The University of Wisconsin Oshkosh
Procedure # UWO.IT.1031.A
Information Security: Data Classification

Original Issuance Date:	September 14, 2016
Last Revision Date:	September 14, 2016
Next Review Date:	March 2017

1. PURPOSE

The purpose of these procedures is to define the steps required to fulfill data classification requirements at UW Oshkosh.

2. RESPONSIBLE OFFICER

Chief Information Officer

3. SCOPE

These procedures apply to all employees of the university.

4. BACKGROUND

The President of the University of Wisconsin System is empowered to establish information security polices under the provisions of Regent Policy Document 255 (https://www.wisconsin.edu/regents/policies/informationtechnologyinformationsecurity/). The UW System and UW Oshkosh are committed to a secure information technology environment in support of institutional mission. These procedures are designed to help ensure effective and consistent information security awareness throughout the University of Wisconsin System.

5. DEFINITIONS

Employees: All faculty, staff, and student-workers.

Individuals: All faculty, students, and staff.

Institutions: All four year campuses of the UW System, UW Colleges, the University of Wisconsin Extension, and UW System Administration.

6. PROCEDURES

1. The Chief Information Officer (CIO) shall work with UW System and institutional data councils to identify a qualified data steward for each data domain, in accordance with UW System policies regarding data domains and stewards.

2. The Office of the CIO provide training for Data Stewards to ensure they understand their roles and responsibilities regarding data classification and management.
3. The Office of the CIO shall educate constituents on their roles and responsibilities regarding data classification and management.
4. With assistance from the Office of the CIO, each Data Steward shall identify the major systems and locations where their data resides, classifying them as high, moderate, or low risk in accordance with UW System Administrative Policy 1031, Information Security: Data Classification (https://www.wisconsin.edu/uw-policies/uw-system-administrative-policies/information-security-data-classification/).
5. Data Stewards shall review data classifications at least annually.
6. Examples of commonly found data elements for each classification include:
    a. High Risk
        i. 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);
        ii. Information as referenced in Wisconsin Statute 134.98 (https://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; or
            4. Deoxyribonucleic acid profile as defined in Wisconsin Statute 939.74(2d)(a) (https://docs.legis.wisconsin.gov/statutes/statutes/939/VI/74) or other unique physical biometric data (including fingerprint, voice print, retina/iris image) that can be used to identify an individual.
        iii. Protected health information (e.g., any information about the health status, provision of health care, or payment, excepting workers compensation);
        iv. Student educational records with identifying references not including directory data
        v. Login/password credentials granting access to high risk data;
        vi. Trade secrets or information which the UW System, by choice, contract, or other agreement, has committed to ensuring confidentiality;
        vii. Information and/or documentation where release would significantly impair the ability to secure the UW System data, operations and facilities;
        viii. University information that is statutorily exempt from public records

requests per Wisconsin Statute 19.31 (https://docs.legis.wisconsin.gov/statutes/statutes/19/II/31).

b. Moderate Risk
   i. Information that is proprietary or produced only for use by members of the UW System community, such as project plans, email reports, and procedure documents plans;
   ii. Student educational records without identifying references;
   iii. Information protected under the Family Educational Rights and Privacy Act (FERPA) (https://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html) that is not specifically classified as high risk;
   iv. Institutionally developed and/or owned computer applications and/or source code not designated as public domain;
   v. Directory information for employees who have chosen to withhold their personal information;
   vi. Information used for internal purposes or exchanged pursuant to contract that is not considered high risk, such as drafts;
   vii. Donor or other third party partner information maintained by the University;
   viii. Proprietary financial, budgetary or personnel information not explicitly authorized for public release;
   ix. Emails and other communications regarding internal UW System matters that have not been specifically approved for public release;
   x. Unpublished research data not considered high risk.

c. Low Risk
   i. Published directory information;
   ii. Maps, university websites or brochures intended for public use;
   iii. Course catalogs and timetables;
   iv. Press releases;
   v. Institutional statements and other reports filed with federal or state authorities and generally available to the public.

7. REFERENCES

UW System Administrative Policy 1031, Information Security: Data Classification (https://www.wisconsin.edu/uw-policies/uw-system-administrative-policies/information-security-data-classification/)

UW System Administrative Policy 1031, Information Security: Data Classification (https://www.wisconsin.edu/uw-policies/uw-system-administrative-policies/information-security-data-classification/)

UW System Administrative Procedure 1032.A, Information Security: Awareness

(https://www.wisconsin.edu/uw-policies/uw-system-administrative-policies/information-security-awareness/)

UW System Administrative Procedure 1034, Information Security: Acceptable Use (https://www.wisconsin.edu/uw-policies/uw-system-administrative-policies/information-security-acceptable-use/)

UW System Operational Policy GEN 13 Layoff for Reasons of Budget or Program (https://www.wisconsin.edu/ohrwd/download/policies/ops/gen13.pdf)

Regent Policy Document 255, Information Security (https://www.wisconsin.edu/regents/policies/informationtechnologyinformationsecurity/)

Wisconsin Administrative Code s. 35.93, Chapter UWS 4, Procedures for Dismissal (http://docs.legis.wisconsin.gov/code/admin_code/uws/4.pdf)

Wisconsin Administrative Code s. 35.93, Chapter UWS 11, Dismissal of Academic Staff for Cause (http://docs.legis.wisconsin.gov/code/admin_code/uws/11.pdf)

Wisconsin Administrative Code s. 35.93, Chapter UWS 17, Student Nonacademic Disciplinary Procedures (http://docs.legis.wisconsin.gov/code/admin_code/uws/17.pdf)

Wisconsin Statute 19.31 (https://docs.legis.wisconsin.gov/statutes/statutes/19/II/31)

Wisconsin Statute 134.98 (https://docs.legis.wisconsin.gov/statutes/statutes/134/98)

Wisconsin Statute 939.74(2d)(a) (https://docs.legis.wisconsin.gov/statutes/statutes/939/VI/74)

Family Educational Rights and Privacy Act (FERPA) (https://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html)

8. POLICY

These procedures fulfill the requirements of Policy # UWO.IT.1031 Information Security: Data Classification.

9. REVISION HISTORY

09/14/2016	Effective date of UW System policy
06/30/2017	Effective date of UWO Procedures