ACCEPTABLE COMPUTING USE POLICY

SUBJECT:	Acceptable Computing Use Policy
RESPONSIBLE UNIT:	Information Technology Services (ITS)
REFER QUESTIONS TO:	Information Security Officer
EFFECTIVE DATE:	May 19, 2008
APPROVED BY:	 President, CSU East Bay
DISTRIBUTED TO:	CSUEB Community

"To provide an academically rich, multicultural learning experience that prepares all its students to realize their goals, pursue meaningful lifework, and to be socially responsible contributors to their communities, locally and globally." – University Mission Statement

"The University values learning in an academic environment that is inclusive and student-centered. We value engagement in the civic, cultural and economic life of the communities we serve -- locally, regionally, and globally. We value critical and creative thinking, effective communication, ethical decision-making, and multi-cultural competence. We value the open exchange of ideas and viewpoints." – University Values Statement

1.0 PURPOSE

California State University, East Bay (CSUEB) is a public institution fully committed to the ideals of academic freedom, freedom of expression and multicultural diversity. CSUEB provides access to technology resources (e.g., computing hardware, software, electronic information systems, networks, etc.,) for purposes related to its mission and to the responsibilities and necessary activities of its faculty, students and staff. These resources are vital for the fulfillment of the academic, research and business needs of the CSUEB community. To promote and protect these ideals and resources, this policy is intended to define acceptable and unacceptable computing uses and practices on the university campuses and among members of the university community.

2.0 SCOPE

This policy exists within the framework of existing CSUEB policies and applicable state and federal laws that may be related to the use of technology resources and applies to all members of the university community including students, faculty, staff, administrators and contractors. University guests are covered by a separate acceptable computing use policy.

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 and mission-critical operations must ensure that appropriate backups of software and data are maintained. Departmental administrators are responsible for assuring that staff members are trained in the established back up procedures.

- **Protection against degradation of operation.** Users should avoid unnecessary printing, storage of unnecessary files, or unnecessary execution of programs that degrade system performance. Employee should consult with their unit administrator to determine appropriate definitions for unnecessary printing, storage, or program execution. And students should consult with their instructors to determine appropriate definitions for unnecessary printing, storage, or program execution.

- **Use of Central University Storage.** CSUEB provides resources to electronically store and maintain university data. Storage of personal information not related to university business must be limited to incidental and minimal use, and must not interfere in any way with the storage and maintenance of university data. Employees should consult with their unit

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 information on university computers for the use or retrieval of others, whether on bulletin boards, intranets, or the World Wide Web, are responsible for the content they publish and are required to comply with all CSUEB policies and procedures as well as state and federal laws concerning appropriate use of computers, copyrighted material, and fair use of intellectual property.

- **Licensed Software.** Software must be used in a way that is consistent with copyright laws. No more than the authorized number of copies of a software product may be made. If a temporary evaluation license is granted, the time limits of the software use must be observed.

- **Personal Financial Gain**. In accordance with Section 8314 of the California Government Code, the use of university owned computer systems for private financial gain is prohibited. Use of university owned computer systems for professional development activities such as research or publication is permitted within the limits of system capacities.

- **Use for Personal Activity by Students**. The use of university computer systems by students for personal activity not related to financial gain may be allowed, provided the use does not interfere with others' use of the machines, or with the efficiency of any affected systems or operations, or with the performance of the assigned duties of a university employee, and provided that consumable university supplies are not used.
- **Harassment or Deliberate Interference with Productivity**. Mischievous or malicious abuse of electronic mail and electronic campus information

services and/or 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 or harass others may result in suspension of computing privileges and/or appropriate disciplinary or criminal action.

2.5 University Responsibility for Information, Illegal Use, Investigations, & Automated Audits

CSUEB provides access to computing resources with the following notification:

- **Information on the Network**. The availability of networked information via CSUEB's computing resources and information services does not constitute endorsement of the content of that information by CSUEB.

- **Illegal Use.** The University does not condone unethical or illegal use of computing resources. Violation of applicable laws or university policy may result in suspension of computing privileges and/or in appropriate disciplinary or criminal action. The University will not provide legal defense for illegal use of its computers or software.

- **Investigations.** Investigations are triggered when the Chief Information Officer (or authorized designee) has probable cause to believe that a violation of law or policy has occurred. During an investigation (formal or informal), a system administrator may be authorized by the Chief Information Officer to inspect a user's computer files. Note that during an investigation users of the University's information technology resources have no inherent right to privacy for the content of information they store on University-owned or leased computing resources or transmittal over University-owned or leased networks, and system administrators may have to examine that content as part of an investigation.

- **Automated Audits.** The university may use automated tools to periodically scan computers, servers, and storage devices connected to the university's network. These scans are designed to detect security related vulnerabilities, such as improperly applied or out of date security patches, improperly configured access ports, unprotected storage of privacy data, etc. If an automated audit results in probable cause that a law or policy has been violated, an appropriate investigation will be launched (see **Investigations** above).

3.0 ENFORCEMENT

Any student, faculty, staff, or administrator found to be in violation of the above provisions may be subject to disciplinary action pursuant to the applicable California Education Code provisions. Represented employees are subject to the disciplinary process under Education Code section 89535 and their respective collective bargaining agreement. Student conduct

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