Policy Number: 129

EASTERN WORLD WIDE WEB (WWW) APPROPRIATE USE POLICY

Information Technology Services 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 EIU students, faculty and staff. Proper use respects intellectual property rights.

Legitimate instructional computing is work done by an officially registered 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 Information Technology Services 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 Information Technology Services facilities or services that violates another person's intellectual property rights is improper.
- Any use of Information Technology Services facilities or services that violates any university policy, any local, state or federal law, or which is obscene or defamatory is improper.
- Any use resulting in commercial gain or private profit (other than allowable under university intellectual property policies) 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 person's legitimate use of the facility. This includes noisy and over-exuberant conduct.

DAMAGE

Avoid actions that would damage Information Technology Services 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.

COPYRIGHT

Refer to Eastern Illinois University Regulation 16a. and applicable sections of the Federal Copyright Act, including fair use provisions I Section 107 of H.R. 2223, to avoid violating the copyright law as you contemplate copying software, digital images, and other electronic media. You should also review the report of the Information Infrastructure Task Force (IITF) for concerns about digital images and educational multimedia.

HARASSMENT

Avoid using the 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 an Information Technology Services 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.

Don't 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. Do not make copyrighted or licensed material accessible from a Web page without the specific written permission of the copyright owner.

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. Read the policy topic "Rules for Access to UNIX Source Code" for more information on Unix license restrictions.

WWW SPECIFIC CLAUSES

General policies for computer use apply to those who develop or are responsible for the development of web pages on our World Wide Web server. However, the ability to publish electronically creates some unique opportunities and concerns. Style issues are covered within the EIU Publications Policy at http://139.67.11.100/PUBSMANUAL/pubman.html. The following four web-specific clauses are necessary.

1. Privacy

   People have a right to privacy. Employees acting within the scope of their employment may not place any item(s) (regardless of whether the person can be identified) such as, but not limited to, pictures, videos, audio-clips, or information about an individual(s) without the express written permission of the individual(s). The exception is those items that are determined to be necessary for university administrative functions.

2. Fair Warning

   Users of the EIU WWW must realize material put on the WWW is available to a wide audience, often beyond that originally intended for the material. There must be a recognition that, in different contexts, material may be construed in a manner different from that of the original intention of the author(s). Therefore, at the request of the appropriate university official(s), an information provider will provide a warning page at one level before any WWW page(s). This will be a standard page expressing that the content below may not be suitable for all audiences. WWW users, particularly minors, have a right to a "fair warning."

3. Use of University Name, Seal, and Logo

   Use of the university name, seal, and logo is not permitted except as allowed and/or required by university policy and regulations.

4. Personal Home Pages and WWW Servers

   EIU provides Internet/WWW access and resources for conduct of university functions. Personal use, *e.g.* development and posting of personal home pages and WWW servers, is permitted insofar as such activity does not disrupt, due to time, place, or manner, the conduct of university functions and as long as it is in compliance with the remainder of this and other university policies. The official EIU home page will not link directly to personal pages

ENFORCEMENT

When instances of improper use come to its attention, Information Technology Services will investigate them. During those investigations Information Technology Services 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 Information Technology Services to:

- Limit the access of those found using facilities or services improperly;
- Refer flagrant abuses to deans, department heads, the responsible vice president, the university flagrant abuses to deans, department heads, the responsible vice president, the university police, 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 AND LICENSED SOFTWARE

One of the big factors in the increasing popularity of the UNIX operating system at EIU 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. License 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 that the buyer agrees to abide by the rules of the license. Most workstation-based software that is issued with the installation of a UCAN workstation is licensed software. NCSA Telnet and Kermit packages are noted exceptions. Sellers can specify just about any rules they desire so long as the buyer agrees to those rules. And just to make life interesting, 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. As a user of one of EIU's systems, you may find source code to such programs in various system directories.

2. Source Code at EIU

Whenever possible, most UNIX system administrators at EIU 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 EIU to have access to the source code while others stipulate restrictions. Therefore, you may find that you have access to a source code that is restricted by a license agreement. Just because you have access does not mean you have the right to port a program to another system.

When it comes to the UNIX operating system and its associated utilities and libraries, EIU adheres to license agreements with IBM, Sun Microsystems, the University of California at Berkeley, and other vendors that redistribute UNIX. These license agreements specify the rules under which we may have access to the source code in the first place.

If you have a UNIX system of any kind and want to obtain source access, please follow these 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 EIU and the Sun Corporation.
- When in doubt, do not assume you have the right to copy sources from another UNIX system to your own; contact the SUN license administrator at EIU or the administrator of the system from which you wish to copy the sources before doing so.

WASTE

Avoid any wasteful use of Information Technology Services facilities. This includes squandering expendable resources, processor cycles, disk space, or network bandwidth. Use expendable resources such as paper prudently, and recycle them if possible. Use a system whose capacity is appropriate to the size of the computing task.

REQUESTS FOR SERVICES

Information Technology Services is the central coordinating department for computerized instruction, research, and administrative functions of the university. If a change in or addition to programming or networking 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 Information Technology Services.

Information Technology Services 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 Information Technology 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 currently not 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 of Information Technology Services or the Assistant Director for Operations.

MICROCOMPUTER AND NETWORK SERVICES

Information Technology Services shall provide the following services:

1. Maintenance

   Services provided by Information Technology Services staff shall include the repair of microcomputers that are currently approved for maintenance support and consultation on microcomputer and software purchases. Replacement parts are a part of this service fee; however, if, in the judgment of the Information Technology Services 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 IBM PC/XT/AT, Zenith,

Swan, Apple, or other covered microcomputer that was purchased from an account other than an appropriated account and that is on inventory.

2. Network Support Services -- Uniform Campus-wide Area Network (UCAN)

   Information Technology Services 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 is to be maintained and modified by Information Technology Services staff only. UCAN software components should all be treated as licensed software by end users.

PRINTERS, PLOTTERS AND MODEMS

Information Technology Services 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

Information Technology Services 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 are the responsibility of the individual user. You are best able to assess the level of privacy and security of the data and text files that you create.

Approved:
President
February 4, 1998

Monitor: Vice President for Business Affairs