Policy Title:	Acceptable Use of Information Technology Resources Policy

Governing Body:	Finance and Administration	Policy Number:	FAD.038
Policy Contact:	Chief Information Officer	Date Revised:	
Custodial Office:	Information Technology	Date Approved:	
Approved By:		Next Review:	
Related Policy:	Updates FAD.038 and renames it from “Computing Resources Acceptable Use Policy”		

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
1.3	Significant rewrite, renamed from “Computing Resources Acceptable Use Policy” to “Acceptable Use of Information Technology Resources Policy”	Pending

A. Purpose

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

B. Definitions

- **Information Resources:** All computing, networking, and information resources at Southern Oregon University, including data.
- **User(s):** A user is any agent or entity who engages with SOU’s information resources. This definition is not limited to persons and explicitly includes programmatic agents (e.g. computer programs, scripts) and artificially intelligent agents.
- **Authorization:** Authorization refers to the formal permission granted to you to work with an Information Resource. Authorization is granted by someone with authority over the Information Resources included within the scope of your authorization. Authorization also includes the scope of what you are permitted to do with those Information Resources you are permitted to access. Authorization can be revoked. Exceeding your authorization to interact with an Information Resource is a violation of this policy. If you get permission ahead of time from the appropriate authority, the scope of your authorization is expanded to include those new permissions, so it’s not a violation.
- **Data Owner:** A data owner is a person in charge of a piece of information. They are authorized by the

University President to establish a classification for that information (public, sensitive, etc.) and to control who has access to it.

C. Policy Statement

1. Terms and Conditions for Use

Southern Oregon University provides information resources to the university community of students, faculty, staff, vendors, affiliates, and guests in support of the university's mission. Users of SOU's information resources shall use the resources supplied to them 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.

The primary purpose of Southern Oregon University's information resources is for business and academic activities that support the mission of the university. Usage of SOU's information resources beyond the scope of the mission of the university may be subject to review and curtailment and may result in disciplinary consequences.

Users do not own the accounts they use to access SOU's information resources. Accounts issued to users are intended to be for the exclusive use of a single person unless the Information Technology Department has explicitly indicated otherwise. Users must not share their account credentials (passwords or other authentication factors) with persons not authorized to have access to the credentials by the Information Technology Department. Users have a responsibility to keep their account credentials secure and confidential. The Information Technology department may immediately and without notice suspend accounts that are suspected or known to be in violation of this policy. See the Enforcement section of this policy.

Users must adhere strictly to licensing agreements and copyright laws that govern all material accessed or stored using SOU's information resources.

2. Applicability

This policy applies to all users of SOU's information resources, whether affiliated with Southern Oregon University or not, and to all uses of those resources regardless of the user's location at the time of use.

When accessing information resources (systems, networks, and data) belonging to other organizations from SOU's systems or networks, users are responsible for obeying the policies set forth herein for acceptable use plus any policies governing the use of the other organization's information resources.

3. Prohibitions

Conduct which violates Southern Oregon University's codes of conduct also violates this policy to the extent the conduct involves SOU's Information Resources. Conduct which breaks the law or other university policies, such as committing fraud or falsifying records, violates this policy to the extent the conduct involves SOU's Information Resources. For more examples of specific conduct which violates our acceptable use policy, reference the Acceptable Use of Information Technology Resources Supplemental Standard. Conduct which violates this policy includes, but is not limited to, the activities listed below.

- Accessing confidential, protected, or private information about a person with a relationship to Southern Oregon University (such as their educational records) without their consent, without authorization from an appropriate data owner (see definitions), or outside of your job duties which require you to access the information. The handling of such information, when it is authorized, must comply with SOU's Privacy Policy and Data Handling Policy and must only occur when a legitimate need to know exists. For example, an employee may have access to look up a student's biographical and contact information to perform their job duties, but using that access to look up a favorite student's birthday, phone number, or home address outside of their job duties would violate this policy, even if the employee had the best of intentions.

- Knowingly running or installing on any computer system or network, or giving to another user, a program intended to damage or otherwise violate the confidentiality, integrity, or availability of SOU's information resources.
- Masking, spoofing, forging, borrowing, or lending an identity used to interact with any information resource without formal authorization from SOU's Chief Information Officer or the Information Security Manager.
- Participating in any activities that violate existing federal and state laws, university regulations and policies or terms and conditions for specific systems or services while using SOU's information resources.
- Unauthorized interception or modification of information transmissions originating from SOU's information resources, destined for SOU's information resources, or using SOU's information resources.
- Accessing SOU information resources without authorization, or outside of your job duties, or aiding and abetting another person in accessing SOU's information resources in violation of this policy.
- Using SOU's information resources to violate the confidentiality, integrity, or availability of other organizations' information resources. Examples include gaining unauthorized access, making unauthorized modifications, and denying services.
- Attempting to violate the confidentiality, integrity, or availability of SOU's information resources by any means without the explicit consent of Southern Oregon University. This includes, but is not limited to, the following behaviors: 1) Mapping SOU's networks and systems, 2) Scanning SOU's networks and systems for vulnerabilities, 3) Attempting to circumvent security controls, 4) Attempting to steal credentials or identities, 5) All attempts to gain unauthorized access to SOU's information resources.
- Using university resources for commercial activity or personal financial gain such as creating products or services for sale, mining cryptocurrency, or selling access to SOU information resources to unauthorized parties.
- Violating copyright laws or software licensing agreements and their fair use provisions through inappropriate reproduction, dissemination, or use of peer-to-peer (P2P) technologies to obtain or disseminate copyrighted materials or another person's intellectual property.

4. Enforcement

Violations of this acceptable use policy will be reported to the appropriate oversight personnel for possible disciplinary action and may also be reported to law enforcement depending on the nature of the violation. An individual's access to SOU's information resources may be suspended immediately and indefinitely 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 of America.

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

D. Policy Consultation

E. Other Information

For more examples of prohibited behaviors, see Acceptable Use of Information Technology Resources Supplemental Standard.

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.