Scope
This policy will define the designation, roles, and responsibilities for those responsible for the protection of campus owned and managed data. The data that will be governed by this policy is defined in UW-System policy 1031.

Definitions
- **Data Custodian:** Data custodians are the party tasked with maintaining and securing the enterprise systems that house the institution’s data. They perform the technical work to enable access and permissions approved by the data steward. This may be university staff or a third-party such as a vendor or the UW-System.
- **Data Steward:** An individual who has direct responsibility to ensure that a data domain is classified, and access is secured appropriately. The data steward collaborates with institutional Security, Privacy and Data Officers. As defined by UWSA policy 1031.
- **Data Domain:** The collection of data, belonging to a specific functional area, for which an institutional employee functioning as a data steward is responsible. Examples of Data Domains are:
  - Academic Records
  - Admissions
  - Athletics
  - Development (Advancement)
  - Financial Aid
  - Human Resources
  - Technology Services
  - Institutional Research
  - Student Health and Counseling

- **Data Management Working Group:** The mission of the Data Management Working Group is to make recommendations regarding data governance and ensure policy requirements are met.

Administrative Procedure
The University of Wisconsin-River Falls owns its institutional data. UW System Administration and individual UW institutions, as well as units and departments within those institutions, have stewardship responsibilities for portions of that data. Every member of the UW System community with access to institutional data and information, including external parties, shares an important responsibility to protect that data.
Although not everyone who has access to UW System data and information is classified as a Data Steward, it is the responsibility of Data Stewards to ensure that information resources for which they have responsibility, are only accessed and used by people and processes in accordance with UW System policy and which have an appropriate business need.

Responsibilities

Leadership Responsibilities

- Data Stewards and Data Custodians assignments are made by the leadership within the unit responsible for the collection, maintenance, and destruction of the data. Upon assignment, the responsible party must notify DoTS via email or by creating a service request. For new and renewed services, DoTS will assist with the identification of the data steward and custodian and the classification of the data during the acquisition process.

Chief Information Security Officer Responsibilities

- Following the identification of a new Data Steward or Data Custodian the Chief Information Security Officer will provide training on the roles and responsibilities defined in UW-System policies and maintain documentation of data steward and custodian assignments and the satisfaction.

Data Management Working Group Responsibilities

- On a quarterly basis, the Data Management Working Group will review the list of Data Steward and Custodian assignments and ensure training has been completed.

Data Steward Responsibilities

- Data stewards will have all roles and responsibilities that are defined in UW-System policies specifically UW-System policy 1031 and related procedures.
  - Data Stewards will classify the data in their assigned data domain according to UW-System policies.
  - The data classifications will be documented and shared with the Data custodian and the UW-River Falls Chief Information Security Officer.
- Data stewards are responsible for evaluating requests for access and approving access to data within their data domain. UW-Board policy 25.3 provides guidance for evaluating access.
- Data stewards must maintain knowledge of IT security policies and other requirements that may need to be met to access the data (ex: non-disclosure agreement, Criminal background check).

Data Custodian Responsibilities

- Data custodians are responsible for enabling access or providing a mechanism for granting and revoking access to data.
- Data custodians must verify that appropriate approvals from data stewards has been obtained.
- Data custodians must maintain records of the approvals for access granted.
Authority
The UW-River Falls Chancellor issues this policy in accordance with the Administrative Policy process. The Division of Technology Services is responsible for the administration of this policy. To request an exception to this policy, mail to: administrative-policy@uwrf.edu.

Sanctions and Appeals Process
Failure to adhere to the provisions of this policy may result in appropriate disciplinary action as provided under existing procedures applicable to students, faculty, and staff, and/or civil or criminal prosecution.

Contact
To direct questions about this policy, mail to: administrative-policy@uwrf.edu.