Policy Concept Form

All policy proposals including new policy concepts, recommendations to revise, or requests to repeal must be submitted via this form to the University Secretary. The Secretary will forward completed concept forms to the President's Policy Advisory Council for consideration pursuant to I.03.01 Policy on University Policies. When submitting a policy concept form, please keep the following university definition of "policy" in mind:

> *A University Policy ("Policy") is a policy that (1) has broad application or impact throughout the University community, (2) must be implemented to ensure compliance with state or federal law, (3) is necessary to enhance the University's mission, to ensure institutional consistency and operational efficiency, or to mitigate institutional risks; or (4) is otherwise designated by the Board or the President as a University Policy subject to the Policy- Making Process authorized in section 4. A policy establishes rights, requirements or responsibilities. Excluded from this definition are things such as, but not limited to, implementation guides, operating guidelines, internal procedures, and similar management controls and tools.*

Name:	Will Laney
Email:	wlaney@uoregon.edu
Phone:	541-346-9700
University Affiliation:	Chief Information Security Officer

Policy Subject Matter (please included existing policy number(s) if available)

The University does have and Acceptable Use policy (https://it.uoregon.edu/acceptable-use-policy) and an Acceptable Use policy addendum (https://it.uoregon.edu/aup-addendum), but these were only Information Services policies and not University (capital P) Policies. This draft policy is not a redline from these existing unit-level policies due to the substantial nature of the revisions. A new draft was started from scratch. To view the existing unit-level policies, please see the links above

Statement of Need and Desired Result (please describe what we accomplish with the proposed action)

This will formalize (and greatly update) approved and not approved activities on University computers and devices connected to the University's network.

Affected Policy Stakeholders (please list all known impacted stakeholders and the nature of those impacts)

This policy will affect all individuals of the University who either use UO computers or connect to the UO network.

Proposed Action (i.e., new, revision, repeal)

Mostly new (as it was not really a University Policy) but you could also say revision.

University of Oregon
Acceptable Use Policy for Information Technology Resources

REASON FOR POLICY

This Policy establishes the acceptable use of computing and other technology resources and facilities ("IT resources") at the University of Oregon ("UO").

PERSONS AFFECTED BY THIS POLICY

All persons who use UO IT resources, including UO employees, students, contractors, vendors, guests, and any other user allowed access to UO IT resources.

WEBSITE ADDRESS FOR THIS POLICY

[XXXXXXXXXXXXXXX]

RESPONSIBLE OFFICE

For questions about this policy, please contact the Chief Information Security Officer at 541-346-9700 or ciso@uoregon.edu.

ENACTMENT & REVISION HISTORY

This Policy replaces the "UO Acceptable Use of Computing Resources Policy" (https://it.uoregon.edu/acceptable-use-policy). This Policy also replaces the "University of Oregon Acceptable Use of Computing Resources" Addendum (https://it.uoregon.edu/aup-addendum) to the Oregon Department of Administrative Services' Statewide Policy on Acceptable Use of State Electronic Information Systems (DAS 03-21), dated February 20, 1997.

POLICY

1.0 Overview

This policy is intended to further UO's educational, instructional, research, and administrative activities, and promote free and open inquiry and discussion, while acknowledging that UO IT resources are government property and therefore subject to certain restrictions. This policy is also intended to help ensure fair allocation of IT resources to avoid needless disruption.

Under ORS Chapter 352, UO is a government entity performing governmental functions and exercising governmental powers, and UO IT resources are UO property. Further, UO owns information stored on UO computer systems, such as email containing UO administrative data, communications pertaining to UO business, and other proprietary information.

In general, UO IT resources may be used only for UO business related activities. Furthermore, information related to UO business activities are subject to the Oregon Public Records Law and UO employees have no expectation of privacy in such information except as specifically recognized by law.

Incidental and limited personal use of UO IT resources by employees may be permitted if it is minimal, does not interfere with UO's or the employee's ability to carry out UO business, and does not violate terms of this policy, other UO policies, or applicable state and federal law.

