Data Stewardship Standard

Approved 11/16/2020

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 University Data.

Roles and Responsibilities:

Data Steward: Data stewards are university officials (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 IT and data managers to mediate concerns. See University Data Stewards List.

Data Manager: Data managers are university officials with management responsibility for the appropriate collection, distribution and use of a defined segment of university data. Along with 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 and work with IT and data stewards to address concerns. See University Data Managers List.

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: Data custodians are individuals designated by one or more relevant data managers as responsible for the operation and maintenance of a university IT system, managing a specific subset of university data and/or 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. See University Data Custodians List.

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.

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.

System Administrator: The university staff member responsible for 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.

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 university data and rating its 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).
- **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 university data 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 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.
- 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 changes positions or job functions (e.g. through 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 in the request approved by the data manager.
- Access to university data is requested using the appropriate Access Request Process. Requests may also be submitted by accessing the IT Service Portal directly. Supervisors are responsible for approving data access requests for their employees and must ensure 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 owner/data custodian.

Data Administration: 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 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.

Security:

- Appropriate security measures shall be undertaken to protect university data from compromise or unauthorized access, modification, destruction or disclosure.
- Highly confidential should not be transmitted via email.
- Data/system users share responsibility and are accountable for their use and access of university data.
- 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: The functions of managing, maintaining and operating hardware and software platforms (system environments). Responsibility for system management and 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 authentication services, 2) collects or stores protected or highly confidential university data, or 3) interfaces with one of the university's critical systems or IT resources must follow the System Implementation and Project Management Policy (See JMU Policy 1202) and works 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 Data Stewardship and Information Security Framework).
- 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. Although such data may or may not be subject to specific legal restrictions, in all cases it 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.
- See Guidelines for Data Storage and Collaboration. Specific questions should be directed to the appropriate data manager or IT Information Security Officer

(ISO@jmu.edu).

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 manager, 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.