AR 2515 Computer and Network Use

Purpose

The Santa Monica Community College District provides a wide array of technology resources to staff, students and faculty. These resources are intended to advance the educational, scholarly, and service missions of the District. This document describes the general regulations covering the use of technology computing facilities which are under the direction of Santa Monica College Information Technology (IT) department and its staff.

Technology computing resources are a limited and finite resource that each and every user needs to respect. Every user is expected to use the technology resources in a manner which does not infringe upon use of those facilities by other people and which does not waste either "soft" resources (e.g., computer time) or "hard" resources (e.g., paper, disk space, documentation materials). The guidelines discussed here are intended to insure that the security of the system is protected consistent with the user's right to privacy and fair share of available resources.

Users agree to read and abide by this regulation. The Vice President responsible for Information Technology or designee is responsible for providing interpretation, which will be modified periodically in light of experience gained and legal and administrative developments that occur.

System Security

1. 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 security violations of this policy, including unlawful activity. Files will be disclosed to third parties as required by law. Users will be notified of such access whenever possible.

    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 security 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. 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.

    d. Users will relinquish access to computing and network resources upon permanent separation from the District.

e. The District and the IT staff will seek to maintain system security, but users should not assume that their accounts or the files or information they store on or their use of District-owned or –administered computers will remain private. Users should not assume their email messages are private communications, nor that their use of technology resources will not be monitored as part of the District's routine operations. As all electronic mail is a form of public record, users should have no expectation of privacy in their use of electronic mail, as the IT department may regularly choose to inspect, disclose, retain or dispose of electronic correspondence as part of the District's routine operations.

f. The IT department will make reasonable efforts to maintain the security of account names, numbers, passwords, directories and files. However, no computer system is completely secure. Even with all the safeguards taken by the District to control privacy and security, it may still be possible for some user to gain access to another user's accounts through actions or accidents beyond any reasonable control. As a result, each user must take full advantage of password and file protection security mechanisms provided by their computer and its operating system.

g. 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.

2. Users may not intentionally send email or develop other electronic information inaccurately attributed to another person.

3. No computers or network accounts shall be used for unlawful purposes, or in violation of district policies or procedures.

Appropriate and Inappropriate Use

1. It is impossible to provide an exhaustive definition of inappropriate computer use, or a complete set of examples to cover every conceivable situation. Users who have questions about which computer uses are appropriate and which are not should inquire about their intended use by contacting the IT department.

   Without limitation, the following examples shall be construed by all of the campus community as examples of inappropriate use of technology resources:

   - users shall not interfere with system performance or another user's use of the system
   - users shall not disclose their passwords or lend their account to any other individual, apart from IT staff
   - users shall not gain access to accounts, files, passwords or resources intentionally and without authorization of the account holder
   - users shall not use technology resources for non-District fundraising or commercial purposes.
   - users shall not use technology resources for any activities which violate state or federal laws. Computing resources may not be used to intimidate, threaten or harass individuals, or violate the college's policies concerning relationships between college constituencies. Such activities include, but are not limited to, using computing resources to store, print, or send obscene, slanderous, or threatening messages.

   2. 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. The District may 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.

Process for Suspension and Termination of Use

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

1. Emergency Suspensions

a. 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.

b. 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 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.

2. Non-Emergency Suspensions and Terminations

a. 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.

b. A suspension may be appealed in writing to the Vice President of 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.

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

d. 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.

e. Sanctions for violations of this regulation 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 regulation. In addition, the District and/or third parties may pursue criminal and/or civil prosecution for violations of law.

Personal Responsibility

1. As a representative of the District, users must accept personal responsibility for reporting any misuse of the network to relevant IT staff. This includes, but is not limited to, users who suspect that their District-provided computers or network accounts have been accessed without their permission. These users are expected to change their password as soon as it is reasonably possible to do so and to report the suspected activity to relevant IT staff.

2. 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. On a regular basis and in accordance with the current security practices of the computing industry, IT staff may require users to change their passwords.

   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. District-provided network accounts may only be used by the user to whom they are assigned unless otherwise authorized by the District. 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.

   d. 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.

   e. Users are responsible for actions of others who use their network accounts with their permission.

   f. Users are responsible for logging off and for protecting their private account.

Users gain access to computer systems by being assigned an account on the college's computer network. Possession of an account may allow its owner to access various systems, databases, student records, websites and use peripheral devices such as printers. Each employee member is assigned an account for his/her use in their professional activities.

AR 2515 is governed by Article 27, Computer and Network Use, in the District/Faculty Collective Bargaining Agreement.

Revised 11/6/2009