Users of UO IT resources may have access to valuable UO resources, to sensitive data, and to internal and external networks. It is therefore essential that all users behave in a responsible, ethical, and legal manner.

2.0 Objective / Purpose

The purpose of this document is to outline acceptable uses of UO IT resources and to educate users about their individual legal and ethical responsibilities when using those resources.

This policy is not intended to preclude uses of UO IT resources that are specifically authorized by Collective Bargaining Agreements to which UO is a party.

3.0 Scope

This policy is directed to all UO employees, students, contractors, vendors, guests, and any other user with authorized access to UO IT resources. It applies to all users of UO IT resources and data, whether affiliated with the UO or not. It applies to all use of those resources and data, whether on campus, via cloud-based servers, or from remote locations (e.g., through a virtual private network or "VPN"), and covers all devices attached to UO's network, whether via a UO-owned computer or device or one personally owned by the individual.

4.0 Appropriate Uses

4.1 UO IT resources are provided for UO business-related purposes, including support for the UO's teaching, research, and public service missions, its administrative functions, and student and campus life activities.

4.2 Employees may make incidental personal use of UO IT resources in compliance with this Policy and other UO policies. Such use must be minimal, and cannot interfere with the fulfillment of that employee's job responsibilities or disrupt the work environment or the UO's ability to carry out UO business. Personal use that inaccurately creates the appearance that UO is endorsing, supporting, or affiliated with any organization, product, service, statement, or position is prohibited.

4.3 Students may make personal and academic use of personally owned computers using UO IT resources in compliance with this Policy and other UO policies.

5.0 Compliance with Federal and State Laws and UO Policies: All users of UO IT resources must:

5.1 Abide by all federal, state, and local laws, regulations, rules and UO policies, including but not limited to laws that preclude public resources from being used for political campaigning under ORS Chapter 260.432.

5.2 Abide by all software contracts and licenses applicable to their particular uses. The UO has entered into contracts for many of its software and network resources which require each individual using them to comply with those agreements.

5.3 Abide by federal copyright laws when using UO IT resources. Do not use, copy, or distribute copyrighted material unless you have a legal right to do so. The unauthorized use or publishing of copyrighted material with UO IT resources is prohibited, and users are personally liable for consequences stemming from such unauthorized use.

5.4 Refrain from using UO IT resources for commercial purposes or any other private financial gain, except as authorized in writing pursuant to UO's conflict of interest and outside employment policies

5.5. Refrain from using electronic mail systems for broadcasting any unsolicited email or for any purpose prohibited by federal or state law.

6.0 Policy Requirements: All users of UO IT resources:

6.1 Shall not use UO IT resources without proper authorization. All users must use only those IT resources that they are authorized to use and use them only in the manner and to the extent authorized.

6.2 Shall not use UO IT resources to attempt unauthorized use, or from assisting in, encouraging, or concealing from authorities any unauthorized use (or attempt at such use), or to willfully interfere with other individuals' authorized uses of any UO computer or network facility.

6.3 Shall not endanger or circumvent the security or security mechanism of any UO IT resource. All users must also refrain from any attempt to degrade system performance or capability, damage systems or intellectual property of others. Users shall not create, install, or knowingly distribute a malicious program that interferes with the confidentiality, integrity or availability of data on any computer or network facility.

6.4 Shall not connect any device to any of UO's IT resources (including but not limited to its networks) unless the device meets technical and security standards set by UO procedures.

6.5 Must fairly utilize shared IT resources in accordance with Unit policies and/or procedures set for the computers involved and cooperate fully with the other users of the same equipment.

6.6 Shall not use UO IT resources to transmit any communications that reasonably could be considered obscene, harassing, threatening or discriminatory by the recipient or another viewer. For more information on UO policies in this area, see the Office of Affirmative Action & Equal Opportunity web site.

