SAN DIEGO STATE UNIVERSITY

CONFIDENTIALITY STATEMENT

I understand that any access I am granted to protected information and data is based on my agreement to comply with the following terms and conditions:

- I will comply with the state and federal laws, SDSU, and CSU policies that govern access to and use of information contained in employee, applicant, and student records.
- My right to access information and/or data is strictly limited to the specific information and data that is relevant and necessary for me to perform my job- related duties.
- I am prohibited from accessing information or data that is not relevant and necessary for me to perform my job-related duties.
- I will be a responsible user of information and data.
- I will store information and data that I obtain under secure conditions.
- I will maintain the privacy and confidentiality of the information and data that I obtain.
- Before sharing information or data with others, electronically or otherwise, I will ensure that the recipient is authorized to receive that information or data and understands his/her responsibilities as a user.
- I will sign off any system containing confidential information when I am not actively using it.
- I will keep my password(s) to myself, and will not disclose them to others unless SDSU Human Resources and my supervisor authorize such disclosure in writing.
- I will store and secure confidential and sensitive information, data, reports, etc. in a manner that will maintain their confidentiality when I am not actively using them.
- I will dispose of confidential reports in a manner that will preserve their confidentiality when I have finished using them.
- I will not misuse personal or confidential information or data that I obtain through my employment.
- I will refer to the SDSU Information Security Plan to identify campus specific standards and procedures, including a complete definition of protected information: http://security.sdsu.edu/iso/secplan.htm.
- I will complete all assigned security awareness training in a timely manner.
- I will seek assistance from my supervisor or the IT Security Office when in doubt of my responsibilities for information security.

8105.00 | Responsible Use Policy

Effective Date: 11/20/2013 | **Revised Date**: 11/20/2013

POLICY OBJECTIVE

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

POLICY STATEMENT

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 (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.

1.0 Scope

1.1 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.

1.2 The CSU RESPONSIBLE USE POLICY shall apply to the following:

a) All campuses.

b) Central and departmentally managed campus information assets.

c) All users employed by campuses or any other person with access to campus information assets.

d) All categories of information, regardless of the medium in which the information asset is held or transmitted (e.g. physical or electronic).

e) Information technology facilities, applications, hardware systems, and network resources owned or managed by the CSU.

1.3 Auxiliaries, external businesses and organizations that use CSU information assets must comply with the CSU RESPONSIBLE USE POLICY.

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

Section 3.0	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 4.0	User - Responsibilities	This section highlights policy specifics related to access, responsible use, network and information system integrity, trademarks and patents, and incidental use.
Section 5.0	CSU and Campus Responsibilities	This section highlights specific requirements for CSU and campus officials.
Section 6.0	Policy Enforcement	This section describes a process for addressing violations of the CSU RESPONSIBLE USE POLICY.

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

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

b) Other institutions: Concordia College, Montana State University, University of Albany, University of Michigan, and Virginia Tech

2.0 Policy Management

2.1 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 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.

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

2.3 Each campus through consultation with campus officials and key stakeholders must develop policies, standards, and implementation procedures referenced in the CSU RESPONSIBLE USE POLICY.

3.0 General Principles

3.1 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.

3.2 Use of CSU information assets shall be consistent with the education, research, and public service mission of the CSU, applicable laws, regulations, and CSU/campus policies. Note: The term "information assets", along with many other important terms and concepts, is defined in the CSU ICSUAM Policy Glossary: https://csyou.calstate.edu/ICSUAM/Pages/Policy-Glossary.aspx.

3.3 All users (e.g., faculty, staff, students, third parties) are required to comply with CSU and campus policies and standards related to information security.

3.4 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.

3.5 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 can be found at: https://csyou.calstate.edu/Projects-Initiatives/ATI/Pages/default.aspx.

3.6 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.

3.7 The CSU 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 may be available to a broad and diverse audience including those outside the university.

3.8 Other than publicly designated official CSU sites, the CSU does not generally monitor or restrict content residing on CSU 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.

3.9 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.

3.10 The CSU 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 4.5 below.

3.11 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.

4.1 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.

4.2 Responsible Use of Information Assets

4.2.1 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.

4.2.2 Users must not use or access CSU information assets in a manner that:

a) Conflicts with the CSU mission;

b) Violates applicable laws, regulations, contractual agreements, CSU/campus policies or standards; or

c) Causes damage to or impairs CSU information assets or the productivity of CSU users through intentional, negligent or reckless action.

