I. INTRODUCTION
   A. CSU Information Security Policy
   B. References
   C. Responsibilities for Campus Information Resource Personnel

II. PHYSICAL SECURITY
   A. Protection Against Natural/Accidental Disasters
   B. Protection Against Intentional Disasters
   C. Management Controls and Procedures

III. DATA SECURITY
   A. Ownership
   B. Access to Data
   C. Data Protection
   D. Data Validity and Integrity
   E. Privacy

APPENDICIES

Appendix A  Computing Practices and Security Awareness for Users
Appendix B  California Penal Code - Section 502
Appendix C  Access To and Use of CSULB Computing Resources

08/21/97
I. INTRODUCTION

A. CSU INFORMATION SECURITY POLICY

The Board of Trustees (BOT) of the California State University CSU) is responsible for protecting the confidentiality of information in the custody of the CSU, the security of the equipment where this information is processed and maintained, and the related privacy rights of the CSU students, faculty and staff concerning this information. This policy applies to all students, faculty and staff, consultants employed by the CSU, or any other person having access to CSU information technology resources. The unauthorized modification, deletion, or disclosure of information included in CSU data files and data bases can compromise the integrity of CSU programs, violate individual privacy rights, and possibly constitute a criminal act. This responsibility is delegated to the campus Presidents in accordance with CSU policies. In order to implement these policies and procedures, each campus President and the Chancellor should designate an Information Security Officer (ISO) to oversee this important program.

To ensure that the Information Security Officer is not in a position of conflict of interest, he/she should not have immediate direct responsibility for a data processing facility (e.g. computer operations manager), nor should he/she be an official having program responsibility for the confidential information. If possible, he/she should be independent of, and have no personal responsibility for campus programs that rely on the confidential information or computer operations which manipulate and store the information. The responsibilities and duties of the Information Security Officer are delineated, at a minimum, in this policy statement.

If the Campus Information Security Officer and the campus Information Resource Manager are not the same person, the Information Security Officer should keep the Information Resource Manager informed of any changes of security and confidentiality procedures affecting the Information Resource Management program. Similarly, the campus Information Resource Manager should provide coordination and services support to the Information Security Office in the area of security and confidentiality as requested.

B. REFERENCES
Article 1, Section 1, of the Constitution of the State of California, defines pursuing and obtaining privacy as an inalienable right.

The Information Practices Act of 1977 (Civil Code Section 1798, et seq.) places specific requirements on State agencies in the collection, use, maintenance, and dissemination of information relating to individuals.

The California Public Records Act (Government Code Sections 6250-6265) provides for the inspection of public records.

The Comprehensive Computer Data Access and Fraud Act (Penal Code Section 502) affords protection to individuals, businesses, and governmental agencies from tampering, interference, damage, and unauthorized access to lawfully created computer information systems. It allows for civil action against any person convicted of violating the criminal provisions for compensatory damages.

Title V section 42396.2(d) of the California Code of Regulations confirms the right to privacy in California and states an intent to implement it within the CSU.

The Family Education Rights and Privacy Act (20 U.S.C. Section 1232g) (commonly referred to as FERPA or the Buckley Amendment) is a federal statute applicable to every institution which receives federal funds. It protects students (and former students) from the release of personal information about them. It provides for the right of a student to inspect and review his or her own education record, the right to request the records be amended, and the right to some control over the disclosure of personally identifiable data from such records.

C. RESPONSIBILITIES FOR CAMPUS INFORMATION RESOURCE PERSONNEL

The physical security of computer-stored information is the responsibility of the computer installation holding such information and includes but is not limited to delivery of output, disposal of waste material, and on-site access, as required by the owners of the data. The computer installation is also responsible for providing the means of controlling access to confidential information by terminals and programs as required by the owners of the data.

Administrative control of the access to and use of computer-stored information is the responsibility of the user which collects or receives and
maintains that information. All confidential files shall have access restricted by such owner through passwords or other similar means. The owner of confidential data must also establish and periodically disseminate the rules of access.

**PRESIDENT**

1. Responsible for protection of all campus information resource assets and proper reporting of all losses and violations of information confidentiality, security, and privacy policies and procedures.


3. Delegates review and investigative authority to Information Security Officer.

4. Ensures independence of Information Security Officer and the compliance function.

5. Provides necessary resources for the Information Security Officer to carry out his/her function.

6. Provides necessary training for the Information Security Officer to carry out his/her function.

**INFORMATION SECURITY OFFICER**

1. Promotes and encourages good security policies and procedures.

2. Performs appropriate risk analysis.

3. Prepares and maintains a manual of campus security procedures for applications, data bases, remote access, distributed processors, and microcomputers.

4. Monitors to ensure compliance of privacy and information security policies and procedures.

5. Identifies and reduces vulnerabilities.

6. Informs campus President and others about security matters.

7. Coordinates determination of the priority and data sensitivity of applications and other information processing activities.
8. Coordinates cost/benefit analysis to determine level of security required.

9. Ensures establishment and existence of backup, disaster, and recovery capabilities.

10. Develops campus-specific public access implementation policies and procedures.

11. Following notification by Public Safety, investigates violations of security and confidentiality policies and procedures.

12. Annually develops a summary report of computing equipment losses and violations of security and confidentiality policies and procedures.

13. Implements procedures to assist in the development of security awareness in personnel.

14. Develops plans to test existing security safeguards.

15. Annually, performs audit of all confidentiality and security policies and procedures to ensure highest confidence in those policies and procedures.

PROGRAM MANAGEMENT

1. Identifies and classifies sensitive data.

2. Identifies authorized users of data.

3. Assists with the identification of exposures related to vulnerabilities.

4. Makes public access decisions based on decision-making criteria with the concurrence of the Information Security Officer.

5. Maintains required level of security.

6. Applies sanctions and disciplines for security violations.

7. Reports to Public Safety all computing equipment losses due to theft.

8. Reports to the Information Security Officer all violations of security and confidentiality policies and procedures.
9. Develops and implements procedures to foster awareness in personnel of the importance of, and responsibility for, the security of computing equipment, data, and information.

SYSTEM DEVELOPMENT AND PROGRAMMING MANAGEMENT

1. Understands and implements CSU security policies and procedures.
2. Understands security problems in a data processing environment.
3. Addresses data security requirements in all systems development.
4. Explains available security tools to program managers.
5. Tests security measures.
6. Implements technical security measures specified by program manager.
7. Reports to Public Safety all losses of equipment due to theft.
8. Reports to the Information Security Officer all violations of security and confidentiality policies and procedures.
9. Develops and implements procedures to foster awareness in personnel of the importance of, and responsibility for, the security of computing equipment, data, and information.

DATA PROCESSING MANAGEMENT

1. Provides logical security features and tools for use by program managers.
2. Describes procedure requirements to protect against natural, accidental, and intentional disasters.
3. Describes required facilities management controls and procedures.
4. Reviews system development designs for adequacy of security provisions.
5. Ensures that security provisions are implemented as designed.

7. Provides assurance that computer information is adequately secured prior to implementing general public access.

8. Regularly inventories computing equipment and reports unexplained losses to the Information Securities Officer and other proper officials.

