CALIFORNIA STATE UNIVERSITY
BAKERSFIELD

Acceptable Computer and Network Use Policy

CSU Bakersfield Policy

Document Number:	ITS-90.001	**Last Revision Date:**	
Responsible Office:	Information Technology Services	**Effective Date:**	
Primary Author:	CIO & AVP of Information Technology		

General Description

Purpose:

This acceptable use policy governs the use of computers and networks on the CSUB campus. As a user of these resources, you are responsible for reading and understanding this policy. This document protects the consumers of computing resources and system administrators and the integrity of computing hardware and networks.

Scope:

All users of university computer and network resources.

Policy/Procedure

Part 1

I. Introduction
II. Rights and Responsibilities
III. Existing Legal Context
IV. Enforcement

Part 2

I. Conduct Which Violates this Policy

Part 1

I: Introduction

This acceptable use policy governs the use of computers and networks on the CSUB campus. As a user of these resources, you are responsible for reading and understanding this policy. This document protects the consumers of computing resources and system administrators and the integrity of computing hardware and networks.

II: Rights and Responsibilities

Computers and networks can provide access to resources on and off campus, and allow you to communicate with other users worldwide. Such open access is a privilege and requires that individual users act responsibly. Users must respect the rights of other users, respect the integrity of the systems and related physical resources, and observe all relevant laws, regulations, and contractual obligations. Since electronic information is volatile and easily reproduced, users must exercise care in acknowledging and respecting the work of others through strict adherence to software licensing agreements and copyright laws.

III: Existing Legal Context

All existing laws (federal and state) and University regulations and policies apply, including not only those laws and regulations that are specific to computers and networks, but also those that may apply generally to personal conduct.
Users do not own accounts on University computers, but are granted use privileges. The privilege is accepted with the condition that system administrators and other University employees have the right to access user files when necessary to protect the integrity of computer systems or the rights or property of the University. For example, system administrators may examine or make copies of files that are suspected of misuse or that have been corrupted or damaged. User files may be subject to search by law enforcement agencies under court order if such files contain information which may be used as evidence in a court of law.
Misuse of computing, networking, or information resources may result in the loss of computing and/or network access. Additionally, misuse can be prosecuted under applicable statutes. Users may be held accountable for their conduct under any applicable University or campus policies, procedures, or collective bargaining agreements. Illegal production of software and other intellectual property protected by U. S. copyright law is subject to civil damages and criminal punishment including fines and imprisonment.
Other organizations operating computing and network facilities that are reachable via the CSUB network may have their own policies governing the use of those resources. When accessing remote resources from CSUB facilities, users are responsible for obeying both the policies set forth in this

document and the policies of the other organizations. Top

IV: Enforcement

Minor infractions of this policy, when accidental, such as consuming excessive resources or overloading computer systems, are generally resolved informally by the unit administering the accounts or network. This may be done through electronic mail or in-person discussion and education.
Repeated minor infractions or misconduct which is more serious may result in the temporary or permanent loss of computer access privileges or the modification of those privileges. More serious violations include, but are not limited to unauthorized use of computer resources, attempts to steal passwords or data, unauthorized use or copying of licensed software, repeated harassment, and threatening behavior. In addition, offenders may be referred to the their sponsoring advisor, department, employer, or other appropriate University office for further action. If the individual is a student, the matter may be referred to relevant administrators for disciplinary action.
Any offense which violates local, state, or federal laws may result in the immediate loss of all University computing privileges and will be referred to appropriate University offices and/or law enforcement authorities.Top

Part II

I: Conduct which violates this policy

Conduct which violates this policy includes, but is not limited to the activities in the following list.

- Unauthorized use of a computer account.
- Using the Campus Network to gain unauthorized access to any computer systems.
- Connecting unauthorized equipment to the campus network.
- Unauthorized attempts to circumvent data protection schemes or uncover security loopholes. This includes creating and/or running programs that are designed to identify security loopholes and/or decrypt intentionally secure data.
- Knowingly or carelessly performing an act that will interfere with the normal operation of computers, terminals, peripherals, or networks, e.g., deleting programs or changing icon names.
- Knowingly or carelessly running or installing on any computer system or network, or giving to another user a program intended to damage or to place excessive load on a computer system or network. This includes, but is not limited to, programs known as computer viruses, Trojan Horses, and worms.
- Deliberately wasting/overloading computing resources, such as printing too many copies of a document.
- Violating terms of applicable software licensing agreements or copyright laws.
- Violating copyright laws and their fair use provisions through inappropriate reproduction or dissemination of copyrighted text, images, etc.

- Using university resources for commercial activity, such as creating products or services for sale.
- Using electronic mail to harass or threaten others. This includes sending repeated, unwanted e-mail to another user.
- Initiating or propagating electronic chain letters.
- Inappropriate mass mailing. This includes multiple mailings to newsgroups, mailing lists, or individuals, e.g. "spamming," "flooding," or "bombing."
- Forging the identity of a user or machine in an electronic communication.
- Transmitting or reproducing materials that are slanderous or defamatory in nature, or that otherwise violate existing laws or university regulations.
- Attempting to monitor or tamper with another user's electronic communications, or reading, copying, changing, or deleting another user's files or software without the explicit agreement of the owner.
- People need to be aware that transmitting pornographic material may be in violation of federal law.
- People need to be aware that pirating of computer software without permission is in violation of federal law.