

The University of Wisconsin Oshkosh
Policy # UWO.IT.1031
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 this policy is to establish a method of categorizing data assets based on risk to the University of Wisconsin System and to facilitate the application of appropriate controls to adequately protect data of all types.

2. RESPONSIBLE OFFICER

Chief Information Officer.

3. SCOPE

This policy applies to all University of Wisconsin System data.

4. BACKGROUND

The President of the University of Wisconsin System is empowered to establish information security policies under Regent Policy Document 25-5

(<https://www.wisconsin.edu/regents/policies/information-technology-information-security/>)

The UW System is committed to a secure information environment in support of its mission. The data classification types described within this policy are designed to help ensure satisfactory and consistent data classification throughout the computing environments of all UW System institutions.

In order to establish the safeguards required for particular types of data, it is necessary to determine the level of risk associated with the data. Data classification assigns such levels and determines the extent to which technical, administrative, and physical controls should be applied to protect the data from theft, alteration, loss of integrity, and/or misuse.

5. DEFINITIONS

Data Steward: An individual who has direct responsibility to ensure that a data set is classified appropriately. The data steward collaborates with institutional Security, Privacy and Data Officers.

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

6. POLICY STATEMENT

1. Data shall be classified in one of three categories:
 - a. **High Risk:** Any data where the unauthorized disclosure, alteration, loss, or destruction may:
 - i. cause personal or institutional financial loss or the unauthorized release of which would be a violation of a statute, act or law;
 - ii. constitute a violation of confidentiality agreed to as a condition of possessing or producing or transmitting data;
 - iii. cause significant reputational harm to the University; or,
 - iv. require the UW System to self-report to the government and/or provide public notice if the data is inappropriately accessed.
 - b. **Moderate Risk:** Any data if released to unauthorized individuals could have a mildly adverse impact on the institution or UW System mission, safety, finances, or reputation. Data not specifically identified in another level is categorized as a "Moderate Risk."
 - c. **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.
2. There may be data which may be catastrophic to human life if there were unauthorized disclosure, alteration, loss, or destruction. This type of data is outside the scope of this policy and should be evaluated on a case-by-case basis.
3. It is the responsibility of the applicable data steward(s) to evaluate and classify data for which he or she is responsible according to the definitions in this policy. A data steward may classify specific data elements at a higher level than identified in UW System Administrative Procedure 1031.A, *Information Security: Data Classification* (<https://www.wisconsin.edu/uw-policies/uw-system-administrative-policies/information-security-data-classification/>).
4. A data steward may not reclassify to a lower level any data that is specifically classified in the procedure.
5. Proper data security handling must be implemented commensurate with the sensitivity of the data and the risk to the UW System.

7. REFERENCES

UW System Administrative Policy 1030, Information Security: Authentication
(<https://www.wisconsin.edu/uw-policies/uw-system-administrative-policies/information-security-authentication/>)

Policy # UW0.IT.1031: Information Security: Data Classification

UW System Administrative Procedure 1030.A, Information Security: Authentication
(<https://www.wisconsin.edu/uw-policies/uw-system-administrative-policies/information-security-authentication/information-security-authentication/>)

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 1031.A, Information Security: Data Classification
(<https://www.wisconsin.edu/uw-policies/uw-system-administrative-policies/information-security-data-classification/information-security-data-classification/>)

UW System Administrative Policy 1032, Information Security: Awareness
(<https://www.wisconsin.edu/uw-policies/uw-system-administrative-policies/information-security-awareness/>)

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 Policy 1033, Information Security: Incident Response
(<https://www.wisconsin.edu/uw-policies/uw-system-administrative-policies/information-security-incident-response/>)

UW System Administrative Policy 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 25-5, Information Security
(<https://www.wisconsin.edu/regents/policies/information-technology-information-security/>)

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)

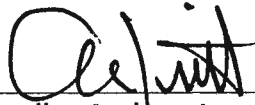
8. PROCEDURES

Procedure # UWO.IT.1031.A that implements this policy is available at http://it.uwosh.edu/wp-content/uploads/2015/07/PROC_1031.A_DataClassification_20170621.docx.pdf.

9. REVISION HISTORY

09/14/2016	Effective date of UW System policy.
06/30/2017	Approved by Chancellor Leavitt.

APPROVED BY:



Chancellor Andrew Leavitt