9. Reports to Public Safety all equipment losses due to theft.

10. Reports to the Information Security Officer all violations of security and confidentiality.

11. Develops and implements procedures to foster awareness in personnel of the importance of, and responsibility for, the security of computing equipment, data, and information.

12. Insures adequacy of safeguards of irrecoverable corporate data assets.

INDIVIDUAL USERS

1. Strictly observes all laws, policies, and procedures related to privacy, confidentiality, and security of information.

2. Reports to Public Safety all losses of equipment due to theft.

3. Reports to the Information Security Officer all violations of security and confidentiality policies and procedures.

4. Develops and implements procedures to foster awareness in personnel of the importance of, and responsibility for, the security of computing equipment, data, and information resources.

PUBLIC SAFETY

1. Participates in the development of the campus’ statement of security procedures.

2. Receives and investigates all reports of computing equipment thefts.
3. Responsible for, at a minimum, annual reporting to the Information Security Officer of thefts, specifically identifying information technology resources.

II. PHYSICAL SECURITY

A. Protection Against Natural/Accidental Disasters

Fire Plan - All employees should be familiar with the building fire plan. An annual Fire/Emergency Exit Drill must be coordinated with the University Police Fire/Emergency Planning coordinator. All areas have portable fire extinguishers available for use in emergencies and each employee must be aware of their location and method of use. Managers will visually inspect all fire fighting equipment in their area of responsibility. A deficiency record will be maintained pertaining to the following:

1. Fire hose and fire extinguishers are at their assigned locations.

2. All fire extinguishers equipped with a dial must indicate a “good” reading.

3. All fire extinguishers are sealed and tagged, indicating the type and serviceability.

4. Any variation from the above must be reported to the University Police Fire/Emergency Planning Coordinator (extension 4101) as soon as discovered.

The record should indicate: The date, time, who called, who they talked to and nature of discrepancy. The record must also show when the discrepancy was corrected.

The record will be available for inspection/review at any time.

In the event of a fire, or the smell of smoke: Call University Police Department Emergency 9-1-1. However, if you become fearful for your safety, sound the alarm and follow the established evacuation procedures.

Report
The location of the fire.
What is burning.
Any/all injuries - all handicapped personnel requiring assistance.
Your name.

Utilize the nearest fire alarm box.

Comply with evacuation instructions.

Send someone to meet the University Police Department.

Types of Fires

Class A. Fires in ordinary combustibles such as paper, wood, cloth, etc., which are extinguished by cooling.

Class B. Fires involving flammable liquids such as gasoline, oil, alcohol, benzine, ether, etc., which are extinguished by smothering.

Class C. Fires involving electrical equipment, appliances, and wiring in which the use of a non-conductive extinguishing agent is recommended.

Extinguish Class A fires with water.
Extinguish Class B fires with carbon dioxide or Halon (1211).
Extinguish Class C fires with carbon dioxide or Halon (1211).

However, water may be used after the involved area has been deenergized. All employees must know the location of all electrical control panels.

Types of Fire Extinguishers: It is important to use the correct type of extinguishing agent on any type of fire. Extinguishers should be of the type most suitable for the “class” of fire which may occur.

Extinguishers are classified as Type A, B, and C. Prolonged use of water possesses the greatest cooling effect of any readily available known substance. Since a cooling effect is required for Class A fires, water should be used.

A dense, heavier than air gas, powdered chemical, or foam should be used in Class B fires. The desired effect in Class B fires is smothering to exclude air. Class C fires require extinguishment by use of a non-conductive agent.
Fire Abatement Plan - The Computer Center can be characterized as a large electrical complex containing large quantities of flammable paper, card stock, etc. The fire hazard can be considered high.

Disaster Plan - A disaster is defined here as any circumstance where actual or anticipated interruption of regular Computer Center service occurs. Earthquakes, floods, enemy attacks, power loss, a fire, a bombing or explosion, a bomb threat, a riot, or civil disturbance are all disasters.

To Deal with Disaster -

1. Know the location of campus shelters.
2. Know the telephone number of the University Police Department’s Emergency Operations Center.
3. Know how to evacuate the area and where to go.
4. University Police Officers will take command during disasters.
5. Shut down and secure the Computer Center before exiting the building.
6. Call the University Police Department for assistance, extension 4101 or 9-1-1.

Work immediately critical to the University will be planned for off-site processing during lengthy emergencies.

Computer staff will report to the Computer Center from the University Police Department.

Evacuation Plan - Evacuation orders will come from the University Police Department.

1. All electrically powered equipment will be powered down in the event of an emergency to minimize loss of data.
2. Room lights will be left on to facilitate rescue and fire work.

Employee Safety and Welfare
Procedural guidelines for the safety and welfare of University employees are promulgated for the information of all concerned. Although disorders may not interrupt work routines on the campus, the following procedures are provided for employees guidance in the event local interruptions do occur:

1. In the event of a disturbance, disorder, march on campus, or similar activity, employees are urged to remain at their work and away from the scene. (Curious observers are sometimes involved because of their mere presence in the area.)

2. Unless otherwise directed, the highest level supervisor present in the area has the authority to release employees from work when he/she considers the circumstances warrant such precautions. The supervisor present shall direct employees to report to another area on campus safely away from the disturbance and shall remain with the employees in the area selected. He/she will contact the Staff Personnel Office for further instructions and advise the employees when it is safe to return to their work.

3. If necessary to evacuate a building, all persons should stay at least 200 feet away. The fire alarm system may be used to evacuate buildings for reasons other than fire.

In addition to the above guidelines relative to leaving and returning to workstations during disturbances on campus, the following recommendations are considered appropriate:

1. Be sure files and cabinets furnished with locks are locked and the office is not open. Be careful with office and file keys in your possession. Keep them in a safe place -- not in a place where they can easily be picked up by unauthorized personnel. Keeping personal items of value in your desk or in your work area is not advisable.

2. Your physical safety is of the utmost importance. **DO NOT** attempt to fight to protect property, records, etc.

3. If you suspect an object to be a bomb, stay away and get behind a wall if possible, a desk, or other solid protection. Do not touch or move the object.

4. Do nothing to provoke demonstrators -- be courteous regardless of how you might feel about the situation and do not engage in arguments.
5. The University Police Department can be contacted in case of an emergency by calling 9-1-1. Another extension is 4101. They are prepared to respond and to provide assistance as necessary.

**Telephoned Bomb Threats**

Telephoned bomb threats on this campus have occurred during the past several years. In the past, most threats were received by the switchboard operator. But, under the Ericsson system, they may be received on any telephone. The following policies and procedures are to protect persons and property, and to reduce disruption of normal activities to a minimum.

The telephone procedure by an employee receiving a threat is as follows:

1. When a bomb threat telephone call is received, the person receiving the call will attempt to hold the call as long as possible and ask the caller detailed questions regarding:
   
   a) When is the bomb going to explode?
   b) Where is the bomb right now?
   c) What kind of bomb is it?
   d) What does it look like?

