

Policy 1205
Data Stewardship Policy

Date of Current Revision: February 2024

Primary Responsible Officer: Associate Vice President for Information Technology and CIO

1. PURPOSE

This policy establishes uniform data management practices for ensuring the availability and protection of university data and applies to all university data collected, stored or maintained by administrative, academic or other units, employees or agents of the university regardless of its source or where it resides. Institutional policy as well as state and federal law prohibit individuals from using university data for purposes other than approved university business.

2. AUTHORITY

The Board of Visitors has been authorized by the Commonwealth of Virginia to govern James Madison University. See Code of Virginia § 23.1-1600; § 23.1-1301. The board has delegated the authority to manage the university to the president.

STATE OR FEDERAL STATUTE AND /OR REGULATION

Laws such as the Family Educational Rights (20 USC 1232g et. seq.) and Privacy Act (FERPA), the Virginia Government Data Collection and Dissemination Practices Act (Code of Virginia § 2.2-3800), and the Virginia Freedom of Information Act (Code of Virginia § 2.2-3700) require the university to provide appropriate data stewardship.

3. DEFINITIONS

Data Classification

A grouping of data for risk management and security purposes based on its level of sensitivity and the impact to the university should the data be disclosed, altered or destroyed without authorization.

Data Custodian

Individual designated by one or more relevant data managers as responsible for the operation and maintenance of a university information technology system, managing a specific subset of university data and/or for overseeing a hosted system for which they are the system owner. Within their area of assigned **responsibility**, the data custodian ensures appropriate access controls are established and maintained and that system controls and information security requirements are met as part of on-going operations.

For research data, the principal investigator is considered to be a data custodian and is responsible for adhering to this and other university policies and standards. The principal investigator is therefore charged with the **creation**, integrity, preservation and security of research data, as well as appropriate marking and reporting of all university intellectual property that may be included in, or derived from, the research data.

Data Manager

University official with management responsibility for the appropriate collection, distribution and use of a defined segment of university data. Along with Information Technology (IT), data managers are responsible for establishing and executing data management standards and procedures to help ensure appropriate stewardship and security of university data. Data managers also assign data custodians for data management accountability as described in this policy and work with the AVP for IT and data steward(s) to address concerns.

Data Steward

University officials (typically at the level of associate vice president, associate provost or their designee) who work with Information Technology (IT) to provide policy-level direction related to a defined segment of university data. The data steward ensures appropriate management accountability for university data by providing guidance and advice to their data manager(s). The data steward also works with the AVP for IT, the Director of IT Policy and Compliance and data managers to mediate concerns.

Data Stewardship Standard

Procedural requirements developed to support the data stewardship policy. The data stewardship standard provides for consistent control and security relative to specific data elements and domains. This standard applies across all information systems and uses of university data.

Data User

Individuals (employees, students, visiting faculty and researchers, contractors, volunteers of the university) who create, have access to or use university data.

Research Data

Research is a systematic experiment, study, evaluation, demonstration or survey designed to develop or contribute to general knowledge (basic research) or specific knowledge (applied research) by establishing, discovering, developing, elucidating or confirming information about, or the underlying mechanism relating to, matters to be studied. Research data may include but is not limited to technical information, computer software, laboratory and other notebooks, printouts, worksheets, other media, survey, memoranda, evaluations, notes, databases, clinical case history records, study protocols, statistics, findings, conclusions, samples, physical collections, and other supporting materials created or gathered in the course of research.

System Administrator

Individual responsible for the implementation and operation of a university system at the direction of the system owner and appropriate data steward/data manager/data custodian. The system administrator provides day-to-day administration and implements security controls and other capabilities as assigned.

System Owner

The individual responsible for overall functionality of an information system and for appropriate stewardship of the data it includes. The system owner works in cooperation with IT to evaluate, license, and implement the system and establish necessary controls to ensure appropriate functionality and security are achieved. In some cases, the system owner may also be a data custodian.

University Data

Data collected, maintained or used by university personnel, contractors or partners as part of their job responsibilities, for operation of the university or to fulfill its mission. University data may reside in different automated systems and in different physical locations, but are to be considered part of a single, shared resource. This resource consists of information represented in a variety of data elements, types, and forms maintained by individuals, administrative/academic units or business partners to provide functionality to the university. All such data owned and managed by or on behalf of the university is considered university data unless explicitly noted otherwise in writing.

4. APPLICABILITY

All university data and systems are subject to this policy regardless of whether they reside on-campus or elsewhere, whether they are paid or free, or how they are licensed or acquired. Provisions of other university policies, standards and procedures, as well as state or federal laws, may also apply.

