The University of Wisconsin Oshkosh
Data Governance Policy-DRAFT 08/28/2023

Original Issuance Date:	MMMM DD, YYYY
Last Revision Date:	MMMM DD, YYYY
Next Review Date:	MMMM DD, YYYY

- **PURPOSE**
  - Establish a governance structure to address the risks and responsibilities associated with the sharing of personal data owned or managed by the University of Wisconsin (UW) Oshkosh.
  - Create a standard for requesting and granting access to UW Oshkosh data.
  - Ensure that UW Oshkosh manages internal and external data requests in a consistent and appropriate manner in accordance with the following University of Wisconsin System Policies:
    - UW System Administrative Policy 1030: *Information Security: Authentication*
    - UW System Administrative Policy 1031: *Information Security: Data Classification and Protection*
    - UW System Administrative Policy 1032: *Information Security: Awareness*
    - UW System Administrative Policy 1040: *Information Security: Privacy Policy*

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

- **SCOPE**
  This policy applies to *all data owned or managed by UW Oshkosh*. To the extent possible, the elements of Section 6 of this policy should be incorporated into contracts with third-party providers.

- **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: *Information Technology: Information Security*. UW Oshkosh is not only required but committed to a secure information technology environment. 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 policy is designed to establish a governance structure, create a standard for reviewing requests and granting access to university data, and ensure 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* for a list of general terms and definitions. Terms and definitions found within this policy include the following:

Key Roles:

- **Ad Hoc Committee Members**: Content experts called on by the Data Governance Chair or Committee to serve in an advisory capacity. May be asked to attend a regular Committee meeting or provide written advice in regard to a data request.
- **Chief Information Security Officer (CISO)**: Individual with oversight of university enterprise information systems and processes.
- **Chief Privacy Officer (CPO)**: Individual responsible for managing risks related to information privacy laws and regulations.
- **Data Custodian:** A UW System employee that has been given *operational responsibility for the security of the asset or the data* hosted on the asset. It does not mean that the asset belongs to the owner in a legal sense. Responsibilities include:
  - Managing Data User access and modification requests as authorized by appropriate Data Stewards.
  - Providing and updating procedures in conjunction with Data Stewards
- **Data Governance Committee**: Manages, protects, and ensures the integrity of all university data. Responsible for creation and support of data governance policies and procedures to ensure University compliance with applicable information security and privacy policies and regulations. Provides organized framework for data decisions including collection, access, definitions, privacy, and security. *Ad hoc* content experts may be called upon in an advisory capacity by the Data Governance Committee
- **Data Steward:** A Data Steward is a data expert *assigned* to a Data Domain and accountable to a *Data Trustee***.** The Data Steward *collaborates* with the Chief Information Security Officer (CISO) and Institutional Chief Privacy Officer (CPO), the Data Governance Committee, and Risk Executives, *to ensure that appropriate, clear, and consistent controls are in place to protect data* in a manner commensurate with its value to the university. Institutional Data Stewards have delegated *responsibility for all aspects of how data is acquired, used, stored, and protected* throughout its entire lifecycle from acquisition through disposition. Data Stewards may escalate decisions to their Data Trustee when ambiguity exists, practice conflicts with other data domain practices, or novel circumstances arise.
- **Data Trustee:** Data Trustees are *University officials* (e.g., Vice Chancellors, Vice Provosts, Deans, etc.) who have both *oversight and policy-level responsibility* for institutional datasets. Data Trustees are accountable for managing, protecting, and ensuring the usefulness of institutional data and hold decision-making authority regarding the data for a given Data Domain. A Data Trustee appoints the Data Steward(s) to a data domain.
- **Data User:** University units or individuals who have been granted access to institutional data to perform assigned duties or in fulfillment of assigned roles or functions within the university This access is granted solely for the conduct of university business.
- **Employee:** Faculty, staff, or students who are employed by the *institution*, whether compensated or voluntary.

