Policy Number: **11-20-010**

Policy Title: **ACCEPTABLE USE OF COMPUTING AND TELECOMMUNICATIONS RESOURCES**

Effective Date: **July 18, 2014**

1. Applicability

This policy applies to all users of OHSU computing, telecommunications and wireless resources, including but not limited to computers, computer systems, networks, portable digital assistants (PDAs), telephones, pagers, cellular phones, smart phones, electronic tablets, wireless cards, and two-way radios, whether affiliated with OHSU or not, and to all uses of those resources, whether on campus or from remote locations. These resources are hereinafter referred to as "Computing and Telecommunications Resources." Additional guidelines or directives may be established by OHSU to apply to specific computers, computer systems, networks, or applications.

2. Requirements

A. Legal

A user of Computing and Telecommunications Resources shall comply with all federal, Oregon, and other applicable laws; all applicable OHSU rules and policies; and all applicable contracts and licenses. Examples of such laws, rules, policies, contracts, and licenses include, but are not limited to, the laws of libel, privacy, copyright, trademark, and child pornography; the Electronic Communications Privacy Act and the Computer Fraud and Abuse Act, which prohibit "hacking", "cracking", and similar activities; Federal Communication Commission regulations; applicable Internal Revenue Service Regulations; the OHSU's Code of Conduct; the OHSU's sexual harassment policy; and all applicable software licenses. Users who engage in communications with persons in other states or countries or on other systems or networks should be aware that they may also be subject to the laws of those other states and countries and the rules and policies of those other systems and networks. Users are responsible for ascertaining, understanding, and complying with the laws, rules, policies, contracts, and licenses applicable to their particular uses.

B. Authorized

A user of Computing and Telecommunications Resources shall use only those resources that they are authorized to use and use them only in the manner and to the extent authorized. Ability to access computing resources does not, by

itself, imply authorization to do so.

Users are responsible for ascertaining what authorizations are necessary and for obtaining them before accessing any computing resource. Accounts and passwords may not, under any circumstances, be shared with, or used by, persons other than those to whom they have been assigned by OHSU.

A user of Computing and Telecommunications Resources shall respect the privacy of other users and their accounts, regardless of whether those accounts are securely protected. The ability to access other persons' accounts does not, by itself, imply authorization to do so.

C. **Reasonable**

A user of Computing and Telecommunications Resources shall respect the finite capacity of those resources (including, for example, bandwidth, disk space and CPU time) and limit use so as not to consume an unreasonable amount of those resources or to interfere unreasonably with the activity of other users.

D. **Personal**

A user of Computing and Telecommunications Resources shall not use those resources for personal commercial purposes or for personal financial or other gain, except as may be authorized under the OHSU Integrity Office policy for Management of Outside Activities or institution established news groups.

Incidental personal use of Computing and Telecommunications Resources for other purposes is permitted when the use:

(1) does not unreasonably consume those resources;

(2) does not interfere with the performance of the user's job or other OHSU responsibilities;

(3) does not consume an unreasonable amount of the user's time;

(4) does not concern subjects inappropriate in a work or study environment (e.g. accessing pornographic web sites);

(5) does not result in unauthorized use or disclosure of confidential OHSU information, including protected health information, through use of electronic media such as blogs, podcasts, discussion forums and other social media;

(6) is consistent with OHSU's mission of healthcare, education, research and community service; and

(7) is otherwise in compliance with this and other OHSU policies including requirements to reimburse OHSU where required under Policy 03-25-080.

Further limits may be imposed upon personal use in accordance with normal supervisory responsibilities.

E. **E-Mail and OHSU Communications**

All email communication containing OHSU "restricted" information (as defined in Information Security Directive 700-00001) must be generated and stored using OHSU.EDU or other OHSU approved email systems.

Communications over the e-mail system shall be professional and appropriate for the workplace or group setting. E-mail may not be used for personal solicitations or advertising or other activities except through OHSU provided electronic news group systems for those types of activities. Propagation of chain letters is specifically prohibited.

Falsifying e-mail headers (e.g. providing a false sender's address) or routing information so as to obscure the origins of mail or mail routes is forbidden. Altering the content of a message attributed to another is not permitted unless the changes are explicitly noted.

Announcements, bulletins, and documents deemed by management to be of value and interest to the well-being of employees and students are an integral part of the system. All broadcast e-mail (unsolicited messages sent to more than 50 OHSU addresses across departments) must be submitted and approved by Strategic Communications, except:

(1) as otherwise authorized by collective bargaining agreements;

(2) as otherwise authorized by Strategic Communications;

(3) as deemed necessary by the leader or executive sponsor of individual OHSU units or OHSU-chartered groups for the purpose of communicating with their constituencies;

(4) as otherwise provided for in the Emergency Preparedness policy, 01-40-001.

In all cases, messages of a strategic nature should be developed in collaboration with Strategic Communications.

F. **Representing OHSU**

A user of Computing and Telecommunications Resources shall not state or imply that they speak on behalf of OHSU or use OHSU trademarks and logos without authorization to do so. Affiliation with OHSU does not, by itself, imply authorization to speak on behalf of OHSU. Authorization to use OHSU trademarks and logos on Computing and Telecommunications Resources may be

granted only by the Strategic Communications Department. The use of appropriate disclaimers is encouraged.

