2.5.1 Policy on Responsible Use of University Computing Resources

Introduction

This policy governs the proper use and management of all University of San Diego computing and network resources. This policy applies to all users of university computing resources, whether affiliated with the university or not, and whether on campus or from remote locations.

The university's computing resources include, but are not limited to, computers, computer systems, networks, electronic and mobile communications systems, telephone and data systems, internet connections, software, and related hardware and infrastructure that are owned, leased, acquired, developed or maintained by the university ("computing resources"). The university provides these resources to support the university's mission; instruction, academics, scholarship, research and service; administrative functions; student and campus life activities; and the free exchange of ideas among members of the university community and between the university and the wider local, national, and world communities.

The right of academic freedom applies to the use of university computing resources. So, too, however, do the responsibilities and limitations associated with that right. The use of university computing resources is a revocable privilege. The use of university computing resources, like the use of any other university resource or activity, is subject to the normal requirements of legal, ethical, authorized and appropriate behavior. Users must abide by all applicable restrictions, whether or not they are integrated into the computing resources and whether or not they can be circumvented by technical means.

Users, including university employees and students, should understand that their expectations of privacy and ownership in their use of university computing resources are limited and may be unfounded. The university, including university counsel and the Chief Information Officer (see "Security and Privacy" below), will engage in activities authorized by this policy with due and careful regard for the interests of university employees and students in academic freedom, privacy, and employee or student proprietary information.

Statement of Policy

All users of university computing resources must:

- **Comply with all federal, state and other applicable laws; all applicable university policies and standards; and all applicable contracts and licenses.** Examples of such laws, policies, contracts and licenses include but are not limited to

the laws of libel, privacy, copyright, trademark, patent, trade secret, discrimination and harassment, obscenity, and child pornography; computer-related laws that prohibit "hacking," "cracking," and other similar activities; the university's Student Code of Rights and Responsibilities or other applicable student rules; the university's policies, including but not limited to policies prohibiting discrimination and harassment, or illegal, dishonest and fraudulent behavior while engaging in university-related business or activities; and all applicable software licenses. Users who engage in electronic communications with persons in other states or countries or on other systems or networks should be aware that they may also be subject to and should comply with the laws of those states or countries and the rules and policies of those other systems and networks.

- **Use only those computing resources that they are authorized to use and use them only in the manner and to the extent authorized.** Ability to access or use computing resources does not, by itself, imply authorization to do so. Users are responsible for determining which authorizations are necessary and for obtaining them before using university computing resources. Provision by university authorities of a university computer, an ID, and a password to an employee or a student implies authorization for that person to make normal use of that computer, subject to the provisions of this policy. Unless authorized by the university's Office of Information Technology Services, user IDs and passwords may not, under any circumstances, be shared with or used by persons other than those to whom they have been assigned by the university.

- **Respect the privacy of other users and their accounts, regardless of whether those accounts are securely protected.** Ability to access or use another person's account does not, by itself, imply authorization to do so. Users are responsible for ascertaining what authorizations are necessary and for obtaining them before proceeding.

- **Respect the finite capacity of the university's computing resources and limit use so as not to consume an unreasonable amount of those resources or to interfere unreasonably with the activity of other users.** Although there is no set bandwidth, disk space, CPU time, or other limit applicable to all uses of university computing resources, the university may require users of those resources to limit or refrain from specific uses in accordance with this standard. The reasonableness of any particular use will be judged in the context of all of the relevant circumstances.

- **Follow applicable limitations or prohibitions on the use of university resources for personal commercial activities, personal financial or other gain, or political activity.** The use of university computing resources for personal commercial activities, personal financial or other gain, or political activity may be limited or prohibited by university policy or applicable law. Users are responsible for knowing and following the applicable policies or other restrictions that apply to the use of university computing resources for these purposes.

- **Refrain from stating or implying that they speak on behalf of the university and from engaging in prohibited use of university trademarks and logos on university computing resources.** Affiliation with the university does not, by itself, imply authorization to speak on behalf of the university. Unauthorized use of university trademarks and logos on university computing resources is not permitted. The use of appropriate disclaimers is encouraged.

