

Policy Title:	Computing Resources Acceptable Use Policy
---------------	---

Governing Body:	Finance and Administration	Policy Number:	FAD.038
Policy Contact:	Chief Information Officer	Date Revised:	06/16/2016
Custodial Office:	Information Technology	Date Approved:	
Approved By:	President/Cabinet	Next Review:	
Related Policy:	SOU Information Security Policy FAD.040		

### Revision History

Revision Number:	Change:	Date:
1.1	Update to template format, significant changes	6/3/2013
1.2	Template update, removal of OUS references	6/16/2016

### A. Purpose

This acceptable use policy governs the use of computing, networking, and information resources at Southern Oregon University.

### B. Policy Statement

<p><b>1. Terms and Conditions for Use</b></p> <p>Southern Oregon University provides computing, information, and networking resources to the university community of students, faculty, and staff in support of the university's mission. All use of these resources shall be in a legal, ethical, and responsible manner. Users must respect the rights of other users, respect the integrity of the systems and related physical resources, and observe all relevant laws, regulations, and contractual obligations. Any other uses, including uses that jeopardize the integrity of the network, the privacy or safety of other users, or that are otherwise illegal, are prohibited.</p> <p>The primary purpose of electronic systems and communications resources is for university-related activities only.</p> <p>Users do not own accounts on university computers, but are granted the privilege of exclusive use. Users may not share their accounts with others, and must keep account passwords confidential.</p> <p>Users must adhere strictly to licensing agreements and copyright laws that govern all material accessed or stored using university computers and networks or university-contracted services.</p> <p><b>2. Applicability</b></p>
--

This policy applies to all users of university computing, information, and network resources, whether affiliated with Southern Oregon University or not, and to all uses of those resources, whether on campus or from remote locations.

When accessing remote systems from SOU systems or network, users are responsible for obeying the policies set forth herein as well as the policies of other organizations.

### **3. Prohibitions**

Conduct which violates this policy includes, but is not limited to the following:

- Accessing confidential information about a person (such as their educational records) without their consent or other authorization.
- Knowingly running or installing on any computer system or network, or giving to another user, a program intended to damage or to place excessive load on a computer system or network.
- Masking or forging the identity of an account, individual, or machine.
- Participating in any activities that violate existing federal and state laws, university regulations and policies or terms and conditions for specific electronic services, databases, etc. accessible through the Southern Oregon University or Oregon University System networks.
- Unauthorized interception or diversion of network transmissions.
- Using a computer account that you are not authorized to use. Obtaining a password for a computer account other than your own, or giving your password to anyone else.
- Using network and computing to gain unauthorized access to any computer system or exploit security flaws.
- Using university resources for commercial activity such as creating products or services for sale.
- Violating copyright laws or software licensing agreements and their fair use provisions through inappropriate reproduction, dissemination, or use of peer to peer technologies to obtain or disseminate copyrighted text, images, music, video, or other copyrighted material.

### **4. Security and Privacy**

Southern Oregon University employs various measures to protect the security of its computing, information, and networking resources. Users should be aware that their uses of university computer and network resources are not private. While the university does not routinely monitor individual usage, the normal operation and maintenance of the university's computing resources require backup, logging of activity, the monitoring of general and individual usage patterns, and other activities that are necessary for information security and the provision of service. In addition, the university reserves the right to review, monitor and/or capture any content residing on, or transmitted over, its computers or network at its sole discretion. The university reserves the right to limit access to its computers or network, and to remove or limit access to material residing on its computers or network.

### **5. Enforcement**

Violation of these policies will be reported to the appropriate area for possible disciplinary action. An individual's access to computer resources may be suspended immediately upon the discovery of a possible violation of these policies. Penalties may be imposed under one or more of the following: Southern Oregon University regulations, Oregon law, or the laws of the United States.

This policy may be revised at any time without notice. All revisions supersede prior policy and are effective immediately upon approval.

C. Policy Consultation

Business Affairs Council, Tech Council, Provost's Advisory Council

D. Other Information

Replace this sentence with other information

The Policy Contact, defined above, will write and maintain the procedures related to this policy and these procedures will be made available within the Custodial Office.