

Responsible Use Agreement

Last Updated: 7/1/2022

The CSU Information Security policy provides and defines user, including faculty, staff, students, third parties, and CSU responsibilities with respect to the use of CSU information assets.

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 (e.g., faculty, staff, students, third parties, etc) 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 ensuring 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 information assets among members of the CSU community. This policy is not intended to prevent, prohibit, or inhibit the sanctioned use of CSU 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.

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 Responsible Use Policy shall apply to the following:

CSU Maritime Academy Responsible Use Agreement

5. Information technology facilities, applications, hardware systems, and network resources owned or managed by the CSU.
6. Auxiliaries, external businesses and organizations that use CSU information assets must comply with the Responsible Use Policy.

Procedures

The 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 Chief Information Security Officer shall be responsible for overseeing a periodic 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 Responsible Use Policy.

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 CSU resources for the protection of all members of the CSU community.

1. Use of CSU information assets shall be consistent with the education, research, and public service

7. 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.

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 CSU. Rather, these statements are designed to support an environment for teaching and learning by ensuring that CSU resources are used appropriately.

- a. All users (e.g., faculty, staff, students, third parties) are required to comply with CSU and campus policies and standards related to information security.
 - b. All users (e.g., faculty, staff, students, business partners) are required to help maintain a safe computing environment by notifying appropriate CSU officials of known vulnerabilities, risks, and breaches involving CSU information assets.
 - c. 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 video.
-
- a. Users are expected to use good judgment and reasonable care in order to protect and preserve the integrity of CSU equipment, its data and software, and its access.
 - b. Users must not use or access CSU information assets in a manner that:
 - i. Conflicts with the CSU mission;
 - ii. Violates applicable laws, regulations, contractual agreements, CSU/campus policies or standards; or
 - iii. Causes damage to or impairs CSU information assets or the productivity of CSU users through intentional, negligent or reckless action.
 - c. Users must take reasonable precautions to avoid introducing harmful software, such as viruses, into CSU computing and networking systems.
 - d. Unless appropriately authorized, users must not knowingly disable automated update services configured on CSU computers.
 - e. Users must take reasonable precautions to

CSU Maritime Academy Responsible Use Agreement

- h. Users who publish or maintain information on CSU 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.
 - i. 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.
 - j. 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.
 - k. 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. Refer to CSU Information Security Policy 8075 Information Security Incident Management.
 - l. Title 5 of the California Code of Regulations (5 CA ADC § 41301) defines grounds for student discipline with respect to responsible use of technology. Illegal file-sharing and other copyright violations are a violation of Title 5 of the California Code of Regulations (5 CA ADC § 41301).
- a. Individuals who access, transmit, store, or delete Level 1 or Level 2 data as defined in the CSU Information Asset Management Policy must use all reasonable efforts to prevent unauthorized access and disclosure of confidential, private, or sensitive information.
 - b. The CSU Information Asset Management Policy requires:
 - i. Users must not provide access or transmit Level 1 or Level 2 data to another user without prior approval from the data owner or custodian.
 - ii. Users must not access or transmit unencrypted Level 1 data over a public network.
- a. The CSU 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 CSU information systems may be subject to privacy laws.
 - b. 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:
 - i. The activity is permitted under CSU or campus policy.
 - ii. The activity is defined in the user's job description.

CSU Maritime Academy Responsible Use Agreement

- iv. 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 CSU information assets.
 - v. The activity is conducted to comply with an applicable law, regulation, or under the guidance of law enforcement or legal counsel.
-
- a. The owner or custodian of credentials, such as a username and password, that permit access to a CSU 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.
 - b. Users must take reasonable steps to appropriately protect their credentials from becoming known by, or used by others.
 - i. 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:
 - ii. Using or attempting to use the account to access, modify, or destroy CSU or non-CSU information assets for which a user is not normally authorized.
 - iii. Disclosing passwords to any party or including passwords in documentation.
 - iv. Embedding passwords in software code.
 - c. With the exception of publicly accessible CSU information assets, users must not transfer or provide access to CSU information assets to outside individuals or groups without proper authorization.
 - d. Users of CSU information assets must not purposefully misrepresent their identity, either directly or by implication, with the intent of using false identities for inappropriate purposes.
 - e. In the few instances where special circumstances or system requirements mandate that multiple users

CSU Maritime Academy Responsible Use Agreement

- v. Does not interfere with the performance of the assigned duties of a university employee.
- vi. Does not result in a loss to the University.

CSU Responsibilities

The CSU has broad responsibilities with respect to protecting its information assets. These include but are not

My signature acknowledges that I have read, understood, and will adhere to the California State University Maritime Academy Information Security Responsible Use Policy and Agreement. I also acknowledge that I will report violations immediately to the Information Security Office through 707-654