Northeastern Oklahoma A&M College Computer Use Policy

I. Purpose and Scope

1.01 Access to modern information technology is essential to the pursuit and achievement of excellence across the Northeastern Oklahoma A&M College (NEO) mission of instruction, research and academic advancement. The privilege of using computing systems and software, as well as internal and external data networks, is important to all members of the NEO community. The preservation of that privilege for the full community requires that each individual student, faculty member, staff member, and administrator comply with institutional and external standards for appropriate use. This policy will establish the general guidelines for the use of NEO computing resources equipment, services, software, and computer accounts by students, faculty, staff and administration.

II. Definitions

2.01 Abuser. Any user or other person who engages in misuse of computing resources as defined in Section 3.02 of this Policy.
2.02 Computing resources - includes computers, computer equipment, computer assistance services, software, computer accounts provided by NEO, information resources, electronic communication facilities (including electronic mail, telephone mail, Internet access, network access), or systems with similar functions.
2.03 Computer account - the combination of a user number, username, or userid and a password that allows an individual access to a mainframe computer, externally hosted service or some other shared computer or network.
2.04 Information resources - data or information and the software and hardware that render data or information available to users.
2.05 Network - a group of computers and peripherals that share information electronically, typically connected to each other by either cable or satellite link.
2.06 Peripherals - special-purpose devices attached to a computer or computer network, such as printers, scanners, plotters, and similar equipment.
2.07 Server - a computer that contains information shared by other computers on a network.
2.08 Software - programs, data, or information stored on magnetic media (tapes, disks, diskettes, cassettes, etc.). Usually used to refer to computer programs.

2.09 System Administrator - faculty, staff, or administrators employed by a central computing department such as Information Technology (IT) whose responsibilities include system, site, or network administration and other faculty, staff or administrators whose duties include system, site, or network administration. System administrators perform functions including, but not limited to, installing hardware and software, managing a computer or network, and keeping a computer operational. System administrators include any persons responsible for a system which provides the capability to assign accounts to other users.
2.10 User - any individual who uses, logs in, attempts to use, or attempts to log in to a system, whether by direct connection or across one or more networks, or who attempts to connect to or traverse a network, whether via hardware, software or both. Each user is responsible for his or her use of the computer resources and for learning proper data management strategies.

III. Policy

3.01 Appropriate Use of Computing Resources. The computing resources provided by NEO are primarily intended for teaching, educational, research and administrative purposes, and may generally be used only for authorized NEO-related activities. Use of the computing resources is governed by all applicable NEO policies, including, but not limited to, sexual harassment, copyright, and student and employee disciplinary policies, as well as by applicable federal, state and local laws.
3.02 Prohibited Use of Computing Resources. NEO characterizes misuse of computing and information resources and privileges as unethical and unacceptable. Misuse constitutes cause for taking disciplinary action. Misuse of computing resources includes, but is not limited to, the following:
a. attempting to modify, remove, or add computer equipment, software, or peripherals without proper authorization;

b. accessing computers, computer software, computer data or information, or networks without proper authorization, regardless of whether the computer, software, data, information or network in question is owned by NEO, including,

but not limited to, abuse or misuse of networks to which NEO belongs or computers at other sites connected to those networks;

c. circumventing or attempting to circumvent normal resource limits, logon procedures and security regulations;

d. sending fraudulent computer mail, breaking into another user's electronic mailbox, or reading another user's electronic mail without his or her permission;

e. sending any fraudulent electronic transmission, including but not limited to fraudulent requests for confidential information, fraudulent submission of electronic purchase requisitions or vouchers, and fraudulent electronic authorization of purchase requisitions or vouchers;

f. violating any software license agreement or copyright, including copying or redistributing copyrighted computer software, data, or reports without proper, recorded authorization;

g. using NEO computing resources to harass or threaten others;

h. using NEO computing resources for development, posting, transmission of, or link to, any of the following: commercial or personal advertisements; solutions; promotions; destructive programs; political material; messages which are fraudulent, harassing, obscene, indecent, profane, intimidating, or otherwise unlawful; or any other unauthorized or personal use;