4.2.3 Users must take reasonable precautions to avoid introducing harmful software, such as viruses, into CSU computing and networking systems.

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

4.2.5 Users must take reasonable precautions to ensure their personal and/or CSU- provided devices (e.g., computers, tablets, smart phones) are secure before connecting to CSU information assets.

4.2.6 Users must close or secure connections to CSU information assets (e.g. remote desktop, virtual private network connections) once they have completed CSU-related activities or when the asset is left unattended.

4.2.7 Users must promptly report the loss or theft of any device, which grants physical access to a CSU facility (e.g., keys, access cards or tokens), or electronic access (passwords or other credentials) to CSU resources.

4.2.8 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.

4.2.9 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.

4.2.10 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.

4.2.11 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.

4.2 Protection from Data Loss

4.2.1 Individuals who access, transmit, store, or delete Level 1 or Level 2 data as defined in the CSU Data Classification Standard1 must use all reasonable efforts to prevent unauthorized access and disclosure of confidential, private, or sensitive information.

[1] The CSU Data Classification Standard is located here.

a) 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.

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

4.3 Prohibition Against Unauthorized Browsing and Monitoring

4.3.1 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.

4.3.2 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:

a) The activity is permitted under CSU or campus policy.

b) The activity is defined in the user's job description.

c) The activity is conducted under the authority and supervision of an approved CSU official acting within his or her job responsibilities.

d) 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.

e) The activity is conducted to comply with an applicable law, regulation, or under the guidance of law enforcement or legal counsel.

4.4 Responsibility of Account Owners

4.4.1 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.

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

a) 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:

b) 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.

c) Disclosing passwords to any party or including passwords in documentation.

d) Embedding passwords in software code.

4.4.3 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.

4.4.4 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.

4.4.5 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 CSU procedures designed to mitigate risk associated with shared access accounts.

4.5 Incidental Use

4.5.1 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.

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

a) Does not violate applicable laws.

b) Is not in pursuit of the individual's private financial gain or advantage.

c) Does not interfere with the operation or maintenance of University information assets.

d) Does not interfere with the use of University information assets by others.

e) Does not interfere with the performance of the assigned duties of a university employee.

f) Does not result in a loss to the University.

5.0 CSU Responsibilities

5.1 The CSU has broad responsibilities with respect to protecting its information assets. These include but are not limited to controlling access to information, responding to and addressing information security incidents, complying with laws and regulations, and ensuring the logical and physical 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 https://csyou.calstate.edu/ICSUAM/Pages/ICSUAM-8000.aspx.

5.2 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 network services; monitoring actions on information systems; checking information systems attached to the network for security vulnerabilities; disconnecting information systems that have become a security hazard; or, restricting data to/from information systems and across network resources. These activities are not intended to restrict, monitor, or utilize the content of legitimate academic and organizational communications.

6.0 Policy Enforcement

6.1 The CSU respects the rights of its employees and students. In support of the CSU Information Security policies https://csyou.calstate.edu/ICSUAM/Pages/ICSUAM- 8000.aspx 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.

6.2 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. Suspension, block or restriction to information assets in such a manner as to substantially affect the ability to complete assigned coursework or job duties shall be considered disciplinary actions subject to §6.3.

6.3 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 CSU Information Security policies must be handled in accordance with the established student conduct process. Auxiliary employees who violate the CSU policies may be subject to appropriate disciplinary actions as defined by their organization's policies. Third party service providers who do not comply with CSU policies may be subject to appropriate actions as defined in contractual agreements and other legal remedies available to the CSU.

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

Benjamin F. Quillian
Executive Vice-Chancellor/Chief Financial Officer Approved:

November 20, 2013

INFORMATION PRACTICES ACT OF 1977, CALIFORNIA CIVIL CODE

As outlined in HR Letter 2005-01, each campus and the Chancellor's Office have the legal responsibility to administer and comply with provisions of the Information Practices Act (IPA) which is contained in §1798 - §1798.78, of the California Civil Code. The IPA can be found on the Web at: http://www.privacy.ca.gov/code/ipa.htm. The IPA places specific requirements on state agencies in relation to the collection, use, maintenance and dissemination of information relating to individuals. Careless, accidental, or intentional disclosure of information to unauthorized persons can have far-reaching effects, which may result in disciplinary action against those involved in unauthorized disclosure (§1798.55) and civil action against the CSU with a right to be awarded reasonable attorney's fees, if successful. For reference, the following **summary** is provided:

Article 1: General Provisions and Legislative Findings

§1798.1 The Legislature declares that the right to privacy is a personal and fundamental right protected by Section 1 of Article I of the Constitution of California and by the United States Constitution and that all individuals have a right of privacy in information pertaining to them. The Legislature further makes the following findings:

a) The right to privacy is being threatened by the indiscriminate collection, maintenance, and dissemination of personal information and the lack of effective laws and legal remedies.

b) The increasing use of computers and other sophisticated information technology has greatly magnified the potential risk to individual privacy that can occur from the maintenance of personal information.

c) In order to protect the privacy of individuals, it is necessary that the maintenance and dissemination of personal information be subject to strict limits.

