

Board of Regents

REGENT POLICIES

Regent Policy Document 25-3 (formerly 97-2)

Acceptable Use of Information Technology Resources

Scope

This policy covers authorized users who access information technology (IT) resources under the control of the University of Wisconsin (UW) System including but not limited to: currently enrolled students; employees; authorized contractors, vendors, and guests; and other authorized users as determined by UW institutions.

Purpose

The purpose of this policy is to outline the expectations of the Board of Regents regarding the acceptable use of IT resources by authorized users and to establish the parameters for the use of IT resources.

Policy Statement

IT resources are essential tools in accomplishing the UW System's mission of disseminating and extending knowledge, fostering the free exchange of ideas, and providing effective support for teaching, research, and public service functions. It is the policy of the UW System Board of Regents that access to and use of UW System IT resources is a privilege that extends to authorized users for use in fulfilling the missions of the UW System and UW institutions, and for appropriate university-related activities.

UW System IT resources include all electronic equipment, facilities, technologies, and data used for information processing, transfer, storage, display, printing, and communications by the UW System and/or any UW institution. These include, but are not limited to, computer hardware and software, computer labs, classroom technologies such as computer-based instructional management systems, and computing and electronic communications devices and services, modems, email, networks, telephones, voicemail, facsimile transmissions, video, multi-function printing devices, mobile computer devices, data, multimedia and instructional materials. This definition also includes services that are owned, leased, operated, provided by, or otherwise connected to UW System resources, such as cloud computing or any other connected/hosted service provided.

Acceptable and Unacceptable Uses of Information Technology Resources

Acceptable use of UW System IT resources includes any purpose related to the direct and indirect support of the System's educational, research, service, student and campus life activities; administrative and business purposes; financial systems; and human resources administration. Authorized users are provided access to IT resources in order to support their studies, instruction, research, duties as employees, official business with the UW System and/or any UW System institution, and other university-sanctioned activities according to their roles and responsibilities.

Authorized users must not engage in unacceptable use of UW System IT resources, which includes but is not limited to the following:

1. Sharing or transferring authentication details to others, or using another user's authentication credentials such as network IDs and passwords, or other access codes or circumventing user authentication which could allow unauthorized users to gain access to UW System IT resources, except as required for administrative or business

purposes;

2. Violation of federal, state, or local laws; institutional policies, rules or guidelines; or licensing agreements or contracts;
3. Harassment of, threats to or defamation of others; creation of a hostile environment; stalking; and/or illegal discrimination;
4. Widespread dissemination of unauthorized email messages (e.g., mass mailings, spam, email chain letters); or
5. Intentionally damaging, disrupting, or exposing IT resources or data to unauthorized access or harm.

In addition to the examples stated above, unacceptable use of UW System IT resources for employees, authorized contractors and vendors, also includes the following:

6. Storage, display, transmission, or intentional or solicited receipt of material that is or may reasonably be regarded as obscene, sexually explicit, or pornographic, except as such access relates to bonafide, university-related academic or research pursuits or as needed to investigate violations of this policy or laws;
7. Outside employment, commercial activities, or other forms of private financial gain;
8. Campaigning for public office or soliciting political contributions;
9. Political lobbying, except for specific employees designated to lobby on behalf of a the UW System or one of its institutions;
10. Wagering or betting, except as it relates to bonafide, university-related academic or research pursuits;
11. More than minimal use for private or personal purposes that interferes with work or job performance or that interferes with the activities of other employees, students, or other authorized users.

Authorized users must not use UW System IT resources to speak on behalf of the UW System or use the UW System trademarks or logos without authorization. Affiliation with the UW System does not, by itself, imply authorization to speak on behalf of the UW System. The UW System is not responsible for the content of documents, exchanges or messages, including links to other information locations on the internet that reflect only the personal ideas, comments, and opinions of individual members of the university community, even when this content is published or otherwise circulated to the public at large by means of UW System IT resources.

Privacy and Security

The UW System shall take reasonable measures to protect the privacy of its IT resources and accounts assigned to authorized users. However, the UW System cannot guarantee absolute security and privacy. Any activity on UW System IT resources may be monitored, logged and reviewed by UW System-approved personnel or may be discovered in legal proceedings or in response to public records requests. Generally, the contents of user accounts will be treated as private and not examined or disclosed except:

- as required for system maintenance or business necessity, including security measures;
- when there exists reason to believe an individual is violating the law or UW System or institutional policy;
- to meet the requirements of the Wisconsin Public Records Law or other laws; regulations; or institutional policies, rules, or guidelines; or
- as permitted by applicable law or policy.