This policy applies to all employees, students, visiting faculty and researchers, affiliates, and volunteers of the university.

This policy applies equally to university data in digital and non-digital forms. Protection and stewardship of university data in non-digital form (paper, oral, etc.) is the responsibility of individuals and their managers as part of office operations.

5. POLICY

As a member of the higher education community and an agency of the Commonwealth of Virginia, the university collects a large variety of data and is required to make data available for many different purposes. The university is obligated to protect the confidentiality, integrity, and availability of data for all concerned while also protecting individual privacy rights.

The University strives to maximize the value of university data. Data value is best increased through widespread availability balanced with thoughtful management and use. Detractors such as loss, misuse, want of maintenance, and restrictive access can severely diminish the value, and it is the actions of individuals that most directly affect this value equation. This policy outlines the necessary standards and processes that shall guide individual actions and through which the University will deliver the best possible value outcome.

6. PROCEDURES

Information Technology (IT) provides policies, standards, and guidelines that govern the stewardship of university data and can be found on the [IT Policies and Standards website](#). Together, they provide necessary guidance to constituents on the use of university data and information technology and carry weight equivalent to university policy.

6.1 Data Stewardship Standard

The [Data Stewardship Standard](#) defines responsibilities and requirements for each classification of university data (public, protected, highly confidential). The standard details data management roles, classification practices and procedures for data access, and review.

Several of these requirements are worthy of specific note and are considered university policy:

- Access to University Data shall be granted for a specified use and in keeping with the specific job responsibilities of the person being granted access.
- Further distribution of University Data or use of University Data for a purpose other than that for which it was requested and approved is a violation of university policy.
- Highly confidential data shall not be collected or stored outside the central system of record without the written approval of the Data Manager(s).
- The data stewardship standard shall include a list of authorized data managers along with their scope of data management responsibility. Data elements classified as highly confidential shall also be listed along with the additional procedures required for their use.
- Data users and system owners shall identify all data that will be collected or otherwise included in a new system and submit it to IT for review prior to acquisition or development. Systems containing highly confidential or certain types of protected data shall also require annual reviews performed by IT.

6.2 Data Stewardship and Information Security Framework

[The Data Stewardship and Information Security Framework](#) provides an overview of the University's approach to the management and protection of university data and is based on the policies, standards, and procedures that outline the roles and responsibilities of key stakeholders, the classification of data and systems, and a strategy for continual assessment of data stewardship.

6.3 Standard for Acquisition and Assessment of Technology

The Standard for Acquisition and Assessment of Technology outlines the process for requesting new systems and uses of technology at JMU regardless of their cost. The process is used to evaluate new systems as well as current systems that are being expanded or renewed.

6.4 Related Policies and Standards

There are other university policies and standards that relate to the data and technology use including, but not limited to:

- Policy [1109](#) - Records Management
- Information Security – Policy [1204](#)
- Appropriate Use of Information Technology Resources – Policy [1207](#)
- Student Privacy – Policy [2112](#)
- [IT Project Management Standard](#)

7. RESPONSIBILITIES

In cooperation with data stewards and data managers, Information Technology shall maintain the Data Stewardship and Information Security Framework as part of the IT policy website.

Certain officials/individuals (data stewards, data managers, data custodians, and system owners) shall sustain specific roles and responsibilities as detailed in the data stewardship standard and elsewhere in the data stewardship standard.

Data managers shall ensure appropriate classification of university data and work with Information Technology to establish necessary security and access controls for data in electronic form.

All data users shall adhere to the terms and conditions for acquiring and using university data and information technology.

Individuals responsible for the creation or collection of University Data are responsible for adhering to the Data Stewardship and Information Security Framework and all related requirements. Questions about how to apply the framework shall be directed to IT Policy and Compliance or the appropriate Data Manager.

Data users, data custodians, and system owners shall ensure use of only storage locations and systems approved by IT in accordance with the data classification.

University data shall be shared or transferred to individuals or systems outside the university only with the written approval of the appropriate data manager or data custodian.

All departments, offices, and employees that generate, receive, or maintain public records under the terms of this policy are also responsible for compliance with Policy [1109](#) (Records Management).

Data managers, along with IT, are also responsible for providing guidance to departments and individuals regarding collection, processing, storage, and retention of university data using manual or electronic information systems.

8. SANCTIONS

Sanctions will be commensurate with the severity and/or frequency of the offense and may include termination of employment.

9. EXCLUSIONS

None.

10. INTERPRETATION

The authority to interpret this policy rests with the president and is generally delegated to the associate vice president for information technology and CIO, in conjunction with the appropriate data stewards.

Previous version: November 2020

Approved by the president: February 2009