

1 Approved by CSULB Academic Senate in May 1996 and by President Maxson in August 1996

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

- 3 • 1. Introduction
- 4 • 2. Policy
  - 5 ○ 2.1. Basic Rights
    - 6 ▪ 2.1.1. Privacy
    - 7 ▪ 2.1.2. Freedom of Speech
    - 8 ▪ 2.1.3. A Fair Share of Resources
  - 9 ○ 2.2. Governing Principles
    - 10 ▪ 2.2.1. Individual Access
    - 11 ▪ 2.2.2. Responsible Use
    - 12 ▪ 2.2.3. Illegal Acts
    - 13 ▪ 2.2.4. No Commercial Use
    - 14 ▪ 2.2.5. Fair Sharing
- 15 • 3. Examples of Violations
  - 16 ○ 3.1. Sharing Passwords
  - 17 ○ 3.2. Unauthorized Access
  - 18 ○ 3.3. Abuse of Authority
  - 19 ○ 3.4. Copyrighted Material
  - 20 ○ 3.5. Unauthorized Remote Activities
  - 21 ○ 3.6. System Crashing and Viruses
  - 22 ○ 3.7. Forging Messages
  - 23 ○ 3.8. Harassment
  - 24 ○ 3.9. Interception
  - 25 ○ 3.10. Failure to Protect Account
  - 26 ○ 3.11. Academic Dishonesty
  - 27 ○ 3.12. Violating Priorities
  - 28 ○ 3.13. Interfering With Others
- 29 • 4. Response to Violations
  - 30 ○ 4.1. Legal Sanctions
  - 31 ○ 4.2. University Sanctions
  - 32 ○ 4.3. Investigation and Review of Charges
- 33 • 5. Disclaimers
- 34 • 6. Glossary

35

36

## 37 **1. INTRODUCTION**

38 In support of its mission to provide excellent instruction, modern research, and meaningful  
39 service, California State University, Long Beach (CSULB) offers computing resources to its  
40 students, faculty, and staff. These resources contribute to the work of all members of the  
41 University community and, therefore, must be used with great care.

42 This document is intended to help set the tone for computing and for the use of computing  
43 resources at CSULB: respect for the rights of all users and fair use by all so as to guarantee  
44 equitable access to all users. The goal of the University in providing computing resources is to  
45 give users powerful tools to further their academic endeavors. (Administrative computing  
46 resources at CSULB -- those not used in academic endeavors -- are not addressed by this policy.)  
47 The privacy of all users and of all of their files is a fundamental right that should be respected by  
48 all. You should never use the computing resources in any way that violates the privacy of others.  
49 Clearly defined procedures established to protect your rights will consistently be followed as the  
50 University maintains the computing system.

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

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

## 61 **2. POLICY GOVERNING ACCESS TO AND USE OF CSULB COMPUTING** 62 **RESOURCES**

### 63 **2.1. THREE BASIC RIGHTS**

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

- 69 • Privacy
- 70 • Freedom of speech
- 71 • A fair share of resources

72 It is unethical and a violation of this policy for any person to violate these rights.

73 All users, in turn, are expected to exercise common sense and decency (due regard for the rights  
74 of others) with respect to the public computing resources, thereby reflecting the spirit of  
75 community and intellectual inquiry at the University. Access is a right that may be limited or  
76 revoked if an individual misuses the right or violates applicable University policies or state or  
77 federal laws.

78 • 2.1.1. Privacy

79 Although not legally required to do so, CSULB computer and information services departments  
80 respect the privacy of all users. System administrators and their staff may not log onto a user's  
81 account or view a user's files without explicit permission from the user (for example by setting  
82 file access privileges). Exceptions arise when the user's account is suspected either of disrupting  
83 or endangering the security or integrity of any network systems or services or of violations of  
84 applicable University policies or federal or state law. Even then, the system administrator must  
85 normally obtain prior approval of the appropriate departmental administrator unless grave danger  
86 to the continued operation of the systems requires or reasonably appears to require emergency  
87 action.

88 This does not preclude system administrators from maintaining and monitoring system logs of  
89 user activity. Moreover, automated searches for files that endanger system security or integrity  
90 are performed regularly to protect all our users. System administrators may take appropriate  
91 actions in response to detection of such files (typically removal of those files, and possibly  
92 suspension of the user's account until the matter can be resolved).

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

98 • 2.1.2. Freedom of Speech

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

107

108

109 • 2.1.3. A Fair Share of Resources

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

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

117 **2.2. PRINCIPLES GOVERNING USE OF COMPUTING RESOURCES**

118 2.2.1. User access is granted to an individual and may not be transferred to or shared with  
119 another without explicit written authorization by the appropriate system administrator or  
120 designee.

