

# Data Stewardship Standard

Approved 08-25-08

## Purpose:

This standard establishes operating requirements and processes necessary to carry out the university's Data Stewardship Policy and provide for effective management and protection of the University Data Resource.

## Roles and Responsibilities:

**Data Stewards** are the university division heads (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 stewards work together to assure that data stewardship policies and standards are established, maintained and enforced. A list of the university data stewards and their area of data stewardship responsibility will be maintained by IT as part of this standard (See [Data Stewards List](#)).

**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. A list of the university data managers and their scope of data management authority will be maintained by IT as part of this standard (See [Data Managers List](#)).

As a group data managers are responsible for data classification and policy implementation. Individual data managers approve access, resolve data access concerns and perform other data administration activities for their assigned portion of the university data resource.

With the approval of the appropriate data steward certain data management responsibilities may be further delegated by the data manager. Any such delegation shall be documented using the [Delegation of Data Stewardship Responsibilities](#) form.

**Data Custodian:** An individual or organization in physical or logical possession of data for the university (data owner). Data custodians are responsible for protecting the data in their possession from unauthorized access, alteration, destruction, or usage and providing for general controls such as secure storage and backup. For example, Information Technology is the data custodian for data stored in the central systems it manages, while individual users have data custodian responsibility for any data stored on their workstation or other individually-managed device.

**Data /System User:** An individual who, by virtue of their university role or job function, has been approved to access/make use of data or information systems owned/operated by or on behalf of the university. Training may be required prior to granting access to certain data and/or systems. Training requirements are identified as part of the Access Request Process for each system. See <http://www.jmu.edu/computing/ittraining/isaccess.shtml>.

**System Owner:** the university manager(s) responsible for working in cooperation with Information Technology to define requirements, select an IT system, and direct its operation to assure functional outcomes in keeping with university objectives.

**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.

## General Requirements

### **Data Collection and Maintenance:**

- The university community has a right to expect the integrity of university data resource. Therefore, data will be collected and maintained to guarantee its consistency, reliability, timeliness and accuracy and to avoid duplication and disparity across databases or systems.
- Electronic data shall be collected and maintained as close as possible to the source or creation point of the data as identified by the data manager, independent of what office or individual within the University needs the data. Each manual or computer process through which data passes shall be designed to add value. Duplication of data is to be avoided.

**Data Classification:** Data managers, with input from Information Technology, are responsible for assessing the types of data that make up the university data resource and for rating their need for protection based on confidentiality, integrity and availability. University data shall be classified in one of three categories:

- **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.)
- **Protected Data:** university data individually requested and approved by a data manager for a specific business use and which is subject to the general provisions associated with university information security
- **Highly Confidential Data:** university data which, because of its associated legal restrictions or potential security ramifications, is approved for use only on a very limited basis and only with special security precautions

**Data Access:** Data access is granted to an individual data user for a specific purpose. The capability to view, update and/or extract data contained in the university data resource shall be granted to data users according to their role and job function within the University.

- Access shall be approved only for legitimate university purposes and is subject to university policy, confidentiality rules, relevant state/federal laws and other restrictions based on the use case and the classification of data involved.
- The university data stewards are ultimately responsible for the security and integrity of the data maintained within their areas of responsibility. All levels of management, however, are responsible for ensuring that individuals functioning as data custodians,

system managers, system administrators or data/system users within their areas of accountability are aware of their responsibilities as defined in this standard and the related Data Stewardship Policy. (See <http://www.jmu.edu/JMUpolicy/1205.shtml>).

- Access privileges are assigned to the individual data user. However, the extent of access privileges will be defined and implemented according to the role and job function of the data user's position/job classification rather than on an individual basis. If a user is changes positions or job functions (e.g thru promotion, transfer, separation, etc.), that individual's privileges will be eliminated or changed according to the new position.
- Data/system users shall access and make use of university data only as specified and approved in the request approved by the data manager.
- Access to the university data resource is requested using the appropriate Access Request Process (See <http://www.jmu.edu/computing/ittraining/isaccess.shtml> page link to various access request processes). Supervisors are responsible for approving data access requests for their employees and must assure they are properly trained and aware of their responsibilities in handling university data.
- Access requests are approved by the appropriate university data manager(s) and implemented by IT or the appropriate system manager/data custodian.

