Data Stewardship and Information Security Framework

The purpose of this Data Stewardship and Information Security Framework is to provide an overview of James Madison University's approach to the management and protection of university data in accordance with university policies as well as applicable laws, regulations, and contractual obligations. The Framework 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.

As stated in University Policy 1205 – Data Stewardship, university data is defined as 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 be 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.

Technology Solution Request (TSR)

Any JMU department, organization or individual seeking to acquire technology systems or services from a third-party provider are required to complete a Technology Solution Request (TSR) within the IT Service Portal. The TSR should include a detailed description of the request, the data involved, and confirmation of budget/supervisor approval. Once the TSR is received by Information Technology (IT), an IT Sponsor is assigned to review the TSR, obtain additional information from the requester as necessary and work to determine a data and system classification.

Data Classification

The university is obligated to protect the confidentiality, integrity and availability of its data in accordance with University Policy 1205 – Data Stewardship. To meet these obligations, IT begins by classifying all university data as public, protected or highly confidential as defined in the Data Stewardship Standard. There are three critical roles that govern the classification and management of university data – Data Steward, Data Manager, and Data Custodian. Each of these roles are detailed below. Data classifications are assigned by the appropriate data manager with input from IT and are based on the level of sensitivity and impact to the university should the data be improperly disclosed, altered or destroyed without authorization.

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.

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.

System Classification

After a data classification has been determined, a system classification is assigned for risk management and security purposes. System classifications are assigned by IT with input from the associated data manager(s) based on a four tier, risk-based scale. A system may receive a classification of 1 – 4 with class 1 being assigned to systems containing highly confidential data, classes 2 and 3 for protected data, and class 4 for public data. System classifications determine the level of risk assessment performed by IT.

Risk Assessment

Systems containing highly confidential or protected data and classified as a class 1 or 2 system require a formal risk assessment be performed by IT's Technology Review Board (TRB). The TRB is comprised of various IT staff including representatives from Information Security, Technical Services, and Information Systems. The TRB will perform a risk assessment and formally document risks and major findings as well as any risk mitigation recommendations. Risk mitigation recommendations will be shared with the system owner for review and acceptance.

For systems classified as a class 3 or 4 system, a less stringent risk assessment is performed based primarily on the type and scope of data involved. See the Standard for Acquisition and Assessment of Technology Systems for more information on the risk assessment process.

Annual System Review

Class 1 and 2 systems containing university data classified as highly confidential or protected are subject to annual system reviews. Through the annual system review process, IT works with the system owner to verify any changes to the system, including new features/modules and additional data input, collect the associated System Management Plan and confirm recommended risk mitigations are in place as necessary. In addition, IT obtains and reviews the vendor's SOC 2 report (i.e. evaluation of the vendor's security infrastructure and approach performed by an external auditing firm) to ensure required security controls are implemented and operating effectively. A summary of the system review is documented and shared with the TRB and associated data manager(s). Any new risk mitigation recommendations are also included in the summary and shared with the system owner for review and acceptance.