i. taking advantage of another's naiveté or negligence to gain access to any computer account, data, software, or file that does not belong to the user or for which the user has not received explicit authorization to access;

j. physically interfering with other users' access to the NEO computing resources;

k. encroaching on others' use of NEO computer resources, including but not limited to: disrupting other users' use of computer resources by excessive game playing; by sending electronic chain letters or other excessive messages, either locally or off-campus; printing excessive copies of documents, files, data or programs; modifying system facilities, operating systems, or disk partitions; attempting to crash or tie up an NEO or network computer; or damaging or vandalizing NEO or network computing resources, equipment, software, or computer files;

l. disclosing or removing proprietary information, software, printed output or magnetic media without the explicit permission of the owner;

m. reading other users' data, information, files, or programs on a display screen, as printed output, or via electronic means, without the owner's explicit permission; or

n. violating any applicable federal, state or local law.

3.03 User Responsibility. All users of NEO computing resources must act responsibly. Every user is responsible for the integrity of these resources. All users of NEO-owned or NEO-leased computing resources must respect the rights of other computing users, respect the integrity of the physical facilities and controls, and respect all pertinent license and contractual agreements. It is the policy of NEO that all members of its community act in accordance with these responsibilities, relevant laws and contractual obligations, and the highest standard of ethics.

3.04 Password Protection. Each user is responsible for maintaining absolute security of any password or password right granted to the user. Passwords must not be "shared" with another user. Password security helps to protect the NEO system against unauthorized access.

3.05 Computing Resource Access. Access to NEO's computing resources is a privilege granted to NEO students, faculty, staff and administrators. NEO reserves the right to limit, restrict, or extend computing privileges and access to its information resources.

3.06 Freedom of Communication. It is the intention of NEO to maximize freedom of communication for purposes that further the goals of NEO. NEO places high value on open communication of ideas, including those new and controversial.

3.07 General Right of Privacy. A general right of privacy should be extended to the extent possible to the electronic environment. NEO and all electronic users should treat electronically stored information in individual files as confidential and private. Contents should be examined or disclosed only when authorized by the owner, approved by an appropriate institution official, or required by law. Privacy is mitigated by the following circumstances.

a. NEO is an agency of the State of Oklahoma and therefore subject to the Oklahoma Public Records Act. For NEO employees, electronic information created in the performance of their duties may be public records, just as are paper records. Such records may be subject to review and/or release under Oklahoma law. All computer files and e-mail communications, unless subject to a specific privilege, are subject to production under the Oklahoma Public Records

Act and, when relevant, to discovery in civil litigation. In these cases, disclosure of personal e-mail or files not related to the specific issue discussed in any Public Records request or discovery will be avoided to the extent allowed by law.
b. Administrative files of NEO are generated as part of the process of managing the institution. Files that employees create or maintain can be reviewed by supervisors within this administrative context. Generally, faculty research files and files relating to scholarly endeavor will not be subject to such a review.
c. There is an acknowledged trade-off between the right of privacy of a user and the need of system administrators to gather necessary information to ensure the continued functioning of these resources. In the normal course of system administration, system administrators may monitor any computing activity or examine activities, files, electronic mail, and printer listings to gather sufficient information to diagnose and correct problems with system software or hardware. Sometimes system administrators may monitor computing activity or access files to determine if security violations have occurred or are occurring. In that event, the user should be notified as soon as practical. System administrators at all times have an obligation to maintain the privacy of a user's files, electronic mail, and activity logs.
d. Computer systems and stored data are subject to review by authorized personnel for audit purposes or when a violation of NEO policy or law is suspected.
3.08 Disclaimer. NEO makes no warranties of any kind, whether express or implied, regarding the electronic communications facilities or services it provides. NEO will not be responsible for any damages suffered by a user through the use of the NEO electronic communications facilities or services, including, but not limited to, loss of data resulting from delays, nondeliveries, misdeliveries, or service interruptions caused by its own negligence or by any error or omissions or any user. Use of any information obtained via the Internet will be at the user's risk. NEO specifically denies any responsibility for the accuracy or quality of information obtained through its electronic communications facilities and services.