Key Terms

- **Control:** Any physical, administrative, management, technical, or legal method that is used to prevent, detect or correct risks. Controls are also known as safeguards or countermeasures. Examples include but are not limited to policies, procedures, programs, techniques, technologies, guidelines, and organizational structures.
- **Data:** Information collected, stored, transferred, or reported for any purpose, whether electronic or hard copy.
- **Data Access:** The ability of a person, program, or device to obtain and use data for a

specific purpose or task.

- **Data Classification:** UW System uses the following qualifiers to classify *data*:
  - **High Risk:** The loss of confidentiality, integrity, or availability of data that could result in a **significant or catastrophic impact** to individuals, mission, assets, or operations of UW System.
  - **Moderate Risk:** The loss of confidentiality, integrity or availability of data that could result in a **serious impact** to individuals, mission, assets or operations of the UW System.
  - **Low Risk:** The loss of confidentiality, integrity, or availability of data that could result in a **minimal impact** to individuals, mission, assets or on the operations of the UW System.
- **Data Domain**: Data domains are specific areas of responsibility for data management and use, often defined by function or department.
- **Data Privacy:** Encompasses how and when information is collected, accessed, processed and disclosed, and whether the disclosure involves consent or notice.
- **Data Security:** Encompasses the administrative, technical, and physical measures used to protect information. Data privacy cannot exist without data security.
- **External Network:** A network not controlled by the organization.
- **Personal Data:** The collective definition of Personal Identifiable Information (PII) and Protected Health Information (PHI).
- **Personal Identifiable Information (PII):** Information which can be used to distinguish or trace the identity of an individual alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual.
- **Protected Health Information (PHI):** Any information about health status, provision of health care, or payment for health care that is created or collected by a Covered Entity (or a Business Associate of a Covered Entity) and can be linked to a specific individual. This includes any part of a patient's medical record or payment history.
- **University Data**: Data or information that the University collects, generates, or is responsible for the care of.

POLICY STATEMENT

- **Data Governance Committee**
  - The Data Governance Committee shall oversee the creation and execution of campus policies and procedures to ensure compliance with all applicable regulations and information and privacy policies.
  - The Data Governance Committee shall oversee the proper storage and sharing of data owned and managed by UW Oshkosh.
  - Shall perform risk assessments and create recommendations to campus administration to mitigate risks.
  - Shall create quarterly and annual reports to campus administration on compliance efforts as well as data usage, annually or as needed.
  - This Committee shall review policies and prepare procedures which mitigate risks associated with collection and sharing of certain data owned or managed by UW Oshkosh and covered by this policy.
  - This Committee shall receive requests for and grant authorization, where appropriate, for the data steward to collect and share data covered under this policy.

- This Committee shall also assist the university with risk assessment and mitigation relegated to concerns with shared data.
- This Committee shall consist of the Committee members or their designees and Data Stewards or others, as necessary to be determined by the Committee.
- This Committee shall consist of the CISO/CPO, the Registrar, and the Director of Institutional Research. The committee is accountable to the Responsible Officer.
- The Assistant Chancellor for Institutional Effectiveness shall serve as the Responsible Officer for the data governance committee.
- The Chief Information Security Officer (CISO) shall serve as chair of the committee.
- In consultation with the Responsible Officer, the Committee may add additional committee members as needed. The Chair may convene a larger council or advisory team of Data Stewards and/or subject matter experts to review trends, provide periodic updates, resolve issues, etc.

