CSU The California State University: Working for California

RESPONSIBLE USE POLICY

Contact:

William Perry
Chief Information Security Officer

The California State University
Office of the Chancellor
401 Golden Shore
Long Beach, CA 90802-4210
(562) 951-4638 phone
wperry@calstate.edu

October 18, 2012

Table of Contents

1.0 INTRODUCTION

The California State University (CSU) provides access to information assets for purposes related to its mission and to the responsibilities and necessary activities of its faculty, students and staff. These resources are vital for the fulfillment of the academic, research and business needs of the CSU community. This policy defines user, system administrator and CSU responsibilities with respect to the use of CSU information assets in conjunction with the CSU Information Security Policy.

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 is at the heart of a university's fundamental mission of discovery and advancement of knowledge and its dissemination to students and the public. The CSU is committed to upholding and preserving the principles of academic freedom: the rights of faculty to teach, conduct research or other scholarship, and publish free of external constraints other than those normally denoted by the scholarly standards of a discipline.

This policy is intended to define, promote and encourage responsible use of CSU and campus information assets on the campuses and among members of the campus community. This policy is not intended to prevent, prohibit, or inhibit the sanctioned use of campus information assets as required to meet the CSU's core mission and campus academic and administrative purposes.

The requirements stated within this policy must not be taken to supersede or conflict with applicable laws, regulations, collective bargaining agreements or other CSU and campus policies.

2.0 SCOPE

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.

The CSU Responsible Use policy shall apply to the following:

- All campuses.
- Central and departmentally managed campus information assets.
- All users employed by campuses or any other person with access to campus information assets.
- All categories of information, regardless of the medium in which the information asset is held or transmitted (e.g. physical or electronic).
- Information technology facilities, applications, hardware systems, and network resources owned or managed by the CSU.

Auxiliaries, external businesses and organizations that use campus information assets must comply with the CSU Responsible Use Policy.

This policy establishes basic responsibilities for all users, the CSU and campuses, and describes expectations for responsible use in the following sections:

Section 4.0	***General Principles***	This section sets forth basic policy principles. Situations or behaviors not specifically mentioned in sections 5.0 – 7.0 may be addressed through application of these basic principles.
Section 5.0	***User - Responsibilities***	This section highlights policy specifics related to access, responsible use, network and information system integrity, trademarks and patents, and incidental use.
Section 6.0	***System Administrator/ Service Provider Responsibilities***	This section describes system administrators and highlights specific requirements for system administrators and other service providers, whether they are professional staff, faculty, student administrators, consultants, or business partners.
Section 7.0	***CSU and Campus Responsibilities***	This section highlights specific requirements for CSU and campus officials.
Section 8.0	***Policy Enforcement***	This section describes a process for addressing violations of the CSU Responsible Use Policy.

The development of this policy was expedited by reference to policies from:

- ***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 Tech

3.0 POLICY MANAGEMENT

The CSU Responsible Use policy shall be updated as necessary to reflect changes in the CSU's academic, administrative, or technical environments, or applicable laws and regulations. The CSU Information Security Management Department shall be responsible for overseeing a bi-annual review of this policy and communicating any changes or additions to appropriate CSU stakeholders.

The policy may be augmented, but neither supplanted nor diminished, by additional policies and standards adopted by each campus.

Each campus through consultation with campus officials and key stakeholders must develop policies, standards, and implementation procedures referenced in the CSU Responsible Use policy.

4.0 GENERAL PRINCIPLES

The purpose of these principles is to provide a frame of reference for 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 information assets shall be consistent with the education, research, and public service mission of the University, applicable laws, regulations, and CSU/campus policies. Please note that the term "information assets" along with many other important terms and concepts is defined in the CSU Information Security Glossary.

- It is the policy of the CSU to make information assets and services accessible in order to meet the needs of CSU students, faculty, staff, and the general public. Information regarding the Accessible Technology Initiative may be found at: http://www.calstate.edu/accessibility.

- 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.

- 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, may be available to a broad and diverse audience including those outside the university.

- 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. However, the CSU reserves the right to use appropriate means to safeguard its data, preserve network and information system integrity, and ensure continued delivery of services to users. These activities are not intended to restrict, monitor, or use the content of legitimate academic and organizational communications.

- In the normal course of system and information security maintenance, both preventive and troubleshooting, system administrators and service providers may be required to view files 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 must 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 required to comply with CSU and campus policies related to information security.

- 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 information assets.

- 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, at paragraph 5.5 below.

- All investigations of CSU or campus policy violations, non-compliance with applicable laws and regulations or contractual agreements will be conducted in accordance with appropriate CSU and campus procedures.