2. Alert the supervisor immediately by writing the nature of the call on a piece of paper or some other means.

3. The supervisor will immediately call the University Police Department, extension 4101 or 9-1-1, and give the following information:

   a) Identify location and department.
   b) Identify by name, the person calling.
   c) Explanation of the threatening call and bomb scare.
   d) Give the number the incoming call is on.

4. In no case should any person, other than a University Police Officer, touch or move any suspected object or container.

**Bomb Search Procedures**
The University Police Department will conduct the bomb search. The Computer Center supervisor may be required to aid in this task because of his/her familiarity with the physical plant.

All suspicious objects will be reported immediately to the University Police Department.

No attempt should be made to move, touch, cover, or jar any suspicious object.

Evacuation will be ordered, if deemed necessary.

**Evacuation of Buildings or Areas**

1. Required evacuation will normally be initiated by the use of the existing fire alarm system, followed by additional announcements by University Police Officers stationed outside the building. When the fire alarm is sounded, total evacuation is **MANDATORY**.

2. Evacuation should be made calmly and smoothly. Elevators should be utilized only for evacuating paraplegic or otherwise handicapped persons. Remember that in practically every case, the purpose of a bomb threat is to create disruption and panic. You can assist by keeping all persons calm.

3. Persons leaving the building or area should be instructed to:
   a) Take personal belongings with them.
   b) Leave doors and windows open and lights on.
   c) Go to an area at least two hundred feet from the building and out of line of any glass windows or doors of that facility.

4. Key personnel, in the event of evacuation, should go to the University Police vehicle being used as a command post nearby to be available to assist the officers with information or crowd control.

**Suspicious Packages**

In a University this size, packages, briefcases, and similar objects are commonplace. However, there may be times when an object is so
noticeably unusual, by either its means of delivery or locations, as to become “suspicious”. In such a situation, the University Police Department should be called immediately (dial 9-1-1). In no case should the object be touched or moved by non-police personnel.

**Written Bomb Threat**

A bomb threat may be received in written form at the Computer Center. On reading such a threat, the University Police Department will be notified immediately. The documents will not be further handled once the contents are determined.

**Fire Threats**

Title 19 of the California Administrative Code requires colleges and universities to hold a fire drill on campus in order to familiarize students on evacuation procedures in case of emergency. During fire drill, the following procedures will be followed:

1. The fire warning system will be activated simultaneously in all buildings on campus. The fire alarm in the residence halls consists of a continuous bell ringing and klaxon-type horn in all other buildings.

2. When the fire alarm rings, all personnel will leave the buildings at a walk and move at least 200 feet away from the buildings.

3. All other personnel in the open when the warning sounds, shall remain in the open and at least 200 feet away from the buildings.

4. The evacuation of all classrooms shall be under the direction of instructors; occupants of rooms other than classrooms, including offices, shall leave buildings immediately by using the nearest exits.

5. Upon evacuation from the building due to various circumstances, **POWER-OFF COMPUTER AND EQUIPMENT**.

6. The fire drill will continue for 10 minutes when normal activities will resume.

**Procedures to be Followed in Cases of Sudden Illness, Injury, or Apparent Death:**
1. Procedures to be followed during regular college business hours:
   a) Dial 9-1-1 for any emergency.
   b) Emergency calls on extension 9-1-1 between the hours of 8:00 a.m. and 6:00 p.m. are monitored simultaneously by
      the Health Center and the University Police Department. Based upon the information received, Medical personnel
      may be dispatched directly to the scene. Upon arrival, Medical personnel will determine what treatment is required
      and whether an ambulance is to be called.

2. At times other than regular business hours:
   a) Dial 9-1-1 for any emergency.
   b) Emergency calls will be handled by the University Police
      Department. Based upon information received, the Long
      Beach Paramedics and/or ambulance may be dispatched at
      the same time the University Police unit is dispatched.
      Taking information as to an obviously critical condition, a
      University Police Officer upon arrival at the scene will
      determine whether Paramedics and/or ambulance should be

3. In the event of death, the University Police Department will respond
   to the scene. Except by an officer, the body should not be touched
   or moved. The body should be covered, if possible. University
   Police will assume the responsibility except for notification of next
   of kin should be made by a co-worker, friend or acquaintance of the
   family through means of a personal visit rather than by telephone.
   The person who undertakes to inform the relative must act with due
   care. A delicate duty has been assumed and if a co-worker or
   friend of the family cannot be found on campus, the informant
   should endeavor to find someone such as a minister, doctor or off-
   campus friend to break the news gently and in person to the family.

B. Protection Against Intentional Disasters

The general policy of Information Technology Services is to restrict access
   to the production control and computer room areas to authorized
   personnel only. Other personnel will be admitted on a need-to-enter
   basis. Entrance to Information Technology Services may be authorized
   only by the Assistant Vice President for Information Technology Services,
   the Information Security Officer, or their designees.
All doors for normal access to the computer operations area shall have self-locking electronic or combination locks. Combinations shall be changed as employees terminate and at regular intervals.

All unauthorized or attempted intrusions shall be reported to the Assistant Vice President for Information Technology Services or the Information Security Officer when the Assistant Vice President for Information Technology Services is not available.

**Limited Access**

Access to other computer room shall be denied to all except authorized Information Technology Services personnel, Information Technology Services management, authorized vendor personnel, University Police, Fire Marshal, and assigned building maintenance personnel. All such personnel will be named on a “Authorized Access List.” Other management personnel and visitors may be admitted if proper authorization is obtained from the Assistant Vice President for Information Technology Services or the Information Security Officer when the Assistant Vice President for Information Technology Services is not available.

Access by any personnel, other than those named on the Authorized Access List during non-scheduled hours, shall be controlled and shall require prior notification and authorization from the Assistant Vice President for Information Technology Services or the Information Security Officer when the Assistant Vice President for Information Technology Services is not available.

**Internal Security**

All computer operations personnel shall be trained in emergency procedures. Use of emergency switches and power-down procedures shall be understood by all operations personnel. There shall be emergency lighting in the computer and support areas. The auxiliary lighting system shall be tested at least twice a month.

All personnel shall be trained in the proper evacuation procedures to be used in the event of fire or acts of violence. Regularly scheduled drills shall be held and appropriate instructions shall be posted.

Smoking, eating, or drinking shall not be permitted in the computer room or tape library. These areas shall be kept clean.
Only authorized persons shall operate the computer system.

Confidential program listings and carbons which are not to be retained shall be placed in a designated area in the controlled environment. The material shall be removed at specified time and destroyed by shredding.

If material includes personal data such as names, addresses, phone numbers, and social security numbers or gives any information which can be identified with a particular person, the material shall be treated as confidential material.

**Personnel Identification**

Only those persons with acceptable identification and whose names appear on the Information Technology Services Authorized Access List or who have acceptable signed authorization from the Information Technology Services Assistant Vice President, the Information Security Officer, or their designee shall be admitted to the Information Technology Services Operations area.

All computer room visitors (a visitor is defined as a person whose name does not appear on the active Information Technology Services Authorized Access List) shall sign in and out on a log maintained at the desk of the Senior Computer Operator. Included on the log shall be name, organization, date, time in and out.

