The University of Wisconsin Oshkosh
Policy UWO.IT.1034
Information Security: Acceptable Use

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

This policy replaces and supersedes the former GEN 1.3.(1). Acceptable Use of Computing Resources policy.

1. PURPOSE

The purpose of this policy is to establish parameters for the acceptable use of information technology resources owned or under the control of the University of Wisconsin System. This policy establishes the behaviors for acting in a responsible, ethical, and legal manner that respects the rights of community members who access or rely upon the information technology resources of the UW System, or who may have personal, confidential, private, proprietary, or copyrighted data and information stored within the UW System's information technology resources.

2. RESPONSIBLE OFFICER

UW Oshkosh Chief Information Officer

3. SCOPE

This policy covers all those who access information technology resources under the control of UW System institutions. These information technology resources include:

- Information technology assets and systems administered by UW System institutions
- Authorized and unauthorized information technology resources operated by others residing on UW System networks, off-site networks, or within cloud-based services
- Personally owned computers and devices used to access UW System information technology resources
- All devices that connect by wired or wireless connections to UW System networks.

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 technology environment in support of its mission. The UW System aims to afford broad access to information resources for university students, faculty, and staff for use in fulfilling the University's missions and for appropriate university related activities. Information technology resources support the research and instructional missions, as well as the administrative operations of the UW System. The access and use of these resources is a privilege granted to authorized individuals. These persons have access to valuable UW System resources that might include moderate or high risk data, as well as access to internal and external networks, systems, and data connected through the UW System's computing infrastructure.

5. DEFINITIONS

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. All individuals granted access to University of Wisconsin System information technology resources shall agree to and accept responsibility for:

    a. Using only the information technology resources for which they are authorized.

b. Utilizing appropriate authentication mechanisms to access information technology resource.

c. Not attempting to access information technology resources for which their authorization may be erroneous or inadvertent.

d. Only using accounts, passwords, and/or authentication credentials that they have been authorized to use consistent with their role at the UW System institution.

e. Protecting and not sharing their account, password, and/or authentication credentials.

f. Only sharing data with others as defined by applicable policies and procedures.

g. Not using UW System information technology resources to represent the interests of any non-University group or organization unless authorized by an appropriate University department or office.

h. Not using any hardware or software that is designed to assess or weaken security strength unless authorized by the institutional CIO or their designee(s).

i. Not engaging in disruptive "spamming" (i.e., sending unsolicited electronic communication to groups of recipients at the same time).

j. Not forging identities or sending anonymous messages unless the recipient has agreed to receive anonymous messages.

k. Only acting in a way that will not harm, damage, corrupt, or impede authorized access to information resources, systems, networks, equipment, and/or data.

l. Not using UW System information technology resources to alter, disrupt, or damage information technology resources of another person or entity.

m. Not using UW System information technology resources to upload, download or distribute copyrighted or illegal material that results in violation of law.

n. Complying with all licenses and contracts relative to information technology systems that are owned, leased, or subscribed to by the UW System.

o. Not using UW System information technology resources to sell or solicit sales for any goods, services, or contributions for commercial, political or non-university

activities unless such use conforms to UW System policies governing the use of University resources.

p. Complying with applicable local, state or federal laws, and institutional policies, rules, and guidelines as they relate to information technology resources.

2. Employees shall only access UW System information for purposes consistent with their status as employees.

3. Individuals may not use UW System resources to support the nomination of any person for political office or to influence a vote in any election or referendum.

4. Individuals may use UW System information technology resources for incidental use but shall use non-University sources, such as email, internet access, and other information technology services, for activities of an extensive nature that are not related to University purposes.

5. If an individual or group is determined to have violated this Acceptable Use 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

No specific procedures are associated with this policy.

9. REVISION HISTORY

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

APPROVED BY:

Chancellor Andrew Leavitt