Computer Users' Privileges and Responsibilities

Introduction

This document constitutes a University-wide policy for the management of computer data networks and the resources they make available, as well as standalone computers that are owned and administered by Indiana University. The policy reflects the general ethical principles of the University community and indicates, in general, what privileges and responsibilities are characteristic of the University computing environment. Because some networks operate in environments in which some of the specific items in this policy do not apply, system administrators are free to create policies that are at variance to this one. In such cases the system administrators should make relevant variances known to their users.

Terminology

A number of terms used below have very specific meanings in the context of this document. We define them here:

- Network - The complete mechanism by which computers and peripherals are connected.
- Network capacity - The quantitative dimension by which networks are measured.
- Networked computer - A computer system that is connected to any IU data network.
- Shared computing resource - A networked computer and its peripherals that can be used by more than one person.
- Central - Refers to networked computers and peripherals purchased, maintained, and operated by University Information Technology Services and made available to the entire University community.
- Campus - Refers to networked computers and peripherals purchased, maintained, and operated by the computing center of a given IU campus.
and made available primarily to that campus community.

- **Departmental** - Refers to networked computers and peripherals purchased by University departments or other administrative units, primarily for the use of the unit's personnel.

- **Individual** - Refers to networked computers purchased for use by an individual member of the University community, and which can be made available to other individuals or groups.

- **System manager** - The person or group responsible for the operation and security of one or more networked computers (the person or group with system privileges).

- **System administrator** - The person having executive authority over one or more networked computers.

### General Policies

Computer and network use has become an essential part of many University activities. While much computing is now done on privately controlled computers (personal computers, workstations, and so forth) most information sources and telecommunications systems reside on shared, central computers, or use shared networks. Distributed resources such as microcomputer clusters provide additional computing tools. University Information Technology Services (UITS), together with computing centers at each campus, as well as many academic departments and administrative units, have responsibility for providing and maintaining shared computing tools. General policies regarding the resources IU provides are outlined below.

- **Access** - Indiana University will provide access to appropriate central and campus computing resources, and to their attached networks, to all members of the University community whose work requires it. Fees are charged for some services.

- **Availability** - Indiana University will make its central and campus computing resources and networks available to users with the fewest interruptions possible.

### Security
Central and campus resources

Indiana University will help users of its central and campus shared computing resources protect the information they store on those resources from accidental loss, tampering, or unauthorized search, or other access. Appropriate information on the security procedures implemented on each central or campus resource will be made available by the system administrator.

In the event of inadvertent or non-malicious actions resulting in the loss of or damage to that information, or the invasion of the user's privacy, the IU computing centers will make a reasonable effort to mitigate the loss or damage. The University will provide an industry-standard level of system security on University-maintained systems. Users are responsible for maintaining properly the protections under their control, specific to files associated with their computer accounts. Users may request that arrangements be made to protect information stored on such resources. These requests will be honored at the discretion of the unit that manages the resource.

Other resources

The system administrators of departmental and individual computing resources are responsible for the security of information stored on those resources, for making appropriate information on security procedures available to users of those systems, and for keeping those systems free from unauthorized access.

Confidentiality

In general, information stored on computers is considered confidential, whether protected by the computer operating system or not, unless the owner intentionally makes that information available to other groups or individuals. Indiana University will assume that computer users wish the information they store on central and campus shared computing resources to remain confidential. IU computing centers will maintain the confidentiality of all information stored on their computing resources.

Similarly, privileged information on account usage (i.e., that available only to users with system privileges) will be held in confidence.
Requests for disclosure of confidential information will be reviewed by the administrator of the computer system involved. Such requests will be honored only when approved by University officials authorized by the campus involved, or when required by state or federal law. Except when inappropriate, computer users will receive prior notice of such disclosures.

Note: Indiana State law requires that public records be made available to any citizen who requests them. Exceptions are made for records concerning research conducted under the auspices of an institution of higher education; examinations and students' scores; interuniversity or interagency advisory or deliberative material communicated for the purpose of decision making; diaries, journals, or other personal notes serving as the functional equivalent of a diary or journal; administrative or technical information that would jeopardize a recordkeeping or security system; and computer software owned by the University or entrusted to it.