All visitors to the operations area shall be escorted to and from their destination by an employee of Information Technology Services. Visitors shall not be left unattended.

When appropriate, all packages, briefcases, tool cases, etc., shall be inspected upon entering and before leaving the operations area.

The Authorized Access List shall be updated periodically to reflect hiring, separations, and newly authorized accesses.

**Software Security**

Storage of backup data sets shall be maintained in a fireproof safe. The backup of all user data sets, programs, documentation, and procedures for recreating data sets is the responsibility of the user.
The operating systems shall have protection to prevent by-passing of security utilities.

All permanent mass storage files shall use, and change as necessary, access and modification privacy codes to prevent unauthorized access, tampering or destruction. Access and modification of blanks or asterisks shall not be used and will not be accepted for processing.

All permanent tape files shall be internally labeled and shall contain privacy codes to prevent unauthorized access, tampering, and destruction. Privacy codes shall be changed periodically.

Only members of the Information Technology Services Operation Support group and other persons as may be specifically authorized by the Information Technology Services Assistant Vice President or designee, shall have access to operating systems.

C. Management Controls and Procedures

Management control is the plan of organization and methods within the department which is designed to safeguard its records, check the reliability of its data, promote operational efficiency, and encourage adherence to prescribed policies.

Management Responsibility

The Assistant Vice president for Information Technology Services is responsible for the establishment of organizational, administrative, and procedural controls which are necessary to prevent access to data for unauthorized or improper purposes, reduce the incidence of error, and obtain optimum results from computer operations. Controls can be divided into groups as follows:

1. Each employee should fully understand his or her duties, responsibilities, and limits of authority.

2. Job Assignments, facilities, and procedures should be arranged so that, as far as possible, no one person will have complete control over an entire transaction of a related series of operations without the intervention of another employee or employees to provide a cross-check.

3. In the assignment of duties and responsibilities, an organization chart should be maintained and be kept current and, as an adjunct,
specific duty statements should be published and understood by all staff members.

4. To be effective, internal controls must be reviewed periodically because of changes in personnel and duties. The most elaborate system of internal controls will not prevent inefficiencies or fraudulent practices unless adequate and continuous supervision is exercised. Controls must be consistent with the hazards involved and the cost of controls should be commensurate with the risk.

5. Security procedures should be distributed to all management and responsible staff personnel and made available to all others who have a need to know.

6. Principal points and important employee instructions for security procedures should be posted on employee bulletin boards.

7. Emergency phone numbers should be prominently listed in internal phone booklets and maintained around the computer facility for emergency calls.

8. All electrical appliances, such as lamps and clocks, used in or around the computer facility, must be UL approved.

9. Emergency electrical and air conditioning shut-off switches and gas shut-off valves should be clearly marked and precise instructions posted nearby as to when and how they are to be used.

10. Management should, wherever possible, eliminate possible sources of computer failure or transient malfunctions. Permanent or temporary conditions that create dust, excessive moisture, or conditions that promote corrosion should be avoided.

11. Documentation for operational programs, manuals of system operating instructions, and other vital and important records should be stored in record protection equipment having a fire-resistant rating of one hour or better or at an off-site location.

12. In order to apply proper safekeeping for difficult-to-replace records, securities, negotiable instruments, checks for deposit, highly confidential information or similar materials, should be stored in safes or vaults with at least a four hour fire-resistant rating or at an off-site location.
III. **DATA SECURITY**

Since information may reside in Information Technology Services which could be detrimental to people’s interest if allowed in unauthorized hands, every Information Technology Services employee shall exercise caution and care when handling data. Disclosure of the data to any unauthorized person either in detail or summary is absolutely prohibited and could result in discipline including termination.

The Information Technology Services Assistant Vice President shall periodically make inspections of sensitive files, computer and visitor logs, and precautionary procedures to ensure the maintenance of appropriate security measures.

All new employees of Information Technology Services shall review this security manual annually. All new University employees will receive data security information at their initial employee orientation. (See Appendix A)

The Information Technology Services Assistant Vice President shall make certain that all Information Technology Services employees receive security briefings according to schedule.

The staff of Information Technology Services, when appointed, will be subject to a background investigation which will be conducted during the course of their recruitment. The results of this investigation will be communicated only to the Information Technology Services Assistant Vice President.

Inventory of magnetic tapes and disk packs shall be taken at periodic intervals and missing items shall be reported to the Information Technology Services Assistant Vice President or the Information Security Officer when the Information Technology Services Assistant Vice President is not available.

Scratch tapes and disk packs shall be degaussed, blanked, or overwritten.

### A. Ownership of Files

Data resident on data files is the property of other user holding the account number under which the data file was created.

All data files shall be physically maintained in the Information Technology Services facilities unless released at the request of the owner. A log of data file transactions shall be maintained.
The data file owner assumes responsibility for the confidentiality of the data when the physical data file or processed data is removed from Information Technology Services.

The data file owner is responsible for the prudent duplication of otherwise irreplaceable data files.

B. Access to Data Files

Data may be accessed by the owner of the data file.

Authorization for access of data must be in writing with a copy forwarded to Information Technology Services.

If necessary, data may be accessed by a member of the CSU staff having direct line authority over the data file owner. In such instances, the data file owner shall be so informed.

Information Technology Services shall prevent unwarranted disclosure of information from discarded printed and other output by shredding output with confidential information.

C. Data Protection

There shall be a separate data file storage area with procedures provided for logging data files IN and OUT; keeping a current list identifying persons who are authorized to receive data files; keeping records to indicate the precise locations of all data files at all times; performing follow-up work to retrieve issued data files not returned to the library within prescribed time limits; and identifying data files which are no longer needed in accordance with established file expiration dates.

All data files shall be clearly labeled. The label shall show the name of the file and the associated account number.

Data files shall be brought to the computer room for processing only. They shall be returned as soon as possible to the library after processing.

D. Data Validity and Integrity
The integrity of a data file begins with its internal label. Label errors will not be accepted; when a label error occurs, the operator shall abort the job.

Once data has become machine readable, its validity and integrity shall continue to be checked by appropriate program controls such as label checking, edits for numeric and alphabetic fields, oversize amounts, blank fields, sequence checking, counting of records in and out of sorts, utilities, and user programs. As applicable, programmed output controls shall use exception reports listing unacceptable transactions or input records, errors, and warning messages. Aborts shall occur if critical control errors are found.

Manual output controls shall include procedures for routing of output and dismountable files, disposal of extra copies and carbons, and delivery of data and reports in a confidential and secure manner.

Generally, audit trails and control functions shall provide the input for file reconstruction.

When appropriate, manipulation of the data in a file shall result in applicable exception lists, activity reports, and other documents which will be instrumental in identifying security violations. When applicable, the following provisions shall be used to establish security controls:

1. Logs of transactions from terminals including identity of terminal and user number.
2. Logs of additions, updates, and deletions.
3. Tables of users authorized to use particular systems and files.
4. Logs of files accessed and the identification of users.

As appropriate, the production control section shall verify the proper execution of reports.

