CSU The California State University: Working for California

RESPONSIBLE USE POLICY

Contact:

Cheryl Washington
Interim Senior Director, System-wide Information Security Management

The California State University
Office of the Chancellor
401 Golden Shore
Long Beach, CA 90802-4210
(562) 951-4190 phone
cwashington@calstate.edu

October 27, 2008

1.0 Introduction

The California State University (the CSU or the University) must ensure that use of the CSU and campus information systems, data, and network resources are consistent with established policies and applicable laws. This policy is intended to promote and encourage responsible use and is not intended to prevent, prohibit, or inhibit the sanctioned use of campus resources as required to meet the University's core mission and campus academic and administrative purposes.

The University guidelines stated within this policy provide some specifics. However, they should not be taken to supersede or conflict with federal or California law, applicable regulations, other CSU and campus policies, or the laws of other states where material is accessed electronically via campus resources by users within those jurisdictions or material originating within those jurisdictions is accessed via campus resources.

The CSU regards the principle of academic freedom to be a key factor in assuring the effective application of this policy and related standards. Academic freedom encompasses the right of faculty to full freedom, within the law, in research and in the publication of results, freedom in the classroom in discussing their subject, and freedom from institutional censorship or discipline when they speak or write as citizens.

Use of campus information systems, data, and network resources is granted to users in support of instruction, research, studies, duties as employees, official business with the University, and/or other University-sanctioned activities. Access to campus information systems, data, and network resources is predicated on the user's acceptance of and adherence to the responsibilities detailed in CSU and campus policies.

2.0 Scope

This policy applies to all users (e.g., executives, managers, faculty, staff, students, guests, business partners, and others) of CSU data, computer networks, equipment, or computing resources. It is the collective responsibility of all users to ensure the confidentiality, integrity, and availability of information assets owned, leased, or entrusted to the CSU and to use CSU assets in an effective, efficient, ethical, and legal manner.

This policy establishes basic rights for all users, the CSU and campuses, and describes expectations for responsible use to ensure those rights in the following:

Section 3.0	***General Principles***	This section sets forth basic policy principles. Situations or behaviors not specifically mentioned in sections 4.0 – 6.0 may be addressed through application of these basic principles.
Section 4.0	***User Rights and Responsibilities***	This section highlights policy specifics related to access, responsible use, network and information system integrity, trademarks and patents, and incidental use.
Section 5.0	***System Administrator/ Service Provider Rights and Responsibilities***	This section describes system administrators and highlights specific expectations for system administrators and other service providers, whether they are professional staff, faculty, student administrators, consultants, or business partners.
Section 6.0	***CSU and Campus Rights and Responsibilities***	This section highlights specific expectations for CSU and campus officials.
Section 7.0	***Policy Enforcement***	This section describes a process for addressing misuse of CSU and campus resources.

The development of this policy was expedited by policies of:

- CSU campuses: Bakersfield, East Bay, Fresno, Humboldt, Long Beach, Monterey Bay, Northridge, San Diego, San Luis Obispo, San Marcos, and Sacramento.

- Other institutions: Concordia College, Montana State University, University of Albany, University of Michigan, and Virginia Technical

3.0 General Principles

CSU resources [e.g., Information Technology (IT) resources] are to be used to support the education, research, and public service missions of the University. The purpose of these principles is to specify user responsibilities and to promote the ethical, legal, and secure use of campus resources for the protection of all members of the CSU community.

- Use of CSU resources shall be consistent with the education, research, and public service mission of the University, federal and state laws, applicable regulations, and CSU and campus policies.
- The Responsible Use Policy shall apply to all users of resources owned, leased, or entrusted to the CSU.
- It is the policy of the CSU to make information technology resources and services accessible to all CSU students, faculty, staff, and the general public regardless of disability. Information regarding the Accessible Technology Initiative may be found at: http://www.calstate.edu/accessibility.
- IT provides an important means for both public and private communication. All users, including those with expanded privileges (e.g., system administrators and service providers), shall respect the privacy of person-to-person communications in all forms including telephone, electronic mail and file transfers, graphics, and television to the fullest extent possible under applicable law and CSU policy.
- The University shall respect individuals' rights to use CSU resources free from intimidation and harassment.
- The University respects freedom of expression in electronic communications on its computing and networking systems. Although this electronic speech has broad protections, all University community members are expected to use the information technology facilities considerately with the understanding that the electronic dissemination of information, particularly on the computing and networking systems, must be available to a broad and diverse audience.
- Other than publicly designated official University sites, the CSU does not generally monitor or restrict content residing on campus systems or transported across its networks.
- If there is reasonable cause to believe that a user has violated CSU or campus policy, federal/state laws, applicable regulations, or contractual obligations, the University reserves the right to take any of the following actions:
  - To have appropriate staff (e.g., IT staff) access the computing systems and networks including individuals login sessions.
  - Limit an individual's access to its networks.
  - Remove or limit access to University computers and/or materials posted on University computers.

