UNIVERSITY OF RICHMOND

Policy Manual

Policy #:	IRM-4007	**Policy Title:**	Administrative Data Management Policy
Effective:	08/01/2020	**Responsible Office:**	Information Services
Date Approved:	07/27/2020	**Approval:**	Vice President for Information Services and Chief Information Officer
Replaces Policy Dated:	N/A	**Responsible University Official:**	Vice President for Information Services and Chief Information Officer

PURPOSE:

The purpose of this policy is to:

1. Facilitate assignment of appropriate access to and responsibility for University data used for official educational, administrative, and financial data input, reporting, and dissemination.
2. Establish a standard and structure for data stewardship and ownership.

SCOPE:

This policy applies to the University and all of its Affiliates. As used in this policy, the term "Affiliates" means organizations or entities in which the University owns a controlling interest or has the right to elect the majority of the entity's governing board.

INDEX:

POLICY STATEMENT:

IRM-4007.1 – Definitions

Administrative Data: Data that is gathered, produced, stored, and/or disseminated concerning any aspect of the University's operations. Such data includes, but is not limited to, general ledger/accounting, human capital management, student, alumni/development, space management, student housing data, and also includes any

data derived from the use of such data. Administrative data specifically does not include faculty-generated classroom data nor faculty- or student-generated research data.

Data Classification: Details and examples of University data classification levels are contained in the University's Data Security Policy. University data is classified as: confidential, restricted, official use only, or public.

Data Stewardship Domain: A University administrative or operational area, function or process and the authoritative data elements created, collected, and managed by that area throughout the lifecycle of that data, regardless of the Transactional System(s) in which they reside (e.g., Finance data).

System-of-Record: An information storage system that is the authoritative data source for a given data element or piece of information (e.g., Banner).

Transactional System: An information processing system involving the collection, modification and retrieval of data, as contrasted with systems used solely for analytics or reporting. (e.g., Slate).

IRM-4007.2 – Policy Statement

1. University Ownership of Administrative Data – Administrative Data is owned by the University of Richmond. As such, all members of the University community have the obligation to appropriately use and safeguard the data, in all formats and in all locations.
    a. To the extent possible, Administrative Data should be collected and stored with common definitions, and consistent formats and data entry standards to foster data accuracy and consistency in reporting and data integration, (e.g., consistency in country codes in student and alumni applications).
    b. Administrative Data must be safeguarded to maintain the confidentiality and privacy of personally identified and personally identifiable information in accordance with University policies.

2. Data Classification – Administrative Data is categorized as Confidential, Restricted, Official Use Only or Public following the University's Data Security Policy and must be safeguarded appropriately.

3. Access and Confidentiality – Access to University Administrative Data is based on the business needs of the University and should enhance the ability of the University to achieve its mission. Employees shall have access to the Administrative Data needed to perform their official responsibilities. Individually identifiable data shall be available to the extent necessary to perform administrative tasks; unit record data will be provided only when aggregate data or other alternatives cannot effectively meet the business need. The Data Management Committee is responsible for ensuring that procedures are developed by functional offices to address those cases in which a member of the University community seeks permission to access Administrative Data beyond that which is needed for the normal performance of their duties.

    Because no computer system is completely immune from unauthorized access or attempted access (e.g., "hacking"), applying layered security controls (e.g., multiple levels of access permissions) will better safeguard University computers and our ever-expanding body of Administrative Data, which is often sensitive. In order that the proper controls are applied, it is the responsibility of each person accessing Administrative Data to:
    a. Know the classification of the Administrative Data being used.

b. Follow the appropriate security measures.
c. Consult Related Policies for further information.

Specific policies implementing data access and security, including those developed by functional areas shall be reviewed by the Data Management Committee to ensure consistency with this policy.

4. Training – Before an individual is permitted access to Administrative Data in any form, training in the use and attributes of the data, functional area data policies, and University policies regarding data is strongly encouraged. The Data Stewards shall establish the appropriate levels of training for all such individuals within their units.