5.0 USER RESPONSIBILITIES

This section describes user responsibilities governing access, responsible use, network and information system integrity, 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 appropriately.

5.1 Responsible Use of Information Assets

Users are expected to use good judgment and reasonable care in order to protect and preserve the integrity of university equipment, its data and software, and its access.

- Users must not use or access campus information assets in a manner that
  - Conflicts with the CSU mission;
  - Violates applicable laws, regulations, contractual agreements, CSU/campus policies or standards; or
  - Causes damage to or impair campus information assets or the productivity of CSU users through intentional, negligent or reckless action.

- Users must take reasonable precautions to avoid introducing harmful software, such as viruses, into university computer hardware, software or data storage media.

- Unless appropriately authorized, users must not knowingly disable automated update services configured on university computers.

- Users must take reasonable precautions to ensure that their devices (e.g., computers, PDAs, smart phones, etc.,) are secure before connecting remotely to CSU information assets.

- Users must close or secure connections to campus desktop or system resources (i.e. remote desktop, virtual private network connections, etc.) once they have completed University-related activities or when the asset is left unattended.

- 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), or electronic access (passwords or other credentials) to University resources.

- Users who publish or maintain information on University information assets are responsible for ensuring that information they post complies with applicable laws, regulations, and CSU/campus policies concerning copyrighted material and fair use of intellectual property.

- Software must be used in a way that is consistent with the relevant license agreement. Unauthorized copies of licensed or copyrighted software may not be created or distributed.

- Per Section 8314.5 of the California Government Code, it is unlawful for any state employee, or consultant, to knowingly use a state-owned or state-leased computer to access, view, download, or otherwise obtain obscene matter. “Obscene matter” as used in this section has the meaning specified in Section 311 of the California Penal Code. “State owned or state-leased computer” means a computer owned or leased by a state agency, as defined by Section

11000, including the California State University. This prohibition does not apply to accessing, viewing, downloading, or otherwise obtaining obscene matter for use consistent with legitimate law enforcement purposes, to permit a state agency to conduct an administrative investigation, or for legitimate medical, scientific, or academic purposes.

- A user who has knowledge (or reasonable suspicion) of a violation of this policy must follow applicable CSU and campus procedures for reporting the violation. A user must not prevent or obstruct another user from reporting a security incident or policy violation.

5.2 Protection from Data Loss

Individuals who access, transmit, store, or delete Level 1 or Level 2 data as defined in the CSU Data Classification Standard must use all reasonable efforts to prevent unauthorized access and disclosure of confidential, private or sensitive information.

- Users must not access or transmit Level 1 or Level 2 data to another user without prior approval from the data owner or custodian.

- Users must not access or transmit unencrypted Level 1 data over a public network.

5.3 Prohibition against Unauthorized Browsing and Monitoring

The University supports and protects the concepts of privacy and protects the confidentiality and integrity of personal information maintained in educational, administrative, or medical records. Information stored in campus information systems may be subject to privacy laws.

- Users must not browse, monitor, alter or access email messages or stored files in another user's account unless specifically authorized by the user. However, such activity may be permitted under the following conditions:

    - The activity is permitted under CSU or 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 acting within his or her job responsibilities
    - 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 information assets.
    - The activity is conducted to comply with an applicable law, regulation, or under the guidance of law enforcement or legal counsel.

5.4 Responsibility of Account Owners

The owner or custodian of credentials, such as a username and password, that permit access to a campus information system or network resource is responsible for all activity initiated by the user and performed under his/her credentials. The user shall assist in the investigation and resolution of a security incident regardless of whether or not the activity occurred without the user's knowledge and as a result of circumstances outside his or her control.

- Users must take reasonable steps to appropriately protect their credentials from becoming known by, or used by others.

- Users who have been authorized to use a password-protected account must follow established procedures for setting, maintaining, and changing passwords. Unless specific prior authorization has been granted, users are prohibited from:

    - Using or attempting to use the account to access, modify, or destroy campus or non-campus information assets for which a user is not normally authorized.
    - Disclosing passwords to any party or including passwords in documentation.
    - Embedding passwords in software code.

- With the exception of publicly accessible campus information assets, users must not transfer or provide access to campus information assets to outside individuals or groups without proper authorization.

- Users of campus information assets must not purposefully misrepresent their identity, either directly or by implication, with the intent of using false identities for inappropriate purposes.

- In the few instances where special circumstances or system requirements mandate that multiple users access the same account, extreme care must be used to protect the security of the account and its access password. Management of this account must conform to written or published campus procedures designed to mitigate risk associated with shared access accounts.

