Internal Governing Policies

#128 - Computer Services - Use of Computing Center Facilities and Services

---

Approved: October 23, 2003

Monitor: Vice President for Business Affairs

Information Technology Services (ITS) provides computing facilities and services for the legitimate instructional, research, and administrative computing needs of the University. Proper use of those facilities and services supports the legitimate computing activities of students, faculty and staff. Proper use respects intellectual property rights.

Legitimate instructional computing is work done by an officially registered EIU student, faculty, or staff member in direct or indirect support of a recognized course of study. Legitimate research computing is work approved by an authorized official of a University department. Legitimate administrative computing is work performed to carry out official University business.

Intellectual property rights begin with respect for intellectual labor and creativity. They include the right to acknowledgment, the right to privacy, and the right to determine the form, manner and terms of publication and distribution.

Proper computing use follows the same standards of common sense and courtesy that govern use of other public facilities. Improper use violates those standards by preventing others from accessing public facilities or by violating their intellectual property rights. Therefore, the basic policy of the University on proper use is:

- Any use of ITS facilities or services unrelated to legitimate instructional or research computing is improper if it interferes with another's legitimate instructional or research computing.
- Any use of ITS facilities or services that violates another's intellectual property rights is improper.
- Any use of ITS facilities or services that violates any local, state or federal law or which is obscene or defamatory is improper.

The following sections describe some known instances of improper use. They do not constitute a complete list. When new occasions of improper use arise, they will be judged and regulated by the basic policy stated above.

Disruptive Conduct. Avoid behavior at any computing facility that would interfere with another's legitimate use of the facility. This includes noisy and over-exuberant conduct.

Damage. Avoid actions that would damage ITS facilities, hardware, software, or files.

Access to Files. Avoid reading or using others' files without their permission. Proper usage standards require everyone to take prudent and reasonable steps to limit access to their files and accounts.

Fraud and Forgery. Avoid sending any form of electronic communication that bears a fraudulent origin or identification. This includes the forging of another's identity on electronic mail or news postings.

Harassment. Avoid using University computing facilities to harass anyone. This includes the use of insulting, obscene or suggestive electronic mail or news, tampering with others' files, and invasive access to others' equipment.

Networks. Avoid using local, national, and international networks for things that are not legitimate instructional or research activities of the University. This includes, but is not limited to, articles for commercial gain posted on electronic news networks and repeated attempts to access restricted resources.

Unauthorized Use of Accounts. Avoid accessing an account not specifically authorized to you, whether it is on a ITS system or one at another place. Avoid using an account for a purpose not authorized when the account was established, including personal and commercial use.

Do not engage in computing activities that are designed to invade the security of accounts. Attempts to decipher passwords, to discover unprotected files, or to decode encrypted files are examples.

Proper usage standards require that everyone take prudent and reasonable steps to prevent unauthorized access.

Unauthorized Use of Software. Do not make unauthorized copies of licensed or copyrighted software. Avoid actions that are in violation of the terms or restrictions on the use of software defined in official agreements between the University and other parties.

Examples include the copying of software from personal computers unless it is clearly and specifically identified as public domain software or shareware that may be freely redistributed, and the copying of restricted Unix source code.

Enforcement. When instances of improper use come to its attention, ITS staff will investigate them. During those investigations ITS reserves the right to access private information, including the contents of files and mailboxes, while making every effort to maintain privacy.

Investigations that discover improper use may cause ITS to:

- Limit the access of those found using facilities or services improperly;
- Refer flagrant abuses to Deans, Department heads, the applicable Vice President, the University Police Department, or other authorities for appropriate action;
- Disclose private information to other University authorities.

Users who violate this policy may have their computing privileges terminated and may be subject to disciplinary action by the University in accordance with appropriate policies or judicial affairs procedures.

RULES FOR ACCESS TO UNIX SOURCE CODE

One of the major factors in the increasing popularity of the UNIX operating system at the University is how easily UNIX source code applications can be moved among different variations of the UNIX system. This process, commonly called porting, often requires nothing more than copying and compiling an application to move it from one UNIX platform to another. The porting process is so simple that it is easy to lose sight of the ownership of individual programs and the license agreement restrictions on their source code.

1. Licensing Agreements

   Source code for computer programs is usually owned by the organization that developed the programs. Since many of these organizations have an economic stake in their developmental investment, they don't just give it away. At a minimum, they usually declare their copyright on the programs, but legally, a more powerful means exists--a license agreement.

   Software license agreements are contracts in which the seller agrees to provide the program, and perhaps its source code, provided the buyer agrees to abide by the rules of the license. Most work station-based software that is issued with the installation of a UCAN work station is licensed software. NCSA Tenet and Kermit packages are noted exceptions. Sellers can specify just about any rules they desire so long as the buyer agrees to those rules; every seller of computer software seems to have its own special rules to follow. Licensed software must not be duplicated distributed, modified, or used without authorization.

