University of Wisconsin
Whitewater

Data Confidentiality Agreement

The University of Wisconsin-Whitewater (UW-W) is the owner of all institutional data available in all types of university electronic systems or physical formats. An individual's (employees, student employees, consultants, third-party vendors, etc.) access to university data is granted on a need-to-know basis and as required to perform job duties and business functions. Institutional data is categorized into three risk categories: high risk, moderate risk, and low risk (see **UW System Administrative Policy 1031**).

- High Risk – Any data where the unauthorized disclosure, alteration, loss, or destruction may cause personal or institutional financial loss or the unauthorized release of which would be a violation of a statute, act, or law. Examples are:
    - information protected from unauthorized disclosure by legislation such as the Health Insurance Portability and Accountability Act (HIPAA), or industry standards such as Payment Card Industry Data Security Standard (PCI DSS);
    - information referenced in **s. 134.98, Wis. Stats**. An individual's last name and the individual's first name or first initial, in combination with and linked to any of the following elements, if the element is not publicly available information and is not encrypted, redacted, or altered in a manner that renders the element unreadable:
        - Social Security Numbers;
        - driver's license numbers and state resident/personal identification numbers;
        - financial account numbers (including credit or debit card numbers, bank account numbers) and associated security codes or passwords granting access to an individual's account;
        - deoxyribonucleic acid profile (as defined in **s. 939.74(2d)(a)), Wis. Stats**.;
    - protected health information (e.g., any information about the health status, provision of health care, or payment, excepting workers compensation);
    - student educational records regulated under FERPA in conjunction with identifying references such as student identification numbers (excluding directory data)

- Moderate Risk – Any data if released to unauthorized individuals could have a mildly adverse impact on the institution or UW System's mission, safety, finances, or reputation. Examples are:
    - information that is proprietary or produced only for use by members of the UW System community;
    - student educational records without identifying references;
    - FERPA-related information not specifically classified as high risk;
    - directory information for employees who have chosen to withhold their personal information;
    - donor or other third-party partner information maintained by the University;
    - proprietary financial, budgetary, or personnel information not explicitly authorized for public release;
    - citizenship status, ethnicity, gender/gender identity;
    - unpublished research data not considered high risk.

- Low Risk – Any data where the unauthorized disclosure, alteration, loss, or destruction would have no adverse impact on the mission, safety, finances, or reputation of the institution or UW System. Generally, public information is classified as low risk.

University of Wisconsin
Whitewater

Access to institutional data is approved by the Data Steward, an individual who has direct responsibility to ensure that a data domain is classified appropriately. Every individual or entity with access to UW-W Institutional Data has an obligation to use and secure institutional data, which includes student, employee, financial, and medical information; appropriately.

Individuals and entities with access to institutional data must agree to:

- Respect electronic computing resources and systems and my impact on them.
- Utilize information available for my use in my official role at UW-W only. No additional uses of information or sharing of information may be made without appropriate authorization.
- Removal of official record copies of documents from the office where they are maintained is permissible only when authorized to do so and in the performance of office duties.
- Keep all passwords and access codes confidential and out of sight of others.
- Keep all confidential (high-risk) information and records however maintained or stored, safeguarded against inappropriate use or access by others. Physical documents must not be left unattended and must be securely stored in locked storage.
- Never store confidential (high-risk) information in any format on a thumb drive. All devices that access high-risk data must be managed in an institution or UW system-approved manner (even though your UW-W Google Drive account is an institutional-approved storage solution, it is not appropriate for high-risk data. Please use a **Network Drive** instead). The system must be locked and logged out when unattended.
- When accessing confidential (high-risk) data, encryption needs to be applied at rest and in transit.
- Report any infractions in the use or release of information to the appropriate data steward.
- Follow all Federal, State, UW System, and University regulations and policies regarding data release and security.
- Destroy stored institutional data securely per **UW System retention schedules**.
- Remove UW System data from their personally-owned devices before the devices are discarded or replaced, or before the individual is no longer employed with the UW System; unless explicitly authorized to retain the data (such as University retirees are allowed to retain access to email).
- If the individual is unsure which category of data they are accessing (low, moderate, or high risk), they will clarify their understanding by contacting **security@uww.edu**.

Annual training for information security awareness is required for current employees and completion of security awareness training within 30 days for new employees (**policy 1032**).

Users who fail to adhere to the provisions of this policy may result in the suspension or loss of access to UW System IT resources; appropriate disciplinary action as provided under existing procedures applicable to students, faculty, and staff; civil action; or criminal prosecution. To preserve and protect the integrity of UW System IT resources, there may be circumstances where a UW institution may immediately suspend or deny access to the resources (**Regent Policy 25-3: *Failure to Comply with Information Technology Resource Policy***)

I have read the UW Whitewater Data Confidentiality Agreement above. I understand my responsibilities and obligations regarding data security and confidentiality.

Name: _____

Signature: _____ Date: _____