Policy 1205
Data Stewardship Policy

Date of Current Revision: May 2016
Primary Responsible Officer: Assistant Vice President for Information Technology and CIO

---

1. PURPOSE

This policy establishes the methodology by which the university will manage its data and assigns responsibilities for the control and appropriate stewardship of university data.

2. AUTHORITY

The Board of Visitors has been authorized by the Commonwealth of Virginia to govern James Madison University. See Code of Virginia section 23-164.6; 23-9.2:3. The board has delegated the authority to manage the university to the president.

STATE OR FEDERAL STATURE 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 Custodians
Individuals or organizations in physical or logical possession of data for the university (data owner).

Data Managers
University officials having direct operational level responsibility for information management related to the capture, maintenance, dissemination and use of data and for any data administration activities delegated by the data stewards.

Data Owner
The university is the owner of all data collected, stored and/or managed by university employees or using university resources. Collectively all data owned and/or managed by or on behalf of the university is referred to as the University Data Resource.

Data Stewards
The university vice presidents (or their designees) who have planning and policy level responsibility for data within their areas and management responsibilities for defined segments of the university data resource.

Data Stewardship Standards
Procedural requirements developed to support the Data Stewardship policy. The Data Stewardship Standard was developed by the university's data managers in cooperation with Information Technology and approved by the data stewards. To provide consistent control and security relative to a particular data item, these standards apply across all information systems and uses of the data.

Highly Confidential Data
University data which, because of its associated legal restrictions or potential security ramifications, is authorized for use only on a very limited basis and only with special security precautions.

Information Technology maintains a list of data items identified as highly confidential. See the Data Stewardship Standard for details.

Protected Data
Personally identifiable information (PII) and/or other data worthy of protection and discretion in its distribution and use; this type of university data is individually requested and approved by a data manager for a specific business use and is subject to the general provisions associated with university information security. See the Data Stewardship Standard for details.

Public Data
University data which can be shared without restriction to the general public (e.g. university course listings, publicity and news articles, directory listings, etc.).

System Manager
The university manager responsible for implementation and operation of a university system at the direction of the System Owner and appropriate Data Steward/Data Manager. The System Manager oversees the System Administrator who provides day-to-day administration and implements security controls and other capabilities as assigned.

System Owner
The academic/administrative unit head 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 Information Technology (IT) to define requirements, select and implement the system and establish necessary controls to assure appropriate functionality and security are achieved. The system owner is identified/documented during the Technology Solution Request (TSR) process and revisited with IT as job responsibilities/other circumstances necessitate a change.

University Data Resource
Data owned by the university may reside in different automated systems and in different physical locations, but in aggregate these data may be thought of as forming 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 part of the University Data Resource.

4. APPLICABILITY

All data collected, stored, processed or distributed as part of the University Data Resource is subject to this policy and the more specific provisions of the Data Stewardship Standard. Other university policies and state or federal laws may also apply.

Certain types of data are public. Others types of data have usage restrictions, are protected by federal and state privacy legislation, or are critical to the mission of the university or the functioning of its colleges, departments, or programs. Non-public data types require controls to protect confidentiality, integrity and availability. General instructions as well as specific requirements for thoughtful data stewardship are outlined in the Data Stewardship Standard and extend to all forms of the data. For example, those data stored in printed or written reports, transmitted via facsimile, downloaded from the university's various administrative or academic systems, and information processed or stored using local systems (including but not limited to departmental servers, networks or individual-use devices) are included.

5. POLICY

Data/information, in all forms, is a strategic asset of the university. Distribution and appropriate protection of computer and information resources is a fundamental responsibility of Information Technology. This policy establishes key roles and responsibilities for protecting confidentiality, integrity and availability of university data. However, individuals and unit/system managers throughout the university share this responsibility. For example, in cases where university information is not stored in electronic form or, is used locally and takes forms other than those protected within central information systems managed directly by IT, protection is incumbent on the relevant unit headsystem owner and the individual user.

This policy is based on four basic principles:

- the university is the owner of all university data (the University Data Resource);
- the greatest benefit of data is gained through its shared and thoughtful use but is diminished by misuse or lack of appropriate protection;
- access to non-public data is managed based on the mission and needs of the university and;
- the Data Stewardship Policy and Standard are in place along with other related policies to achieve an appropriate mix of three core elements of information security—confidentiality, integrity and availability.

All university data shall be classified in one of three categories:

- Public—data which may or must be open to the general public; data with no existing restrictions on access.
- Protected—data for which access must be guarded due to proprietary, ethical or privacy considerations. Data in this classification may be personally identifiable and must be protected from unauthorized access, modification, transmission, storage or other misuse. Though such data may or may not be subject to specific legal restrictions, it is to be protected in all cases and acquired, accessed or used only as authorized.
- Highly Confidential—data having such an acute sensibility to confidentiality or security concerns that it requires highly elevated levels of access restriction and security control. Data in this classification generally carry specific legal restrictions, have underground commercial value and are targeted by highly damaging forms of compromise or misuse. Therefore, highly confidential data shall be collected, used or disclosed only for a single, specific purpose and only after explicit, documented approval from the appropriate university data manager(s).

6. PROCEDURES

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:

- 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
- 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
- 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

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.

7. RESPONSIBILITIES

All university employees, students, affiliates and others granted access to university data or information systems are responsible for understanding the terms and conditions under which they are to acquire and use university data. The Data Stewardship Standard, the Appropriate Use of Information Technology Resources - Policy 1207, the Information Security - Policy 1204 and other policies and procedures related to data and information technology use are available on the Information Technology policy website and shall be considered as appendices to this policy.

Responsibilities are also assigned to specific individuals and groups as part of the data stewardship effort. Primary among these are Data Stewards, Data Managers, and System Owners. Specific responsibilities are detailed in the Data Stewardship Standard and related policies and procedures.

As new data items are developed, the individual(s) responsible for the creation or collection of the data are responsible for identifying its relationship to the Data Stewardship Policy and Standards to assure that storage and access of the data is appropriately managed. This shall include working with Information Technology to identify/document the appropriate data manager.

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.

Data managers 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: March 2014
Approved by the President: February 2009