

**PM 2009 - 12**

**11/05/2009**

**President Mildred García**

## **USE OF INFORMATION TECHNOLOGY SERVICES AND RESOURCES AND ELECTRONIC MAIL SYSTEMS OR SERVICES**

### **1. Purpose**

It is the purpose of this policy to set forth the policy of California State University, Dominguez Hills (University) relating to the use of the University's Information Technology Services & Resources (hereinafter referred to as "information technology resources") and the University's electronic mail systems or services. The intent of this policy is to:

- a. Establish policy on privacy, confidentiality and security in information technology resources and electronic mail systems or services;
- b. Ensure that University information technology resources and electronic mail systems or services are used for purposes appropriate to the University's mission;
- c. Inform the University community about the applicability of laws and University policies to information technology resources and electronic mail systems or services;
- d. Ensure that information technology resources and electronic mail systems or services are used in compliance with federal and state laws and related University policies; and,
- e. Avoid the misuse of the University's information technology resources and electronic mail systems or services.

### **2. Definitions**

For purposes of this policy, the following definitions shall apply:

- a. "Electronic mail systems or Information Services" shall mean and include the use of electronic information or telephonic systems in the communicating or posting of information or material by way of electronic mail, bulletin boards, World Wide Web (Internet) or other such electronic tools any messaging system that depends on computing facilities to create, send, forward, reply to, transmit, store, hold, copy, download, display, view, read or print computer

records for purposes of asynchronous communication across computer network systems between or among individuals or groups, that is either explicitly denoted as a system for electronic mail or is implicitly used for such purposes, including services such as electronic bulletin boards, list servers, and newsgroups.

- b. "Information technology resources" shall mean and include computers, networks, servers and other similar devices that are administered by the University and for which the University is responsible. "Networks" shall mean and include video, voice and data networks, routers and storage devices.

### **3. General**

The University encourages the use of its information technology resources and electronic mail systems or services to share information and knowledge in support of the University's mission of education, research and public service and to conduct the University's business. In this regard, the University supports and provides information technology resources to faculty, staff and students, including, but not limited to, electronic mail systems or services, Web access and publishing and information sharing. This policy governs all use of the University's information technology resources and electronic mail systems or services.

Access to the University's information technology resources and electronic mail systems or services is a privilege, not a right, and must be treated as such by all users of these resources. All users must act honestly and responsibly. Every user is responsible for the integrity of the information technology resources and electronic mail systems or services. All users must respect the rights of other users, respect the integrity of the physical facilities and controls, and respect all pertinent license and contractual agreements related to the University's information technology resources and electronic mail systems or services. All users shall act in accordance with these responsibilities, and the relevant local, state and federal laws and regulations. Failure to so conduct oneself in compliance with this policy may result in the denial of access to the University's information technology resources and/or electronic mail systems or services in part or in whole.

The University is a provider of a means to access the vast and growing amount of information available through electronic information resources. The University is not a regulator of the content of that information and takes no responsibility for the content of the information except for that information the University itself and those acting on its behalf create. Any persons accessing information through the University's information technology resources must determine for themselves and their charges whether any source is appropriate for viewing.

Accepting any account and/or using the University's information technology resources or the University's electronic mail systems or services shall constitute an agreement on behalf of the user or other individuals accessing such information technology resources or electronic mail systems or services to abide and be bound by the provisions of this policy.

The University may restrict or prohibit the use of its information technology resources and/or its electronic mail systems or services in response to complaints presenting evidence of violations of University policies or state or federal laws. When it has been determined that there has been a violation, the University may restrict or prohibit access by an offending party to its information technology resources or its electronic mail systems or services through University-owned or other computers or remove or limit access to material posted on University-owned computers or networks.

#### **4. Policy Scope**

This policy applies to:

- a. All information technology resources and electronic mail systems or services owned or managed by the University;
- b. All information technology resources and electronic mail systems or services provided by the University through contracts and other agreements with the University;
- c. All remote access to the University's information technology resources and electronic mail systems or services;
- d. All users of University information technology resources and electronic mail systems or services; and,
- e. All University electronic mail systems or services and Web pages in the possession of the University employees or of other users of information technology resources provided by the University.

#### **5. Responsibility for Policy**

The Chief Information Officer of the University is responsible for working with the University community to keep this policy current. Each unit of the University may develop, publish and maintain specific procedures necessary to implement this policy.