- **Roles & Role Authority**
  - Data governance authority rests with the Chancellor of UW Oshkosh; this policy identifies roles that shall assist the Chancellor.
  - The Data Governance Committee shall create and submit policy and policy changes to the University related to data sharing and prepare and/or approve related procedures. The Committee shall also oversee the training of all committee members, Data Trustees, and Data Stewards.
  - The Data Governance Committee members shall convene, as needed, to recommend policy and procedural changes that enable the university to share data timely while mitigating risk. The Data Governance Committee shall receive and authorize Data Trustees and Data Stewards to manage and share data covered under this policy.
  - Assigned Data Trustees shall be responsible for ensuring that the university is following its policies and complies with federal and state laws and regulations.
  - Data Stewards are data experts assigned to a Data Domain by the Data Trustee for each domain, as defined by their organizational department. Data Stewards help define, implement and enforce data handling and management for their assigned domain. Responsibilities include:
    - Identifying major data systems where their responsibility resides
    - Classify data and work with their Data Trustee to review classifications annually
    - Review and approve requests for access to data
    - Complete training and participate in ongoing data policy discussions
    - Escalate decisions regarding data to their Data Trustee if ambiguity exists
  - Data Stewards shall be identified, typically by role, and responsible for the collection, storage, sharing, and disposition of data within their department's domain. In some instances, multiple departments may share the same data. When this occurs, the Data Trustees are consulted before approving a data request.
  - Data Custodians will manage Data User access and modification requests as authorized by the Data Steward and will create and update procedures in collaboration with the assigned Data Steward.
  - Data Users (i.e. requestors) include individuals, groups, or systems, internal or external to the university, requesting the use or access to data that is not within their domain of authority. Data Requestors shall submit their formal requests in

writing to the Data Governance Committee. This request shall include an acknowledgement of review and acceptance of the university's data governance policies and procedures.
- All committee members, Data Trustees, Data Stewards and Data Custodians shall receive initial training and training updates as recommended by the Data Governance Committee (See also *'Training'*, below).

- **Training**
  - All Committee members, Data Trustees, Data Stewards and Data Custodians shall receive initial training and training updates as recommended by the Data Governance Committee. This training shall be beneficial in helping participants to understand data governance, data classification (See '*UWSA Procedure 1031.A'*, below), handling personal data (See '*UWSA Procedure 1040.A*', below), requesting data, and sharing data.
  - Data Users will review and accept the university's current policies and procedures for data governance prior to submitting a request for data.

- **Data Collection**
  - The Data Governance Committee shall ensure that all data requests submitted are deemed acceptable, either as requested or modified, to UW System Administrative Policy 1031: Information Security: Data Classification and Protection, and UW System Administrative Policy 1040: Information Security: Privacy Policy, prior to collecting data.
  - Once approved, the Data Governance Committee shall authorize the proper collection and release of data as outlined in *UWSA Procedure 1040.A*, below.

- **Data Requests & Approvals**
  - Requests for data must route through the proper approval process established by the Data Governance Committee.
  - Data requests shall include the requestors' contact information and organizational affiliation, what data is requested, and why the data is needed.
  - Once reviewed, the Data Governance Committee shall approve, decline, or modify data request and authorize the data trustees and data stewards to release the authorized data, if any.
  - Approving Authority for conflict resolution shall be the responsibility of the Assistant Chancellor of Institutional Effectiveness.

- **Data Dissemination & Destruction**
  - The use of personal data shall be limited to the purpose for which it was collected. Personal data may only be disclosed to third parties with the consent of the Data Subject, or under the following conditions: legal requirements, authorized persons, protection of interests, or emergencies (as defined in *UW System Administrative Procedure 1040.A.: Information Security: Privacy Procedure*, below).
  - The Data Governance Committee shall confirm the timeline in which the data will be used and understand the method of destruction for personal data.

- UW System and UW Oshkosh shall limit the storage and retention of personal data to that required to reasonably serve the individual's, group's, or institution's academic, research, administrative functions, or other legally permitted purposes.
- All internal data requests must be reviewed by the data governance committee.

- **REFERENCES**

  - *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

- **PROCEDURES**

  The UWO Data Governance Procedure implements this policy and is available at: [insert link]

- **REVISION HISTORY**

[Date]	[Brief revision description]