The UW System has the right to employ appropriate security measures, to investigate as needed, and to take necessary actions to protect UW System IT resources. The UW System may also have a duty to provide information relevant to ongoing investigations by law enforcement. UW institutions will work with authorized users to protect their privacy interests, as well as those of the UW System.

Authorized users must not violate the privacy of other users. Technical ability to access unauthorized resources or others' accounts does not by itself imply authorization to do so, and it is a violation of this policy to access others' accounts unless authorized to do so for a legitimate business purpose.

Other Limitations on Use of Information Technology Resources

In addition to the general principles set forth in this policy, the use of IT resources may be affected by other laws and policies; included among these are: federal copyright laws and privacy laws related to student records; state statutes related to computer crimes and political activities of state employees; ethical standards of conduct; dismissal for cause;

standards and disciplinary processes related to academic and nonacademic misconduct by students; and conduct on university lands.

Failure to Comply with Information Technology Resource Policies

Failure to adhere to the provisions of this policy may result in the suspension or loss of access to UW System IT resources; appropriate disciplinary action as provided under existing procedures applicable to students, faculty, and staff; civil action; or criminal prosecution. To preserve and protect the integrity of UW System IT resources, there may be circumstances where a UW institution may immediately suspend or deny access to the resources.

Oversight, Roles, and Responsibilities

This policy constitutes the UW System's policy on the acceptable use of IT resources. It applies systemwide and may not be replaced, superseded, or substantially recreated by other systemwide or institutional policies. Institutions may supplement this policy only for specific programs or services after consultation with the UW System Chief Information Officer. In order to assist members of the university community in fulfilling their responsibilities with respect to use of IT resources, each UW System institution shall post this policy on its website.

It is the responsibility of authorized users to comply with this policy.

The chancellor is responsible for implementing this policy and operating the institution's IT resources consistent with the above-stated provisions.

Related Regent Policies and Applicable Laws

- Family Educational Rights and Privacy Act (FERPA)
- Gramm-Leach-Bliley Act (GLBA)
- Federal Copyright Law
- Chapter 11, Wisconsin State Statutes, Campaign Financing
- Chapter 19, Subchapter II, Wisconsin State Statutes, Public Records and Property
- Section 943.70, Wisconsin State Statutes, Computer crimes.
- Chapter UWS 4 Wisconsin Administrative Code, Procedures for Dismissal
- Chapter UWS 7 Wisconsin Administrative Code, Dismissal of Faculty in Special Cases
- Chapter UWS 8 Wisconsin Administrative Code, Unclassified Staff Code of Ethics
- Chapter UWS 11 Wisconsin Administrative Code, Dismissal of Academic Staff for Cause
- Chapter UWS 14 Wisconsin Administrative Code, Student Academic Disciplinary Procedures
- Chapter UWS 17 Wisconsin Administrative Code, Student Nonacademic Disciplinary Procedures
- Chapter UWS 18 Wisconsin Administrative Code, Conduct on University Lands
- Chapter UWS 21 Wisconsin Administrative Code, Use of University Facilities
- Regent Policy Document 20-22, Code of Ethics
- Regent Policy Document 21-4, Identity Theft Detection, Prevention, and Mitigation
- Regent Policy Document 25-4, Strategic Planning and Large or High-Risk Projects
- Regent Policy Document 25-5, Information Technology: Information Security

History: Res. 7461, adopted 06/06/1997, created Regent Policy Document 97-2; subsequently renumbered 25-3; Res. 10950, adopted 10/06/2017, amended Regent Policy Document 25-3.

SEE ALSO:

UW System Human Resources Practice Directive WE A, *Use of Information Technology Resources* (<https://www.wisconsin.edu/ohrwd/practice-directives/use-of-information-technology-resources/>) (formerly WE 4)

SYS 1030: *Information Security: Authentication* (<https://www.wisconsin.edu/uw-policies/uw-system-administrative-policies/information-security-authentication/>)

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

SYS 1032: Information Security: Awareness (<https://www.wisconsin.edu/uw-policies/uw-system-administrative-policies/information-security-awareness/>)

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

[UW System Administrative policies are included for reference and are separate from Regent Policy Documents adopted by the Board.]

OFFICE OF THE BOARD OF REGENTS

1860 Van Hise Hall

1220 Linden Dr.

Madison, WI 53706

☎ [608.262.2324](tel:608.262.2324)

✉ board@wisconsin.edu