Data Stewardship Framework

Stewardship Vision & Framework

Data Hero! University Data Stewards are responsible for the management and/or coordination of management activities to ensure the quality, availability, and security of University data. Data Stewards, both technical and functional, work in collaboration with other University personnel in order to minimize risk associated with accessing, processing, storing, transmitting and receiving data and information systems. Stewards are crucial in ongoing institutional efforts to leverage our valuable data assets in service to our institution, our students, faculty, and staff, and our community.

Data Stewards are often the first point of contact for questions related to student, academic, research, outreach, and organizational administration data. Responsibilities may include coordination of relevant policies, standards and procedures for data management and security (e.g., data entry, storage, quality control, and secure access). These compliance, control and data protections are stewardship functions that contribute to managing risk to the University.

Data stewardship responsibilities—and means of executing those responsibilities—vary across institutional functional areas and across data types within the institution. The UMS Data Stewardship framework formalizes already-existing stewardship functions and provides support for stewards in the forms of compiled resources and connection to other stewards and steward supports.

Stewardship Roles: Stewards, Managers, & Users

Broadly, data stewardship responsibilities fall into three categorical roles: Data Steward, Data Manager, and Data User. Often, the Steward and Manager roles exist within the department of the data, while the User role may be within the same department of the data and is often outside of the department. These three roles are described in more detail on the following pages. It is important to consider these roles from an action perspective rather than a person perspective. Essentially, these roles are not exclusive; a single individual may be a user of a given dataset, as well as carrying out routine data management functions for that data, and providing strategic oversight for the same dataset.

Data Stewards

Responsible for the strategic oversight of data assets & assurance of university compliance with internal & external regulations. Data Stewards’ responsibilities may include:

1. Classifying data elements into the appropriate UMS Data Classification level.
2. Collaborating with organizational unit and technical staff to ensure technology solutions adequately support unit procedures and security requirements, and are designed and implemented as expected
3. Ensuring appropriate data management throughout the data and systems life cycles, from receipt/creation through retention and disposition
4. Reviewing— and assisting with as appropriate—education, training and resources to ensure University personnel are adequately able to perform data management functions consistent with University responsibilities and duties
5. Reviewing— and assisting with as appropriate—policy and procedures for data management with third parties and with University units external to the organizational unit.
Data Managers

Perform operational functions in alignment with Stewards’ oversight of data and compliance. Data Managers’ responsibilities may include:

1. Assisting in the documentation and dissemination of Institutional Data storage, processing and transmission methods by the University and by other authorized users of the data.
2. Coordinating or implementing appropriate controls to protect the confidentiality, privacy, integrity and availability of Institutional Data.
3. Working with the Information Security Office to monitor security risks and potential threats to confidentiality, integrity and availability of Institutional Data.
4. Documenting procedures to ensure consistent storage and transmission of Institutional Data.
5. Provisioning and deprovisioning access to Institutional Data in accordance with university policy & any applicable regulations.
   a. Granting or removing access as employees join or leave the organization
   b. Granting or removing access to align personnel with university needs
   c. Providing user access information
   d. Performing regular audits of user access

Data Users

Responsible for the secure & ethical access, usage, dissemination, and destruction of data in their own devices and files. Data Users’ responsibilities may include:

1. Complying with all institutional guidance on data access, ethical usage, appropriate publication, and timely destruction of data.
2. Complying with all security standards to minimize risks incurred as a result of authorized access, usage, publication, and destruction.
3. Reporting suspected or known security breaches to the Information Security Office and their supervisor.
4. Reporting data errors or suspected errors to appropriate individuals (Steward, Manager).
5. Reporting data inconsistencies and data documentation gaps to Data Governance.
6. Timely completion of all applicable trainings are required and encouraged for UMS data users.