ARTICLE V: INFORMATION TECHNOLOGY AND TELECOMMUNICATIONS
Section 2. Information Systems/Technology Policies

Policy 2.1: Microcomputer Use
Issued: June 1, 2002

The tremendous changes in the computer industry in the past several years have led more and more professionals to microcomputers and powerful workstations to support the activities of their organizations. But the rapid and uncontrolled proliferation of these systems creates a potential for incompatibilities of hardware and software, and for waste and duplication of effort that triggers the need for some over-all guidance in their selection and use.

1) Justification

It is the responsibility of the managers of each functional unit to review their operation and determine if automated data processing support could benefit their department. Users are encouraged to seek help from University Computer Services (UCS) in this process. UCS can help identify and define needs, evaluate alternatives, and propose one or more solutions if appropriate. As with any other purchase, the funding is the responsibility of the individual department.

2) Review

Proposals for automated support, whether hardware, software, or services, must be presented to University Computer Services for review. UCS will evaluate whether the purchase creates any unnecessary or undesirable incompatibilities, if it is an appropriate use of automated resources, and if the identified needs can be met through sharing of resources. It is the departmental manager's responsibility to identify their needs; it is the responsibility of UCS to decide how those needs are best met through automated support. If UCS and the department cannot reach an agreement, both recommendations shall be forwarded to the appropriate Vice President for a decision.

3) Training

The current generation of microcomputers are high powered professional workstations. These workstations, when combined with appropriate software and training, can enhance work quality and productivity. Complex applications may require professional programming expertise and may have to be referred to Central Data Processing for support.

4) Operations and Management

University Computing Services is charged with operations and management of all campus networks and multiuser systems while, departments are responsible for operating and managing application software. Departments pursuing new applications should seek advice and coordination from UCS toward planning and implementation.

5) Maintenance

Equipment maintenance is the responsibility of each individual user. Maintenance contracts are not generally recommended but are available through most vendors. Users should expect to spend approximately 15% of the list price of their equipment in annual maintenance.

ARTICLE V: INFORMATION TECHNOLOGY AND TELECOMMUNICATIONS
Section 2. Information Systems/Technology Policies

Policy 2.2:Computer and Information Code of Conduct Policy
Issued: June 1, 2002

Chicago State University
Division of Information Technology
Computer and Information Code of Conduct Policy for Chicago State University Employees

I Adhering to Federal, State and University Regulations and to Generally Accepted Standards of Professional and Ethical Behavior

All employees of Chicago State University (CSU) are expected to familiarize themselves with and to adhere to all applicable federal, state, University and Board Trustee rules, policies and procedures in their personal on-the-job conduct. This includes adhering to all University policies and procedures covering equal opportunity and nondiscrimination and avoiding actions and behavior prohibited under federal and state statutes, rules and regulations and University and Board policies and regulations. Pursuant to the applicable provisions of the State Universities Civil Service Merit System, collective bargaining agreements and University and Board procedures, disciplinary action may be taken against employees who fail to meet these responsibilities.

II Protecting Data and Information Privacy

All Chicago State University records, including both written documents and electronic data are to be regarded as confidential.

Students records are particularly sensitive because of the Family Educational Rights and Privacy Act of 1974 (FERPA), which requires post-secondary educational institutions and agencies to conform to fair information practices in their handling of student data. Among the provisions of the act are the requirements that data be used only for intended purposes and that those employees responsible for student data take reasonable precautions to prevent misuse of it. In accordance with the provisions of FERPA, Chicago State University grants employee access to student data only on a need-to-know basis and only for appropriate administrative, research, educational, or service functions, including but not limited to counseling and/or advising students, reporting to state and federal agencies, administering financial aid, conducting internal ad hoc reporting, etc.

Protection of Chicago State University records and compliance with FERPA rests ultimately upon the individuals entrusted with access to data.