3. **Security**

OHSU employs various measures to protect the security of its Computing and Telecommunications Resources and of their users' accounts. Users must comply with OHSU Information Security Policies and Directives and OHSU Information Security Guidelines. Users must engage in applicable "safe" practices, for example, by establishing appropriate access restrictions for their accounts, keeping the network virus-free, safeguarding passwords, ensuring proper physical safeguards, and protecting the confidentiality of electronic protected health information. In addition to the policies, directives, and guidelines referenced in this policy, users of telecommunications resources such as personal digital assistants (PDAs), smart phones, electronic tablets, or similar personal devices who are using a personal device for business purposes must comply with the security policies outlined in OHSU Managed PDA Security Policy and Information Security Directive ISD-700-00011 (wipe personal unit) and all the terms and conditions outlined in underlying ITG terms and conditions. See applicable information security policies and directives at www.ohsu.edu/xd/about/services/integrity/policies/ips-policies-by-category.cfm. All users must follow the Confidentiality of Health Information policy, 01-05-012, and only use encrypted OHSU owned or encrypted OHSU approved personally-owned electronic media to access electronic protected health information, unless an OHSU approved exception is in place.

4. **Expectation of Privacy**

A. **Generally**

Computing and Telecommunications Resources are not private. For example, communications made by means of these resources are subject to Oregon's Public Records Law to the same extent as they would be if made on paper. The normal operation and maintenance of Computing and Telecommunications Resources require 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 rendition of service.

B. **Reason to Access Activity**

In addition, OHSU may access or monitor the activity and accounts of individual users of Computing and Telecommunications Resources, including individual log in sessions and communications, without notice, when:

(1) The user has voluntarily made them accessible to the public, as by posting to Usenet or a web page;

(2) It is necessary for OHSU work and business-related reasons (e.g. a person is on vacation or sick leave and access to some files is needed to further

institution business);

(3) It reasonably appears necessary to do so to protect the integrity, confidentiality, availability, or functioning of OHSU generally or Computing and Telecommunications Resources in particular, or to protect OHSU from liability;

(4) There is reasonable cause to believe that the user has violated, or is violating, OHSU policy;

(5) There is reasonable cause to believe that the user is engaging in unlawful activity;

(6) An account appears to be engaged in unusual or unusually excessive activity, as indicated by the monitoring of general activity and usage patterns; or

(7) It is otherwise required by law.

Any such access or individual monitoring, other than that specified in 4.A. and B.(1) above, required by law, or necessary to respond to perceived emergency situations, must be authorized in advance by three of the following individuals: Human Resources Director, Legal Counsel, Chief Information Officer, and Information Security Officer. The head of the unit which employs the individual will be notified of such access when appropriate. OHSU, at its discretion but subject to any applicable laws, may disclose the results of any access or monitoring, including the contents and records of individual communications, to appropriate OHSU personnel or law enforcement agencies and may use those results in OHSU disciplinary proceedings and/or legal proceedings.

C. **Monitoring as a Job or Service Requirement**

OHSU may also authorize access and monitoring of an employee's or agent's actual communications over its Computing and Telecommunications Resources where customer service is a primary responsibility of an employee's job duties. Such monitoring must be authorized by the Human Resources Director and employees in positions subject to monitoring shall be notified of such activity.

5. **Remote Access to OHSU Computing Resources**

A. OHSU employees and students may be authorized secure remote access to information assets owned by or in custody of OHSU. Remote access may be granted by the department director or other appropriate authorizing authority where appropriate to fulfill a person's work or other responsibilities.

B. Remote access for contractors, business partners, referring physicians, other health care providers or other approved users with significant business justification may be approved on a case-by-case basis by an appropriate

authorizing authority.

C. Applicants for remote access must submit the OHSU Remote Access form. Information technology support vendors may also be granted remote access for system and application maintenance as negotiated in the support contracts.

D. Noncompliance with the requirements of a remote access authorization or with other provisions of this policy, as determined by the authorizing authority, may result in immediate loss of access privileges and possible corrective or legal action against the violator without notification.

6. **Enforcement**

Users who violate this policy may be denied access to Computing and Telecommunications resources and may be subject to other penalties and disciplinary action, both within and outside of OHSU, including any actions authorized by security policies or any policy applicable to personal devices. Violations will normally be handled through OHSU procedures applicable to the relevant user. However, OHSU may temporarily suspend or block access to an account, prior to the initiation or completion of such procedures, when it reasonably appears necessary to do so to protect the integrity, confidentiality, or availability of OHSU or other computing resources or to protect OHSU from liability.

Related Policies and Procedures:

Policy 01-05-010, Confidentiality
Policy 01-05-012, Confidentiality of Health Information
Policy 01-40-001, Emergency Preparedness
Policy 03-25-080, Employee Discounts and Personal Use of Institutional Resources
OIO Policy, Management of Outside Activities
ISD-700-00001, Information Security Rules
ISD-700-00006, Secure Storage of Electronic Restricted Information
ISD-700-00011, Computing Device & Electronic Media Reuse and Disposal
ISD 700-00012, Physical Safeguards for Computing Devices and Electronic Media
ISD 700-00013, Emergency Access to User Accounts and Files
ISD 700-00019, Information System Security Baselines

Related Forms: **OHSU Computer Access Form**
Service Observation (Quality Monitoring) Form

Implementation Date: June 23, 1998

Revision History: March 1, 2001; August 8, 2001; January 10, 2006; January 13, 2009; October 22, 2010; August 1, 2011; June 13, 2013; July 18, 2014

Responsible Office: OHSU Integrity Office