Article 2: Definitions

§1798.3. As used in this chapter:

a) The term "personal information" means any information that is maintained by an agency that identifies or describes an individual, including, but not limited to, his or her name, social security number, physical description, home address, home telephone number, education, financial matters, and medical or employment history. It includes statements made by, or attributed to, the individual.

…

c) The term "disclose" means to disclose, release, transfer, disseminate, or otherwise communicate all or any part of any record orally, in writing, or by electronic or any other means to any person or entity.

Article 5: Agency Requirements

§1798.14. Each agency shall maintain in its records only personal information which is relevant and necessary to accomplish a purpose of the agency required or authorized by the California Constitution or statute or mandated by the federal government.

§1798.18. Each agency shall maintain all records, to the maximum extent possible, with accuracy, relevance, timeliness, and completeness…

§1798.20. Each agency shall establish rules of conduct for persons involved in the design, development, operation, disclosure, or maintenance of records containing personal information and instruct each such person with respect to such rules and the requirements of this chapter, including any other rules and procedures adopted pursuant to this chapter and the remedies and penalties for noncompliance.

§1798.21. Each agency shall establish appropriate and reasonable administrative, technical, and physical safeguards to ensure compliance with the provisions of this chapter, to ensure the security and confidentiality of records, and to protect against anticipated threats or hazards to their security or integrity which could result in any injury.

§1798.22. Each agency shall designate an agency employee to be responsible for ensuring that the agency complies with all of the provisions of this chapter.

Article 6: Conditions Of Disclosure

§1798.24. No agency may disclose any personal information in a manner that would link the information disclosed to the individual to whom it pertains... [Exceptions to this rule are listed in the statute.]

Article 7: Accounting For Disclosures

§1798.29. (a) Any agency that owns or licenses computerized data that includes personal information shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement...or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

…

Article 10: Penalties

§1798.55. The intentional violation of any provision of this chapter or any rules or regulations adopted thereunder, by an officer or employee of any agency shall constitute a cause for discipline, including termination of employment.

§1798.56. Any person who willfully requests or obtains any record containing personal information from an agency under false pretenses shall be guilty of a misdemeanor and fined not more that five thousand dollars ($5,000), or imprisoned not more than one year, or both.

TITLE 5, CALIFORNIA CODE OF REGULATIONS

Sections §42396 through §42396.5 of Title 5 of the California Code of Regulations address privacy and the principles of personal information management applicable to the California State University. Title 5 can be found on the Web at: http://ccr.oal.ca.gov/. For reference, the following summary is provided:

§42396.2 Principles of Personal Information Management. The following principles of personal information management shall be implemented within The California State University:

(a) There should be no personal information system the existence of which is secret.

(b) Personal information should not be collected unless the need for it has been clearly established in advance.

(c) Personal information should be appropriate and relevant to the purpose for which it has been collected.

(d) Personal information should not be transferred outside The California State University unless the transfer is compatible with the disclosed purpose for which it was collected.

(e) Personal information should be used as a basis for a decision only when it is accurate and relevant.

(f) There should be procedures established by which a person may learn what personal information about him or her has been retained by The California State University and where lawful, have those records disclosed to him or her, pursuant to the provisions of this Article.

(g) There should be established within The California State University procedures by which a person may request in writing addition to or deletion of personal information about himself or herself which does not meet the principles in this section. Such requests should be honored within a reasonable length of time or the person should be permitted to file a concise statement of dispute regarding the personal information which shall become a permanent part of the record, or, the disputed personal information should be destroyed.

(h) Precautions should be taken to prevent the unauthorized access to or use of personal information retained by The California State University.

These principles shall be construed and implemented so as to be consistent with all federal and state laws otherwise regulating or allowing for the use of personal information, including but not limited to Education Code Section 89546 relating to employee records.