E. Privacy

Information Technology Services realizes that the increasing use of computers and information technology, while beneficial to the efficient operation of management, has magnified the potential for
harm to individual privacy which can occur from collection, maintenance, use, and dissemination of personal information. It recognizes the right of privacy and, accordingly, treats all data as confidential. Further, under the directives of the Information Practices Act of 1977 and SAM section 4846.5, employees are required to bring any information which might indicate a possible infringement of the right of privacy to the attention of the Information Technology Services Assistant Vice President or the Information Security Officer when the Information Technology Services Assistant Vice President is not available.

Information Technology Services recognizes the following general principles regarding personal data:

1. Personal data should not be collected and maintained unless it contributes to the operations and management of the University in the reasonable performance of functions for which it is legally responsible.

2. Personal data collected by one state agency should be shared with other state agencies only to the extent that there is determined authorized need.

3. Personal data should be protected as necessary to ensure that such data is used only for lawful purposes within the University and not made available to outside individuals or groups except as provided by law and with the proper responsible authorization.

4. If personal data is released to outside individuals or groups by proper authorization, it should be in an anonymous form where personal identification is removed and the number of data records is sufficiently large to preclude individual identification.

5. Personal data shall be audited periodically to ensure its continued need and accuracy. Procedures shall exist for correction of inaccuracies.

6. The physical environments where personal data is processed and stored shall be audited with such frequency as is needed to ensure the maintenance of adequate safeguards against damage, alteration, theft, and possible penetration by unauthorized persons.
APPENDIX A

COMPUTING PRACTICES AND SECURITY AWARENESS FOR USERS

Security is the concern of all CSULB computing users. Users are encouraged to use CSULB computers for legitimate educational or administrative computing. However, some users may be tempted to abuse this privilege. Any department operating computer systems is responsible for securing the systems and for informing users of expected standards of conduct:

1. COMPLIANCE WITH SECURITY MANUAL - Users accessing CSULB computers must follow the policies published in the CSULB Security Manual. Disciplinary actions will be based upon violations as explained in the Security Manual.

2. UNAUTHORIZED COMPUTER USE - The use of CSULB computer systems for unauthorized activities is forbidden by state law. Each user is responsible for the proper usage of the computer and must use it only for the purposes for which it was authorized. Examples of unauthorized uses are attempts to modify operating systems and applications software, access of files belonging to other users without their explicit permission, use of computers for profit, use of electronic mail to send damaging or harassing mail, physical damage to computer systems, etc.

3. DISCONTINUANCE OF SERVICE - Provision of computing services to any user may be suspended if security violations, as described in the CSULB Security Manual, are discovered.

4. MICROCOMPUTERS - All users must remain alert to the many security threats to personal computers, particularly those computers that are located in work areas that are accessible to the public. Staff are encouraged to question the presence of outsiders in work areas and to report any unusual occurrences to the Information Security Officer. Users of personal computers are cautioned to treat the associated data files with the same degree of care they would employ for other confidential automated and manual files.

5. PASSWORDS - In the case of those resources protected by password, users should frequently change their password to keep someone else from accessing and tampering with their data.

6. PRIVACY - Users should respect other users’ rights to privacy. That is, you should not access, copy, modify, or destroy the computer work of others. Each timesharing or fileserv account belongs to an individual or a department. Individual user names and passwords belong solely to the
owner of the account and must not be given out to anyone else. Programs and files belong to the owner of the account containing the programs and files. They are private and confidential; only the owner can explicitly give permission for another user to access them. The same principle applies to files stored on network file servers or other electronic data storage devices. Interception of network or other communications data traffic is considered equivalent to the violation of privacy described above.

7. COURTESY - Courtesy, kindness, and sensitivity to the needs of others should mark all use of the facilities. Insofar as possible, proficient users should be willing to help and advise less proficient users. Deliberately offensive material must not be sent or stored on the systems; e.g., obscenities, slanders, insults, demeaning, or unnecessarily embarrassing remarks or information. Users should use resources as efficiently as possible so as not to adversely impact other users. A user should not deprive other users access to the resources by attempting to crash systems, modifying standard system configurations, filling storage devices with useless data, playing computer games, deliberately loading the computer network, failing to observe time limits for the use of lab resources, etc.

8. NETWORKS - Access to wide-area networks, such as CSUnet and the Internet, of which the University is a part, is a privilege, not a right. It is vital to the continuance of the University’s membership in these networks that no abuses take place which reflect on our ability to use these facilities responsibly. Under no circumstances should unauthorized use be made of the computing resources at other sites. In particular, attempts to defeat the security of computer systems belonging to other institutions, and unauthorized copying of files stored on machines belonging to other institutions must not be attempted. The network should not be used in a way that limits other traffic through it. This means that only important messages should be transmitted to other sites, and that large files should be transferred at night only. Network mail and messages should not be sent to people unknown to the sender. It is poor etiquette at best and harassment at worst to send messages to strangers.

9. ELECTRONIC MAIL - Use of electronic mail and message services should be confined to appropriate communications. Misuse of these services, including but not limited to harassment with their aid, will constitute a violation of the University policy. Authorized Computer Center personnel may access others’ files when necessary for the maintenance of the systems.

To help inspire user awareness, the following penal information is provided:
COMPUTER CRIME DEFINITION - California Penal Code Section 502 states that any person is guilty of a felony who intentionally accesses or causes to be accessed any computer system or computer network for the purpose of:

1. Devising or executing any scheme or artifice to defraud or extort.
2. Obtaining money or property or services with false or fraudulent intent, representations, or promises.
3. Maliciously accessing, altering, deleting, damaging, or destroying any computer system, program, or data.

VIOLATION OF CALIFORNIA PENAL CODE 502 - If you illegally use a University computer system, you may be found:

1. Guilty of a felony which is punishable by a fine not exceeding ten thousand dollars ($10,000), or by imprisonment in the state prison for 16, 24, or 36 months, or by both such fine and imprisonment; or
2. Guilty of a misdemeanor which is punishable by a fine not exceeding five thousand dollars ($5,000), or by imprisonment in the county jail not exceeding one year, or by both such fine and imprisonment.

Reporting of security problems - Any person who wishes to report an unauthorized computer intrusion, or security violation, or wishes to suggest improvements should contact the Information Security Officer at extension 58357.
APPENDIX B

CALIFORNIA PENAL CODE - SECTION 502

6. CALIFORNIA PENAL CODE - SECTION 502

502. [Definitions: Computer crimes: Status as felonies: Construction of section.]

a. For purposes of this section:

1. “Access” means to instruct, communicate with, store data in, or retrieve data from a computer system or computer network.

2. “Computer system” means a machine or collection of machines, excluding pocket calculators which are not programmable and capable of being used in conjunction with external files, one or more of which contain computer programs and data, that performs functions, including, but not limited to, logic arithmetic, data storage and retrieval, communication, and control.

3. “Computer network” means an interconnection of two or more computer systems.

4. “Computer program” means an ordered set of instructions or statements, and related data that, when automatically executed in actual or modified form in a computer system, causes it to perform specified functions.

5. “Data” means a representation of information; knowledge, facts, concepts, or instructions, which are being prepared or have been prepared, in a formalized manner, and are intended for use in a computer system or computer network.

