CALIFORNIA STATE UNIVERSITY, LONG BEACH

Subject: **Access To and Use of CSULB Computing Resources**	
Department: Academic Senate	Reference No.:
Division: **Academic Affairs**	Issue Date: **August 1996**
References: **Academic Senate Policy 96-18**	Revision Date: **NA**
Web Links: **Academic Senate Policy 96-18**	Expiration Date: **NA**

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.

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 accidently 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 p; permission to use a CSULB computing resource according to appropriate limitations, controls, and guidelines
Commercial purpose p; a goal or end involving the buying and/or selling of goods or services for the purpose of making a profit
Computing resource p; any computing/network equipment, facility, or service made available to users by CSULB
Data p; a representation of facts, concepts, or instructions suitable for communication, interpretation, or processing by human or automatic means
Disk space allocation p; the amount of disk storage space assigned to a particular user by University Computing Services or the appropriate system administrator
Fair share of resources p; the University is the final arbiter of what constitutes "a fair share of resources." Nothing in this policy shall be construed to give any member of the University community the right to question: (a) the University's budgetary policies or (b) any restrictions imposed on the use of computer resources and facilities
Fair use p; 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 p; a collection of data treated as a unit
Inappropriate use of authority or special privilege p; 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" p; an electronic mail message that contains destructive program code
Password p; a string of characters that a user must supply to meet security requirements before gaining access to a particular computing resource
Proscribed act p; any act that violates state or federal law or established University policies
Prudent and responsible use p; 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 p; any computing action or behavior that accesses remote site facilities via a CSULB computing resource
Remote site p; any computing/network equipment, facility, or service not part of, but connected with, CSULB computing resources via a communications network
"Robot posting" p; an electronic mail message or newsgroup posting which has been generated by a computer program
"Spam" p; colloquial jargon for mass distribution of unsolicited and unwanted electronic mail or newsgroup postings
System administrator p; 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 p; the transfer of a signal, message, or other form of intelligence from one location to another
Usage record p; information or data indicating the level of usage of computing resources by a particular user
User p; any individual - whether student, faculty, staff, or individual external to CSULB - who uses CSULB computing resources
User id p; a character string that uniquely identifies a particular user to a CSULB computing resource

FORMS: NA