EFFECTIVE: 01/01/2013 REVISION NO: 1

ACCEPTABLE USE OF INFORMATION TECHNOLOGY RESOURCES

OBJECTIVE:

Information technology resources are valuable assets provided to enhance the core functions of Southwestern College. The use of the college's information technology resources is a privilege extended to authorized users for education, research, service, and administration. This **ACCEPTABLE USE OF INFORMATION TECHNOLOGY RESOURCES POLICY** governs the use of the college's information technology resources in an atmosphere that encourages free exchange of ideas and an unwavering commitment to academic freedom. The college community is based on principles of honesty, academic integrity, respect for others, and respect for others' privacy and property. The college seeks to:

- protect the confidentiality and integrity of electronic information and privacy of its users, to the extent required or allowed under federal and state law.
- ensure that the use of electronic communications complies with the provisions of college policy and state and federal law; and
- allow for the free exchange of ideas and support of academic freedom.

The college cannot protect users from the presence of material they may find offensive. The presence of such material must not be represented or construed as an endorsement or approval by the college.

This policy applies to all students, staff, and others, referred to as users throughout this policy, while accessing, using, or handling the Southwestern College's information technology resources. In this policy, "users" include but are not limited to subcontractors, visitors, visiting scholars, potential students, research associates, grant and contract support personnel, media representatives, guest speakers, and non-college entities granted access. All "users" are required to be familiar with and comply with this policy.

POLICY:

SCOPE

Individuals Covered

In this policy, “users” are those who access, use, or handle the college’s IT resources. They include, but are not limited to: students, faculty, staff, subcontractors, visitors, visiting scholars,

potential students, research associates, grant and contract support personnel, media representatives, guest speakers, and non-college entities or individuals who are granted access.

Resources Covered

This policy applies to all college IT resources, whether individually controlled, shared, stand-alone, or networked. It applies to all computers and communication facilities owned, leased, operated, or provided by the college or otherwise connected to college IT resources. These include, but are not limited to: networking devices, personal digital assistants, telephones, wireless devices, personal computers, workstations and any associated peripherals and software, whether used for administration, research, teaching, or other purposes. This policy also applies to all personally owned devices used to store, process, or transmit college information or that are otherwise connected to college IT resources.

COMPLIANCE

At minimum, individual college units (such as campuses or institutes, departments and divisions) must follow these principles and rules while connected to college IT resources.

GENERAL POLICY

1) All users are expected to comply with college policies and follow security best practices and processes where possible.

PRIVACY

2) User privacy

   The college provides electronic resources to users to help the college fulfill its mission. The college employs electronic devices that may monitor electronic data, software, and communications. Although no active monitoring of content is performed, there should be no expectation of privacy for any information stored, processed, or transmitted on college IT resources.

   As required by law, the college hereby notifies users that email may be made available to law enforcement if legally required, unless the email is covered by other laws such as HIPAA or FERPA.

3) College rights

   Users should be aware that any activity on systems and networks may be monitored, logged, and reviewed by college approved personnel or may be discovered in legal proceedings. All documents created, stored, transmitted, or received on college computers and networks may be subject to monitoring by systems administrators.

   The college reserves the right to access, monitor, review, and release the contents and activity of an individual user's account(s), including email, on any account on any college-owned or non-college-owned resource on or off college property connected to college networks. This action may be taken to maintain the network's integrity and the rights of those with authorized access, to safeguard against threatened security of a computer or network system, to protect from other suspected misuse of college

resources, or to respond to the legitimate business needs of the college. Prior approval from the VP for Information Technology or another authorized college office (such as the Office of General Counsel, Audit and Consulting Services) or a subpoena or court order must precede this action.

USER RESPONSIBILITIES

4) Users will:

a. Comply with college policies and follow college best practices where possible to maintain the confidentiality, integrity, and availability of computer systems and information on all devices under their control.
b. Make regular backups of information and files as appropriate.
c. Control and secure physical and network access to IT resources and data.
d. Properly log out of sessions.
e. Monitor access to their accounts. If a user suspects unauthorized activity or that their account has been compromised, they must report it and change passwords immediately.
f. Install, use, and regularly update virus protection software.
g. Where technically possible, abide by the password protection best practices specified for each IT resource.
h. Use only the passwords and privileges associated with their computer account(s) and use those account(s) only for their authorized purpose.
i. Respect and honor the rights of other individuals with regard to intellectual property, privacy, freedom from harassment, academic freedom, copyright, and use of IT resources.
j. Use College provided software in a manner that strictly adheres to all licensing provisions, including installation, use, copying, number of simultaneous users, and other terms of the license.

5) Users will not:

a. Provide access codes to any unauthorized user.
b. Use accounts, access codes, privileges or IT resources for which they are not authorized.
c. Tamper, modify, or alter any restrictions or protections placed on their accounts, the college's system, or network facilities.
d. Physically damage or vandalize IT resources, or use IT resources to damage other college resources or systems.
e. Commit copyright infringement, including file sharing of video, audio, or data without permission from the copyright owner.
f. Use IT resources to introduce, create, or propagate computer viruses, worms, Trojan horses, or other malicious code.
g. Obtain extra IT resources or gain access to accounts for which they are not authorized.
h. Eavesdrop on or intercept other users' transmissions.

i. Attempt to degrade the performance or availability of any system or to deprive authorized users access to any college IT resources.
j. Misrepresent their identity with actions such as IP address "spoofing," email address falsification, or social engineering.
k. Send email chain letters or mass mailings for purposes other than official college business.
l. Use college resources to relay mail between non-college email systems.
m. Engage in activities that violate state or federal law, a College contractual obligation, or another College policy or rule including but not limited to Human Resources policies and Standards of Conduct for students.
n. Comment or act on behalf of the college over the Internet without authorization.
o. Connect devices (such as switches, routers, hubs, computer systems, and wireless access points) that are not approved by the central campus or institutional IT organization to the network.
p. Use without authorization any device or application that consumes a disproportionate amount of network bandwidth.
q. Respond to electronic requests (email, instant message, text message, etc.) that ask for generally protected information, such as passwords, social security numbers, or credit card numbers.