"Reasonable cause" exists when facts and/or circumstances sufficiently convince a reasonable person to conclude:

- A violation of CSU or campus policy, state/federal law, applicable regulation, or contractual obligations has occurred.
- A member or group within the campus community has been detrimentally affected by some action.

All investigations of CSU or campus policy violations, non-compliance with federal/state laws and applicable regulations or contractual agreements will be conducted in a fair and equitable manner following established CSU and campus procedures.

- In the normal course of system maintenance, both preventive and troubleshooting, system administrators and service providers may be required to view file and monitor content on the CSU and campus networks, equipment, or computing resources. These individuals shall maintain the confidentiality and privacy of information unless otherwise required by law or CSU/campus policy.
- Campus servers and computing services should be properly configured so as not to pose a security risk or otherwise adversely affect existing University servers and services. All University system and network administrators or other service providers are expected to implement practices to satisfy "due diligence" in respect to security requirements.
- All users (e.g., faculty, staff, students, business partners, etc.) are required to help maintain a safe computing environment by notifying appropriate campus officials of vulnerabilities, risks, and breaches involving campus technology.
- The University recognizes and acknowledges employee incidental use of its computing and network resources within the guidelines defined in the "Incidental Use" section of this policy.
- This policy may be supplemented with additional guidelines developed by campuses.

4.0 User Rights and Responsibilities

This section describes rights and responsibilities governing access, responsible use, network and information system integrity, trademarks and patents, and incidental use. These statements are not designed to prevent, prohibit, or inhibit faculty and staff from fulfilling the mission of the University. Rather, these statements are designed to support an environment for teaching and learning by ensuring that CSU resources are used properly.

4.1 Authorized Use and Access

- Unless otherwise authorized, the owner of an account on a campus information system or network resource is responsible for all activity initiated by the user and performed under his/her account. A user cannot be held responsible for activities that may occur without his/her knowledge (e.g., hacking). When such an event occurs, the user will be required to assist in the investigation of the incident.
- Account owners must appropriately protect their account and authentication credentials.
- Users who have been authorized to use a password-protected account must follow established procedures for setting, maintaining, and changing passwords and may not disclose the password or otherwise make the account available to others without explicit authorization per established procedures. Users are prohibited from:

- Attempting to access, modify, or destroy University or non-University information systems, data or network resources for which a user is not properly authorized.
- In general, users must not monitor information systems or networks or capture the data residing on or transmitted through campus resources. However, such activity may be permitted under the following conditions:
  - The activity is permitted under CSU and campus policy.
  - The activity is defined in the user's job description.
  - The activity is conducted under the authority and supervision of an approved campus official.
  - The activity is part of a classroom exercise conducted under the supervision of a faculty member. In this case, the faculty member must ensure the exercise does not result in a breach of confidentiality, availability and integrity of campus data, information systems, or networks.
  - The activity is conducted to comply with an applicable law or under the guidance of law enforcement or legal counsel.
- With the exception of publicly accessible campus information technology resources, users must not transfer or extend access to University information technology resources to outside individuals or groups without prior approval of authorized University personnel. Such access must be limited in nature and fall within the scope of the educational mission of the University.

4.2 Responsible Use

- Users must not use campus information systems, data, or network resources for purposes that are inconsistent, incompatible, violate, or are in conflict with the University's mission, federal/state law, applicable regulations, contractual agreements, or University regulations and policies.
- Users must not use a University owned/leased computer system without permission or authorization.
- Users must not add, delete, alter, or destroy data or software without authorization.
- Users must not send unencrypted protected University data (defined as "Level 1" in the CSU Data Classification Standard) over a public network. Such data includes, but is not limited to: Social Security number, credit card information, and medical information.
- Users may not make software available for copying on a computer without authorization or unauthorized copies of computer data or documentation.
- Harassment of others via University information systems or network resources is prohibited under California State Penal Code Section 653m, other applicable laws, and University policies. It is a violation of this policy to use electronic means to harass, threaten, defame, or otherwise cause harm to a specific individual or threaten groups of individuals, whether by direct or indirect reference, or by creating a hostile environment. Campus information systems or network resources must not be used to print, send, or store fraudulent or harassing messages and/or materials. No e-mail, messages (voice or electronic), or web pages may be created or sent that may constitute intimidating, hostile, or offensive materials based on gender, race, color, religion, national origin, sexual orientation, or disability.
- University information systems or network resources must not be used to store, distribute, or transmit obscene or offensive material. These restrictions may not prohibit such access or retention if such materials are being used for a specific academic purpose. Access, storage, and

transmission of child pornography using CSU or campus resources ARE strictly prohibited at all times.

