Technology Acceptable Use Policy

Purpose

To establish and define the "acceptable use" of University of Central Oklahoma ("University" or "UCO") information technology assets, electronic resources, including, but not limited to, computer facilities and services, computers, networks, electronic mail services, data and electronic information, web, video, and voice services.

Scope

This Policy applies to:

1. All divisions, colleges and units established by the University that exercise any information technology (IT) function relating to the mission of the University except for those specifically exempted in writing by the President of the University.

2. All faculty, staff, and students; academic and administrative units and organizations; affiliated entities, agents, contractors, and volunteers of the University, members of the community who use and/or administer University computer and telecommunications systems, or any information system or system asset (as defined in the information security policy) that connects directly or indirectly to any University owned, leased, contracted, or operated computer or telecommunication system.

Standard Details

1. GENERAL CONSENT

Individuals with access to the University's information technology resources ("Information Systems" or "Information Assets") are responsible for their appropriate use, and by their use, agree to comply with all applicable University, policies, guidelines and standards, and applicable State and Federal laws and regulations. For use and access to be acceptable, individuals must demonstrate respect of:

a. The rights of others privacy.
b. Intellectual property rights (e.g., as reflected in licenses and copyrights).
c. Ownership of information.
d. System mechanisms designed to limit access.
e. An individual's right to be free of intimidation, harassment, and/or retaliation.

2. PRINCIPLES OF ACCEPTABLE USE:

All individuals granted access to UCO Information Systems must agree to and accept the following:

a. Only use the UCO Information Assets for which they are authorized by UCO.
b. Utilize appropriate and University-provided, hosted, or sponsored authentication mechanisms to access Information Assets.
c. Make no attempts to access information technology resources for which their authorization may be erroneous, inadvertent, or inconsistent with their role at UCO.
d. Only use accounts, passwords, and/or authentication credentials that have been authorized to use consistent with their role at UCO.
e. Protect, and not share, their account, password, and/or authentication credentials.
f. Only share data with others as defined by applicable policies, standards, guidelines, and procedures, and dependent on their assigned role.
g. The use of UCO Information Systems to represent the interests of any non-University group or organization is not permitted unless authorized by an appropriate University department or office or that could be taken to represent UCO.
h. UCO information technology resources will not be used as an instrument to terrify, intimidate, threaten, harass, annoy or offend another person(s).This includes, but is not limited to:
    1) Using university information technology resources to actively engage in procuring, viewing, downloading or transmitting material that is in violation of sexual or gender-based harassment or hostile environment workplace laws;
    2) Using university information technology resources to access pornography, or engage in unlawful discrimination or threats of violence.
i. Attempts to or use of any hardware or software designed to assess or weaken security strength of UCO systems, unless authorized by the Chief Information Officer (CIO) or the Chief Information Security Officer or his or her designee(s), is prohibited.
j. Sending or forwarding of disruptive "spamming" (i.e., sending unsolicited electronic communication to groups of recipients at the same time), or acting in a way that will harm, damage, corrupt, or impede authorized access to Information Systems, networks, equipment, and/or data is prohibited.
k. Forging identities is not permitted. Sending anonymous messages without authorization is not allowed.

l. The installation or uninstallation of software or alteration of UCO-installed applications or security protection software on UCO owned, leased, or contracted equipment without the prior approval of Office of Information Technology (OIT) is not allowed.
m. The use of UCO owned, lease, or contracted systems and/or equipment for personal gain is not permitted.
n. Use of packet sniffing software, password cracking tools, hacking tools, tor-browsers, peer-to-peer (P2P) software, or related activity unless authorized by the Chief Information Officer (CIO) or the Chief Information Security Officer or his or her designee(s) is prohibited.
o. Make no attempt to subvert or by any means attempt to bypass the University's security, identity management, authorization, accounting, authentication, auditing, system management protocols, processes, or systems.
p. The use of UCO Information Systems or resources to upload, download or distribute copyrighted or illegal material which results in violation of law is prohibited.
q. UCO Information Systems used in violation of or contrary to university policy, standard, guidelines and procedures, local, state, or federal regulations or laws is not permitted.
r. Comply with all licenses and contracts related to Information Systems which are owned, leased, or subscribed to by UCO, and comply with applicable local, state, or federal laws, and institutional policies or enterprise service level agreements, rules, and guidelines as they relate to Information Systems. This includes international export control laws regarding exporting software, technical information, encryption software, or technology.
s. Websites are to be developed and maintained responsibly in compliance with university policy, and applicable state and federal laws. The Office of Information Technology and the Office of University Communications and Public Relations will review and monitor departmental and college websites to ensure technical integrity and protection of the University's image. Please refer to the UCO Web Presence Guidelines.