Enforcement

Users who violate this policy may be denied access to university computing resources and may be subject to other penalties and disciplinary action, both within and outside the university. Violations will normally be handled through the university's disciplinary procedures applicable to the relevant user. For employees, the corrective action may range from verbal warnings up to and including termination of employment. For students, the corrective action will be imposed in a manner consistent with the Student Code of Rights and Responsibilities or other applicable rules, and can include dismissal from the university. For individuals who are not students or employees of the university, corrective action within the reasonable control of the university, and as appropriate under the circumstances, will be initiated.

The university may temporarily suspend or block access to an account prior to the initiation or completion of any disciplinary procedures, when it reasonably appears necessary to do so in order to protect the integrity, security or functionality of university or other computing resources, to protect the university from liability, or otherwise when appropriate under the circumstances. The university may also refer suspected violations of applicable law to appropriate law enforcement agencies.

A report regarding a suspected violation of this policy may be directed to the Chief Information Officer.

Security and Privacy

The university employs various measures to protect the security of its computing resources and of users' accounts. Users should be aware, however, that the university cannot guarantee such security. Users are expected to engage in "safe computing" practices by establishing appropriate access restrictions for their accounts, guarding their passwords, and changing their passwords regularly. Also, users should ensure the installation of anti-virus software and appropriate updates for personally-owned computers connecting to the university's network and computers.

While the university does not routinely monitor individual usage of its computing resources, the normal operation and maintenance of the university's computing resources require the backup and caching of data and communications, the logging of activity, the monitoring of general usage patterns, and other such activities that are necessary for the rendition of service.

The university also may specifically access and monitor the accounts of individual users of university computing resources, including individual login sessions and communications, without notice, when there is reasonable cause to do so, including for

example when: (a) the user has voluntarily made them accessible to the public, as by posting to the university's website or any webpage, whether affiliated with the university or not; (b) it reasonably appears necessary to do so to protect the integrity, security, or functionality of university or other computing resources or to protect the university from liability; (c) there is reasonable cause to believe that the user has violated or is violating this policy; (d) an account appears to be engaged in unusual or unusually excessive activity, as indicated by the monitoring of general activity and usage patterns; (e) it reasonably appears necessary to do so to facilitate the continuity of business functions at the university; (f) it reasonably appears necessary to do so as part of an audit conducted internally at the university or by outside auditors or governmental agencies; or (g) it is otherwise required by law. Any such individual access or monitoring, other than that specified in part (a) or necessary to respond to perceived emergency situations, must be authorized in advance by the Chief Information Officer (or, in the absence of the CIO, a director-level employee within Information Technology Services) and university counsel, following consultation with appropriate university officials prior to authorizing the individual access or monitoring.

The university will maintain documentation of the authorizations to access or monitor individual user activity or information stating the purposes for which authorization is given. Activities associated with accessing, monitoring, and investigating users' activity and information shall be limited to the purposes for which such university and/or third party activity is authorized.

When the contents of a current employee's or student's university owned computer or communications associated with an individual's university computing account are accessed or monitored under this policy, the individual will be notified as soon as practicable that the access or monitoring occurred, provided the notification is permitted by law and will not interfere with any investigation by the university or other outside agency. Notification is not required when the access or monitoring was conducted under part (a).

The university, in its discretion, may disclose the results of any such general or individual access or monitoring, including the contents and records of individual communications, to appropriate university personnel or law enforcement agencies and may use those results in appropriate university disciplinary processes.

On an annual basis, General Counsel and the Chief Information Officer shall provide a report to the Cabinet, accessible by the University Senate, regarding: the number of times the authorization required by this policy was requested to monitor the accounts of group or individual users of university computing resources; the number of times such authorization was given; and a general description of the purposes for requests and authorizations. The report shall be made in a manner that does not directly or indirectly identify the individual users involved or reveal any confidential or private information.

Other Standards

Information Technology Services may implement and maintain additional standards governing the use of university computing resources, or specific computers, computer

systems, networks, electronic communications systems or related hardware. Users are expected to be familiar with and comply with all applicable standards. For more information, please contact Information Technology Services.

(June 26, 2007)