EL PASO COMMUNITY COLLEGE PROCEDURE

For information, contact Institutional
Effectiveness: (915) 831-6740

CS-2 **Computer System Security**

APPROVED: November 3, 1986 **REVISED**: September 1, 1995
Year of last review: 2021
AUTHORIZING BOARD POLICY: CS

Classification: Institutional
Responsible Vice President or Associate Vice President: Vice President of Information Technology/Chief Information Officer
Designated Contact: Executive Director of ERP Support Services

---

OBJECTIVE: To establish a process for responsible computing at El Paso County Community College District (EPCCCD).

PROCEDURE:

I. In support of its mission of teaching and public service, EPCCCD provides access to computing and information resources for students, faculty*, and staff, within institutional priorities and financial capabilities.

II. All members of the District community who use the District's computing and information resources must act responsibly.

A. Every user is responsible for the integrity of these resources.

B. All users of District-owned or District-leased computing systems must respect the rights of other computing users, respect the integrity of the physical facilities and controls, and respect all pertinent license and contractual agreements.

C. It is the Policy of EPCCCD that all members of its community act in accordance with these responsibilities, relevant laws and contractual obligations, and the highest standard of ethics.

III. Access to the District's computing facilities is a privilege granted to District students, faculty, and staff.

A. Access to District information resources may be granted by the owners of that information based on the owner's judgment of the following factors:

1. Relevant laws.

2. Contractual obligations.

3. Requestor's need to know.

4. Sensitivity of the information.

5. Risk of damage to or loss by the District.

IV. The District reserves the right to limit, restrict, or extend computing privileges and access to its information resources.

A. Data owners -- whether departments, units, faculty, students, or staff -- may allow individuals other than District faculty, staff, and students access to information for which they are responsible, so long as such access does not:

1. Violate any license or contractual agreement.

2. Violate any District Policy.

3. Violate any federal, state, county, or local law or ordinance.

*** Note: The word "faculty" denotes instructors, counselors and librarians.**

V. District computing facilities and accounts are to be used for the District-related activities. District computing resources are not to be used for commercial purposes or non-District-related activities without written authorization.

VI. Violations of this procedure may result in administrative and/or criminal actions.

A. Such administrative action may include, but is not limited to:

1. Suspension or restriction of the computing privileges of the violator.

2. Inspection of any files or programs in question.

B. It should be understood that nothing in these guidelines precludes enforcement under the laws and regulations of the State of Texas, any municipality or county therein, and/or the United States of America.

VII. Client Responsibilities

A. Use the District's computing facilities and Information resources, including hardware, software, networks, and computer accounts, responsibly and appropriately, respecting the rights of other clients and respecting all contractual and license agreements.

B. Use only those computers and computer accounts for which you have authorization.

C. Use mainframe accounts only for the purpose(s) for which they have been issued.

D. Use District-owned microcomputers and advanced work stations for District-related projects only.

E. Be responsible for all use of your accounts and for protecting each account's password. (Do not share computer accounts. If someone else learns your password, you must change your password).

F. Report unauthorized use of your accounts to your supervisor or other appropriate District authority.

G. Cooperate with requests from a Manager of Information Technology concerning Information about computing activities.

NOTE: Under certain circumstances, a Manager of Information Technology is authorized to access your computer files.

H. Take reasonable and appropriate steps to see that all hardware and software license agreements are faithfully executed on any system, network, or server that you operate.

I. Each client is ultimately responsible for their own computing and work using a computer.

VIII. Examples of Misuse of Computing and Information Resource Privileges.

A. The District characterizes misuse of computing and information resources and privileges as unethical and unacceptable and as just cause for taking disciplinary action.

B. Misuse of computing and information resources and privileges includes, but is not restricted to, the following:

1. Attempting to modify or remove computer equipment, software, or peripherals without proper authorization.

2. Accessing computers, computer software, computer data or information, or networks without proper authorization, regardless of whether the computer, software, data, information, or network in question is owned by the District. (If you abuse the networks to which the District belongs or the computers at other sites connected to those networks, the District will treat this matter as an abuse of your EPCCCD computing privileges

3. Circumventing or attempting to circumvent normal resource limits, log on procedures, and security regulations.

4. Using computing facilities, computer accounts, or computer data for purposes other than those for which they were intended or authorized.

5. Sending fraudulent computer mail, breaking into another user's electronic mailbox. or reading someone else's electronic mail without permission.

6. Sending any fraudulent electronic transmission, including but not limited to, fraudulent requests for confidential information, fraudulent submission of electronic purchase requisitions or journal vouchers, and fraudulent electronic authorization of purchase requisitions or journal vouchers.

7. Violating any software license agreement or copyright, including copying or redistributing copyrighted computer software, data, or reports without proper, recorded authorization.

8. Violating the property rights of copyright holders who are in possession of computer-generated data, reports, or software.

9. Using the District's computing resources to harass or threaten other users.

10. Using the District's computing resources by accessing an account that belongs to another individual.

11. Take advantage of another user's naiveté or negligence to gain access to any computer account, data, software, or file that is not your own and for which you have not received explicit authorization to access.

12. Physically interfering with others' access to the District's computing facilities.

13. Disclosing or removing proprietary information, software, printed output or magnetic media without the explicit permission of the owner.