5.5 Incidental Use

University-owned/managed information assets are provided to facilitate a person's essential work as an employee, student, or other role within the University. Use of university owned computer systems for University-related professional development or academic activities such as research or publication is permitted within the limits of system capacities.

Personal use of campus information assets must be no more than "de minimus" (e.g. must have so little value that accounting for it would be unreasonable or impractical,). Individuals may use campus information assets for occasional incidental and minimal personal use provided such use:

- Does not violate applicable laws.
- Is not in pursuit of the individual's private financial gain or advantage
- Does not interfere with the operation or maintenance of University information assets.
- Does not interfere with the use of University information assets by others.
- Does not interfere with the performance of the assigned duties of a university employee. Does not result in a loss to the University.

6.0 SYSTEM ADMINISTRATOR/SERVICE PROVIDER 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 shall 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 action or intervention by the system administrator or service provider. In such circumstances, applicable laws, regulations, and CSU/campus policies, standards, procedures, and contractual agreements bind their actions.

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

System administrators have the same responsibilities as any other user of the campus information assets including respect for the privacy of other users' information. They also have a primary responsibility to ensure the confidentiality, integrity, and availability of the information assets 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.

System administrator responsibilities for managing CSU information assets include but are not limited to ensuring:

- **Compliance with Standards:** Ensure servers meet campus configuration requirements before the unit is installed on a campus network.
- **Information Asset Maintenance:** Work with appropriate management and technical staff to ensure systems are operating efficiently.
- **License Compliance:** Ensure that hardware and software products are installed consistent with license agreements.
- **Adequate Performance & Capacity:** Monitor for performance and capacity planning and intercede where needed to prevent misuse or misappropriation of system resources.
- **Security Updates:** Apply operating system and software product patches and security upgrades in a timely manner.
- **Protection from Disruption:** Take necessary precautions to safeguard systems. This includes, but is not limited to, performing scans to diagnose problems or analyzing network traffic, if authorized.
- **Confidentiality of information:** Protect the confidentiality of CSU and user data in the event such information is exposed to the system administrator or service provider during the

performance of duties. If such content is exposed and becomes known to the system administrator or service provider, it must be respected as protected and confidential.

- **Investigation of Security Incidents:** During the performance of duties, if information is uncovered that indicates a potential breach of security has occurred, action must be taken following CSU and campus written 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 the information assets, 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. Appropriate campus officials must be promptly notified and an appropriate review must be conducted to follow up on the emergency action.

7.0 CSU AND CAMPUS RESPONSIBILITIES

The CSU has broad responsibilities with respect to protecting CSU information assets. These include but are not limited to controlling access to information, ensuring the physical security of the information assets, responding to and addressing information security incidents, complying with laws are regulations, ensuring the security of the underlying technology used to store and transmit information. CSU Policies related to these activities are found in the Integrated CSU Administrative Manual and can be accessed at http://www.calstate.edu/icsuam/sections/8000/.

The CSU retains ownership or stewardship of information assets owned (or managed) by or entrusted to the CSU. The CSU reserves the right to limit access to its information assets and to use appropriate means to safeguard its data, preserve network and information system integrity, and ensure continued delivery of services to users. This can include, but is not limited to: monitoring communications across campus network services; monitoring actions on the campus information systems; checking information systems attached to the campus network for security vulnerabilities; disconnecting information systems that have become a security hazard; or, restricting data to/from campus information systems and across network resources. These activities are not intended to restrict, monitor, or utilize the content of legitimate academic and organizational communications.

8.0 POLICY ENFORCEMENT

The CSU respects the rights of its employees and students. In support of the CSU Information Security policy http://www.calstate.edu/icsuam/sections/8000/, and this Responsible Use Policy, campuses must establish procedures that ensure investigations involving employees and students suspected of violating the CSU Information Security policy are conducted. These procedures must comply with appropriate laws, regulations, collective bargaining agreements, and CSU/campus policies. Additionally, campuses must develop procedures for reporting violations of this policy.

The CSU 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 CSU resources or to protect the CSU from liability.

Allegations against employees that are sustained may result in disciplinary action. Such actions must be administered in a manner consistent with the terms of the applicable collective bargaining agreement and the California Education code. Student infractions of the CSU Information Security policy must be handled in accordance with the established student conduct process. Auxiliary employees who violate the requirements of the policy may be subject to appropriate disciplinary actions as defined by their organization's policies. Third party service providers who do not comply with this policy may be subject to appropriate actions as defined in contractual agreements and other legal remedies available to the CSU.

The CSU may also refer suspected violations to appropriate law enforcement agencies.