The University of Wisconsin Oshkosh
Policy # UWO.IT.1032
Information Security: Awareness

Original Issuance Date:	September 14, 2016
Last Revision Date:	September 14, 2016
Next Review Date:	September 14, 2019

1. PURPOSE

The purpose of this policy is to ensure that all individuals and organizations that access University of Wisconsin System information technology assets are exposed to Information Security awareness materials and have a level of understanding commensurate with their role within the University.

2. RESPONSIBLE OFFICER

Chief Information Officer

3. SCOPE

This policy applies to any individual or entity that has access to non-public University of Wisconsin System information. This policy does not cover members of the general public, who may have casual or incidental access to publicly accessible information technology resources made available by the UW System.

4. BACKGROUND

The President of the University of Wisconsin System is empowered to establish information security polices 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 technology environment in support of its mission. The information security awareness training described within this policy is designed to help ensure satisfactory and consistent information security awareness throughout all UW System institutions.

5. DEFINITIONS

Compensating Control: A data security measure that is designed to satisfy the requirement for some other security measure that is deemed too difficult or impractical to implement and that meets the intent and rigor of the original control.

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

High Risk Data: Data assets classified as high risk as defined in UW System Administrative Policy 1031, Information Security: Data Classification (https://www.wisconsin.edu/uw-policies/uw-system-administrative-policies/information-security-data-classification/).

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.

Low Risk Data: Data assets classified as low risk as defined in UW System Administrative Policy 1031, Information Security: Data Classification (https://www.wisconsin.edu/uw-policies/uw-system-administrative-policies/information-security-data-classification/).

Moderate Risk Data: Data assets classified as moderate risk as defined in UW System Administrative Policy 1031, Information Security: Data Classification (https://www.wisconsin.edu/uw-policies/uw-system-administrative-policies/information-security-data-classification/).

6. POLICY STATEMENT

1. Any individual or entity that has access to moderate or high risk data shall:
    a. Upon hire and annually thereafter, acknowledge and accept the UW System Acceptable Use Policy and any applicable institutional Acceptable Use Policy.
    b. Annually complete information security awareness training, which acknowledges that they are aware of security best practices and their roles in protecting the university's systems and data.
2. All newly hired employees shall complete the information security awareness training within 30 days of their initial hire date.
3. All contractors, consultants and business partners shall accept and abide by UW System acceptable use policies prior to being given access to university systems and data resources, when possible.
4. For students with access to only their own data, the institution shall on an annual basis:
    a. Provide notification of the UW System Acceptable Use Policy and any applicable institutional Acceptable Use Policy.
    b. Provide access to an information security awareness training that includes security best practices and explains their roles in protecting the University's systems and data.
5. Each UW System institution shall implement an information security awareness program that:
    a. Ensures individuals are aware that information security is an integral part of their day-to-day activities
    b. Shall be reviewed and updated as appropriate on an annual basis.

6. Individuals shall complete information security awareness training, as determined by the institution, appropriate to their role and risk classification of the data they can access.
7. Each UW System institution will keep an up-to-date record of who has completed information security awareness training.
8. Any individual or entity who fails to complete the required annual training, may be subject to disciplinary action including but not limited to removal of access to UW System non-public data until such requirements have been met.
9. If an individual or group is determined to have violated this policy, the UW System institutions may elect to take action, which includes:
    a. The restriction and possible loss of information technology resource access privileges.
    b. Appropriate disciplinary action including, but not limited to, termination from employment with 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/)

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.1032.A that implements this policy is available at http://it.uwosh.edu/wp-content/uploads/2015/07/PROC_1032.A_SecurityAwareness_20170621.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