**Data Confidentiality Acknowledgement**

The University of Wisconsin-Green Bay (UWGB) is the owner of all institutional data available in all types of university electronic systems or physical formats. An individual’s (employees, student employees, volunteers, alumni, third-party vendors, etc.) access to university data is granted as required to perform job duties and for educational purposes. Institutional data is categorized under UW System Policy into three risk categories: high risk, moderate risk, and low risk (see [SYS 1031, *Information Security: Data Classification and Protection*](https://www.wisconsin.edu/uw-policies/uw-system-administrative-policies/information-security-data-classification-and-protection/)).

**Categories:**

1. **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:
   1. 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);
   2. information referenced in [**s. 134.98, Wis. Stats**.](http://docs.legis.wisconsin.gov/statutes/statutes/134/98) 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:
      1. Social Security Numbers;
      2. driver’s license numbers and state resident/personal identification numbers;
      3. 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;
      4. deoxyribonucleic acid profile (as defined in [**s. 939.74(2d)(a)), Wis. Stats**.;](http://docs.legis.wisconsin.gov/document/statutes/939.74(2d)(a))
   3. Personal Health Information as protected by System and Federal Policy (e.g., any information about the health status, provision of health care, or payment);
   4. student educational records as defined by the Family Educational Rights and Privacy Act ([FERPA](https://www.uwgb.edu/ferpa/)) in conjunction with identifying references such as student identification numbers (excluding directory data)
2. **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:
   1. information that is proprietary or produced only for use by members of the UW System community;
   2. student educational records without identifying references;
   3. educational records not otherwise classified as “High Risk” under FERPA;
   4. directory information for employees who have chosen to withhold their personal information;
   5. donor or other third-party partner information maintained by the University;
   6. proprietary financial, budgetary, or personnel information not explicitly authorized for public release;
   7. citizenship status, ethnicity, sex, gender identity;
   8. unpublished research data not considered high risk.
3. **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.

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

**In accessing any institutional data, all individuals and entities adhere to the following provisions:**

1. Respect electronic computing resources and systems and understand how use can impact such systems.
2. Utilize information available for exclusively for educational and business purpose.
3. Keep all passwords and access codes confidential and out of sight of others.
4. Keep all confidential (high-risk) information and records however maintained or stored, safeguarded against inappropriate use or access by others.
5. Not store high-risk information in any format on a thumb drive or on an unauthorized web storage solution.
6. Use only devices and systems which are managed in an institutionally approved manner, or through software that is institutionally approved, for accessing medium or high-risk institutional data. The system must be locked and logged out when unattended.
7. When accessing medium and high-risk data, utilize encryption at rest and in transit.
8. Report any infractions in the use or release of information to [security@uwgb.edu](mailto:security@uwgb.edu).
9. Follow all Federal, State, UW System, and University regulations and policies regarding institutional data release and security.
10. Destroy stored institutional data securely per [UW System retention schedules.](https://uwm.edu/libraries/archives/uwm-records-management/general-record-schedules/)
11. Remove all 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; Seek guidance from my supervisor or [security@uwgb.edu](mailto:security@uwgb.edu) if I am unsure which category of data I am accessing (low, moderate, or high risk).
12. Ensure that data that is entered into institutional systems is accurate.
13. Educate myself on institutional data definitions and commit to accurately presenting data in alignment with the established definition(s).

Annual training for information security awareness is required for current employees, student employees and others who have general access granted by the University. Individuals and agencies may not access institutional data until they have completed the training required for that access. A 30-day grace period for new employees may apply as consistent with the policy of the operational area ([SYS 1032, *Information Security: Awareness*](https://www.wisconsin.edu/uw-policies/uw-system-administrative-policies/information-security-awareness/)).

Failure of employees and student employees to adhere to the above requirements may be subject to disciplinary action as well as the suspension or loss of access to UW System IT resources; and third-party actions including but not limited to civil action and criminal prosecution. Third parties who are found to be in violations of these requirements will have access terminated and be subject to further action including but not limited to termination of contract and permanent removal of access to UW Green Bay IT resources.

To preserve and protect the integrity of UW System IT resources, UW Green Bay may immediately suspend or deny access to the resources without prior notice if, in its own determination, the action of the individual or agency action places data or other IT security at risk ([Regent Policy 25-3: *Failure to Comply with*](https://www.wisconsin.edu/regents/policies/acceptable-use-of-information-technology-resources/)[*Information Technology Resource Policy*](https://www.wisconsin.edu/regents/policies/acceptable-use-of-information-technology-resources/)).

I have read the above provisions and agree that by accessing any institutional data I am acknowledging the above responsibilities and obligations regarding data security and confidentiality.

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

Employee Signature Date