6. “Financial instrument” includes, but is not limited to, any check, draft, warrant, money order, note, certificate of deposit, letter of credit, bill or exchange, credit or debit card, transaction authorization mechanism, marketable security, or any computer system representation thereof.

7. “Property” includes, but is not limited to, financial instruments, data, computer programs, documents associated with computer systems and computer programs, or copies thereof, whether tangible or intangible, including both human and computer system readable data, and data while in transit.
8. "Services" includes, but is not limited to, the use of the computer system, computer network, computer programs, or data prepared for computer use, or data contained within a computer system, or data contained within a computer network.

b. Any person who intentionally accesses or causes to be accessed any computer network for the purposes of (1) devising or executing any scheme or artifice to defraud or extort or (2) obtaining money, property, or services with false or fraudulent intent, representations, or promises shall be guilty of a public offense.

c. Any person who maliciously accesses, alters, deletes, damages, or destroys any computer system, computer network, computer program, or data shall be guilty of a public offense.

d. Any person who violates the provisions of subdivision (b) or (c) is guilty of a felony and is punishable by a fine not exceeding five thousand dollars ($5,000), or by imprisonment in the state prison for 16 months, or two or three years, or by both such fine and imprisonment, or by a fine not exceeding two thousand five hundred dollars ($2,500), or by imprisonment in the county jail not exceeding one year, or by both such fine and imprisonment.

e. This section shall not be construed to preclude the applicability of any other provision of the criminal law of this state which applies or may apply to any transaction. [1979 ch 858 1.]
Appendix C

California State University, Long Beach Policy Statement
96-18
August 6, 1996

Access To and Use of CSULB Computing Resources

This policy was recommended by the Academic Senate on May 16, 1996 and concurred by the President on June 3, 1996.

1. Introduction
2. Policy
2.1. Basic Rights
2.1.1. Privacy
2.1.2. Freedom of Speech
2.1.3. A Fair Share of Resources
2.2. Governing Principles
2.2.1. Individual Access
2.2.2. Responsible Use
2.2.3. Illegal Acts
2.2.4. No Commercial Use
2.2.5. Fair Sharing
3. Examples of Violations
3.1. Sharing Passwords
3.2. Unauthorized Access
3.3. Abuse of Authority
3.4. Copyrighted Material
3.5. Unauthorized Remote Activities
3.6. System Crashing and Viruses
3.7. Forging Messages
3.8. Harassment
3.9. Interception
3.10. Failure to Protect Account
3.11. Academic Dishonesty
3.12. Violating Priorities
3.13. Interfering With Others
4. Response to Violations
4.1. Legal Sanctions
4.2. University Sanctions
4.3. Investigation and Review of Charges
5. Disclaimers
6. Glossary
1. Introduction

In support of its mission to provide excellent instruction, modern research, and meaningful service, California State University, Long Beach (CSULB) offers computing resources to its students, faculty, and staff. These resources contribute to the work of all members of the University community and, therefore, must be used with great care. This document is intended to help set the tone for computing and for the use of computing resources at CSULB: respect for the rights of all users and fair use by all so as to guarantee equitable access to all users. The goal of the University in providing computing resources is to give users powerful tools to further their academic endeavors. (Administrative computing resources at CSULB -- those not used in academic endeavors -- are not addressed by this policy.) The privacy of all users and of all of their files is a fundamental right that should be respected by all. You should never use the computing resources in any way that violates the privacy of others. Clearly defined procedures established to protect your rights will consistently be followed as the University maintains the computing system.

Careful and ethical use of computing resources is the responsibility of every user. As a user of these resources, you agree to be subject to the guidelines of the "Policy Governing Access To and Use of CSULB Computing Resources." These guidelines apply to all computing resources provided by the University; some guidelines are more directly related to time sharing systems, some to microcomputers and local area networks, and some to all systems. This document includes and expands upon those guidelines, and contains a glossary of the technical terms used in the policy.

Acknowledgements: This Policy has been adapted primarily from the policy in use at the University of Kentucky, with additional ideas from the University of Delaware (especially the section on plagiarism!) and elsewhere.

In the text that follows, the Policy itself is set in straight, bold type; comments, explanations, and expansions are set in straight, non-bold type.

2. Policy Governing Access To and Use of CSULB Computing Resources

2.1. Three Basic Rights

The right of access to University computing resources is analogous to, and in many ways an extension of, the right of access to the University Library and other instructional facilities. Access to these resources is granted to an individual by California State University, Long Beach solely for the grantee's own use. Every user of CSULB computing resources has three basic rights regarding computing:

Privacy
Freedom of speech
A fair share of resources
It is unethical and a violation of this policy for any person to violate these rights. All users, in turn, are expected to exercise common sense and decency (due regard for the rights of others) with respect to the public computing resources, thereby reflecting the spirit of community and intellectual inquiry at the University. Access is a right that may be limited or revoked if an individual misuses the right or violates applicable University policies or state or federal laws.

2.1.1. Privacy

Although not legally required to do so, CSULB computer and information services departments respect the privacy of all users. System administrators and their staff may not log onto a user's account or view a user's files without explicit permission from the user (for example by setting file access privileges). Exceptions arise when the user's account is suspected either of disrupting or endangering the security or integrity of any network systems or services or of violations of applicable University policies or federal or state law. Even then, the system administrator must normally obtain prior approval of the appropriate departmental administrator unless grave danger to the continued operation of the systems requires or reasonably appears to require emergency action. This does not preclude system administrators from maintaining and monitoring system logs of user activity. Moreover, automated searches for files that endanger system security or integrity are performed regularly to protect all our users. System administrators may take appropriate actions in response to detection of such files (typically removal of those files, and possibly suspension of the user's account until the matter can be resolved).

Nonetheless, with hackers constantly probing for weaknesses in network security tools, it is unrealistic to consider anything placed on a computer that provides any services over the Internet to be truly private. Any message that you send over the network may, if you accidentally use an erroneous address, be routed to an unintended recipient. Moreover, the intended recipient may choose to forward your message to anyone without prior notice.

2.1.2. Freedom of Speech

CSULB respects the principle of academic freedom and does not attempt to censor authorized user's electronic messages or publications. If there is any doubt, users must include caveats to make it clear that they speak only for themselves, and not the University. Threats to or harassment of other users or groups whether on or off campus does not fall within the bounds of this protection and will not be tolerated. Also banned are flagrant actions which invite responses that could undermine CSULB's ability to operate on the Internet. Freedom of speech does not include the right to speak freely in an inappropriate forum nor does it provide the right to disrupt the activities of others.

2.1.3. A Fair Share of Resources

All users are entitled to their fair and appropriate share of the limited available resources such as disk space, computer time and remote access connect time. The University will
provide access to digital information resources as appropriate, e.g. office computers, classroom and individual access to computer laboratories as well as access to Internet, email, World Wide Web, usenet, data sets, appropriate software and training in the use of these resources.

Members of the University Community may be expected to provide for themselves off-site computing resources, e.g. personal computer, modem, dial-up services, etc.