**Data Administration** is the function of applying formal guidelines and tools to manage the university's information resource. Responsibility for data administration activities is shared among the data stewards, data managers, data custodians and Information Technology (IT). For each new system, the specific responsibilities for system ownership and data/system management and administration shall be identified and documented as part of the System Implementation and Project Management process outlined in JMU Policy 1202. (See <http://www.jmu.edu/JMUpolicy/1202.shtml>).

**Security:**

- Appropriate security measures shall be undertaken to protect the university data resource from compromise or unauthorized access, modification, destruction or disclosure.
- Data/system users share responsibility and are accountable for their use and access of the university's data resource.
- Data/system users and data custodians shall be aware of the restrictions, regulations and other usage provisions that apply to the data they handle and shall participate in education as necessary to appropriate use and care of the data.

**System Management and System Administration** are the functions of managing, maintaining and operating hardware and software platforms (system environments). Responsibility for system management and for the various activities of computer system administration may belong to Information Technology or to other departments or individuals within the University.

- Any individual or department selecting or operating a multi-user system that 1) uses central (ldap) authentication services, 2) collects or stores protected or highly confidential university data, or 3) interfaces with one of the university critical systems or IT resources must follow the System Implementation and Project Management Policy (JMU Policy 1202. See <http://www.jmu.edu/JMUpolicy/1202.shtml>) and work with IT to identify the person(s) designated to perform data stewardship, system management/administration and information security functions relative to the system.

### **Requirements Specific to Classification:**

Because of the varying nature of data handled at the university, certain types of data are treated very differently from others.

#### **Public Data:**

- Public Data is university data which can be shared without restriction to the general public (e.g. university course listings, publicity and news articles, directory listings, etc.)
- Data managers shall provide guidance and communicate to the university community regarding what data can/cannot be treated as public. They shall also resolve any questions or concerns regarding use of such data.
- Data users are accountable for any data they post or share publicly and shall consult with the appropriate data manager to resolve any questions prior to making data public.

#### **Protected Data:**

- Protected data is university data that is individually requested and approved by a data manager for a specific business use and which is subject to the general provisions for university information security.  
(See <http://www.jmu.edu/computing/standards/infosec/>).
- Protected data must be guarded due to proprietary, ethical or privacy considerations. Unauthorized access, modification, transmission, storage or other use of protected data is a violation of university policy. Though such data may or may not be subject to specific legal restrictions, in all cases is to be protected and accessed/used only as authorized.
- Protected data must not be:
  - used for any purpose other than that for which it was requested and approved
  - shared with others without specific approval from the data manager
  - stored in a way that it is exposed to unauthorized access physically or electronically
- A general Best Practices Guide for Handling Protected Data is also available. Specific questions should be directed to the appropriate data manager or IT Information Security.

### **Highly Confidential Data:**

- Highly Confidential data is university data with such an acute sensibility to confidentiality or security concerns that it requires highly elevated levels of access restriction and security control.
- Highly confidential data shall be collected, used or disclosed only for a single specific purpose and only after prior explicit approval documented by the appropriate university data managers.
- In cooperation with the data stewards and data managers, IT will maintain a list of those university data items identified as highly confidential. (See [Highly Confidential Data List](#)).
- Data/system users shall be authorized access to highly confidential data only if a compelling business need exists. The justification for access to highly confidential data shall be documented/approved as part of the Access Request Process.
- Data/system users with approved access to highly confidential data are responsible for the following additional restrictions/protections regarding its use:
  - Highly confidential data shall not be collected or stored outside the central systems of record (Student Administration, Human Resources, Finance, or University Advancement) without the explicit approval referenced above.
  - Highly confidential data shall not be shared with other individuals, departments, agencies or third parties without documented approval of the appropriate data manager
  - In the rare circumstance that approval to store highly confidential data outside the central systems of record is granted by the data manger ,the data shall be:
    - if at all possible, stored on a protected network drive with the appropriate access restrictions, rather than on the local machine’s hard-drive;
    - stored on a local hard drive only if the machine is configured and operating in regular user mode;
    - fully encrypted; and
    - deleted as soon as possible after the approved use is fulfilled.
- A general Best Practices Guide for Handling Highly Confidential Data is also available. Specific questions should be directed to the appropriate data manager or to IT Information Security.