Acceptable Use of Information Systems at
The University of Oklahoma Health Sciences Center

General Principles   Access to computer systems and networks owned, operated, or provided by the University is predicated on compliance with certain responsibilities and obligations and is granted subject to University policies and local, state and federal laws. By using University information systems or computing resources, you agree to abide by and comply with the applicable policies, procedures and laws. Acceptable use must be ethical, reflect academic honesty, and show responsible use in the consumption of shared resources. Acceptable use also demonstrates respect for intellectual property, ownership of data, system security mechanisms, and freedom from intimidation and harassment. Information created or stored on University computer resources, networks and systems may be subject to the Oklahoma Open Records Act.

In making acceptable use of information resources you **MUST**:
- Comply with all University policies, procedures, and local, state, and federal laws
- Use resources only for authorized administrative, academic, research or clinical purposes; or other University business
- Protect your user-ID and system from unauthorized use. (you are responsible for all activities on your user-ID or that originate from your system);
- Access only information that is your own, that is publicly available, or to which you have been given authorized access;
- Comply with all copyright laws, licensing terms, patent laws, trademarks, trade secrets and all contractual terms
- Be responsible in your use of shared resources (refrain from monopolizing systems, overloading networks, degrading services, or wasting computer time, connect time, disk space, printer paper, manuals, or other resources.)

In making acceptable use of information resources you **MUST NOT**:
- Use another person's system, files, or data without express authorization
- Use another individual's user id or password
- Use computer programs to decode passwords or access control information;
- Attempt to circumvent or subvert system or network security;
- Engage in any activity that might be harmful to systems or to any information stored thereon, such as creating or propagating viruses, disrupting services, damaging files, or making unauthorized modifications to or sharing of university data;
- Use university systems for commercial, private, personal, or political purposes, such as using electronic mail to circulate advertising for products or for political candidates;
- Harass or intimidate another person including, but not limited to, broadcasting unapproved, unsolicited messages, repeatedly sending unwanted or threatening mail, or using someone else's name or user-id
- Waste computing resources or network resources including, but not limited to, intentionally placing a program in an endless loop, printing excessive amounts of paper, or sending chain letters or unapproved, unsolicited mass mailings
- Attempt to gain access to information or services to which he/she has no legitimate access rights
- Engage in any other activity that does not comply with the general principles presented above, university policies and procedures, or applicable law;

Enforcement   The University considers any violation of acceptable use principles or guidelines to be a serious offense and reserves the right to copy, monitor and/or examine any files or information residing on University systems, networks, or computing resources allegedly related to unacceptable use, and to protect its systems and networks from events or behaviors that threaten or degrade operations. Violators are subject to disciplinary action including, but not limited to, penalties outlined in the Student Code, Staff Handbook, or Faculty Handbook. Offenders also may be prosecuted under laws including, but not limited to, the Communications Act of 1934 (amended), Family Educational Rights and Privacy Act of 1974, Computer Fraud and Abuse Act of 1986, Computer Virus Eradication Act of 1989, Interstate Transportation of Stolen Property, Digital Millennium Copyright Act, Health Insurance Portability and Accountability Act, Electronic Communications Privacy Act, Oklahoma Open Records Act, and state conflicts of interest laws.

Individuals using computer systems owned by the University do so subject to applicable laws and University policies. The user assumes all risk of loss of materials or data or damage thereto. The University disclaims any responsibility and/or warranties for information and materials residing on non-University systems or available over publicly accessible networks. Such materials do not necessarily reflect the attitudes, opinions or values of the University, its faculty, staff or students. These guidelines should not be construed as a limit on any individual's right under the Constitution of the United States or the laws of Oklahoma.

--- Policy Approved by the Senior Vice President and Provost, January 19, 2000, Revised August 21, 2003

Instructions: Please *print* your name and your primary department or college in the box below, sign and date this policy agreement (page 1), and proceed as instructed for either an OUHSC Employee* or an OUHSC Affiliate**.

I have read and understand the above policy and agree to abide by this policy in my use of OUHSC computer resources.

Computer User (print): _____ , _____ _____ _____
                              Last Name   First Name   Middle Initial   Department or College

User's Signature: _____   Date: _____

Form SEC01(c)   Revised 3/26/08

* Please Print CLEARLY *

User's Name:
LAST   FIRST   MIDDLE INITIAL

National ID # (SSN):   EMPLID:

OUHSC Department/College: Dept Phone #

* OUHSC Status (check ALL that apply) *

___OUHSC Employee (paid by OUHSC)   ___Special Pay   ___OUHSC Student   ___OUHSC Affiliate*   ___Ecopy

___Faculty   ___Adjunct Faculty   ___Volunteer Faculty   ___Staff   ___Temp Staff **   ___Resident   ___Intern   ___Fellow

* Name of Affiliated Organization:

** Length of contract with OUHSC:

After completing, fax both pages of this form to your department computer support personnel for authorization.

* Computer Account Sponsor Only *
(sponsor is authorized in writing by department head)

Access Preferences: Indicate each type of access required.

On Campus   **Remote Access via the VPN Client**

___ Email, Internet, Personal Folders on Moon file and print server   ___ VPN-Group-1 (Allows the following access)
   (includes remote access via the modem pool)   - Exchange 2000 email via the MS Outlook client
                                                                              - Personal folders on Moon file and print server
                                                                              - Intranet web servers

Preferred method of acquiring personal access codes: ___ Campus Mail   ___ Email notification   ___ Pick up in person

As a computer account sponsor, I (1) agree to assume limited responsibility for the use of this user account as outlined in the
OUHSC Information Technology Computer Account Policy and (2) state that this user account is necessary for an official
university activity/endeavor or to conduct university business.

Sponsor's Name: Title:
          Print or Type

Sponsor's Signature: Date:

Account Sponsor ~~ send this form to: IT Account Management, SCB-101 (fax 271-2126).