5. Integrity, Validation, and Correction – Administrative Data must be safeguarded and managed in all formats and media (e.g., print and digital), at all points of access, and in all locations (both on-campus and off-campus) through coordinated efforts and shared responsibilities. Each Data Steward shall be responsible for developing a plan for their functional area to assess the risk of erroneous or inconsistent data and indicate how such Administrative Data, if found, will be corrected. The Data Management Committee will be responsible for ensuring that each functional area uses that plan to develop and implement processes for identifying and correcting erroneous or inconsistent data.

6. Extraction, Manipulation, and Reporting – Extraction, manipulation, and reporting of Administrative Data must be done only for University business purposes and consistent with this and other applicable University policies. Personal use of Administrative Data, in any format and at any location, is prohibited. All data users are expected to be familiar with and conform to the University's Acceptable Use Policy.

IRM-4007.3 – Roles and Responsibilities

See Exhibit 1 for Data Trustees and Data Stewards for each Data Stewardship Domain.

Data Trustee – a senior University official (typically at the level of Vice President or higher) who oversees a Data Steward. Data Trustees are responsible for:

- the establishment of Administrative Data management policies and procedures
- assigning data management accountability to appropriate Data Stewards.

Data Steward – typically a senior operational manager in a functional area responsible for a Data Stewardship Domain. Data Stewards are responsible for all of the following for data within their Data Stewardship Domain:

- developing and documenting data standards
- establishing the business rules and business processes for their respective Data Stewardship Domains
- establishing the business rules and business processes for the Transactional Systems associated with their Data Stewardship Domain
- ensuring compliance with federal regulations, regional accreditation standards, and other rules and regulations associated with management of the data in their Data Stewardship Doman (e.g., GDPR, FERPA, GLBA, PCI) and providing associated training
- ensuring data privacy (e.g., should we collect this data?) and data security (e.g., confidentiality)
- monitoring/overseeing data sharing (e.g., data exports, reporting, data integrations)
- adjudicating requests to access unit record or aggregate data within Data Stewardship Domain

- complying with University Records Retention Policy
- reviewing data access permissions annually
- understanding integrations and their impacts across related Data Stewardship Domains
- providing review and approval of new systems or data integrations that impact data
- acting as data ambassadors to communicate data and process changes
- implementation of this policy.

Data Supervisor – an individual who creates, stores, modifies or otherwise manages Administrative Data within a Data Stewardship Domain. Data Supervisors are responsible for:

- executing business and data processes related to Administrative Data
- maintaining and reinforcing, wherever possible, a uniform set of definitions for commonly consumed data throughout the University (e.g., "enrolled student" should wherever possible have the same meaning throughout the University).

Data User – an individual who accesses Administrative Data to perform their assigned duties. Data Users are responsible for:

- safeguarding their access privileges
- the use of the Administrative Data in conformity with all applicable University policies,
- securing such data.

Information Services (IS) -- information technology experts assigned to transactional and reporting systems that maintain Administrative Data. IS is responsible for:

- overseeing the safe transport and storage of data
- establishing and maintaining the underlying infrastructure
- performing activities required to keep the data intact and available to users
- working with Data Supervisors to develop automated processes to identify erroneous, inconsistent, or missing data
- working with data support groups and Data Stewards to resolve data issues.

Office of Institutional Effectiveness (IFX) – IFX is responsible for:

- working with Data Stewards to develop definitions of commonly used data elements and define how official University metrics are calculated
- promptly reporting data discrepancies and inconsistencies discovered in the course of its work to the appropriate Data Supervisor for resolution
- implementing consistent reporting guidelines across campus based on institutional policies and federal regulations
- providing all external reporting in all Data Stewardship Domains
- assessing and appropriately fulfilling all requests that require data from multiple Data Stewardship Domains

Data Management Committee (DMC) – a University-wide committee primarily composed of Data Stewards and Data Supervisors. The DMC is co-chaired by the Director, Institutional Effectiveness and the Assistant Vice President for Systems and Networks. Data Stewards will share best practices during their meetings, as well as raise concerns that cross functional areas. Designated Data Users may be invited to attend, as appropriate. The DMC is responsible for:

- reviewing the operational effectiveness of Administrative Data management policies and procedures and making recommendations for improvement and change

- providing oversight of all University processes which capture, maintain, and report on Administrative Data
- ensuring regular and appropriate collaborative communication with Data Users on operational changes that may impact business processes and data.