   Some programs are distributed in source form without a license agreement. They may be totally unrestricted (called "public domain") or the owner may retain the copyright but allow free distribution. A lot of useful software designed to run on UNIX systems is distributed this way. A user of University systems may find source code to such programs in various system directories.

2. Source Code

Whenever possible, most UNIX system administrators at the University strive to obtain the source code for programs because it makes it easier to maintain systems and quickly fix problems. In order to obtain source code for commercial software systems, it is necessary to negotiate the "Terms and Conditions" of the software license agreement with each software vendor. Some of those agreements permit anyone at the University to have access to the source code while others stipulate restrictions. Therefore users may find that they have access to a source code which is restricted by a license agreement; having access does not give the right to port a program to another system.

Concerning the UNIX operating system and its associated utilities and libraries, the University adheres to license agreements with IBM, the University of California at Berkeley, and other vendors who redistribute UNIX. These license agreements specify the rules under which the University may have access to the source code originally.

Users with a UNIX system of any kind who want to obtain source access should follow the following rules:

• Check with the source-code vendor to determine if an additional vendor license is required. Follow the vendor's restrictions on redistributing the vendor's source code.

• Source code access for most Sun UNIX systems is provided under agreements between ECN and the Sun Corporation.

• When in doubt, users should not assume the right to copy sources from another UNIX system to their own and should contact the SUN license administrator at ECN or the administrator of the system from which they wish to copy the sources before doing so.

WASTE

Users should avoid any wasteful use of ITS facilities. This includes squandering expendable resources, processor cycles, disk space, or network bandwidth. Expendable resources such as paper must be used prudently and recycled if possible. A system whose capacity is appropriate to the size of the computing task must be used.

REQUESTS FOR SERVICES

ITS is the central coordinating department for computerized instruction, research, and administrative computer functions of the University. If a change in or addition to programming services is desired, a request must be submitted, in writing, to the Associate Vice President for Information Technology Services. The request shall state in detail the change in service desired and shall be signed by the fiscal agent of the requesting unit. Academic computing support requests should be brought to the attention of the Director of Academic Computing, or if

clarification is needed, the request should be discussed with a member of the staff within the Academic Computing Division of ITS.

ITS staff shall not be responsible for initiating changes in administrative mainframe applications; however, they do maintain the right to make suggestions. Applications shall be revised when systems software requires it or when hardware that is necessary for processing reaches obsolescence.

ACQUISITION OF COMMODITIES

The Computer Services operations manager maintains the inventory of supplies necessary for central data processing system operation. The acquisition of microcomputer supplies is the responsibility of the owning department.

Forms that are not currently on inventory must be acquired by the requesting department; however, the acquisition of new forms to be printed by mainframe-connected printers must be coordinated through the Associate Vice President for ITS or the Assistant Director for Computer Operations.

MICROCOMPUTER AND NETWORK SERVICES

ITS shall provide the following services:

1. Maintenance

   Services provided by ITS staff shall include the repair of microcomputers listed in the annual budget instructions and consultation on microcomputer and software purchases. Replacement parts are a part of this service fee; however, if in the judgment of the ITS staff, the microcomputer is beyond repair, the using department shall be responsible for funding any replacement. A maintenance service fee shall be charged for each covered microcomputer that is on inventory and was purchased from an account other than appropriated account (1-xxxxx) or an income fund reserve account (7-706xx).
2. Network Support Services - Uniform Campus-wide Area Network (UCAN)

   ITS staff shall provide for the installation of network hardware and software components and shall service the communications components that are installed by them. The UCAN circuit boards and the electronic equipment within wiring closets are to be maintained and modified by ITS staff only. UCAN software components should all be treated as licensed software by end users.

PRINTERS, PLOTTERS, AND MODEMS

ITS staff shall provide advice and minor repairs for printers, plotters and modems; however, the using department is responsible for major repairs and replacements. Examples of minor repairs would include cleaning, simple mechanical adjustment, and the replacement of a print head that is furnished by the using department.

MAINFRAME, UCAN NETWORK SERVER, AND WORK STATION FILE SECURITY

ITS acts as the custodian of all University data bases or data processing files, but it is not the owner of these files. Individual users should take reasonable precautions regarding the physical security of their equipment and should change their passwords frequently.

The system administrator for servers other than the mainframe will provide mechanisms for backup and password controls. However, the management, security, and backup of files stored on servers other than the campus mainframe is the responsibility of the individual user. Users are best able to assess the level of privacy and security of the data and text files created.