#### **6. Permitted Users**

The University allows members of the University community to use its electronic mail systems or services and information technology resources. Members of the University community include registered students, faculty and staff and faculty and staff emeriti in all University units (including auxiliary units). Permitted users also include California Academy of Mathematics and Science (CAMS) students and faculty as well as registered members of the University Alumni Association.

## 7. Basic Rights of Permitted Users

Every permitted user has four basic rights regarding use of the University's electronic mail systems or services and information technology resources:

- Privacy and confidentiality
- Freedom of speech
- A fair share of resources
- Accessible resources

It is unethical and a violation of this policy for any person to violate these rights.

All permitted users are expected to exercise common sense and decency (due regard for the rights of others) with respect to the University's electronic mail systems or services and information technology resources, thereby reflecting the spirit of the community and intellectual inquiry at the University.

**7.1 Privacy and Confidentiality.** While the University supports each individual's right to personal communication, and will take reasonable steps to ensure the security of the network, messages on University computing resources are potentially accessible to others through normal system administration activities and to the public through public record laws. Accordingly, the University cannot guarantee privacy of electronic mail systems or services. Users, therefore, should exercise extreme caution in using electronic mail systems or services to communicate confidential or sensitive matters. It is best when using electronic mail systems or services to do so with the understanding that your electronic communication may be subject to disclosure.

The University supports each individual's right to privacy of personal files. However, in the normal course of system administration, it may become necessary to examine user files to gather information to diagnose and correct problems. Additionally, while the University does not routinely inspect, monitor or disclose an individual's electronic communications or use of information technology resources without the user's consent, with reasonable cause for suspicion and appropriate administrative authority, files may be examined to determine if a user is

acting in violation of this policy, other University policies or state or federal laws.

Finally, all users of information technology resources and electronic mail systems or services must comply with all applicable University regulations and laws governing personal privacy and the confidentiality of information. Some state and federal laws preserve the confidentiality of identified classes of information (e.g., student educational records, personal employment information or proprietary commercial software). Therefore, all users of information technology resources and electronic mail systems or services are prohibited from seeking, using or disclosing confidential information about others without authorization. This prohibition extends to the use of either electronic mail systems or services or information technology resources for this purpose. All University employees must take necessary precautions to protect the confidentiality of confidential information encountered in the performance of their duties.

**7.2 *Freedom of Speech.*** The University respects the principle of academic freedom and does not attempt to censor permitted user's electronic messages or publications. If there is any doubt, permitted users must include caveats to make it clear that they speak only for themselves, and not for the University. Threats to or harassment of other permitted users or groups whether on or off campus does not fall within the bounds of this protection and will not be tolerated. Also banned are flagrant actions that invite responses that could undermine the University's ability to operate on the Internet. Freedom of speech may be limited to appropriate time, place, and manner of speech restrictions as prescribed by law. Any alleged violations of this section shall be processed pursuant to the procedures contained in Section 13, Violations.

**7.3 *Fair Share of Resources.*** Fair share of resources means access to hardware, software, connectivity, processing time and power, data storage space and similar resources to the extent that this access is:

- feasible within available budgetary constraints,
- allocated in a manner consistent with established budgeting guidelines and procedures,
- appropriate for actual permitted use of electronic mail systems or services and information technology resources, and
- consistent with resources allocated to others with comparable standing and computing needs.

All permitted users are entitled to their fair and appropriate share of the limited available electronic mail systems or services and information technology resources such as disk space, computer time and remote access connect time. The University will provide access to digital information

resources as appropriate, e.g., office computers, classroom and individual access to computer laboratories as well as access to the Internet, email, World Wide Web, Usenet, data sets, appropriate software and training in the use of these resources.

**7.4 Accessible Resources.** All electronic mail systems or services and the use of information technology resources intended to accomplish the academic and administrative tasks of the University shall be accessible to users with disabilities in compliance with applicable laws and University policies. Any needed alternate accommodations to allow such usage shall conform to applicable laws and University policies and guidelines.

## **8. Permitted Use**

University information technology resources and University electronic mail systems or services are to be used for University-related business, i.e., in the support of the teaching, research and public service missions of the University, and of the administrative functions that support these missions. The University's information technology resources or the University's electronic mail systems or services shall not be provided to individual consumers or organizations outside the University except by approval of the President's Office. Such services shall support the mission of the University and not be in competition with commercial providers. Many of the CSU bargaining unit contracts provide for access to the campus e-mail system for official union communications. Nothing in this section will limit or abridge these rights.