- Certain University facilities that provide information technology (e.g., computer labs, laboratories, offices, and libraries) do not provide a private environment for accessing electronic communications or other data. Therefore, users are advised to be aware of their responsibilities for appropriate behavior in public places. Some materials, which may be appropriate for scholarly inquiry in various disciplines, may have a strong possibility of creating an uncomfortable environment for other users. When an uncomfortable environment has been created, parties are encouraged to contact appropriate campus officials to seek assistance in resolving the conflict.
- Users must promptly report the loss or theft of any device which grants physical access to a University facility (e.g., keys, access cards or tokens).
- Users of campus information systems, data, or network resources must not purposefully misrepresent their identity, either directly or by implication, while communicating electronically. This provision is not intended to limit anonymity, where appropriate, but rather to address purposeful and deliberate use of false identities.
- Campus information systems, data, or network resources must not be used to imply University endorsement, including the support or opposition of the University with regards to any religious or political activity or issue. While using University information systems or network resources, users must not imply University endorsement of products or services of a non-University entity, without appropriate approval. Users must not give the impression that they are representing, giving opinions, or otherwise making statements on behalf of the University unless authorized to do so.
- Effective information security is a team effort involving the participation and support of every user. A user who has knowledge (or reasonable suspicion) of a violation of this policy must follow the applicable procedures for reporting the violation to the appropriate personnel at his or her campus. A user must not prevent or obstruct another user from reporting a security incident or policy violation.

4.3 Network and Information System Integrity

- Individuals must not use University-owned/leased or privately-owned/leased technology resources in a manner that purposefully causes damage to or impairs campus information systems, data, or network resources. Such behaviors (e.g., disrupting services, or causing a denial of service to a computer system or network without authorization) are prohibited on both University-owned/leased and privately-owned/leased equipment operated on or through campus resources.
- In accordance with California State Penal Code Section 502 and other policies and laws, activities and behaviors that threaten the confidentiality, availability, and integrity of campus data, networks or information systems are prohibited on both University-owned/leased and privately-owned/leased equipment operated on or through University resources. These activities and behaviors include but are not limited to:
  - Failure to comply with authorized requests from University personnel to discontinue activities that threaten the operation or integrity of information systems, data, or network resources.
  - Providing unauthorized services or accounts on University information systems. University-authorized business and other activities directly related to the academic mission of the University are allowed; however, any information systems running services that may negatively impact management, reliability, or integrity of the University network or other University resources may be disconnected from the network.

- Users are responsible for taking reasonable precautions to avoid introducing malicious software into any University network. Unless appropriately authorized, users must not bypass or turn-off anti-virus software installed on University information systems.
- Users must appropriately protect their devices and credentials that provide access to University protected data against loss, theft, or unauthorized access. Users must take reasonable precautions to ensure that their devices (e.g., computers, PDAs, smart phones, etc.,) are secure before connecting remotely to the CSU information systems, data, or network resources. Users must close connections (including remote connections) to University information systems, data, and network resources once they have completed University-related activities.

4.4 Incidental Use

University information systems and network resources are owned and operated by the University and are to be used for University-related activities and may be used for occasional incidental use. Such resources are provided to facilitate a person's essential work as an employee, student, or other role within the University. Individuals may use campus information resources for occasional incidental personal purposes of a private nature provided such use does not:

- Violate international, federal, or state laws.
- Interfere with the University's operation of its information systems and network resources.
- Burden the University with significant costs.
- Interfere with a person's employment or other obligations to the University.
- Constitute or result in financial gain for someone or something other than the University.
- Create a security risk to the confidentiality, integrity or availability of University resources, data or services.

When significant costs for personal use are incurred, users may be held responsible for reimbursing some or all of the costs to the University.

4.5 System Administrator/Service Provider Rights and Responsibilities

This section highlights specific expectations for system administrators or other service providers, whether they are professional staff, faculty, or business partners.

System administrators and other service providers exist at various levels of the University (e.g., within and outside of central IT). Each system administrator and service provider has the responsibility to offer service in the most efficient, reliable, and secure manner while considering the needs of the total campus community. At certain times, the process of carrying out these responsibilities may require special actions or intervention by the system administrator or service provider. In such circumstances, their actions are bound by federal/state laws, applicable regulations, and CSU/campus policies, standards, procedures, and contractual agreements.