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

127 2.2.2. User access to computing resources is contingent upon prudent and responsible use.

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

136 2.2.3. You may not use computing resources for any illegal or proscribed act.

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

142 2.2.4. You may not use computing resources for any commercial purpose without prior written  
143 authorization from the appropriate Vice President.

144 Work under approved University contracts and grants is covered under the usual internal  
145 approval processes, which serve as the requisite "prior written authorization."

146 2.2.5. Computing resources must be shared among users in an equitable manner. The user may  
147 not participate in any behavior that unreasonably interferes with the fair use of computing  
148 resources by another.

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

### 153 **3. SOME EXAMPLES OF VIOLATIONS**

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

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

160 3.1. Sharing passwords without prior written authorization from the appropriate system  
161 administrator or designee.

162 The consequences of sharing your password can be significant for the system and for you as  
163 well. This action leaves you vulnerable to such things as impersonation by another user.

164 However, even if you are not concerned about the safety of your own account and data, you have  
165 a responsibility to other users to help maintain the security of the system. Your responsibility is  
166 like that of a tenant in an apartment building. Though the tenant may not be concerned about his  
167 or her own apartment, feeling that it contains little or nothing of value, he or she still has a  
168 responsibility to the other tenants to keep the main entrance secure.

169 3.2. Unauthorized accessing, using, copying, modifying, or deleting of files, data, user ids, access  
170 rights, usage records, or disk space allocations; or attempting to modify or remove computer  
171 equipment, software, or peripherals without proper authorization.

172 You are authorized to access, use, copy, modify, or delete files, data, or access rights on your  
173 own account as specified in the Policy. You are not authorized to perform any of these functions  
174 on another user's account or a University system unless specifically given permission by the  
175 account holder, your job description, or the appropriate system administrator or designee.

176 A person who finds a door to another's home unlocked does not have the right to enter the home  
177 simply because it is unsecured. Similarly, the fact that someone's account and its data are  
178 unprotected does not mean that you have the right to access it.

179 3.3. Accessing resources for purposes other than those for which the access was originally  
180 issued, including inappropriate use of authority or special privileges.

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

183 3.4. Copying or capturing licensed software or other copyrighted material (other than under the  
184 fair-use provision of the Copyright laws) for use on a system or by an individual for which the  
185 software is not authorized or licensed, or installing software or other copyrighted material on a  
186 system for which it is not authorized or licensed.

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

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

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

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

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

208 3.5. Use of computing resources for remote activities that are unauthorized at the remote site.

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

212 3.6. Causing computer failure through an intentional attempt to "crash the system," or through  
213 the intentional introduction of a program that is intended to subvert a system, such as a worm,  
214 virus, Trojan horse; a program that creates a trap door; or any similar method or program.

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

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

223 3.7. Intentional obscuring or forging of the date, time, physical source, logical source, or other  
224 header information of a message or transaction.

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

228 3.8. Using any computing resource in a way that is harassing or threatening to another individual.

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

233 3.9. Interception of transmitted information without prior written authorization from the  
234 appropriate system administrator.

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

242 3.10. Failure to protect one's account from unauthorized use (e.g., leaving one's terminal publicly  
243 logged on but unattended).

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

247 3.11. Using computing resources in any way that is academically dishonest.

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

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

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

262 3.12. Violation of priorities for use of computing resources as established by an individual  
263 facility within the CSULB system.

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

268 3.13. Participation in activities which undermine other users access to their fair share of the  
269 resources.

270 Common courtesy should be enough to avoid these problems. Examples of unreasonable  
271 interference include, but are not limited to:

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

279

280

281 **4. RESPONSE TO VIOLATIONS**

282

283 **4.1. LEGAL SANCTIONS**

284

285 Violations of Section 502 of the California Penal Code (dealing with unlawful access or use of a  
286 computer) may be referred to the District Attorney or the police for investigation and/or  
287 prosecution. Similarly, violations of 18 U.S.C. Sec. 1030 (Federal laws dealing with unlawful  
288 access or use of a computer) may be referred to the Federal Bureau of Investigation.

289

290 Sanctions for violation of these state and federal laws may be as severe as a \$50,000 fine and/or  
291 up to 5 years in jail.

292

293 **4.2. UNIVERSITY SANCTIONS**

294

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

302

303 **4.3. INVESTIGATION AND REVIEW OF CHARGES**

304

305 When an appropriate system administrator has reason to believe that a violation may have  
306 occurred, he or she may initiate an investigation and/or suspend computing privileges on a  
307 temporary basis for the individual(s) involved, pending prompt further investigation.

308

309 For cases in which a user's computing privileges are limited or revoked, administrators should  
310 provide a swift, informal internal review process (involving, for example, the appropriate  
311 Department Chair or other officials) to which the user may turn before appealing through other  
312 University channels.

