University of Western States provides computing and networking resources to university guests and constituents, to support the educational, instructional, clinical and administrative activities. This policy governs the allowable use of such resources. Individuals violating this policy may be subject restriction or revocation of access, and/or additional disciplinary actions including dismissal from an academic program, and/or termination of employment,

Scope

This policy applies to all users of university information systems and to all uses of resources, whether on campus or from remote locations. Information systems include all university owned, licensed or managed hardware and software, and use of the university network via a physical or wireless connection, regardless of the ownership of the computer or device connected to the network.

Additional policies or practices may govern use of specific computers, information systems or networks provided or operated by the university.

Acceptable Use

Acceptable use of university information systems:

- Is conducted by authorized users accessing only the computers, accounts and files for which they have authorization;
- Is for university-related purposes and activities;
- Is not intended for personal, political, commercial, financial or other gain;
- Does not disrupt operations; and
- Is not otherwise prohibited by this or other university policies.

Occasional personal use of university information systems is permitted when it does not consume a significant amount of resources, does not interfere with the performance of the user's job or other university responsibilities, does not promote or result in a hostile environment, and is otherwise in compliance with this policy. Additional limits may be imposed upon personal use in accordance with normal supervisory procedures concerning the use of university equipment.

To protect the integrity of university information systems, users are not permitted to engage in any activity that may be purposefully harmful to UWS data, systems or networks.

Required Trainings

Users of university information systems may be required to participate in mandatory trainings for cybersecurity awareness and best practices, and/or to meet regulatory requirements related to HIPAA, PCI-DSS, GLBA, FERPA or other relevant regulations. Additional trainings may be required for employees based on their access levels or roles within the organization, or based on need as demonstrated by past training performance results. Failure to participate in required trainings may lead to administrative sanctions applicable to the user.

User Responsibilities

Users are individually responsible for the appropriate use of all resources assigned to them, including any activity originating from their accounts, which they can reasonably be expected to control. Accounts and passwords may not, under any circumstances, be shared or used by persons other than those to whom they have been assigned by the university. In cases when unauthorized use of accounts or resources is detected or suspected, the account owner is required to immediately change their password and to report the incident to the department of technical services and their supervisor or instructor.

Users are responsible for complying with the provisions in this policy, including participating in required trainings.

Password Management
Users are required to comply with university-established password requirements.

Fair Share of Resources
University information systems are shared and limited, requiring that resources be utilized with consideration for others who also use them. The university may set limits on individual use of a resource through quotas, time limits or other mechanisms to ensure an acceptable level of performance and availability of resources.

Adherence with Laws, Regulations and Policies
While using university systems, users are required to comply with all applicable laws, university rules and policies, copyright laws and regulations, university requirements under FERPA and HIPAA, and the terms of applicable contracts, including software licenses. Refer to related policies as listed below for more information on university policy.

Users who engage in electronic communications with persons in other states or countries or on other systems or networks may also be subject to the laws of those jurisdictions and the rules and policies of those other systems and networks.

Privacy
Use of university information systems should not be considered private. Information contained on or communicated through university information systems is the sole property of the university. While the university does not routinely monitor individual usage of its information systems, the normal operation and maintenance of university systems requires the backup and caching of data and communications, the logging of activity, the monitoring of general usage patterns and other such activities that are necessary for the provision of service.

The university may also specifically monitor the activity and accounts of individual users of university information systems, including individual login sessions and the content of individual communications, without notice, when:

- The user has voluntarily made them accessible;
- It reasonably appears necessary, in the discretion of the vice president overseeing the involved department or the university president, to do so to protect the integrity, security or functionality of university or other systems, or to protect the university from liability;

- There is reasonable cause, in the discretion of the vice president overseeing the involved department or the university president, to believe that the user has violated or is violating this policy or other university polices or laws;
- An account appears, in the discretion of the vice president overseeing the involved department or the university president, to be engaged in unusual or unusually excessive activity; or
- It is otherwise required or permitted by law.

The university, in the discretion of the vice president overseeing the involved department or the university president, may disclose the results of any such general or individual monitoring, including the contents and records of individual communications or data files, to appropriate university personnel or law enforcement agencies and may use those results in applicable university disciplinary proceedings.

Communications made by means of university information systems are generally subject to the Oregon Public Records Law to the same extent as they would be if made on paper.

Acceptable Use Policy Violations
Users who violate this policy may be denied access to university information systems or resources and may be subject to other penalties and disciplinary action, including possible dismissal or termination. Alleged violations are addressed through the university disciplinary procedures applicable to the user.

The university may suspend, block or restrict access to an account, independent of such procedures, when it reasonably appears necessary, in the discretion of the vice president overseeing the involved department or the university president, to do so in order to protect the integrity, security or functionality of university information systems or to protect the university from liability. The university may also remove, without notice, any data, software or content that violates this policy or is interfering with normal operations.

The university may also refer suspected violations of applicable law to appropriate law enforcement agencies.

Related Policies: Policy 1004 Nondiscrimination and Anti-Harassment
Policy 1024 Copyright Violation
Policy 2503 Social Media
Policy 3602 Virtual Private Network (VPN) Access
Policy 3603 Student and Employee Access to Electronic Resources
Policy 3604 Electronic Mail (Email) Use
Policy 9001 Student Conduct
Policy 9009 Student Appeal

Keywords: access, communication, email, file, HIPAA, FERPA, network, privacy, social media, virtual

Policy 3601 Acceptable Use of Information Systems
Established: 03/10/1998
Revision History: 02/09/2021, 07/08/2019, 04/01/2014, 08/30/2012