3. PROTECTING THE SECURITY AND INTEGRITY OF INFORMATION TECHNOLOGY RESOURCES FROM UNAUTHORIZED USE:

a. In order to protect the security and integrity of Information Systems against unauthorized or improper use, and to protect authorized individuals from the effects of any potential abuse or negligence, the University reserves the right to limit, restrict, or terminate any account or use of information assets, and to inspect, copy, remove or otherwise alter any data, file, or system resources that conflicts with authorized use.

b. The University also reserves the right to inspect or check the configuration of Information Systems, UCO-owned or otherwise, for compliance with this policy, and to take actions it deems necessary to protect University Information Assets. The University also reserves the right to control and/or manage use of the frequency spectrum of the University network. Members of the UCO community are required to report transmitting devices upon request.
c. The University reserves the right to require those units or individuals found to have devices that interfere or are suspected to interfere with the operation of University systems, to discontinue the use of such devices, and, if necessary, to remove them from university property.
d. The University shall not be liable for, and the individual assumes the risk of, inadvertent loss of data or interference with files resulting from the University's efforts to maintain the privacy, integrity, and security of the University's Information Assets. The University is not responsible for the content of individuals' personal web spaces, nor the content of servers, programs or files that individuals maintain either in their personally allocated file areas on university-owned computer resources or on personally owned computers connected to or through University Information Systems.
e. The University reserves the right to suspend access to the network, computer, and/or account(s), or to impose sanctions as defined in this policy if individually maintained files, programs, accounts, or services are believed to have been operating in violation of either law or policy.
f. The University retains the right to search and/or seize, for investigative purposes, UCO-owned hardware or systems connected to University Information Assets if there is reason to suspect that such hardware or systems were used either in violation of federal, state, or local law, or in violation of the terms and conditions set forth in university policies governing computer and network usage. Restoration will be at the sole discretion of the University.
g. Personal devices used for University purposes could be subject to law enforcement or court-ordered search and/or seizure for investigative purposes if there is reason to suspect that such hardware or systems were used either in violation of federal, state, or local law.
h. The University shall, to the full extent required under law, cooperate with all legal requests for information, including, but not limited to, disclosure of system user account information when made by any law enforcement officer or legal representatives pursuant to court order, subpoena, or other legal process.
i. The University can enforce the provisions of this policy and the rights reserved to the University without prior notice to the user.

Policy Violations

1. Disciplinary action for violating the policy shall be governed by, but may not be limited to, the applicable provisions of student handbooks, faculty and staff handbook, policies of the University of Central Oklahoma, Board of Regents of Oklahoma Colleges, Oklahoma State Regents for Higher Education, Statutes of the State of Oklahoma and federal law. Persons who violate this policy may have their access privileges to UCO computing and networking systems revoked and/or other disciplinary action, up to and including termination of employment and/or enrollment.

2. All supervisory personnel are responsible for ensuring that these policies, standards, and guidelines are communicated within their respective areas of responsibility. Any user may report University policy or law violations to their immediate supervisor, representative faculty or school personnel or using UCOMMENT.

Resources

Related Policies, Standards, and Requirements:
Information Security Policy,
UCO Web Presence Guidelines

Approved:

Andrew K. Benton

Andrew Benton, President

Date: June 13, 2023