# OLD DOMINION UNIVERSITY
## University Policy

**Policy #3504**
**DATA ADMINISTRATION POLICY**

**Responsible Oversight Executive:** Vice President for Administration and Finance
**Date of Current Revision or Creation:** February 14, 2022

### A. PURPOSE

The purpose of this policy is to establish the framework for administering the University's institutional data.

### 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 7.01(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

Application Administrators - Individuals with administrative application or system privileges, who are responsible to ensure that appropriate controls, mechanisms, and processes are in place to meet the security requirements necessary to protect an information technology resource.

Data Classification - In the context of information security, it is the classification of data based on its level of sensitivity and the impact to the University should that data be disclosed, altered, or destroyed without authorization.

Data Element - In electronic recordkeeping, a combination of characters or bytes referring to one separate item of information such as name, address, or age.

Data Compliance Owners – Data Compliance Owners understand the compliance requirements for the data under their purview, designate the compliance level of their data, and approve the access to and use of the data.

- University Data Compliance Owners oversee compliance for data that is shared or leveraged across the University, such as HR, Finance, Financial Aid, and Student FERPA data.
- Departmental Data Compliance Owners oversee the data that is specific to the departmental application or system that is not overseen by one or more of the University Data compliance Owners.

Data Users – Those authorized to access institutional data and information in order to perform their assigned duties or to fulfill their role in the University community.

Information Security Officer (ISO) – The Old Dominion University employee, appointed by the President or designee, who is responsible for developing and managing Old Dominion University's information security program.

Institutional Data **-** Recorded information that documents a transaction or activity by or with any appointed board member, officer, or employee of the University. Regardless of physical form or characteristic, the recorded information is an institutional record if it is produced, collected, received, or retained in pursuance of law or in connection with the transaction of University business. The medium upon which such information is recorded has no bearing on the determination of whether the recording is an institutional record. Institutional records include but are not limited to personnel records, student records, academic records, financial records, patient records and administrative records. Record formats/media include but are not limited to email, electronic databases, electronic files, paper, audio, video, and images.

Personally Identifiable Information **-** Personally identifiable information (PII) is defined as data or other information that is tied to or which otherwise identifies an individual or provides information about an individual in a way that is reasonably likely to enable identification of a specific person and make personal information about them known. For the purposes of classification at ODU, certain PII can be considered public, such as that designated as directory information under FERPA, or confidential or restrictive based on ability to use the information for harmful purposes such as identity theft.

Research and Scholarly Data ("Research Data") **-** Digitally recorded information (necessary to support or validate a research project's observations, findings, or outputs. Specifically, data that are:

1. Acquired and/or maintained by University employees and/or students in performance of research and/or in pursuit of a scholarly activity;
2. Created or updated in pursuit of a research or scholarly function;
3. Necessary to support research or scholarly findings, establish validity of inventions, and prove ownership of Intellectual Property Rights.

System Compliance Owners – The manager or departmental head responsible for operation and maintenance of a University IT system or overseeing hosted systems under their purview. System Compliance Owners are responsible for the overall compliance and security of their system.

## D. SCOPE

This policy applies to all users of Old Dominion University information technology resources and governs all information technology resources either owned by or operated for University business through contractual arrangements. Users may include employees, students, volunteers, and visitors to the institution. Employees include all staff, administrators, faculty, full- or part-time, and classified or non-classified persons who are paid by the University. Students include all persons admitted to the University who have not completed a program of study for which they were enrolled; student status continues whether or not the University's programs are in session. Visitors include vendors and their employees, parents of students, volunteers, guests, uninvited guests, and all other persons located on property owned, leased, or otherwise controlled by the University or using information technology that is provided by the University.

This policy refers to all data owned, used, created, or maintained by the University whether individually controlled or shared, stand-alone or networked. It applies to all data sources found on equipment owned, leased, operated, or contracted.

## E. POLICY STATEMENT

### Data Administration and Classification

It is the policy of Old Dominion University that the framework for the administration of institutional data is built upon the accepted standards of practice, the understanding of institutional data, and the roles and responsibilities involved in the management of the data.

The security of institutional data and the infrastructure upon which it is processed, transmitted, or stored is patterned after accepted standards for management of information security, such as ISO/IEC 27001/2, Information Technology – Security Techniques - Code of Practice for information security controls, industry best practices and practices of comparable higher education institutions.

Data classifications and associated protective controls account for academic and business needs for sharing or restricting information and the impact associated with such needs. Data classification informs security decisions such as location of stored data, authorization and access requirements, continuity of operations and disaster recovery planning, and are maintained in risk assessment documents. Data classification levels along with certain transmission and storage expectations are found in Information Technology Standard 02.30 – Data Administration and Classification.

### Research and Scholarly Data

Research and scholarly data are generally not considered institutional data and are governed by the Research and Scholarly Data Governance Committee (RSDGC). The RSDGC is a University-level committee charged with oversight of the policy and guidelines for the management of and access to the University's Research Data in accordance with University policies and applicable law.

**Roles and Responsibilities**

The specific responsibilities of Data Compliance Owners, Data Users, Application Administrators, oversight committees, and other security roles are identified within Information Technology Standard 01.2.0 – IT Security Roles and Responsibilities.

Violations of this policy should be reported to the University's Information Security Officer. Any faculty, staff or student found to have violated this policy may be subject to the appropriate disciplinary action.

## F. PROCEDURES

1. Data elements are reviewed and identified by the data compliance owner. Using the data classification levels outlined in Information Technology Standard 02.30 – Data Administration and Classification data compliance owners make classification determinations.

2. System compliance owners in collaboration with the data compliance owner will conduct a System Risk Assessment in accordance with Information Technology Standard 08.1.0 - Risk Assessment Standard for all new and hosted systems that maintain sensitive data. The completed System Risk Assessment will be forwarded to the Information Security Officer.

## G. RECORDS RETENTION

Applicable records must be retained and then destroyed in accordance with the Commonwealth's Records Retention Schedules.

## H. RESPONSIBLE OFFICER

Information Security Officer

## I. RELATED INFORMATION

Board of Visitors Policy 1424, Policy on Intellectual Property
University Policy 3500 - Use of Computing Resources
University Policy 3501 – Information Technology Access Control Policy
University Policy 3505 - Information Technology Security Policy
University Policy 4100 – Student Record Policy
University Policy 5350 – Research and Scholarly Digital Data Management Policy
Information Technology Standard 02.4.0 - IT Asset Control
Information Technology Standard 05.1.0 - IT Security Incident Handling
Information Technology Standard 05.2.0 - Data Breach Notification
Information Technology Standard 05.3.0 - Threat Detection
Information Technology Standard 06.6.0 - Security Monitoring and Logging
Office of Research Volunteer or Visiting Scholar Agreement

**POLICY HISTORY**

**********

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

/s/ J. Douglas Streit — January 4, 2022
Responsible Officer — Date

**Policy Review Committee (PRC) Approval to Proceed:**

/s/ Donna W. Meeks — December 14, 2021
Chair, Policy Review Committee (PRC) — Date

**Executive Policy Review Committee (EPRC) Approval to Proceed:**

/s/ Todd K. Johnson — February 8, 2022
Responsible Oversight Executive — Date

**University Counsel Approval to Proceed:**

/s/ Allen T. Wilson — February 10, 2022
University Counsel — Date

**Presidential Approval:**

/s/ Brian O. Hemphill, Ph.D. — February 14, 2022
President — Date

**Policy Revision Dates:** October 1, 2007; April 16, 2011; December 14, 2015; February 14, 2022

**Scheduled Review Date:** February 14, 2027