2.2. Principles Governing Use of Computing Resources

2.2.1. User access is granted to an individual and may not be transferred to or shared with another without explicit written authorization by the appropriate system administrator or designee.

This principle is intended to protect the integrity, security, and privacy of your account. Sharing access with another individual undermines the security of your account, leaving it vulnerable to abuse by others. By not sharing your account, you protect against unauthorized activities on your account, for which you would be responsible. You may be charged with a violation if someone uses your account with your permission and violates policy. Just as important, sharing or transferring access jeopardizes the security of the entire computing system.

2.2.2. User access to computing resources is contingent upon prudent and responsible use.

Imprudent use of computing resources can lead to consequences affecting many other users, not just yourself. For example, account sharing or spreading computer viruses could undermine the systems potentially destroying the work of many other users. Prudent and responsible use begins with common sense and includes respect for the rights and privacy of other users. For example, prudent and responsible users will protect their passwords by choosing them wisely, keeping them secure, and changing them regularly; will always remember to log off when leaving a terminal; will download backups of their most important files; and will always use virus protection software.

2.2.3. You may not use computing resources for any illegal or proscribed act.

In particular, the user may not use computing resources to violate any state or federal laws or any of the regulations specified in the Governing Regulations, the Administrative Regulations, the CSULB Regulations for Campus Activities, Organizations, and the University Community, the Rules of the University Senate, the Faculty Code, the University System Faculty Handbook, or the Staff Handbook, as applicable.

2.2.4. You may not use computing resources for any commercial purpose without prior written authorization from the appropriate Vice President.

Work under approved University contracts and grants is covered under the usual internal approval processes, which serve as the requisite "prior written authorization."
2.2.5. Computing resources must be shared among users in an equitable manner. The user may not participate in any behavior that unreasonably interferes with the fair use of computing resources by another.

Computing resources are finite and must be shared. During periods of peak demand, administrators may enforce guidelines to require sharing resources for the benefit of everyone. Some facilities may adopt stricter guidelines such as no game playing, no "chat rooms," and so on, if their systems cannot support these activities in addition to academic use.

3. Some Examples of Violations

This section of the Policy consists of a list of several activities that you cannot or should not do. While these are not all of the possible violations, there are still many more things you can do than things you can't do. This list is intended to inform you and to reinforce the principles of fair and responsible computer use that we seek to engender at CSULB.

Violations of these principles or any attempt to violate these principles constitutes misuse. Violations include, but are not limited to:

3.1. Sharing passwords without prior written authorization from the appropriate system administrator or designee.

The consequences of sharing your password can be significant for the system and for you as well. This action leaves you vulnerable to such things as impersonation by another user. However, even if you are not concerned about the safety of your own account and data, you have a responsibility to other users to help maintain the security of the system. Your responsibility is like that of a tenant in an apartment building. Though the tenant may not be concerned about his or her own apartment, feeling that it contains little or nothing of value, he or she still has a responsibility to the other tenants to keep the main entrance secure.

3.2. Unauthorized accessing, using, copying, modifying, or deleting of files, data, user ids, access rights, usage records, or disk space allocations; or attempting to modify or remove computer equipment, software, or peripherals without proper authorization.

You are authorized to access, use, copy, modify, or delete files, data, or access rights on your own account as specified in the Policy. You are not authorized to perform any of these functions on another user's account or a University system unless specifically given permission by the account holder, your job description, or the appropriate system administrator or designee. A person who finds a door to another's home unlocked does not have the right to enter the home simply because it is unsecured. Similarly, the fact that someone's account and its data are unprotected does not mean that you have the right to access it.
3.3. Accessing resources for purposes other than those for which the access was originally issued, including inappropriate use of authority or special privileges.

User privacy is not to be violated; all users are to be protected from unauthorized activity by a system administrator or other users.

3.4. Copying or capturing licensed software or other copyrighted material (other than under the fair-use provision of the Copyright laws) for use on a system or by an individual for which the software is not authorized or licensed, or installing software or other copyrighted material on a system for which it is not authorized or licensed.

CSULB subscribes to the principles expressed in the EDUCOM Guide to the Ethical and Legal Use of Software. According to U.S. Copyright Law, all intellectual works are automatically covered by copyright unless explicitly noted to the contrary. "Unauthorized copying and use of software deprives publishers and developers of a fair return for their work, increases prices, reduces the level of future support and enhancements, and can inhibit the development of new software products."

-- "Using Software: A Guide to the Ethical and Legal Use of Software for Members of the Academic Community" EDUCOM

U.S. Copyright law applies to all software users. For a copy of the EDUCOM guidelines, write or call: EDUCOM, 1112 16th Street, NW, Suite 600, Washington, DC 20036, (202) 872 - 4200.

CSULB does not condone or authorize the illegal copying or possession of software or other copyrighted material. University students and employees are prohibited from copying software illegally and possessing illegal copies of software, whether for course-related, job-related, or private use. Any violations of this policy or of Copyright law are the personal responsibility of the user. The University will not assume any liability for such acts.

Some software may be in the public domain, for use with no fee and no restrictions; some software may be available at no charge but still subject to certain copyright restrictions; some software may be available as "shareware" for a nominal fee. It is the user's responsibility to determine if any of these categories apply to a specific program before copying it, and to submit any shareware fees and comply with all other restrictions. If you are in doubt about the status of any program, contact the appropriate system administrator.

3.5. Use of computing resources for remote activities that are unauthorized at the remote site.

For example, if you are accessing another university's system using a CSULB computing resource, you must follow that school's own computing rules. Your actions reflect upon the entire CSULB community.

3.6. Causing computer failure through an intentional attempt to "crash the system," or through the intentional introduction of a program that is intended to subvert a system,
such as a worm, virus, Trojan horse; a program that creates a trap door; or any similar method or program.

You have a responsibility to other users to help maintain the security of the system. The intentional introduction of a subversive program is considered a grave offense, as are direct, disruptive attacks against other users or systems, such as mail bombs, spam, blanket, or robot postings or any other activity that results in serious disruption of any systems on the Internet.

Taking reasonable precautions is part of your responsibility. If you accidentally launch a process that goes into an infinite loop, consuming CPU time and/or disk space without limit, kill it immediately. If you think you may have accidentally introduced a subversive or dangerous program, contact your local system administrator as soon as possible.

3.7. Intentional obscuring or forging of the date, time, physical source, logical source, or other header information of a message or transaction.

Header information of electronic mail, files, and printouts is an essential part of the identification and documentation of your work. Forging electronic mail or masking identification information -- for amusement, personal gain, or other reasons -- is not allowed.

3.8. Using any computing resource in a way that is harassing or threatening to another individual.

Users of e-mail and other computer-mediated communications are part of an "electronic community" in which responsible citizenship is just as important as it is in other types of communities. Harassment and intimidation are as irresponsible and unwelcome in electronic media as they are in face-to-face contact, and are not permitted.

3.9. Interception of transmitted information without prior written authorization from the appropriate system administrator.

