

UNIVERSITY OF WISCONSIN – GREEN BAY
Employee Confidentiality Agreement

For purposes of this document, "confidential information" is defined below and includes highly sensitive data as defined in the UW-Green Bay Information Security Policy. http://www.uwgb.edu/policies/info_security.asp

Confidential information includes but is not limited to the following:

- Data covered by Wisconsin Privacy Laws (<http://privacy.wi.gov/laws/toc.jsp>)
 - Social Security Numbers
 - Driver's License or State Identification Number
 - Biometric Information (fingerprints, DNA, retina images, etc.)
 - Financial account information (Credit card or bank account numbers, PINs, security codes, etc.)
 - Protected health information
- Other personal information to be protected include:
 - Birth date, home address and phone number, gender, ethnicity, citizenship, visa codes, veteran and disability status, and employee or student identification numbers.
 - Disciplinary actions
 - Donor information
- FERPA covered data (http://www.uwgb.edu/deanofstudents/for_your_info/ferpa.html)
 - Any and all student-related data (grades, class schedules, class lists or memberships)
- Data covered under HIPAA regulations (<https://www4.uwm.edu/legal/hipaa/>) or Chapter 51 of Wisconsin Statutes (<http://www.legis.state.wi.us/statutes/Stat0051.pdf>)
 - Any and all student and employee medical, mental health and substance abuse data (counseling, immunizations, tests, lab results, etc.)
- Login/password credentials given to grant access to systems or resources.
- University information that is exempt from legal open records requests.

During my employment I acknowledge and understand my responsibilities are to:

- Ask my supervisor for clarification if I have questions relating to what constitutes confidential information.
- Use confidential information only as necessary in the performance of my duties and only for its original intended use.
- Get proper authorization from my supervisor if I am asked to disclose or share confidential information.
- Not let others overhear or view confidential information for which I am responsible.
- Control access to confidential information such as preventing unauthorized access to my computer, locking my file cabinets or office door, shredding paper copies before disposal, and deleting files containing confidential information when no longer needed.
- Never store confidential information on personally-owned devices.
- Never store confidential information on university-owned mobile devices (e.g. on laptops or thumbdrives) unless authorized by my supervisor.
- Encrypt confidential information on my university-owned computer, laptop, mobile device or removable storage device (e.g. thumb drive) whenever possible.
- Never take confidential information away from UW-Green Bay unless authorized by my supervisor.
- Notify my supervisor when I no longer need electronic access to confidential information.
- Properly dispose of or return all confidential information to my supervisor upon termination of employment.
- Report any actions which violate confidentiality to my supervisor or the Information Technology Security Officer.

I understand that failure to comply with this agreement may result in discipline up to and including termination of my employment.

I acknowledge that I have read and understand the above information.

Printed Name: _____ Department: _____

Signature: _____ Date: _____

Please send completed form to Human Resources, ES 107
(Exception: For student employees only, please retain this form in departmental files)