6.7 Shall not share a password for any UO IT resource or use another person's password. This includes unauthorized viewing, use, alteration or deletion of another person's computer files, programs, and accounts, or electronic records. Access to such information does not imply permission to view or use it. Users are responsible for ascertaining what authorizations are necessary and for obtaining them before proceeding. For more information, please see the Electronic Records Access Procedure.

6.8 Shall not misrepresent their identity or relationship to the UO when requesting access to or using UO IT resources. Furthermore, no user shall hold themselves out as an official representative of UO, speaking on its behalf, unless that person has been authorized by the UO administration to do so. In circumstances where a reasonable observer might become confused and believe that the speaker is presenting an official UO position, when in fact the content or opinion expressed or displayed is personal, the speaker or writer shall include an appropriate disclaimer clarifying the status of their comments, presentation, or display.

6.9 Shall not modify or reconfigure any UO-owned computer or any devices connected to the UO network facility without proper authorization.

6.10 Users shall take full responsibility for UO data that they store on computers and transmit through network facilities. No one shall use computers or network facilities to store, share, or transmit UO data in ways that are prohibited by law or UO policy. More information on how data is classified at UO can be found in the Data Classification Policy.

6.11 Those who publish web pages on UO owned or administered IT resources shall take full responsibility for what they publish and shall respect the acceptable use conditions for the computer or resource on which the material resides. References and links to commercial sites are permitted, but advertisements, and especially paid advertisements, are not. Users shall not accept payments, discounts, free merchandise or services, or any other remuneration in return for placing anything on their web pages or similar information resources.

6.12 Users of UO IT resources shall comply with the regulations and policies of UO-hosted mailing lists, social media sites, and other public forums.

6.13 System administrators shall refer all disciplinary and legal matters to appropriate authorities.

6.14 Email and other electronic messaging technologies are intended for communication between individuals and clearly identified groups of interested individuals, not for mass broadcasting. (For more information, see Guidelines for Official Mass Email.) UO reserves the right to discard incoming mass mailings, malware, and spam without notifying the sender or intended recipient. UO also reserves the right to block communications from sites or systems that are involved in extensive spamming or other disruptive practices.

6.15 No individual or group may establish or extend network connectivity without prior authorization and discussion with the Information Services Network team.

6.16 As a general matter, UO does not monitor individual usage. However, users should be aware that their uses of UO IT resources are not private. Furthermore, records created, owned, used or retained that relate to the conduct of the public's business are subject to the Oregon Public Records Law. UO reserves the right to monitor the normal operation and maintenance of all IT resources including backup, logging of activity, general usage patterns, and other activities as necessary to evaluate and maintain information security, efficiency, and delivery of service.

7.0 Enforcement and Implementation

7.1 Roles and Responsibilities

Each UO employee and department/unit is responsible for complying with this policy. The Office of the Chief Information Security Officer is responsible for enforcing this policy, and is authorized to create technical and security standards for UO IT resources and protection standards for information stored or transmitted by UO IT resources.

7.2 Consequences of Noncompliance

Violations of this policy may result in the same types of disciplinary measures and consequences as violations of other UO policies, in accordance with applicable UO policies, procedures, and Collective Bargaining Agreements, or, with respect to students, the Student Conduct Code. In some cases, violations of this policy may also constitute violations of state and federal laws, and consequences may include criminal prosecution.

Systems and accounts that are found to be in violation of this policy may be removed from the UO network, disabled, etc., by the Unit or Information Services as appropriate until the systems or accounts comply with this policy.

8.0 Definitions

UO IT Resources – all computers (including but not limited to servers, desktops, laptops, phones, and any networked device that provides computational services) owned or administered by any part of the UO or connected to the UO's communication facilities, including departmental computers, cloud-based services, and all of the UO's computer network facility accessed by anyone remotely (such as using a VPN).

Proper Authorization – permission granted by technical staff after consulting managerial staff and the terms of this Policy. For unit-level issues, this would include authorization by IT Professional staff, after consulting management in the unit. For campus-wide issues this would be authorization by Information Services.