## **9. Use of the University's Name, Logo or Seal**

The use of the University's name is governed by California Education Code Section 89005.5. Compliance with this statute is required by all users of electronic mail systems or services and information technology resources. Without obtaining the permission of the University's President, this statute prohibits the use of the University's name, or any abbreviation of it, in any of the following ways:

- a. To designate a business, social, political, religious or other organization, including but not limited to any corporation, firm, partnership, association, group, activity, or enterprise.
- b. To imply, indicate or otherwise suggest that any product, service or organization is connected or affiliated with, or is endorsed, favored, or supported by, or is opposed by the Trustees of the California State University or any educational institution administered by the Trustees.

Permission is required before the name of any University in the California State University system may be used for commercial purposes.

c. To display, advertise or announce the University's name publicly at, or in connection with, any meeting, assembly, or demonstration, or any propaganda, advertising or promotional activity of any kind which has for its purpose or any part of its purpose the support, endorsement, advancement, opposition or defeat of any strike, lockout or boycott of any political, religious, sociological or economic movement, activity or program. Many of the CSU bargaining unit contracts provide for access to the campus e-mail system for official union communications. Nothing in this section will limit or abridge these rights.

d. Employees may use the university's name in identifying themselves as employees of the university but may not represent their views as those of the university.

## **10. Intellectual Property Considerations**

The contents of all electronic communications and Web publications shall conform to federal and state laws and University policies regarding protection of intellectual property, including laws and policies concerning copyright, patents and trademarks. When the content and distribution of electronic communications and Web publications exceed "fair use" as defined by the federal Digital Millennium Copyright Act of 1998 and the Technology, Education and Copyright Harmonization Act of 2002 (TEACH Act), users of information technology resources shall secure appropriate permission to distribute protected material in any form, including text, photographic images, audio, video, graphic illustrations and computer software.

## **11. Unauthorized Access**

Unauthorized access to the University's information technology resources and the University's electronic mail systems or services is prohibited. No one should use the ID or password of another; nor should anyone provide his or her ID or password to another, except in the cases necessary to facilitate computer maintenance and repairs. When any user terminates his or her relation with the University, his or her ID and password shall be denied further access to University information technology resources and University electronic mail systems or services unless the user has emeritus standing.

## **12. Misuse of Information Technology Resources and Electronic Mail Systems or Services**

Misuse of University information technology resources and the University's electronic mail systems or services is prohibited. Any alleged misuse shall be

processed according to Section 13, Violations of this Policy. Misuse includes, but is not limited to intentionally and knowingly, doing the following:

- a. Using information technology resources or electronic mail systems or services for purposes that could reasonably be expected to cause excessive strain on the University's network or shared network resources that in turn interfere or interrupt others' use of the University's information technology resources or the University's electronic mail systems or services.
- b. Sending spam electronic communications, that is, exploiting the University's electronic mail systems or services for purposes beyond their intended scope to amplify the widespread distribution of unsolicited electronic communications. . Many of the CSU bargaining unit contracts provide for access to the campus e-mail system for official union communications. Nothing in this section will limit or abridge these rights.
- c. Sending letter-bomb electronic communications that is, sending an extremely large electronic communication or sending multiple electronic communications to one or more recipients to interfere with the recipients' use of electronic mail systems or services or other technology resources.
- d. Intentionally engaging in other practices such as "denial of service attacks" that impede the availability of electronic mail systems or services.
- e. Either directly or by implication using a false identity (e.g., sending an electronic communication or creating a Web page under another person's name). However, users may use an alternate name or electronic identification for oneself for privacy or other reasons, so long as this practice clearly does not constitute a false identity. Users may remain anonymous except when publishing Web pages and transmitting broadcasts. False identity does not include a supervisor directing an employee to use the supervisor's identity to transact University business for which the supervisor is responsible.
- f. Attempting to modify or remove computer equipment, software or peripherals without proper authorization.
- g. Accessing without proper authorization computers, software, information or networks to which the University belongs, regardless of whether the resource accessed is owned by the University or the abuse takes place from a non-University site.