If a system administrator or service provider has been instructed to perform an action that conflicts with federal/state laws, applicable regulations, or CSU/campus policies, standards, procedures or contractual agreements, he/she is required to notify appropriate campus officials.

As users of the system they administer, they have the same rights and responsibilities as any other user of the campus information system, data or network resources including respect for the privacy of other users' information. They also have a primary responsibility to ensure the availability, usefulness, integrity and

security of the systems, data and networks they manage. In this capacity their privileges exceed those of other users. The professional ethics of all system administrators and service providers must be at the highest level and their professional ethical conduct must be beyond reproach.

Rights and responsibilities assigned to each system administrator and/or service provider include but are not limited to:

- **Adequate Hardware and Software:** Before any server is installed and placed on a campus network, ascertain the following:
  - Whether the machine is in an appropriate state to be placed on a shared network.
  - If the resource requirements (hardware and software) and system management requirements (people) for both current and future needs are either in place or planned for, to keep the machine in "top running order."
- **Legal Licensing:** Ensure that hardware and software products are installed consistent with license agreements.
- **Monitoring:** Monitor for performance and capacity planning and intercede where needed to prevent misuse or misappropriation of system resources. Monitoring helps ensure that the system resources are not being misused.
- **Security Alerts and Updates:** Monitor sources of system alerts and for applying operating system and software product patches and security upgrades in a timely manner.
- **Precautionary Scans:** Take necessary precautions to safeguard systems against "corruption, compromise or destruction." This includes performing scans for diagnostic problem resolution purposes of the systems they maintain or assessing network traffic into or out of systems they maintain.
- **Confidentiality and Privacy of User Files:** In the course of carrying out one's duties, avoid viewing the contents of a user's files or messages. If such content is exposed and becomes known to the system administrator or service provider, it should be treated as confidential and private.
- **Security Breaches:** During the performance of duties, if information is uncovered that indicates a breach of security has occurred, action must be taken following established CSU and campus procedures. User accounts, services, or systems cannot be capriciously shut down. However, in those instances where a security incident is suspected that will endanger the confidentiality, availability, or integrity of both the system and the files and data of others, the system administrator or service provider may shut down specific accounts or close access to services or systems that appear to be linked to the problem. Immediately after the emergency action is taken, appropriate campus officials should be notified and an appropriate review should be conducted to follow up on the emergency action.

5.0 CSU and Campus Rights and Responsibilities

This section highlights specific rights and responsibilities for CSU and campus officials.

The CSU and campuses reserve the right to:

- Limit access to its resources when there is a violation (or there is reason to believe there has been a violation) of campus policies and standards, contractual agreements, state/federal laws, or applicable regulations.
- Use appropriate means to safeguard its resources, preserve network or system integrity, and ensure continued service delivery at all times.

- Restrict the use of its computing and information technology resources based on institutional priorities and financial considerations.
- Monitor communications across its network services and transaction records residing on campus information systems.
- Scan information systems attached to campus networks for security problems.
- Disconnect information systems that have become a security hazard.
- Restrict material transported across its network or posted on campus information systems as necessary.
- Unless otherwise required by law and/or policy, the University reserves the right to archive and/or remove stored files and messages in order to preserve information system integrity. Except in an emergency, users will be given advance notice prior to the deletion of files or messages.

The CSU is required by California State law to disclose to California residents any breach of campus information systems or network resources which results in unencrypted personal information (as defined in CA CC 1798) being, or reasonably believed to have been, accessed by an unauthorized person.

6.0 Policy Enforcement

The CSU respects the rights of its employees and students. In support of this policy, campuses must establish procedures which assure that investigations involving employees and students suspected of violating this policy are conducted in a fair and equitable manner. These procedures must comply with appropriate regulations (e.g., California Education Code and Title V), collective bargaining agreements and CSU/campus policies. Additionally, campuses must develop procedures for reporting violations of this policy.

The University reserves the right to temporarily or permanently suspend, block or restrict access to information assets, independent of such procedures, when it reasonably appears necessary to do so in order to protect the confidentiality, integrity, availability, or functionality of University resources or to protect the University from liability.

Allegations against employees that are sustained may result in disciplinary action, which may only be administered in a manner consistent with the terms of the applicable collective bargaining agreement in accordance with the applicable provisions of the California Education Code, and/or civil and criminal or prosecution. Student infractions of this policy may be referred to the Office of Student Judicial Affairs. Third party service providers who do not comply with this policy may be subject to appropriate actions as defined in contractual agreements.