1. **Purpose**
   The Chancellor's Office issued the system Responsible Use Policy on November 1, 2014 (Integrated CSU Administrative Manual policy number 8105.0). This policy adds local provisions to the CSU system policy. Policy defines CSU responsibilities with respect to the use of CSU information assets. Reference CSU policy 8105.0 for the full system policy.

2. **Definitions**
   *DMCA:* Digital Millennium Copyright Act of 1988

   *University:* all CSU Stanislaus Departments, Colleges, Divisions, and Auxiliaries.

   *User:* faculty, staff, students, and third parties.

3. **Scope of Policy**
   This policy applies to all members of the University. This policy addresses the responsible use of CSU information assets.

   The local provisions included in this supplemental policy include guidelines for file sharing and copyrighted materials, technology deterrents, dissemination of information, telephone use, access to confidential information, staff confidentiality agreements, and faculty confidentiality agreements.

   Nothing in this policy shall be construed as limiting by the university a user's ability to use copyrighted material in accordance with the Fair Use statute of the United States Copyright Law (17 U.S.C. § 107). For more information and guidelines related to Fair Use, see: [http://www.calstate.edu/gc/Docs/CopyrightManual.pdf](http://www.calstate.edu/gc/Docs/CopyrightManual.pdf)

4. **Policy**

   **4.1 File Sharing and Copyrighted Material**

   As a university system and creators of intellectual property, the California State University has a significant interest in ensuring that all copyrighted material is protected and that the rights of copyright holders and creators of intellectual property are respected and maintained.

   The Internet is now the preferred medium for dissemination of information resources. Abusive use of otherwise legitimate technologies has fostered a lack of respect for the intellectual property of others. Although peer-to-peer file sharing programs can be used for legitimate purposes, they can also be used to distribute music and video content in violation of the DMCA. The university must act to ensure that the appropriate safeguards and policies are in place to discourage such abusive use.
a. Policy
CSU Chancellor’s Office Executive Order 999 (http://www.calstate.edu/EO/EO-999.html) formally states the university’s policy on illegal electronic file sharing and protection of electronic copyrighted material, including, but not limited to music, videos, motion pictures, and Internet accessible content, consistent with the provisions of the DMCA.
Use of any university resource such as computers (hardware or software), network connections, servers, routers, facsimile machines, copy machines and other electronic equipment by any faculty, student, staff or member of the general public to circumvent legitimate copyright protections or illegally access, copy or disseminate copyrighted material is unauthorized.

b. Procedure
The designated agent to receive DMCA notices of alleged copyright infringement is the campus Chief Information Officer in the Office of Information Technology (OIT).
The process followed by OIT when it receives a DMCA infringement notice is as follows:

- Analyze the provided network address information to determine if the identity of the person involved can be established
- Optionally, temporarily disable the network port of the user and immediately contact the individual to explain the situation
- In the case of students, OIT notifies the Office of Judicial Affairs, which in turn contacts the student. If the alleged infringing recording exists as described in the DMCA notice, the student is requested to remove it
- In the case of a staff or faculty member, OIT notifies the Faculty Affairs and Human Resources office
- Upon verification that the recording has been removed, the network port is reactivated (if necessary)
- Notification of the resolution of the complaint, when requested, is provided to the organization which submitted the infringement notice
- Individuals found to have violated university / CSU policies or Title 5 of the California Code of Regulations may be subject to disciplinary proceedings in accordance with the student Code of Conduct and CSU policy

c. Governing Laws
On September 17, 2004 Governor Schwarzenegger issued State of California Executive Order S-16-04 prohibiting the use of state resources to illegally download copyrighted material.
The DMCA, signed into law on October 28, 1998, includes provisions concerning the circumvention of copyright protection systems, fair use in a digital environment, and online service provider liability
Illegal file-sharing and other copyright violations are a Violation of Title 5 of the California Code of Regulations.
Copyright infringement is the act of exercising, without permission or legal authority, one or more of the exclusive rights granted to the copyright owner under section 106 of the Copyright Act (Title 17 of the United States Code).
The 2008 Higher Education Opportunity Act (HEOA) includes several sections dealing with unauthorized file sharing on campus networks, imposing three general requirements on all U.S. colleges and universities:

- An annual disclosure to students describing copyright law and campus policies related to violating copyright law
- A plan to "effectively combat the unauthorized distribution of copyrighted materials" by users of its network, including "the use of one or more technology-based deterrents"
- A plan to "offer alternatives to illegal downloading"

d. Summary of Civil and Criminal Penalties
Copyright infringement is the act of exercising, without permission or legal authority, one or more of the exclusive rights granted to the copyright owner under section 106 of the Copyright Act (Title 17 of the United States Code). These rights include the right to reproduce or distribute a copyrighted work. In the file-sharing context, downloading or uploading substantial parts of a copyrighted work without authority constitutes an infringement.

Penalties for copyright infringement include civil and criminal penalties. In general, anyone found liable for civil copyright infringement may be ordered to pay either actual damages or "statutory" damages affixed at not less than $750 and not more than $30,000 per work infringed. For "willful" infringement, a court may award up to $150,000 per work infringed. A court can, in its discretion, also assess costs and attorneys' fees. For details, see Title 17, United States Code, Sections 504, 505.

Willful copyright infringement can also result in criminal penalties, including imprisonment of up to five years and fines of up to $250,000 per offense.

For more information, please see the Web site of the U.S. Copyright Office at www.copyright.gov, especially their FAQ's at www.copyright.gov/help/faq.

e. Legal Alternatives to Illegal Downloading
In addition to purchasing music and video content through traditional sources, members of the university community can pursue a wide range of alternative methods to enjoy copyrighted content via the Internet. The university provides ample Internet capacity to support use of the technology for playback of video and audio recordings on network-attached devices located on the campus.

When accessing recordings via the Internet, it is important to recall that free content is not necessarily illegal, just as content that is not free is not necessarily legal.

The Recording Industry Association of America (RIAA) and the Motion Picture Association of America (MPAA) have web sites that list legal alternatives to illegal file sharing sites. See http://www.whymusicmatters.com/ for more information.

f. Technology-based Deterrents
The HEOA regulations provide an institution with a range of options for implementing technology-based deterrents to illegal downloading. Multiple mechanisms are employed by CSU Stanislaus:

- Traffic monitoring to identify the largest bandwidth users
- Use of network segmentation techniques and firewall devices
- Registration of devices used on the network to facilitate compliance with university policies
• A vigorous program of accepting and responding to DMCA notices

g. Dissemination of Information
As required by the HEOA, this policy and relevant additional supporting information will be distributed annually to all students, and additionally to staff and faculty, by electronic mail. It will also be published in the Student Handbook and publications intended for students living in the campus residence halls.

A condition of the Student Housing License Agreement is compliance with the rules and regulations outlined in the Village Network User Agreement which incorporates this policy.

4.2 Telephone Use
Telephone use should be consistent with the provisions of Section 4.5 of the Responsible Use Policy which provides for incidental use of university-owned information assets.

Personal phone calls must not interfere with State business. The number and length of personal calls should be kept to a minimum.

Departments are responsible for paying long distance telephone charges.

4.3 Access to Confidential Information
Each campus and the Chancellor’s Office must take necessary measures to protect confidential personal information, which includes, but is not limited to, social security number, ethnicity, gender, home address, physical description, home telephone number, medical history, and performance evaluations.

To protect confidential personal data, each campus and the Chancellor’s Office must follow the measures outlined below:

• Each campus and the Chancellor’s Office must ensure that all employees with access to confidential personal information have a legitimate CSU need to have such access. These employees must understand the responsibility they have under the Information Practices Act and Title 5 to protect sensitive personal data. Training is to be provided, as required.

• Confidential personal information should not be transmitted outside the CSU unless it is for legitimate CSU purposes. Recipients must be informed that the information provided is confidential and is provided for the sole purpose of the specific business need. Also, recipients must be informed that they are responsible for the protection of the information and the destruction of all files after the intended use is satisfied.

The CSU requirements for protecting confidential personal data include the requirement that employees with access to confidential personal data in computerized information systems sign a data confidentiality agreement acknowledging that the employee understands the requirements for protecting confidential personal data.

a. Staff Confidentiality Agreement

For staff, the following statement applies:

“I certify that I have been given a copy of, and have read and understand, the attached summaries of provisions of the California Information Practices Act of 1977 and Title 5, California Code of Regulations, that govern access to and use of information contained
in employee, applicant, and student records, including but not limited to data that is accessible through CSU Stanislaus computing information systems.

I understand that any access I am granted to this 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 and University 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, whether it relates to my own unit or another unit.

- 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.

- I will make every reasonable effort to interpret the information and data I obtain in an accurate and professional manner.

- 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 CO Human Resource Services 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 certify that I have read this Confidentiality Form, I understand it, and I agree to comply with its terms and conditions."

b. Faculty Confidentiality Agreement

*For faculty, the following statement applies:*
“I certify that I have received training on the appended state and federal laws and University policies that govern access to and use of information contained in employee, applicant, and student records, including data that is accessible through the PeopleSoft Human Resource System.

- I understand that I am being granted access to this information and data based on my agreement to comply with the following terms and conditions:

- I will comply with the state and federal laws and University policies that govern access to and use of information contained in employee, applicant, and student records, including data that is accessible through the Human Resource Information System. While a current summary is attached, state and federal laws may be revised that may necessitate additional training and requirements.

- 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 will maintain the privacy and confidentiality of the information and data that I obtain, including its storage and disposal.

- Before sharing information or data with others, electronically or otherwise, I will make reasonable efforts to ensure that the recipient is authorized to receive that information or data. I will sign off the Human Resource Information System prior to leaving the terminal/PC.

- I will keep my password(s) to myself, and will not disclose them to others unless my immediate supervisor authorizes such disclosure in writing.

I understand that if I intentionally misuse personal information or data that I obtain through my employment, I will be subject to disciplinary action up to and including termination.

I certify that I have read this Access and Compliance Form, I understand it, and I agree to comply with its terms and conditions.”

5. Governing Laws

5.1 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 than five thousand dollars ($5,000), or imprisoned not more than one year, or both.

5.2 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.