313

314 If the facts of the case appear to warrant University-level action, an explanation of the causal  
315 events shall be reported to the Office of Judicial Affairs in the case of students, or to the  
316 appropriate Vice President's office for all others. Investigating officials will examine charges of  
317 violations with due respect for individual privacy, the security of other users, and the rights of  
318 due process.

319

320 **5. DISCLAIMERS**

321

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

323

324 5.1 CSULB accepts no responsibility for any damage or loss of data arising directly or  
325 indirectly from the use of these facilities or for any consequential loss or damage.  
326  
327 5.2 Although regular backups are made to protect data in the event of hardware or software  
328 failure, CSULB makes no warranty that all data can or will be restored, and accepts no  
329 responsibility for any damage or loss arising directly or indirectly from the failure of  
330 hardware or software, or from human error.  
331  
332 5.3 Because the goals of CSULB are primarily educational in nature, computer facilities are  
333 generally open to perusal and intrusion by others and security mechanisms may not provide  
334 adequate protection. Although every effort is made to maintain adequate security, CSULB  
335 accepts no responsibility for any loss of privacy, theft or loss of information, damage, or loss  
336 of data arising directly or indirectly from the absence or failure of security mechanisms.  
337  
338 5.4 CSULB makes no warranty, whether express or implied, regarding the computing  
339 services or facilities offered or their fitness for any particular purpose.

## 340 6. GLOSSARY

### 341 **Access right**

342 permission to use a CSULB computing resource according to appropriate limitations,  
343 controls, and guidelines  
344

### 345 **Commercial purpose**

346 a goal or end involving the buying and/or selling of goods or services for the purpose of  
347 making a profit  
348

### 349 **Computing resource**

350 any computing/network equipment, facility, or service made available to users by  
351 CSULB  
352

### 353 **Data**

354 a representation of facts, concepts, or instructions suitable for communication,  
355 interpretation, or processing by human or automatic means  
356

### 357 **Disk space allocation**

358  
359 the amount of disk storage space assigned to a particular user by University Computing  
360 Services or the appropriate system administrator  
361

### 362 **Fair share of resources**

363  
364 Access to hardware, software, connectivity, processing time and power, data storage  
365 space, and similar resources, to the extent that this access is:

- 366 • feasible within available budgetary constraints,

- 367                   • allocated in a manner consistent with established budgeting guidelines and  
368                   procedures,  
369                   • appropriate for actual academic needs for computing resources, and  
370                   • consistent with resources allocated to others with comparable academic standing  
371                   and computing needs.

372       **Fair use**

373                   use of computing resources in accordance with this policy and with the rules of an  
374                   individual CSULB facility; use of computing resources so as not to unreasonably  
375                   interfere with the use of the same resources by others  
376

377       **File**

378                   a collection of data treated as a unit  
379

380       **Inappropriate use of authority or special privilege**

381                   use of one's access right(s) or position of authority in a manner that violates the rules for  
382                   use of those privileges as specified by the appropriate system administrator or designee.  
383

384       **"Mail bomb"**

385                   an electronic mail message that contains destructive program code  
386

387       **Password**

388                   a string of characters that a user must supply to meet security requirements before gaining  
389                   access to a particular computing resource  
390

391       **Proscribed act**

392                   any act that violates state or federal law or established University policies  
393

394       **Prudent and responsible use**

395                   use of computing resources in a manner that promotes the efficient use and security of  
396                   one's own access right(s), the access rights of other users, and CSULB computing  
397                   resources  
398

399       **Remote activity**

400                   any computing action or behavior that accesses remote site facilities via a CSULB  
401                   computing resource  
402

403       **Remote site**

404                   any computing/network equipment, facility, or service not part of, but connected with,  
405                   CSULB computing resources via a communications network  
406

407       **"Robot posting"**

408                   an electronic mail message or newsgroup posting which has been generated by a  
409                   computer program  
410

411       **"Spam"**

412 colloquial jargon for mass distribution of unsolicited and unwanted electronic mail or  
413 newsgroup postings

414

415 **System administrator**

416 any individual authorized by the Chancellor, an appropriate Vice President, Dean, or  
417 other authority to administer a particular computing hardware system and/or its system  
418 software

419

420 **Transmission**

421 the transfer of a signal, message, or other form of intelligence from one location to  
422 another

423

424 **Usage record**

425 information or data indicating the level of usage of computing resources by a particular  
426 user

427

428 **User**

429 any individual -- whether student, faculty, staff, or individual external to CSULB -- who  
430 uses CSULB computing resources

431

432 **User id**

433 a character string that uniquely identifies a particular user to a CSULB computing  
434 resource

435

436