COPYRIGHTS AND LICENSES

6) Violation of copyright law or infringement is prohibited by college policies and state and federal law. Generally, only the owner of a copyrighted work may reproduce, create other works based on the copyrighted work, distribute, perform, or publically display a copyrighted work. Any unauthorized use of copyrighted material, including unauthorized peer-to-peer file sharing, may subject the user to discipline as a violation of one or more provisions of the general standard of conduct in the student handbook or to discipline under the Code of Conduct in the Human Resources Policy and Procedures.

   The college does not actively monitor its network for copyright infringement, but does investigate all complaints or notices. In the event that the college receives notice a potential copyright violation, the college does investigate all complaints or notices.

   Acts of copyright infringement will be addressed according to the Sanctions section of this policy. In addition, infringement of copyrighted work, including unauthorized peer-to-peer file sharing, may also involve civil lawsuits by the copyright owner. Possible penalties include actual damages and profits or statutory damages of up to $30,000 for each work infringed (or up to $150,000 for each willful infringement), court costs, attorney fees, and other civil damages. Criminal penalties for willful infringement may include, depending upon the value of the work(s) infringed, fines and imprisonment for up to 5 years as provided in 18 USC 2319.

7) Software may not be copied, installed, or used on college IT resources except as permitted by the owner of the software and by law. Users will properly license software and strictly adhere to all licensing provisions, including installation, use, copying, number of simultaneous users, and terms of the license.

8) All copyrighted information, such as text and images, retrieved from IT resources or stored, transmitted, accessed, or maintained with IT resources must be used in compliance with applicable copyright and other laws. Copied material must be properly credited using applicable legal and professional standards.

9) Each department that chooses to purchase their own software is responsible and accountable for maintaining records of purchased software licensure. The providing organization is responsible for maintaining records and information related to centrally provided software. These records are subject to internal audit for compliance.

10) Questions not addressed by this policy about computer software use or specific license agreements should be directed to the office of the VP for Information Technology.

PERSONAL USE

11) The college's IT resources are provided for use in conducting authorized college business. Certain users, such as students in college housing and network guests, may use college IT resources for personal needs. Nevertheless, all users are prohibited from using these resources for personal gain, illegal activities, or obscene activities.

a. The prohibition against using the college's IT resources for personal gain does not apply to:

   i. Scholarly activities, including the writing of textbooks or preparation of other teaching materials by faculty members, as recognized in the laws goeverning Patents, Copyrights, and Licensing.

   ii. Consulting and other activities that relate to a faculty member's professional development or as permitted under college policy. For approved consulting and other activities, see policies covering outside services in the campus and institutional faculty policy.

b. Incidental, de minimis personal use of these resources is permitted by this policy, except when such use:

   i. Is excessive or interferes with the performance of the user's college responsibilities.

   ii. Results in additional incremental cost or burden to the college's IT resources.

   iii. Violates any state or federal law or is otherwise in violation of this or any other college policy.

   iv. Results in additional risk to the confidentiality, integrity, and availability to the college’s IT resources. Personal use of college owned IT resources that access or

maintain restricted information (such as medical records, student records, social security numbers, or credit card numbers) is discouraged.

12. College IT resources may not be used for commercial purposes, except as specifically permitted under other written college policies or with the written approval of the VP for Information Technology. Any such commercial use must be properly related to college activities and provide for appropriate reimbursement of taxes and other costs the college may incur by reason of such use.

13. The ".edu" domain on the Internet has rules restricting or prohibiting commercial use; activities not appropriate for the ".edu" domain but otherwise permissible by the college's IT resources policies must use other domain designations.

MISUSE OF IT RESOURCES

14. Users should report all suspected or observed illegal activities to the appropriate college administrative office. Examples include theft, fraud, copyright infringement, illegal electronic file sharing, sound or video recording piracy, hacking, and viewing or distribution of child pornography.

15. Abuse of networks or computers at other sites through the college's IT resources will be treated as an abuse of IT resource privileges.

SANCTIONS

Violations of college policies, state or federal laws, and other misuse of college resources may result in termination of access, disciplinary review, expulsion, termination of employment, legal action, and other appropriate disciplinary action. Notification will be made to the VP of Information Technology, and the appropriate college office (such as the office for student conduct matters, human resources, general counsel, campus, or institute police department) or local and federal law enforcement agencies.

IT is authorized to isolate and disconnect computer systems from the network while responding to a suspected or reported security incident to minimize the risk to the college's network infrastructure. Termination of access may occur without contacting the administrator, user, or custodian of the violating system.

Access to the college's IT resources will only be restored when reasonable assurance that the incident has been resolved is received.