3.09 Copyright Compliance Policy. It is the policy of Northeastern Oklahoma A&M College (NEO) to comply with copyright law. Copyright exists in any original work which exists or is fixed in any tangible medium of expression. Images displayable on computer screens, computer software, music, books, magazines, scientific and other journals, photographs and articles are some of the things subject to copyright. A copyright notice is not required.

Subject to exceptions contained in 17 U.S.C. §§ 107 and 108 **(http://www.copyright.gov/title17/92chap1.html)**, it is a violation of copyright law to copy, distribute, display, exhibit or perform copyrighted works without the authority of the owner of the copyright. In short, 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). In the file sharing context, downloading or uploading substantial parts of a copyrighted work without authority constitutes an infringement.

Content owners are able to track the sharing and downloading of their copyrighted files via the IP address of the file sharer or downloader. Upon proper notice of infringement from the copyright owner to NEO as the Internet service provider in accordance with the Digital Millennium Copyright Act, NEO investigates, takes down any infringing site or material on NEO's network, and blocks access to any infringing sites or material. NEO also investigates to identify the infringing user and takes appropriate action to address misuse in accordance with NEO policies.

Summary of Civil and Criminal Penalties for Violations of Federal Copyright Laws
The unauthorized distribution of copyrighted material, including unauthorized peer-to-peer file sharing, may subject you to civil and criminal liabilities. Penalties for 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. Willful copyright infringement also can result in criminal penalties, including imprisonment of up to five years and fines of up to $250,000 per offense.

Other Consequences of Misuse
A violation of copyright law also constitutes a violation of NEO's policy, and can result in suspension of user accounts and referral to the appropriate divisional authority for disciplinary action. NEO's Plan to Address Copyright Infringement In order to comply with NEO policy and with federal laws and regulations, NEO employs technology-based deterrents including: (i) packet shaping; (ii) automated intrusion prevention; (iii) network segmentation; (iv) firewalls; to limit the ability of illegal peer to peer network function on campus. In addition, NEO educates the NEO community regarding copyright laws and internal policies.

IV. Procedures

4.01 Computer accounts will be issued to authorized users only by NEO IT personnel.

4.02 Prior to issuance of an account and password, all users must execute such forms, including an acknowledgment and acceptance of the terms of this policy, as may be reasonably required by NEO.
4.03 User passwords must be kept private, and may not be disclosed to any other individual or entity. A password must NEVER be posted or placed where it can be discovered by someone other than the user.
4.04 Each user will select a User ID in accordance with rules established by NEO IT. The User ID will be used consistently for all logons.
4.05 Personal passwords will be maintained by the individual user and must be changed at least every 120 days, or at more frequent intervals as the user may elect. Passwords shall be selected in accordance with rules established by NEO IT. In the event another person learns a user's password, the user must immediately change the password.
4.06 Any user who learns of an unauthorized use of his or her account must report the unauthorized use to NEO IT immediately.
4.07 In the event it appears that a user has abused or is abusing his or her computing privileges, or engages in any misuse of computing resources, then NEO may pursue any or all of the following steps to protect the user community:
a. take action to protect the system(s), user jobs, and user files from damage;

b. begin an investigation, and notify the suspected abuser's project director, instructor, academic advisor, department chair or administrative officer of the investigation;

c. refer the matter for processing through the appropriate NEO disciplinary system;

d. suspend or restrict the suspected abuser's computing privileges during the investigation and disciplinary processing. A user may appeal such a suspension or restriction and petition for reinstatement of computing privileges through the procedures existing at the time the user requests an appeal, which procedures will be provided to the appealing user in writing;

e. inspect the alleged abuser's files, diskettes, and/or tapes. System administrators must have reasonable cause to believe that the trail of evidence leads to the user's computing activities or computing files before inspecting any user's files;

f. in the event the misuse also constitutes a violation of any applicable federal, state or local law, NEO will refer the matter to appropriate law enforcement authorities.