This violation is a serious invasion of another user's privacy and is analogous to tapping that person's telephone line. The University respects the right to privacy of all users and endeavors to do all in its power to maintain that right. You should be aware that sometimes, in the course of system maintenance, transmissions are tracked, but the contents are not read. You should also be aware that unauthorized users of the system are not afforded this same protection from invasion of their privacy. This means that the University can and will read transmissions by unauthorized users, to maintain the integrity and security of the computer resources for all authorized users.

3.10. Failure to protect one's account from unauthorized use (e.g., leaving one's terminal publicly logged on but unattended).

When you do not protect your account from unauthorized use, you weaken the security of not only your account, but the entire system. Keeping your password secure and
attending to your account when logged on are key means of protection.

3.11. Using computing resources in any way that is academically dishonest.

Computer-assisted plagiarism is still plagiarism. Unless specifically authorized by a class instructor, all of the following uses of a computer are violations of the University's guidelines for academic honesty and are punishable as acts of plagiarism, which is a form of cheating:

- Copying a computer file that contains another student's assignment and submitting it as your own work
- Copying a computer file that contains another student's assignment and using it as a model for your own assignment
- Working together on an assignment, sharing the computer files or programs involved, and then submitting individual copies of the assignment as your own work
- Knowingly allowing another student to copy or use one of your computer files and to submit that file, or a modification of it, as his or her own individual work.

For further information on this topic read the University Policy on Cheating and Plagiarism; a summary of this policy may be found in the University Bulletin. (Note: this section is based on the University of Delaware policy)

3.12. Violation of priorities for use of computing resources as established by an individual facility within the CSULB system.

Some CSULB computing facilities may have no usage rules beyond those given in this policy statement. However, many have established priorities or restrictions for use of computing resources to ensure that scholarly activities are granted more weight than, for example, recreational game play and other non-academic pursuits. These priorities must be respected.

3.13. Participation in activities which undermine other users access to their fair share of the resources. Common courtesy should be enough to avoid these problems. Examples of unreasonable interference include, but are not limited to:

- Playing games for recreation when another user needs the resource for more scholarly activities.
- Exceeding established disk space, time, or other allocations.
- Intentionally running programs that attempt to execute endless loops.
- Printing large jobs during periods of heavy computer use.
- Printing multiple copies of a document.
- Printing paper copies when "print preview" on a terminal would suffice.

4. Response to Violations

4.1. Legal Sanctions
Violations of Section 502 of the California Penal Code (dealing with unlawful access or use of a computer) may be referred to the District Attorney or the police for investigation and/or prosecution. Similarly, violations of 18 U.S.C. Sec. 1030 (Federal laws dealing with unlawful access or use of a computer) may be referred to the Federal Bureau of Investigation.
Sanctions for violation of these state and federal laws may be as severe as a $50,000 fine and/or up to 5 years in jail.

4.2. University Sanctions

University sanctions are imposed by the appropriate University authority and may include, but are not limited to, limitation or revocation of access rights and/or reimbursement to the University for all damages resulting from the violation, including the computing and personnel charges incurred in detecting and proving the violation of these rules, as well as from the violation itself. Reimbursement may include compensation for staff work time related to the violation and for archiving information related to the incident. In some previous cases, these charges have reached several thousand dollars.

4.3. Investigation and Review of Charges

When an appropriate system administrator has reason to believe that a violation may have occurred, he or she may initiate an investigation and/or suspend computing privileges on a temporary basis for the individual(s) involved, pending prompt further investigation. For cases in which a user's computing privileges are limited or revoked, administrators should provide a swift, informal internal review process (involving, for example, the appropriate Department Chair or other officials) to which the user may turn before appealing through other University channels.
If the facts of the case appear to warrant University-level action, an explanation of the causal events shall be reported to the Office of Judicial Affairs in the case of students, or to the appropriate Vice President's office for all others. Investigating officials will examine charges of violations with due respect for individual privacy, the security of other users, and the rights of due process.

5. Disclaimers

The use and operation of CSULB computing facilities is subject to the following disclaimers:

5.1 CSULB accepts no responsibility for any damage or loss of data arising directly or indirectly from the use of these facilities or for any consequential loss or damage.

5.2 Although regular backups are made to protect data in the event of hardware or software failure, CSULB makes no warranty that all data can or will be restored, and accepts no responsibility for any damage or loss arising directly or indirectly from the
failure of hardware or software, or from human error.

5.3 Because the goals of CSULB are primarily educational in nature, computer facilities are generally open to perusal and intrusion by others and security mechanisms may not provide adequate protection. Although every effort is made to maintain adequate security, CSULB accepts no responsibility for any loss of privacy, theft or loss of information, damage, or loss of data arising directly or indirectly from the absence or failure of security mechanisms.

5.4 CSULB makes no warranty, whether express or implied, regarding the computing services or facilities offered or their fitness for any particular purpose.

6. GLOSSARY

Access right
Permission to use a CSULB computing resource according to appropriate limitations, controls, and guidelines

Commercial purpose
A goal or end involving the buying and/or selling of goods or services for the purpose of making a profit

Computing resource
Any computing/network equipment, facility, or service made available to users by CSULB

Data
A representation of facts, concepts, or instructions suitable for communication, interpretation, or processing by human or automatic means

Disk space allocation
The amount of disk storage space assigned to a particular user by University Computing Services or the appropriate system administrator.

Fair share or resources
Access to hardware, software, connectivity, processing times and power, data storage space, and similar resources, to the extent that this access is:

- feasible within available budgetary constraints,
- allocated in a manner consistent with established budgeting guidelines and procedures,
- appropriate for actual academic needs for computing resources, and
- consistent with resources allocated to others with comparable academic standing and computing needs.

Fair use
Use of computing resources in accordance with this policy and with the rules of an individual CSULB facility; use of computing resources so as not to unreasonably interfere with the use of the same resources by others.

File
A collection of data treated as a unit

Inappropriate use of authority or special privilege
Use of one’s access right(s) or position of authority in a manner that violates the rules for use of those privileges as specified by the appropriate system administrator or designee.

“Mail bomb”
An electronic mail message that contains destructive program code

Password
A string of characters that a user must supply to meet security requirements before gaining access to a particular computing resource

Proscribed act
Any act that violates state or federal law or established University policies

Prudent and responsible use
Use of computing resources in a manner that promotes the efficient use and security of one’s own access right(s), the access rights of other users, and CSULB computing resources

Remote activity
Any computing action or behavior that accesses remote site facilities via a CSULB computing resource

Remote site
Any computing/network equipment, facility, or service not part of, but connected with, CSULB computing resources via a communications network

“Robot posting”
an electronic mail message or newsgroup posting which has been generated by a computer program

“Spam”
Colloquial jargon for mass distribution of unsolicited and unwanted electronic mail or newsgroup postings

System administrator
Any individual authorized by the Chancellor, an appropriate Vice President, Dean, or other authority to administer a particular computing hardware system and/or its system software

Transmission
The transfer of a signal, message, or other form of intelligence from one location to another

Usage record
Information or data indicating the level of usage of computing resources by a particular user

User
Any individual -- whether student, faculty, staff, or individual external to CSULB – who uses CSULB computing resources

User id
A character string that uniquely identifies a particular user to a CSULB computing resource

EFFECTIVE: Fall 1996