IRM-4007.4 – Applicable Regulations and Accreditation Standards

A. SACSCOC Principles of Accreditation 12.5 (Student Records)
B. Health Insurance Portability and Accountability Act of 1996 (HIPAA), Public Law 104-191
C. Payment Card Industry Data Security Standard (PCI DSS)
D. Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99)
E. Red Flags Rule of the Fair and Accurate Credit Transaction Act of 2003 (FACT Act), Public Law 108-159, Section 114
F. Code of Virginia, § 18.2-186.6. Breach of personal information notification.
G. General Data Protection Regulation (GDPR) (EU) 2016/679
H. Gramm- Leach-Bliley Act (GLBA), also known as the Financial Services Modernization Act of 1999, Public Law 106–102, 113 Stat. 1338

RELATED POLICIES:

IRM-2001 – Use of Technology and Information Resources

IRM-4002 – Data Exposure Policy

IRM-4003 – Information Security Policy

IRM-4004 – Data Security Policy

IRM-4006 – General Data Privacy Regulation Privacy Notice

External Party Data Transfer Policy

Responding to Requests for Information About Members of the University Community

ACD-2004 – Privacy of Education Records (FERPA) Policy

POLICY BACKGROUND:

Initial policy approved: July 27, 2020

Policy was reviewed by IT Governance Steering Committee, the school deans, and President's Cabinet prior to approval.

POLICY CONTACTS:

Vice President for Information Services and Chief Information Officer

Exhibit 1: Administrative Data Management Policy

University of Richmond Administrative Data Stewards

July 1, 2020

Data Stewardship Domains and their respective Data Trustees and Data Stewards:

1) **Finance** data
    a. Data Trustee: Executive Vice President and Chief Operating Officer (Dave Hale)
    b. Data Steward(s): University Controller (Laurie Melville), Assistant Controller (Steve Walker*)
    c. Data Stewardship Domains: Budget data, Accounting data, Grants, Investment data (Spider Mgt), Procurement and Accounts Payable data, Student Accounts (Bursar) data, Payroll and Tax data
2) **HR** data
    a. Data Trustee: Executive Vice President and Chief Operating Officer (Dave Hale)
    b. Data Steward(s): Sr. AVP Human Resources (Carl Sorensen), Director HRIS and Operations (Denise Jones*), HR Tech and Business Analyst (Cindy Lloyd)
    c. Data Stewardship Domains: Employment data (Staff, Faculty, Contractors, Temps, etc.), Benefits/Compensation data, Position Control data, Payroll data, Performance data, Learning data, Employee recruiting data, emergency contact data for employees
3) **Student Admission** data
    a. Data Trustee: Vice President for Enrollment Management (Stephanie Dupaul)
    b. Data Steward(s): Sr. Associate Director, Admission (Lindsey Monacell*)
    c. Data Stewardship Domains: admission prospects/inquiries, high school/college data, score reports (SAT, ACT, TOEFL, GRE, GMAT, LSAT), admission applications and related materials, basic parent data (until point of enrollment), application decision history, decision notification, SPCS admission, Law admission, MBA admission
4) **Student Registration** data (for both credit and non-credit students)
    a. Data Trustee: Vice President for Planning & Policy (Lori Schuyler)
    b. Data Steward(s): University Registrar (Susan Breeden*), Sr. Associate Registrar (Kristen Ball), Sr. Associate Registrar (Valerie Caminiti)
    c. Data Stewardship Domains: Student academic history (courses, grades, registration, curriculum, degree audit, transcripts-electronic, transfer, paper, and microfiche; grade changes, transfer work); Graduation (application, conferral, honors, diploma information); Academic Courses (catalog, course set up, schedule); Academic Curriculum (major/minors, degrees, programs, GradTracker); Classrooms (location management for academic buildings); Compliance (FERPA training, NCAA eligibility); Testing Center (exams administered); emergency contact data for students
5) **Financial Aid** and **Student Employment** data
    a. Data Trustee: Vice President for Enrollment Management (Stephanie Dupaul)
    b. Data Steward(s): AVP and Director Student Financial Aid (Chip Bryan), Sr. Associate Director Financial Aid (Kathryn Owens*)
    c. Data Stewardship Domains: financial aid applications, FAFSA applications, CSS Profiles, tax returns, parent/guardian/student income, parent/guardian/student