All Chicago State University employees are expected to maintain and protect the privacy of data and information which they handle or to which they have access as a function of their jobs by following these basic rules:

- ❒ *Don't tamper with or intrude upon any transmission, whether by voice, non-voice or data.*
- ❒ *Don't permit the conversation or communication of another person to be monitored or recorded except as required in the proper management of business.*
- ❒ *Don't allow an unauthorized person to have access to any communication transmitted to our facilities.*
- ❒ *Don't install or permit installation of any device that will enable someone to listen to, observe, or realize that a communication has occurred, except as authorized by an official service or installation order issued in accordance with University practices.*
- ❒ *Don't use information from any communication, or even the fact that a communication has occurred, for your personal benefit or for the personal benefit of others.*
- ❒ *Don't disclose information about student or employee data.*

Report to your supervisor immediately if you believe that the privacy of any communication has been compromised or if you receive a subpoena, court order, or any other type of request for information from anyone (including law enforcement).

Student and employee records are to be held in confidence and treated as University assets. They should be disclosed only upon proper authorization or as directed in University privacy rules or pursuant to lawful process. Any questions about the release of any information from such records should be directed to the Chief Information Officer of the Information Technology Division.

III Handling Copyrighted and Other Proprietary Information

Proprietary information is any information, including any software information, in which either the University or some other person has an exclusive legal interest or ownership right, such as a copyright. The unauthorized reproduction, release or disclosure of such information is prohibited by law, and could have serious legal consequences for both any employee who produces or releases it and for the University.

Questions on whether information is proprietary and the conditions under which it can be released should be referred to your immediate supervisor.

In general, Chicago State University employees are expected to:

- ❒ *Obey U.S. copyright laws and University policy regarding the reproduction of copyrighted software. Most purchased software is copyrighted and may not be copied except to make an archival copy or as an essential step in its utilization.*

- ❒ *Use licensed computer software only as permitted by the specific license.*

When employees leave the department, all documents and records containing proprietary or classified University or department information must be returned to the department. Even after employment ends, former employees have a continuing obligation to safeguard this information.

IV Protecting the Security of Computer Systems

Employees are responsible for ensuring that compute systems and the information they contain are adequately safeguarded against damage, alteration, theft, fraudulent manipulation, and unauthorized access or disclosure. Ultimately, each employee is responsible for the security of information accessed or modified under his or her password or access procedure. Also, as manager or user of university data or University computer resources, each employee must strictly adhere to the specific security measures and controls that have been established.

Any personal or other non-University use of University data communication or University

computer system (mainframe, micro, mini or personal computer) that is not expressly sanctioned by supervisors is forbidden.

V. Employee Acknowledgment of Responsibility

The I. T. D. Computer and Information Security Policy and Non-disclosure Agreement reaffirms the importance of following the highest standards of professional and ethical conduct. Adherence to these standards by all employees is the only sure way the University can maintain the confidence and support of the public.

As summary of these principles, this policy does not include all of the rules and regulations that apply to every situation. Its contents must be viewed within the framework of University policies, practices, and instructions, and the requirements of the law. Moreover, the absence of a University practice or instruction covering a particular situation does not relieve an employee from acting ethically. Employees with questions about a particular situation should consult their supervisor.

Violations of this policy may result in disciplinary action, including possible dismissal.

Within Chicago State University anyone whose designated duties require access to student or employee records may use that information for appropriate research, educational, or service functions. Along with that access comes the responsibility to safeguard the individual's right to privacy and maintain the confidentiality of all records. Recognizing the responsibility that I have regarding any access to CSU records, I agree to the following:

- ❒ *I will access CSU student and employee records only as required to perform assigned duties*

- ❒ *I will store information under secure conditions and make every effort to ensure that individual's privacy.*

- ❒ *I will not release suppressed or private information without authorization and I will not publicly discuss a record in a way that might personally identify that student or employee.*

- ❒ *Unless release of public information is regarded as part of my job, I will notify my supervisor immediately of any request I receive for public records.*

- ❒ *I will not release any information if the student has requested a total suppression of information on himself/herself.*

- ❒ *When I release information on a student, I will divulge only information regarded as "directory" or public information, specifically the student's name, address, telephone listing, date and place of birth, major field of study, classification, participation in officially recognized activities and sports, the weight or height of members of athletic teams, dates of attendance, degree and awards received, and most recent previous educational agencies or institution attended. Furthermore, I will not release public information about students that was requested on the basis of non-public information (e.g. names of all international students, names of all students with a GPA of less than 2.0 etc.)*

I understand that if I violate any of the terms of this agreement I am subject to disciplinary action.

Name (Printed): _____

Signature: _____

Date: _____