The University of Wisconsin Oshkosh
Data Governance Procedure

Original Issuance Date: 03/12/2024
Last Revision Date: 07/08/2024
Next Review Date: 03/07/2027

- **PURPOSE**
  This document establishes the processes required for compliance with **UWO Policy: *Data Governance.***

- **RESPONSIBLE OFFICER**
  Assistant Chancellor of Institutional Effectiveness

- **SCOPE**
  This procedure applies to all data owned, managed or disseminated by UW Oshkosh and governed under **UWO Policy: *Data Governance***.

- **BACKGROUND**
  The President of the University of Wisconsin (UW) System is empowered to establish information security policies under the provisions of Regent Policy Document 25-5. In accordance with this provision, UW Oshkosh is committed to a secure information technology environment supporting its mission. To establish safeguards for certain types of data, it is necessary to oversee the proper collection, handling, sharing, and destruction of data commensurate with the sensitivity of the data and the risk to UW System or UW Oshkosh. This procedure is designed to support **UW Oshkosh Policy**: ***Data Governance***, which establishes a governance structure, creates a standard for reviewing requests and granting access to university data, and ensures that internal and external data requests are managed consistently and appropriately.

- **DEFINITIONS**
  Reference UW System Administrative Policy SYS 1000 Information Security: General Terms and Definitions**,** and **UWO Policy: *Data Governance***, for a list of general terms and conditions.

- **PROCEDURES**
  - **Committee Composition & Process**
    - The Data Governance Committee creates, prepares, and recommends policies and procedures, institutional data standards, guidelines, and protocols to the Chancellor for approval.
    - The Data Governance Committee is charged by the Chancellor to manage, revise and grant access to institutional data following the procedures provided within this document.
    - The goals of the Committee:
    - The Data Governance Committee will be composed of permanent members representing the roles and units displayed in *Exhibit 1: Data Governance Committee Membership*, below. Committee members have the option to delegate by role.
    - The Committee may call on content experts to serve in an advisory capacity to the Committee. These *ad hoc* committee members and may be asked to attend regular Committee meetings or provide written advice for a data request.

  - **Data Domains**
    - Data Trustees are responsible for making decisions about the use of data in their domain. Data domains include the following: Admissions/Enrollment, Facilities, Financial Aid, Financials/Cashiering, Housing, Human Resources, and Student Records.
    - Data authority levels assigned to each domain are displayed in *Exhibit 2: Data Governance Authority Matrix*, below.

  - **Identification of Data Trustees, Stewards, and Custodians**
    - The Data Governance Committee shall create and maintain a list of data domains with the names and contact information of the responsible Data Trustees, Data Stewards and Data Custodians (*Exhibit 2*).
    - Assignment of Data Trustee or Data Steward authority is automatic upon acceptance of any job position listed within *Exhibit 2*.
    - Data Trustees and Data Stewards will be identified by Job Role and Name.
    - Data Custodians will be identified by Job Role only
    - Data Stewards must identify the major system(s) where their data resides, classify those systems according to the classifications defined in UW System Administrative Policy 1031: Information Security: Data Classification and Protection, document the classification, and ensure appropriate controls are implemented.
    - Data Stewards will review data classifications annually, update as needed, and notify the Data Governance Committee Chair of any changes.

- **Training**
    - Data Governance Committee members will receive initial data governance training upon appointment to the Committee, and annual training, through Canvas.
    - The Data Governance Committee shall ensure Data Stewards and Data Custodians receive proper training on data classification and requirements in collecting, processing, storage, disclosure, and destruction of data.
    - Data Trustees, Data Stewards and Data Custodians will complete the Data Governance Canvas course annually and will document training completion.
    - The Data Governance Committee will maintain training documentation and tracking.

- **Data Requests**
    - All data requests must route through the proper approval channel established by the Data Governance Committee and outlined below.
    - Employees are required to submit requests to collect, process, access, disclose or store data that is outside of their data domains using the Data Request Form, found on the Office of Institutional Effectiveness web site.
    - Requests will be logged and analyzed by the Data Governance group within five to ten (5-10) business days. Data Governance reviews incoming requests and maintains the authority to approve, decline, or modify a data request.
    - Data Stewards and Data Custodians will be contacted by Data Governance for approval of the data request:
        a. If Approved: The request will be prioritized against other requests to estimate a completion date. Requestor will be notified of the estimated completion date.
        b. If Declined: The requestor will be notified, and the request will be closed.
        c. If Modified: The requestor will be notified, and the request will be analyzed in its modified state.
    - The Assistant Chancellor for Institutional Effectiveness will serve as the approving authority for conflict resolution.

- **Collection of Data**
    - All forms or systems that collect personal data must comply with the standards set in UW System Administrative Policy 1040: Information Security: Privacy Policy and UW System Administrative Procedure 1040.a.: Information Security: Privacy Procedurehttps://www.wisconsin.edu/uw-policies/uw-system-administrative-policies/information-security-privacy-policy/information-security-privacy-standard/
    - Requests to collect data should specify:
        - Requestor's contact information
        - Requestor's organizational affiliation
        - The purpose for which the data is collected

- The method of data collection
    - The data elements that will be collected
    - How the data will be stored
    - Who will have access to the data
    - Will the data be distributed and how
    - How long the data will be retained
    - How the data will be destroyed
  - All forms that collect personal data are required to provide a 'Notice of Collection of Personal Data" to the data subject, informing them of the purpose for which Personal Data is collected, and must be specified at, or prior to, the time of collection.

- **Accessing and Processing Data**
  - Data collected or requested may only be used for the purpose(s) stated in the request and may not be stored, shared, or reused without the consent of the Data Steward and the data subject.

- **Disclosure of Personal Data**
  - Personal or sensitive data may only be disclosed to third parties with the consent of the Data Steward and Data Subject, or under the following conditions:
    i. **Legal Requirements**: Records may be released in response to a lawful subpoena, warrant, open records request, or court order or where such records could be required or authorized by law to be produced, or a lawful request for any other reason, including disclosure to a government agency.
    ii. **Authorized Persons**: Records may be disclosed to UW System officials and authorized individuals performing work for them who require the information for the performance of their job duties.
    iii. **Protection of Interests**: UW System officials may disclose information contained in records to protect its legal interest when those records may be related to the actions of a Data Subject that UW System reasonably believes may violate or has violated his/her conditions of employment or threaten injury to people or property.
    iv. **Emergencies**: Information may be disclosed if, at the judgment of the designated data steward of such records, disclosure is necessary to protect the health, safety, or property of any person.

- **Storage and Retention of Personal Data**
  - Personal and sensitive data should be limited to that which is required to reasonably serve the institution's academic, research, administrative functions, or other legally permitted purposes. Employees are prohibited from storing

information containing personal data unless a specific business need exists to collect, maintain, and store the information.

- All data must be stored and processed according to the standards of the data classification set by Data Steward and Data Custodian.
- Data should be destroyed at or before the time specified in the data request.

- **RELATED DOCUMENTS**
  - *UW System Administrative Policy 1000, Information Security: General Terms and Definitions*
  - Regent Policy Document 25-5, *Information Technology*: *Information Security*
  - UW System Administrative Policy 1030: *Information Security: Authentication*
  - Policy #UWO.IT.1030, Information Security: Authentication
  - Policy #UWO.IT.1030, Information Security: Data Classification
  - UW System Administrative Procedure 1030.A: Information Security: Authentication Standard
  - UW System Administrative Policy 1031: Information Security: Data Classification and Protection
  - Procedure #UWO.IT.1031.A, Information Security: Data Classification
  - Procedure #UWSA 1031.B: Information Security: Data Protections
  - UW System Administrative Policy 1032: Information Security: Awareness
  - Policy #UWO.IT.1032, Information Security: Awareness
  - Procedure #UWO.IT.1032.A, Information Security: Awareness
  - UW System Administrative Policy 1033: Information Security: Incident Response
  - Policy #UWO.IT.1033, Information Security: Incident Response
  - Procedure #UWO.IT.1033.A.: Information Security: Incident Response
  - UW System Administrative Policy 1040, Information Security: Privacy Policy
  - UW System Administrative Procedure 1040.A, Information Security: Privacy Procedure

Exhibit 1: *Data Governance Committee Membership*

Name	Title/Role	Unit
Daniel Howard	IR Administrator (Chair)	Institutional Research
Jennifer Bonack	Registrar	Registrar's Office
Amy Davis	IR Policy Analyst	Institutional Research

Exhibit 2: *Data Governance Authority Matrix*

	Data Trustee	Data Steward				
Data Domain	**Title**	**Title**	**Name**	**Email**	**Data Classification**	**Service(s)**
Student Records	VC of Academic Affairs	Registrar	Jennifer Bonack	bonackj@uwosh.edu	Highly Sensitive	PeopleSoft SIS Navigate Canvas College Scheduler Image Now RoboRegistrar
	AC of Institutional Effectiveness	IR Administrator	Daniel Howard	howarddc@uwosh.edu	Highly Sensitive	
Admissions/Enrollment	VC of Student Affairs	Admissions Director	TBA		Highly Sensitive	PeopleSoft SIS
		Enrollment Management Director	Erin Grisham	grishame@uwosh.edu	Highly Sensitive	Salesforce
Financial Aid	VC of Student Affairs	Financial Aid Director	Alison Casady	casadya@uwosh.edu	Highly Sensitive	PeopleSoft SIS
Financials/Cashiering	VC of Finance & Administration	Bursar	Sarah Anderson	anderssb@uwosh.edu	Highly Sensitive	PeopleSoft SIS Shared Financials (SFS)
Housing	VC of Student Affairs	Residence Life Director	Lori Develice Collins	develicee@uwosh.edu	Highly Sensitive	StarRez
Human Resources	VC of Finance & Administration	Human Resources Director	Shawna Kuether	kuethers@uwosh.edu	Highly Sensitive	HRS
Facilities	VC of Finance & Administration	Facilities Management Director	Kurt Leibold	leiboldk@uwosh.edu	Highly Sensitive	Archibus/TMA

- **POLICY**
  - **UWO Policy**: ***Data Governance*** provides a formal statement surrounding the procedures presented above and is found on the Institutional Effectiveness Policy website: (www.uwosh.edu/institutional-effectiveness/policy)

- **REVISION HISTORY**

2/28/24	Data Governance Team Approves SOP
7/8/24	Committee Membership & Data Stewards updated, add link to UWO Policy website