- h. Taking actions, without authorization, which interfere with the access of others to information technology resources or electronic mail systems or services.
- i. Circumventing logon or other security measures.
- j. Using information technology resources or electronic mail systems or services for any illegal or unauthorized purpose or for any other purpose that would violate any applicable campus policy that is current and in effect.
- k. Sending any fraudulent electronic communication.
- l. Violating any software license or copyright, including copying or redistributing copyrighted software, without the written authorization of the software owner.
- m. Using electronic mail systems or services to violate the property rights of authors and copyright owners.
- n. Violating the Digital Millennium Copyright Act of 1998.
- o. Using electronic communications to harass or threaten users in such a way as to create an atmosphere that unreasonably interferes with the education or employment experience. Similarly, electronic communications shall not be used to harass or threaten other information recipients, in addition to University users.
- p. Reading other users' information or files without permission.
- q. Academic dishonesty.
- r. Forging, fraudulently altering or falsifying, or otherwise misusing University or non-University records (including computerized records, permits, identification cards or other documents or property).
- s. Using electronic mail systems or services or information technology resources to steal another individual's work, fabricate research data or otherwise misrepresent one's own work.
- t. Launching a computer worm, computer virus or other rogue program.
- t. Downloading or posting illegal, proprietary or damaging material to a University computer.

- u. Transporting illegal, proprietary or damaging material across a University network.
- v. Personal use of any University information technology resource or electronic mail systems or services to access, download, print, store, forward, transmit or distribute obscene material.
- w. Violating any state or federal law or regulation in connection with the use of any information system or electronic mail system or service.
- x. Using the University's electronic mail systems or services or information technology resources to advertise, solicit, offer items for sale or to engage in commercial activities or services unless the email messages relates to a University function and has been approved by the Chief Information Officer.
- y. Using the University's electronic mail systems or services or information technology resources to engage in political advocacy. Many of the System collective bargaining contracts contain a union right's article that provides access to the Campus email system and other information technology resources. Nothing in this section will limit or abridge these rights.
- z. Constructing an electronic mail communication so it appears to be from someone else.

## **13. Violations**

**13.1 Reporting Violations.** Suspected violations of this policy are to be reported to the Chief Information Officer of the University. Upon receipt of such a report or upon learning of a possible violation, the Chief Information Officer, or his/her designee, shall conduct an investigation to determine whether a violation has occurred. Upon completion of his/her investigation, the Chief Information Officer, or his/her designee, shall present his/her findings to the Technology Advisory Council who shall decide what action, if any, should be recommended to the violator's direct supervisor or vice president. Investigations into alleged violations of this policy shall be conducted with due respect for individual privacy, the security of other users and the rights of due process.

**13.2 Actions for Violation of this Policy.** As stated previously, access to the University's information technology resources and the University's electronic mail systems or services is a privilege and not a right. Therefore, violations of this policy may result in discipline. Any discipline will be administered pursuant to the applicable provisions of the affected employee's collective bargaining agreement or the applicable campus policy.

**13.3 Legal Sanctions.** Violations of Section 502 of the California Penal Code (dealing with unlawful access or use of a computer) may be referred to the District Attorney or the police for investigation and/or prosecution. Similarly, violations of 18 U.S.C. 1030 (Federal laws dealing with unlawful access or use of a computer) may be referred to the Federal Bureau of Investigation. Sanctions for violations of these state and federal laws may be as severe as a \$50,000 fine and/or up to five (5) years in jail.

## Acknowledgements

### University Policies

- Electronic Communications Policy, University of California, Office of the President, <http://www.ucop.edu/ucophome/policies/ec/>
- Policy Governing Access to and Use of CSULB Computing Resources (1996), [http://www.csulb.edu/divisions/aa/grad\\_undergrad/senate/documents/policy/1996/18/2/](http://www.csulb.edu/divisions/aa/grad_undergrad/senate/documents/policy/1996/18/2/)

## References

### State of California Statues

- California Education Code Section 89005.5, <http://www.leginfo.ca.gov/>
- California Penal Code Section 502, <http://www.leginfo.ca.gov/>

### Federal Statues and Regulations

- Copyright Act of 1976, <http://www.copyright.gov/title17/>
- Digital Millennium Copyright Act of 1998 (DMCA), <http://www.copyright.gov/legislation/dmca.pdf>
- Technology, Education and Copyright Harmonization Act of 2002 (TEACH Act), <http://www.copyright.gov/title17/92appviii.html>
- U.S. Code, Title 18, 1030, [http://www.usdoj.gov/criminal/cybercrime/1030\\_new.html](http://www.usdoj.gov/criminal/cybercrime/1030_new.html)
- U.S. Department of Education, Family Educational Rights and Privacy Act of 1974 (FERPA), <http://www.ed.gov/policy/gen/guid/fpco/ferpa/index.html>

Revised: