Appropriate Use of Digital Technology Resources	**6-001** **INFORMATION TECHNOLOGIES** **August 2013**

POLICY

Scope and Applicability

1.01 As an institution of higher learning, OSU Institute of Technology (OSUIT) encourages, supports, and protects freedom of expression and an open environment to pursue scholarly inquiry and to share information. Access to networked information resources in general and to the Internet, in particular, supports the academic community by providing a link to electronic information in a variety of formats and covering all academic disciplines. Consistent with other university policies, this policy is intended to respect the rights and obligations of academic freedom while protecting the rights of others. The computing and network facilities of the university are limited and should be used wisely and carefully with consideration for the needs of others. As with any resource, it is possible to misuse computing resources and facilities and to abuse access to the Internet. The university defines digital technology as any device with a microprocessor that reads, views, transmits or stores information (data) on digital media or accesses networked resources. Examples include, but are not limited to, mobile devices such as cell phones, iPods, iPads, Androids, desktops, servers, laptops, tablets, switches, routers, wireless access points, and many networked appliances. The following statements address, in general terms, the university's philosophy about digital technology use.

1.02 This policy is applicable to all individuals using university owned or controlled digital technology facilities or equipment, whether such persons are students, staff, faculty, or authorized third party users of university digital technology information resources. It is applicable to all university information resources whether individually controlled or shared, stand alone or networked. It applies to all digital technology equipment and facilities owned, leased, operated, or contracted by the university. It applies to personally owned devices connected to the university network. This includes, but is not limited to, software, cloud resources, and email accounts, regardless of whether used for administration, research, teaching, or other purposes. A user must be specifically authorized to use a particular digital technology or network resource.

1.03 Individual units within the university may define conditions of use for information resources under their control. These statements must be consistent with this overall policy but may provide additional detail, guidelines and/or restrictions. Such policies may not relax or subtract from this policy. Where such conditions of use exist, enforcement mechanisms defined therein shall apply. These individual units are responsible for publicizing both the regulations they establish and their policies

concerning the authorized and appropriate use of the digital technology for which they are responsible. In such cases, the unit leader shall provide the Executive Vice President with a copy of such supplementary policies prior to implementation thereof. Where use of external networks is involved, policies governing such use also are applicable and must be adhered to.

User Responsibilities and Expectations

2.01 Access to the digital technology infrastructure both within and beyond the university campus including cloud services, sharing of information, and security of the intellectual products of the community all require that each and every user accept responsibility to protect the rights of the community. Access to the networks and to the digital technology resources at OSUIT is a privilege granted to university students, faculty, staff, and third parties who have been granted special permission to use such facilities. Access to university digital technology resources must take into account the following factors: relevant laws and contractual obligations, the requestor's need to know, the information's sensitivity, and the risk of damage to or loss by the university.

2.02 Anyone who accesses, uses, deletes, destroys, alters, or damages university information resources, properties or facilities without authorization, may be guilty of violating state or federal law, infringing upon the privacy of others, injuring or misappropriating the work produced and records maintained by others, and/or threatening the integrity of information kept within these systems. Such conduct is unethical and unacceptable and will subject violators of this policy to disciplinary action by the university, including possible separation from employment, suspension as a student, and/or loss of information systems privileges.

2.03 The university requires members of its community act in accordance with these responsibilities, this policy, the university's student or employee handbook, as appropriate, OSU System policies and procedures, relevant laws and contractual obligations, and the highest standard of ethics. The policies as stated in this policy are intended to ensure that users of university information resources shall:

- respect software copyrights and licenses
- respect the integrity of digital technology information resources
- refrain from seeking to gain unauthorized access
- respect the privacy of other digital technology users

2.04 The university reserves the rights to limit, restrict, or extend digital technology privileges and access to its information resources. Data owners, whether departments, units, faculty, students, or staff, may allow individuals other than university faculty, staff, and students access to information for which they are responsible, so long as such access does not violate any license or contractual agreement, university policy, or any federal, state, county, or local law or ordinance. This is accomplished by use of service and affiliate accounts. Users are personally responsible for all activities logged under their O-Key credentials.

Authorized User Purposes

3.01 Use of digital technology at the university must comply with federal and state law and university policies. University digital technology and O-Key accounts are to be used for the university-related activities for which they are assigned. When users cease to be members of the academic community, such as by graduating or ceasing employment, or when persons are assigned to a new position and/or responsibilities within the university, the access authorization of such person will be reviewed and may be altered. Users whose relationships with the university change may not use digital technology, facilities, accounts, access codes, privileges, or information for which they are not authorized in their new role at the university.

3.02 Users may use only their own O-Key accounts. The negligence or naivete of another user in revealing an account name or password is not considered authorized use. Convenience of file or printer sharing is not sufficient reason for sharing an O-Key account. Users are personally responsible for all use of their O-Key account.

3.03 Appropriate use of digital technology and networking resources includes instruction, independent study, authorized research, independent research, communications, and official work of the offices, units, recognized student and campus organizations, and agencies of the university. Digital technology, services, and networks may not be used in connection with compensated outside work for the benefit of organizations unrelated to the university except in connection with scholarly pursuits, such as faculty publishing activities, or in a purely incidental way. State law prohibits the use of university digital technology and network facilities for personal gain or profit, and use of digital technology resources for unauthorized commercial purposes, unauthorized personal gain, or any illegal activities.

Special User Notifications

4.01 The university makes available both internal and external network resources consisting of hardware, software, data storage and network connectivity. The university accepts no responsibility for any damage to or loss of data arising directly or indirectly from the use of these facilities or for any consequential loss or damage. The university makes no warranty, express or implied, regarding the digital technology services offered, or their fitness for any particular purpose.

4.02 Liability for any loss or damage shall be limited to a credit for fees and charges paid to the university, for use of the digital technology which resulted in the loss or damage.

4.03 The university cannot protect individuals against the existence or receipt of material that may be offensive to them. As such, those who make use of the network are warned that they may come across or be the recipients of materials they find offensive. Those who use email and/or make information about themselves available on the Internet should be forewarned that the university cannot protect them from invasions of privacy and other

possible dangers that could result from the individual's distribution of personal information.

4.04 An individual using university digital technology must do so in the knowledge that they are granted access to university resources in support of their work. The university owns everything stored in its facilities unless it has agreed otherwise. The university has the right of access to the contents of stored data at any time for any purpose for which it has a legitimate need to know. The university will make reasonable efforts to maintain the confidentiality of data stored and transmitted and to safeguard the data from loss, but is not liable for the inadvertent or unavoidable loss or disclosure of the contents.

4.05 Any individual using university digital technology must realize that all digital technology systems maintain audit trail logs or file logs within the device or on the network. Such information as the user identification, date and time of the session, the software used, the files used, the computer time, the storage used, the user account, and other related information is normally available for diagnostic, accounting, and load analysis purposes. Under certain circumstances, this information is reviewed by system administrators, either at the request of an institutional unit, or in situations where it is necessary to determine what has occurred to cause a particular system problem at a particular time. For example, analysis of audit files may indicate why a particular data file is being erased, when it was erased, and which user has erased it.

4.06 Computer and Information Services (CIS) employees and system administrators do not routinely look at individual data files. However, the university reserves the right to view or scan any file or software stored on the computer or passing through the network, and will do so periodically to verify that software and hardware are working correctly, to look for particular kinds of data or software such as computer viruses or malware, or to audit the use of university resources. Violation of policy that comes to the attention of university officials during these and other activities will be acted upon. User data on network servers will be regularly backed up. The university cannot guarantee confidentiality of stored or transmitted data. Users should be aware that use of one of the data networks, such as the Internet, or emails and messages, will not necessarily remain confidential from third parties outside the university in transit or on the destination computer system, as those data networks are configured to permit fairly easy access to transmissions.

Conduct Expectations and Prohibited Actions

5.01 The well-being of all digital technology users depends on the confidentiality, integrity, and availability of the system. Any defects discovered in the system accounting or system security are to be reported to the appropriate system administrators, by way of the CIS service desk, so that steps can be taken to investigate and solve the problem. The cooperation of all users is needed to ensure prompt action. The confidentiality of most systems is maintained by password protection of their O-Key accounts. A digital technology user who has been authorized to use such a protected account may be subject to both criminal and civil liability, as well as university discipline, if the user discloses a

password or otherwise makes the account available to others without the permission of the system administrator.

5.02 Restrictions to ensure computer security and block viruses are to be implemented in a manner that protects university and individual digital technology resources, but does not unduly restrict or limit legitimate academic pursuits.

5.03 The following examples of acts or omissions, though not covering every situation, specify some of the responsibilities that accompany digital technology use at OSUIT and outline acts or omissions that are considered unethical and unacceptable and may result in immediate revocation of privileges to use the university's computing resources and/or the taking of disciplinary action up to and including separation, suspension, and/or legal action:

A. Violating any software license agreement or copyright, including copying or redistributing copyrighted computer software, data, or reports without proper, recorded authorization. Software protected by copyright shall not be copied except as specifically stipulated by the owner of the copyright. Protected software is not to be copied into, from, or by any university digital technology resource, except by license. The number and distribution of copies must be handled in such a way that the number of simultaneous users in a unit does not exceed the number of original copies purchased by that unit, unless otherwise stipulated in the purchase contract. Summary of Civil and Criminal Penalties for Violation of Federal Copyright Laws Copyright infringement is the act of exercising, without permission or legal authority, one or more of the exclusive rights granted to the copyright owner under section 106 of the Copyright Act (Title 17 of the United States Code). These rights include the right to reproduce or distribute a copyrighted work. In the file-sharing context, downloading or uploading substantial parts of a copyrighted work without authority constitutes an infringement. Penalties for copyright infringement include civil and criminal penalties. In general, anyone found liable for civil copyright infringement may be ordered to pay either actual damages or “statutory” damages affixed at not less than $750 and not more than $30,000 per work infringed. For “willful” infringement, a court may award up to $150,000 per work infringed. A court can, in its discretion, also assess costs and attorneys’ fees. For details, see Title 17, United States Code, Sections 504, 505. Willful copyright infringement can also result in criminal penalties, including imprisonment of up to five years and fines of up to $250,000 per offense. For more information, please see the website of the U.S. Copyright Office at http://www.copyright.gov.

B. Interfering with the intended use of the information resources or without authorization, destroying, deleting, altering, dismantling, disfiguring, preventing rightful access to or otherwise interfering with the confidentiality, integrity, or availability of digital technology information resources.

C. Modifying or removing digital technology devices, software, or peripherals without proper authorization.

D. Encroaching on others' use of the university's digital technology. This includes but is not limited to: the sending of chain-letters or excessive messages, either locally or off-campus; printing excessive copies of documents, files, data, or programs; unauthorized modification of system facilities, operating systems, or disk partitions; attempting to crash or tie up any digital technology; causing a denial of service of university resources; damaging or vandalizing university digital technology resources, equipment, software, or data.

E. Developing or using programs which harass other digital technology users or which access private or restricted portions of the system and/or damage the software, hardware or availability of the system. Digital technology users shall use great care to ensure that they do not use programs or utilities which interfere with other users or which modify normally protected or restricted portions of the system or user O-Key accounts. The use of any unauthorized or destructive program may result in legal civil action for damages or other punitive action by any injured party, including the university, as well as criminal action.

F. Using university digital technology resources for commercial purposes or excessive non-university-related activities without written authorization from the university. In these cases, the university will require restitution payment of appropriate fees. This policy applies equally to all university-owned or university-leased digital technology.

G. Using university digital technology resources to generate or access obscene material as defined by Oklahoma or federal law and acceptable community standards or creating a hostile work and/or educational environment.

H. Seeking to gain or gaining unauthorized access to information resources or enabling unauthorized access.

I. Accessing digital technology, software, data, or networks without proper authorization, or intentionally allowing others to do so, regardless of whether the digital technology, software, data, or network in question is owned by the university. For example, abuse of the networks to which the university belongs or the digital technology resources at other sites connected to those networks will be treated as an abuse of OSUIT digital technology privileges.

J. Invading the privacy of individuals or entities that are creators, authors, users, or subjects of the information resources without authorization.

K. Using university digital technology resources to send fraudulent, harassing, obscene, threatening, or other unlawful messages is prohibited. It is the responsibility of any user of an email distribution list to determine the purpose of the list before sending messages to the list or receiving messages from the list. Persons subscribing to an email distribution list or list server will be viewed as having solicited any material delivered by the list as long as that material is consistent with the purpose of the list. Persons sending to a mailing list any materials which are not consistent with the purpose of the mailing list will be viewed as having sent unsolicited material to the mailing list.

L. Transmitting commercial or personal advertisements, solicitations, promotions, or programs intended to harass other users or access private or restricted digital technology or network resources.

M. Seeking to obtain copies of or modify data files, programs, or passwords belonging to other users without the permission of those users. Using programs or devices to intercept or decode passwords or similar access control information.

N. Attempting to circumvent mechanisms intended to protect private information from unauthorized examination by others in order to gain unauthorized access to the system or to private information. Configuring or running software so as to allow unauthorized use.

O. Using university digital technology resources in any manner which violates federal, state, or local laws, or university policies.

P. Using university digital technology resources or O-Key accounts for other than the university-related activities for which they were assigned and intended.

Q. Using digital technology resources to engage in political campaigning or commercial advertisement.

System Administrator Responsibilities

6.01 The Board of Regents for Oklahoma State University and the Agricultural and Mechanical Colleges are the legal owners of all university owned or controlled digital technology and networks. The contents of all data owned or stored on university digital technology are the property of OSUIT unless a written contract signed by the suitable authority exists to the contrary.

6.02 Management of the data which is contained within the various data systems of the university must be administered in a fashion consistent with the mission and efficient operations of the university, applicable state or federal laws, and potentially applicable privacy considerations.

6.03 The system administrator's use of the university's digital technology resources is governed by the same guidelines that apply to any other user. However, the system administrator has additional responsibilities and authorities with respect to the system under their control and its users.

6.04 The system administrator has certain responsibilities to the university as a whole for the systems under their control. These responsibilities are:

A. To take reasonable precautions against theft of, or damage to, the system components.

B. To faithfully execute all hardware and software licensing agreements applicable to the system.

C. To treat information about, and information stored by, the system's users as confidential, as conditioned in this policy, and to take reasonable precautions to ensure the security of the system, network and the information contained therein.

D. To share information about specific policies and procedures that govern access to and use of the system and services provided to the users or explicitly not provided. A written document given to users or login banner messages posted on the digital technology system itself shall be considered adequate notice.

E. To cooperate with the system administrators of other digital technology systems or networks, whether within or without OSUIT, to find and correct problems caused on another system by the use of the system under his/her control.

6.05 The system administrator is authorized to take all reasonable steps and actions to implement and enforce the usage, security, and service policies of the system. System administrators operating digital technology and networks may routinely monitor and log usage data, such as network session connection times, hosts, CPU and disk utilization for each user, security audit trails, network loading, and other relevant data. Administrators may review this data for evidence of violation of law or policy and for other lawful purposes. System administrators may access user data files at any time for maintenance or security purposes. System administrators may access any files for the maintenance of network, digital technology and storage systems, such as backup creation.

6.06 When confidentiality, integrity, availability, or security is threatened, a system administrator is authorized to access all files and information necessary to find and correct the problem or otherwise resolve the situation.

6.07 When a university officer or supervisor believes that access to an unavailable individual's data is required for the conduct of university business, the following procedure shall be followed if there is no indication of wrongdoing:

A. The university official or supervisor shall secure permission to access the data from the Executive Vice President, or designee, of such officer.

B. An appropriate form with the signature of the Executive Vice President shall be presented to the system administrator allowing the system administrator to proceed to access the data.

C. The individual whose data or digital technology has been accessed will be notified as soon as possible by copy of the above referenced form. Where necessary to ensure the integrity of an investigation into the use of university digital technology resources, such notice, with the approval of the Executive Vice President, may be delayed until such time as such investigation would no longer be compromised.

6.08 System administrators are required to report suspected unlawful or improper activities to the proper university authorities. Digital technology users, when requested, have a duty

to cooperate with system administrators in investigations of system abuse. Users are encouraged to report suspected illegal activity or abuse, especially if related to any damage to or problems with their files.

6.09 If an occasion arises when a university officer or supervisor believes that a user is violating state or federal law or university policy, and that access to an individual's data is required in order to conduct an internal investigation into such possibility, system administrators may monitor all the activities of and inspect the files of such specific user on their digital technology and networks. When a system administrator is required to access the individual's data due to suspected violation of the law the Office of Legal Counsel shall be contacted and informed of the matter.

Consequences of Misuse of Computing Privileges

7.01 Users are expected to fully cooperate with system administrators in any investigations of system abuse. Failure to cooperate may be grounds for cancellation of access privileges or disciplinary action.

7.02 Abuse of digital technology privileges is subject to disciplinary action. If system administrators have strong evidence of misuse of digital technology resources, and if that evidence points to the activities or the data files of an individual, they have the obligation to pursue any or all of the following steps to protect the user community:

A. Notify the user's unit leader or supervisor of the investigation.

B. Suspend or restrict the user's access privileges during the investigation.

C. Inspect the user's files on any attached media. System administrators must be certain that the trail of evidence clearly leads to the user's activities or data files before inspecting the user's files.

D. Refer the matter for possible disciplinary action to the appropriate university unit leader.

7.03 Individuals whose privileges to access university digital technology resources have been suspended may request that the Executive Vice President, or designee, review the suspension. The Executive Vice President, or designee, in their discretion, may reinstate privileges, alter any restrictions that have been imposed, or refuse to interfere with the administrative action taken to that time. There is no right to a hearing or appearance regarding such issues, and the decision made by the Executive Vice President, or designee, is final.

Approved: October 2004
Revised: July 2009
Revised: August 2013