Policy 1205
Data Stewardship Policy

Date of Current Revision: November 2020
Primary Responsible Officer: Assistant Vice President for Information Technology and CIO

1. PURPOSE

This policy establishes a framework of uniform data management practices for ensuring the availability and protection of university data. The policy 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

Assistant Vice President for Information Technology and Chief Information Officer (AVPIT)
The university official responsible for overseeing management of university information in digital form. Along with data stewards and data managers, the AVPIT facilitates data stewardship and information security practices to meet the needs and interests of the university. In consultation with the senior vice president for administration and finance and the provost, the AVPIT also works to mediate any conflicts or discrepancies with regard to data protection and stewardship.

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 (see below) as responsible for operation and maintenance of a university information technology (IT) 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 including those set out in the data stewardship and information security framework. 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, 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 AVPIT and data steward(s) to address concerns.

Data Steward
University official (typically at the level of associate vice president, associate provost or their designee) who works with 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 AVPIT, ISO, and data managers to mediate concerns.

Data Stewardship Standards
Procedural requirements developed to support the data stewardship policy. The data stewardship standards provide for consistent control and security relative to particular data elements and domains. These standards apply across all information systems and uses of data.

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

Information Security Officer (ISO)
The individual responsible for maintaining a plan of security policies and practices, keeping abreast of security-related issues internal to the university community and more broadly advocating for necessary data stewardship and security initiatives for the university.

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 Manager
Individual responsible for operation of a university system at the direction of the data custodian/system owner. The system manager shall have the technical skills and system rights necessary to independently perform day-to-day system operations and security activities or work in conjunction with a system administrator assigned to perform some or all such activities under the system manager's direct oversight.

System Owner
The individual responsible for overall functionality of an information system and for appropriate stewardship of the data it includes (e.g., the university registrar is the system owner for the student administration system). 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, contractors, and volunteers of the university.

This policy applies equally to data in digital and non-digital forms. Protection and stewardship of 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 a Commonwealth of Virginia agency, the university collects a huge 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.

To meet these obligations, university data is classified and managed based on its value as a university resource. 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. The university strives to maximize the value of university data. This policy and the data stewardship and information security framework below set out the necessary standards and processes that shall guide individual actions and through which the university will deliver the best possible value outcome.

6. PROCEDURES

This data stewardship and information security framework outlines processes and required elements of the university's data stewardship and information security programs. The framework, along with other IT policies and standards, is available on the IT policy website. Together, they provide necessary guidance to constituents on university information technology use and are to be considered required elements carrying weight equivalent to university policy.

6.1 Data Stewardship Standards

Define responsibilities and requirements for each classification of university data (public, protected, highly confidential). These standards detail: data management roles, classification practices, procedures for data access, and review, etc.

6.2 Information Security Standards

In keeping with the university information security policy (See Policy 1204) these standards define system classification and security requirements related to various systems based on their related data classification and risk. Also included are procedures for system acquisition, risk assessment, and management, etc.

6.3 Related Policies and Standards

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

- Appropriate Use of Information Technology Resources - Policy 1207
- Information Security - Policy 1204
- Other policies and procedures related to data and information technology use are available on the IT policy website and shall be considered part of the university's data stewardship and information security framework

6.4 General Requirements

a. Requirements for each classification (public, protected, highly confidential) are included in the data stewardship standard. Several of these requirements are worthy of specific note and are considered university policy:

b. Access to non-public data shall be granted for a specified use and in keeping with the specific job responsibilities of the person being granted access

c. Further distribution of non-public data or use of non-public data for a purpose other than that for which it was requested is a violation of university policy

d. Highly confidential data shall not be collected or stored outside the designated central system of record without explicit, joint approval of the university data managers**.**

e. The data stewardship standard shall include a list of authorized data managers along with their scope of data management responsibility. Data items classified as highly confidential shall also be listed along with the additional procedures required for their use.

f. 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 certain types of data shall also require annual reviews

7. RESPONSIBILITIES

7.1 In cooperation with university data stewards and data managers, information technology shall m**aintain the Data Stewardship and Information Security Framework as part of the IT policy website.**

7.2 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 and information security framework.

7.3 Data managers shall ensure appropriate classification of university data and work with information technology to establish necessary security and access controls for data in electron**ic form.**

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

7.5 As new university data items are developed, the individual(s) responsible for creation or collection of the data shall identify its relationship to the data stewardship and information security framework and are responsible for adhering to the related requirements. Questions about how to apply the framework shall be directed to the information security officer or the appropriate data manager.

7.6 Data users, data custodians, and system owners shall ensure use of only storage locations and systems approved by IT for the highest (greatest risk) classification of data being processed.

7.7 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.

7.8 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).

7.9 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 assistant vice president for information technology and CIO, in conjunction with the appropriate data stewards.

Previous version: May 2016
Approved by the president: February 2009