Censorship

Free expression of ideas is central to the academic process. IU computer system administrators will not remove any information from individual accounts unless the appropriate system administrator finds that:

- The presence of the information involves illegality (e.g., copyrighted material, software used in violation of a license agreement).
- The information in some way endangers computing resources or the information of other users (e.g., a computer worm, virus, or other destructive program).
- The information is inappropriate, because it is unrelated to or is inconsistent with the mission of the University, involves the use of obscene, bigoted, or abusive material on IU resources, or is otherwise not in compliance with the legal and ethical usage responsibilities listed in the section, "Responsibilities of the User."

IU computing centers may remove from central or campus computers any information that is inappropriate, as defined above. Guidelines for appropriate use of each Indiana University bulletin board system shall be available on that
system. Users whose information is removed will be notified of the removal as soon as is feasible. Users who wish to appeal such removal of information may do so through an appeals board made up of the governing body appropriate to the status of the user.

Responsibilities of the User

Access to computing resources and network capacity is a privilege to which all University faculty, staff, and students are entitled. Access may also be granted to individuals outside the University for purposes consistent with the mission of the University. Certain responsibilities accompany that privilege; understanding them is important for all computer users. These responsibilities are listed below.

Institutional purposes

Use of IU computing resources and network capacity is for purposes related to the University's mission of education, research, and public service. All classes of computer service user may use computing resources and network capacity only for purposes related to their studies, their instruction, the discharge of their duties as employees, their official business with the University, and their other University-sanctioned activities. The use of IU computing resources and network capacity for commercial purposes is permitted only by special arrangement with the appropriate computing center or computer system administrator.

Security

The user is responsible for correct and sufficient use of the tools each computer system provides for maintaining the security and confidentiality of information stored on it. For example:

- Computer accounts, passphrases, and other types of authorization are assigned to individual users and should not be shared with others.
- The user should select an obscure account passphrase and change it frequently.
- The user should understand the level of protection each computer system automatically applies to files and supplement it, if necessary, for sensitive information.
The microcomputer user should be aware of computer viruses and other destructive computer programs, and take steps to avoid being their victim or unwitting vector.

Legal usage

Computing resources and network capacity may not be used for illegal purposes. Examples of illegal purposes include:

- Intentional harassment of other users.
- Intentional destruction of or damage to equipment, software, or data belonging to IU or other users.
- Intentional disruption or unauthorized monitoring of electronic communications.
- Unauthorized copying of copyrighted material.

Ethical usage

Computing resources and network capacity should be used in accordance with the high ethical standards of the University community as described in the "Code of Student Ethics" and the "Academic Handbook." Examples of unethical use follow; some of them may also be illegal.

- Violations of computer system security.
- Unauthorized use of computer accounts, access codes, or network identification numbers assigned to others.
- Intentional use of computer telecommunication facilities in ways that unnecessarily impede the computing activities of others (randomly initiating interactive electronic communications or e-mail exchanges, overuse of interactive network utilities, and so forth).
- Use of computing facilities for private business purposes unrelated to the mission of the University or University life.
- Academic dishonesty (plagiarism, cheating).
- Violation of software license agreements.
- Violation of network usage policies and regulations.
- Violation of another user's privacy.
Facilitative usage

IU computing resource users can facilitate computing in the IU environment in many ways. Collegiality demands the practice of facilitative computing. It includes:

- Regular deletion of unneeded files from one’s accounts on central machines.
- Refraining from overuse of connect time, information storage space, printing facilities, or processing capacity.
- Refraining from overuse of interactive network utilities.
- Refraining from overuse of network capacity.

Sanctions

Violation of the policies described above for legal and ethical use of computing resources will be dealt with seriously. Violators will be subject to the normal disciplinary procedures of the University and, in addition, the loss of computing privileges may result. Illegal acts involving IU computing resources may also be subject to prosecution by state and federal authorities.

Approval

This policy is endorsed by the Academic Computing Policy Committee (ACPC), the Administrative Computing Advisory Committee (ACAC), the Academic Computing Coordinating Committee (ACCC), University Computing Services Deans and Directors, the Academic Deans, the Faculty and Staff Councils, the Academic Program and Priorities Committee, and the Indiana University Student Association (IUSA), fall 1999.