POLICY

CSUEB students, faculty, staff, administrators and contractors are prohibited from utilizing CSUEB information resources for any unlawful, unethical or unprofessional purpose or activity.

2.1 Requirements for Good Judgment and Reasonable Care

Users are expected to use good judgment and reasonable care in order to protect and preserve the integrity of university equipment, its data and software, and its access. Users are expected to comply with the following principles:

- **Precautions against contaminants.** Users must take reasonable precautions to avoid introducing computer contaminants, such as viruses and "Trojan horse" macros, into university computer hardware and software or data storage media. Such precautions include, but are not limited to, using only authorized copies of software, installing updates or patches that correct identified security flaws, installing virus protection software on hard disks and using virus scanning and repair programs as needed. Users must not knowingly disable auto patching services configured on university computers.

- **Protection from theft or damage.** Users must take reasonable steps to protect the equipment and systems from damage or loss due to theft, mischievous or malicious alterations to, or removal of, installed software or machine configurations and/or mischievous or malicious additions of software, hardware, macros, or files that interfere with productivity or computer operations.

- **Protection from data loss.** Individuals with responsibility for University data [redacted]

manager to determine if they are using university storage resources appropriately.

2.2 Prohibition Against Unauthorized Browsing, Unauthorized Use or Release of Private Information

The University supports and protects the concepts of privacy and protects the confidentiality of personal information maintained in educational, medical or employment records. Information stored on CSUEB computers may be subject to state and federal privacy laws. Individuals who store such personally identifiable information (e.g., social security numbers) must use due diligence to prevent unauthorized access and disclosure of confidential, private or sensitive information. Users are expected to comply with the following principles:

- **Unauthorized Browsing**. Because confidential, critical, or important University data or information, intellectual property, or faculty research information may be located in a user's account or computer (workstation, laptop, etc.), browsing, alteration or access of email messages or stored files in another user's account or on another user's computer or removable storage device (disks, USB drives, etc.) is prohibited, even when such files are not password protected, unless specifically authorized by the user. This prohibition does not affect authorized access by a network administrator, computer support technician, or departmental manager where such access is within the scope of that individual's job duties.

- **Protected Private Information**. University employees who are granted access to personal information protected by privacy laws such as the Federal Educational Rights and Privacy Act (FERPA) will be trained in, and are required to adhere to, the applicable policies and laws regarding the access or release of private information.

2.3 Prohibited Use: Obscene Matter

In accordance with Section 8314.5 of the California Government Code, it is unlawful for any state employee, or consultant, to knowingly use a state-owned or state-leased computer to access, view, download, or otherwise obtain obscene matter. This section does not apply to accessing, viewing, downloading, or otherwise obtaining obscene matter for use consistent with legitimate law enforcement purposes, to permit a state agency to conduct an administrative disciplinary investigation, or for legitimate medical, scientific, academic, or legislative purposes, or for other legitimate state purposes. "Obscene matter" as used in this section has the meaning specified in Section 311 of the California Penal Code. "State-owned or state-leased computer" means a computer owned or leased by a state agency, as defined by Section 11000, including the California State University.

2.4 Requirement for Compliance with Laws and Policies

Users are expected to comply with applicable laws and university policies concerning usage of university property, licensing, and copyright or intellectual property rights, and policies and laws covering individual privacy and confidentiality or harassment. Users are expected to comply with the following principles:

- **Responsibility of Account Owners.** The owner of an account on multi-user systems, a computer assigned to multiple users, or an ID on a network, is responsible for all activity performed under the account or ID. Each person must use his/her own account (user ID) and not use, or alter an entry so as to appear to use, any other account (user ID). The password to an account must be kept confidential, must not be released to any other party or included in any documentation and must not be included in any unprotected communication software automatic login script. In the few instances where special circumstances or system requirements mandate that multiple users access the same account, extreme care must be used to protect the security of the account and its access password.

- **Intellectual Property and Copyright Protection.** Users who publish or maintain in8ui7 TEcIei.q.00(me accoe.es accoe.es accoe9<MCID 8 >BD-5(y)-4( )6(comin)-5(t)

is governed by Title V, section 41301 and may be referred to the Office of Student Judicial Affairs. Management Personnel Plan employees are governed by Title V, section 42723. The university may temporarily or permanently suspend, block or restrict access to information technology resources, independent of such procedures, when it reasonably appears necessary to do so in order to protect the integrity, security, or functionality of university resources or to protect the university from liability. When necessary, the employee's job responsibilities will be modified to accommodate access suspensions or restrictions. The university may also refer suspected violations of applicable law to appropriate law enforcement agencies. Contractors found in violation of this policy may be barred from access.

4.0 RELATED INFORMATION

For information about CENIC's acceptable use policy visit http://www.cenic.org/calren/aup.html
For information about California Government Code, Section 8314.5, employee use of state-owned computers for access to "obscene matter" visit http://www.leginfo.ca.gov/cgi-bin/displaycode?section=gov&group=08001-09000&file=8310-8317
For information about California Penal Code, Section 311, definition of "obscene matter" visit http://www.leginfo.ca.gov/cgi-bin/displaycode?section=pen&group=00001-01000&file=311-312.7
For information about California Government Code, Section 8314, employee use of state-owned resources for private gain visit http://www.leginfo.ca.gov/cgi-bin/displaycode?section=gov&group=08001-09000&file=8310-8317

5.0 REVISION HISTORY

This policy will be subject to revision in response to changes in technology or CSUEB operational initiatives.

Review/Revision Date	**Committee/Official**
Original issue date: 08/06/1998	University Information Technology (UIT) Advisory Committee
Review of Revised Draft: October 11, 2007	UIT
Legal Review: October 13, 2007	University Counsel (Eunice Chan)
Administrative Reviews: October 25, 2007	Cabinet & Provost Council
Shared Governance Review: Nov 6, 2007	Academic Senate ExComm
Review of Final Draft: November 8, 2007	UIT
Meet & Confer with Unions: February 20, 2008	CFA (Maureen Loughren), APC (Charles Goetzl), & CSUEU (Jerrie McIntyre, Joseph Corica) CSU CO HR (Sharyn Abernatha), & CSUEB HR (Jim Cimino)
Review of Revised Draft: April 10, 2008	Cabinet, Provost Council, & UIT
Review of Revised Draft: May 15, 2008	CFA, APC, CSUEU, & CSU CO HR
Final Administrative Review: May 19, 2008	Cabinet
Approved: May 19, 2008	Mohammad H. Qayoumi President, CSU East Bay