Santa Monica College
Computer and Network Use Policy
DRAFT

Approved by the Academic Senate on May 14, 2002

Santa Monica Community College District provides a wide array of computing and networking resources to all college employees. These resources are intended to advance the educational, scholarly, and service missions of the District.

By accepting and/or using any District computer or network account, the user understands and agrees to the following:

1. Users are responsible for all use of computers and network accounts provided to them by the District, including backup of files on their district-provided computer and password maintenance.

    a. Responsible use includes using passwords that are not easily deduced by others.

    b. Voluntary unauthorized disclosure of a password may result in suspension, revocation and/or denial of computing privileges. Disclosure of passwords to Information Technology (IT) staff or other District system administrators is considered authorized disclosure.

    c. Users who suspect that their District-provided computers or network accounts have been accessed without their permission are responsible for changing their passwords and are strongly encouraged to report the suspected activity to IT.

    d. District-provided network accounts may only be used by the user to whom they are assigned unless otherwise authorized by the District. Users are responsible for actions taken by others who use their network accounts; for example, if the user forgets to log off. Access to computers and network accounts for maintenance/service purposes by persons responsible for systems and IT is considered authorized**;** users are not responsible for actions taken by these persons.

2. The District will seek to maintain system security, but users should not assume that information in their accounts, or on District-owned or -administered computers they use, is private. Authorized District personnel may obtain access to computing and networking resources only as necessary to service the computing system, retrieve or modify District work, and to investigate suspected violations of this policy, including unlawful activity. Files will be disclosed to third parties as required by law. Users will be notified of access when

notification is required by law and/or District policy.

a. The District cannot and does not guarantee the confidentiality of electronic information. In addition to accidental and intentional breaches of security, the District may be compelled to disclose electronic information as required by law.

b. As part of its necessary routine operations, the District occasionally gains access to network accounts and other computing services it makes directly or indirectly available to the campus community. Suspected policy violations discovered during such routine operations will be reported to the Vice President responsible for Information Technology or designee and/or law enforcement officials. All other information accessed during such routine operations will be treated as confidential, except as otherwise required by this policy or law.

c. The District shall report suspected criminal activity to law enforcement authorities.

d. Unless otherwise prohibited by law, and subject to legal requirements, the District and law enforcement personnel may access computers, network accounts or any other electronic information or technology necessary to investigate suspected violations of this policy or unlawful activity.

e. Users will relinquish access to computing and network resources upon permanent separation from the District. Department heads are responsible for requesting IT to move needed files off separated employees' accounts and District-owned or –administered computers upon separation.

3. Users agree not to violate system security; maliciously interfere with system performance or another user's use of the system; or access network accounts, files or passwords intentionally and without authorization. Users may not intentionally send email or develop other electronic information inaccurately attributed to another person.

4. Users agree to use the computers and network accounts only for lawful purposes that are consistent with District policies and procedures.

5. The District is not responsible for the content of the accounts and other computing services it provides. Users are responsible for all information they access, make available or distribute using the computer/network account.

6. Users may use their computers and network accounts for non-District matters except as otherwise prohibited by this or other District policy or where such use unreasonably interferes with academic uses, job performance or system performance/operations. Such use is subject to the terms of this policy including, without limitation, terms regarding access to information on District computers and accounts.

    a. Any and all information maintained on District-owned computers/network accounts, whether District-related or not, is accessible by the District. Other than to perform

routine operations or as may be legally required, the District will not monitor accounts or access the information stored in computers/network accounts without the user's consent unless such action is necessary to enforce this policy.

b. Employees are strongly encouraged to remove any "personal" information they may have stored on their computers/network accounts prior to ending their relationship with the District. Generally, the District will destroy information left on computers/network accounts. Information will be retained if retention is in the District's best interest. If the District extends an individual's account access beyond the employment separation date, the account is not subject to this provision until the extension has ended.

7. Users agree not to use their computers or network accounts for non-District fundraising and commercial purposes. District personnel may engage in fundraising and commercial activity on behalf of the District in connection with official District-related duties or District-sanctioned activities.

8. Users understand that violation of this policy may result in suspension or termination of computer, network account and other access and, depending upon the circumstances, may result in disciplinary action. Policy violations will be processed through normal District channels. If the activity is also unlawful, it may result in criminal and/or civil prosecution.

a. The District may temporarily suspend a user's computing privileges for security or other administrative reasons. Computing privileges suspended pursuant to this provision will be restored as soon as the threat or concern has been addressed or within three business days, whichever is shorter. Accounts that are suspended for more than three days will be handled as outlined in paragraph 8.c., below, irrespective of whether disciplinary action has been initiated. Absent extenuating circumstances, no account may be suspended pursuant to this policy for more than 10 business days, unless the disciplinary process has been invoked.

b. Suspected violations by District employees will be reported to the employee's supervisor and handled through established channels for disciplinary action.

c. Pending resolution of the disciplinary process, the Vice President responsible for Information Technology or designee may suspend District computing privileges if the alleged violation is reasonably perceived to constitute unlawful activity, pose a substantial risk to the integrity of campus computing or present an imminent threat to the safety or welfare of the campus or members of the college community. In the event of a perceived emergency or where other exigent circumstances demand immediate action, the Vice President responsible for Information Technology or designee may immediately suspend computing privileges and notice will be given to the user as soon as reasonably possible. In non-emergency situations, the Vice President responsible for Information Technology or designee will provide the user with notice of the perceived problem and an opportunity to be heard before privileges are suspended. A suspension may be appealed in writing to the Vice President for Human Resources or

designee within three business days of the effective date of the suspension. The Vice President of Human Resources or designee will provide a written decision to the Vice President responsible for Information Technology and the user within five business days of receipt of the appeal. The Vice President of Human Resources' or designee's decision will remain in effect pending final resolution of the disciplinary proceeding.

d. Sanctions for violations of this policy will be imposed by the administrative official with final responsibility for resolution of the disciplinary process in use, following consultation with the Vice President responsible for Information Technology in the event that sanctions involve campus computing services. Sanctions with respect to campus computing services may include, but are not limited to, suspension or permanent revocation of computing privileges. The District reserves the right to seek restitution and/or indemnification from an employee for damages arising from violations of this policy. In addition, the District and/or third parties may pursue criminal and/or civil prosecution for violations of law.

9. The District assumes responsibility for maintaining system performance and stability.

10. Users agree to read and abide by this policy. The Vice President responsible for Information Technology and the Academic Senate Joint Information Services Committee are responsible for providing interpretation, which will be modified periodically in light of experience gained and legal and administrative developments.