assets, family size/status, home equity, expected family contribution (both FM and IM), need-based grant, scholars, scholarships, athletic funding, Pell grants, loans (federal/private/parent), academic progress, Title IV, withdrawals, award notifications, work study, student employment, W-4's, I9's

6) **Advancement/Alumni** data
    a. Data Trustee: Vice President for Advancement (Martha Callaghan)
    b. Data Steward(s): Asst. VP Advancement Systems (Robb Moore), Director, Advancement Data and Analytics (Jessica Kalista*), Director, Advancement Operations (Sarah Abubakar)
    c. Data Stewardship Domains: Constituent data (alumni, parents, donors, prospective donors), gift data, career/outcomes data
7) **Wellness** data
    a. Data Trustee: Vice President for Student Development (Steve Bisese)
    b. Data Steward(s): Director of Operations, Health and Well-being (Kelly Harris)
    c. Data Stewardship Domains: Student Health (Pyramed, Labcorp), Rec & Wellness (Fusion, Everfi), CAPS (Titanium)
8) **Center for Student Involvement** data
    a. Data Trustee: Vice President for Student Development (Steve Bisese)
    b. Data Steward(s): Director, Center for Student Involvement (Alison Keller), Associate Director Greek Life (Meg Pevarski), Administrative Specialist/Coordinator of Services (Kristen Phelps)
    c. Data Stewardship Domains: Student involvement (extra-curricular) and events (Presence, Eventbrite)
9) **Student Development** and **Housing** data
    a. Data Trustee: Vice President for Student Development (Steve Bisese)
    b. Data Steward(s): Director of Housing and Residence Life (Patrick Benner*)
    c. Data Stewardship Domains: Student Conduct (Maxient), Academic Progress (Maxient), Student Housing (StarRez, Banner)
10) **Campus Services** & **Facilities** data
    a. Data Trustee: Executive Vice President and Chief Operating Officer (Dave Hale)
    b. Data Steward(s): Executive Director Campus Business Services (Jerry Clemmer*)
    c. Data Stewardship Domains: Dining/Catering (Micros, Hospitality Suite), CSGold/OneCard, Event Management, Campus Bookstore, School Dude, HVAC (Talon, Niagara, Thinstack), Building data, Ricoh.
11) **IFX** data
    a. Data Trustee: Vice President for Planning & Policy (Lori Schuyler)
    b. Data Steward(s): Director, Institutional Effectiveness (Melanie Jenkins*)
    c. Data Stewardship Domains: Assessment data (AQUA, Taskstream AMS), course evaluations (CourseEval), survey data (Qualtrics), census files (frozen files for admission, enrollment, faculty, and degree completion stored in Box)
    d. **CROSS-FUNCTIONAL requests**: All cross-functional requests (those that require data from multiple data domains) should be routed to IFX for assessment and fulfillment.
12) **Information Services** data
    a. Data Trustee: Vice President and Chief Information Officer (Keith McIntosh)

Exhibit 1: Administrative Data Management Policy

b. Data Steward(s): Asst. VP Systems and Networks (Troy Boroughs*), Asst VP Telecom, Media and User Services (Doug West)
c. Data Stewardship Domains: Identity data (NetID, URID, network passwords, UR email addresses, DNS names), UR phone numbers, computing assets

**Members of the University of Richmond's Data Management Committee*