Affiliated Entity is hosted, stored, processed, transmitted, managed, or otherwise maintained within University Information Systems pursuant to a contractual or other authorized arrangement with the University, the Affiliated Entity shall comply with the University's Data Governance Program.
    i. Recognizing the unique legal, operational, and regulatory requirements that may apply to certain Affiliated Entities, the DGC may approve exceptions to specific data governance requirements on a case-by-case basis upon a documented determination that the exception is justified, does not materially increase risk to the University, and remains consistent with applicable laws, regulations, contractual obligations, and the objectives of the University's Data Governance Program. Approved exceptions shall be documented and may be subject to conditions, limitations, periodic review, or revocation by the DGC.
    ii. Affiliated Entities may adopt governance requirements that are more restrictive than those established by the University, provided such requirements do not conflict with the Affiliated Entity's contractual obligations to the University or the University's governance of Institutional Data.
2. Nothing in this Policy shall be construed to transfer ownership, custody, control, or legal responsibility for data owned or controlled by an Affiliated Entity to the University. Data owned or controlled by Affiliated Entities shall at all times remain the exclusive property of the applicable Affiliated Entity. The University's participation in the management, storage, processing, transmission, or protection of data owned or controlled by an Affiliated Entity, including through University Information Systems or information technology services, shall not alter the legal status of such data, create University ownership or custodial rights, or otherwise affect the independent legal status of the Affiliated Entity or its records.
3. Affiliated Entities shall be solely responsible for the governance of data owned or controlled by an Affiliated Entity that is in information systems owned, operated, or managed by Affiliated Entities outside of University Information Systems.

L. COMPLIANCE

Violations of this Policy or related data governance standards and procedures may result in corrective action, including required remediation, restriction or revocation of access to Institutional Data or University Information Systems, referral to the appropriate administrative or compliance authority, and disciplinary action in accordance with applicable University policies, employment policies, student conduct standards, contractual obligations, and legal requirements.

M. RECORDS RETENTION

All records created or maintained in administering this Policy shall be maintained in accordance with the Commonwealth Records Retention Schedules.

N. RESPONSIBLE OFFICER

Associate Vice President For Data and Analytics

O. RELATED INFORMATION

Research and Scholarly Digital Data Management Policy - University Policy 5350 | Old Dominion University

Data Administration Policy - University Policy 3504 | Old Dominion University

Access determination and control standard - https://www.odu.edu/computing-standards/access-determination

IT Security Roles and Responsibilities - https://www.odu.edu/computing-standards/it-security-roles

Roles and Responsibility Awareness Sheet - https://www.odu.edu/information-security/system-assessment/roles-awareness

Information Technology Access Control- https://www.odu.edu/about/policiesandprocedures/university/3000/3501

Data Administration & Classification Standard Information Technology Standard 02.3.0 | Old Dominion University

POLICY HISTORY

****

Policy Formulation Committee (PFC) & Responsible Officer Approval to Proceed:

_____ _____

Responsible Officer Date

Policy Review Committee (PRC) Approval to Proceed:

_____ _____

Chair, Policy Review Committee (PRC) Date

Executive Policy Review Committee (EPRC) Approval to Proceed:

_____ _____

Responsible Oversight Executive Date

University Counsel Approval to Proceed:

_____ _____

University Counsel Date

Presidential Approval:

_____ _____

President Date

Policy Revision Dates:

Scheduled Review Date: