

Acceptable Use of Computing Resources

1. Policy Statement

- 1.1. Oregon State University (“university”) is committed to a respectful, safe, and ethical environment. This policy defines the expectations for user’s behavior and use of the university’s computing environment and resources.

2. Reason for Policy

- 2.1. To assure the appropriate use of the university’s computing infrastructure and resources. This policy establishes responsibilities and limitations associated with the use of the university computing environment.

3. Scope & Audience

- 3.1. This policy applies to all academic, research, and administrative departments and offices at all Oregon State University locations; all university faculty, staff, students, visitors, contractors and affiliates; and all resources, systems, infrastructure, devices, facilities and applications in the university’s computing portfolio, whether located on university property or accessed remotely.

4. Definitions

- 4.1. **Computing Resources:** The network and communications infrastructure, facilities, devices, applications, and systems owned and/or provided by the university.
- 4.2. **Information Technology Security Governance Council:** A committee charged with reviewing and recommending IT security policy. The Council is appointed by the Vice Provost for Information Services.

5. Responsibilities & Procedures

5.1. Acceptable use of university computing resources

- 5.1.1. Computing resources are the property of the university and shall be used for legitimate university instructional, research, administrative, public service, and approved contract purposes.
- 5.1.2. Minimal personal use of computing resources may be permitted if it does not interfere with the university's or the employee's ability to carry out university business, and does not violate the terms of this policy.
- 5.1.3. The use of university computing resources is subject to the generally accepted tenets of legal and ethical behavior within the university community. The standards of behavior expected of community members extend to the virtual environment as well.
- 5.1.4. All users of university computing resources must:
 - a. Comply with all federal, state and other applicable laws; all applicable university rules and policies; and all applicable contracts and licenses. Users are responsible for ascertaining, understanding, and complying with the laws, rules, policies, contracts, and licenses applicable to their particular uses.
 - b. Use only those computing resources they are authorized to use and use them only in the manner and to the extent authorized.
 - c. Keep account credentials, including passwords, confidential. Accounts and credentials may not, under any circumstances, be shared with or used by persons other than the individual(s) to whom they have been assigned by the university.
 - d. Refrain from unauthorized viewing or use of another person's computer files, programs, accounts, or data.
 - e. Refrain from unauthorized attempts to circumvent the security mechanisms of any university system.
 - f. Refrain from attempts to degrade system performance or capability, or attempts to damage systems, software or intellectual property of others.
 - g. Refrain from using university computing resources for commercial purposes unrelated to the university, except as specifically authorized.
 - h. When using university computing resources to access non-university resources, observe the acceptable use policies of those non-university organizations.

- i. Abide by federal copyright laws when using university computing resources for the use of or the copying of copyrighted material.
- j. Abide by their supervisor's direction regarding permitted personal use of university computing resources, if any.

5.2. Privacy

- 5.2.1. It is the practice of the university not to monitor individual usage of computing resources unless there is a legitimate business reason to do so. However, employees do not have an expectation of privacy in university computing resources.
- 5.2.2. The university reserves the right to monitor and record the usage of university computing resources as necessary to evaluate and maintain system efficiency and security. The university may further monitor and record the usage of individuals, including the disclosure of individual files when:
 - a. It has reason to believe that activities are taking place contrary to this policy, or state or federal law;
 - b. Necessary to respond to a court order, subpoena, to assist law enforcement, or in response to a request from a federal or state oversight agency;
 - c. Necessary to respond to a request for discovery in the course of litigation; or,
 - d. A legitimate business reason exists.
- 5.2.3. Monitoring will be undertaken only with authorization from the appropriate university personnel.
- 5.2.4. The university may use information gained in this manner in disciplinary or criminal proceedings.

5.3. Enforcement

- 5.3.1. Violations of this policy may result in:
 - a. Removal of content;
 - b. Denial of access to university computing resources;
 - c. Disciplinary actions and/or criminal and civil penalties; or,
 - d. Referral to appropriate law enforcement agencies.

5.3.2. The university may immediately suspend or block access to an account when it appears necessary to do so in order to protect the integrity, security, or functionality of university or other computing resources, or to protect the university from liability.

5.4. Exceptions

5.4.1. Exceptions to this policy must be approved by the Vice Provost for Information Services.

6. Forms & Tools

6.1. None.

7. Frequently Asked Questions

7.1. None.

8. Related Information

8.1. None.

9. History

9.1. Last review date: July 2016.

9.2. Next scheduled review date: July 2019.

10. Website

10.1. http://leadership.oregonstate.edu/sites/leadership.oregonstate.edu/files/08-005_acceptable_use_of_computing_resources.pdf

11. Contacts

Department	Phone Number	Website
Office of Information Security	541-737-3474	http://is.oregonstate.edu/ois