

California State University San Bernardino
CONFIDENTIALITY COMPLIANCE FORM
Statement of Confidentiality of Records and Information Systems
Unit 4 Employees

The California State University (CSU) has responsibility to protect sensitive personal data and maintain confidentiality of that data under the Information Practices Act (IPA), Title 5, and FERPA. Personal data includes, but is not limited to, the following data: Social Security Number (SSN), Date of Birth (DOB), home address, home phone number, physical description, medical history, gender and ethnicity. The Office of the Chancellor issued Coded Memorandum ([HR2002-27](#) and [HR2003-5](#)) detailing the CSU's requirements for protecting confidential data. Additionally, the Office of General Counsel for the CSU issues and maintains a Records Access Manual, which provides an overview of federal and state law governing access to records possessed by the CSU.

In light of rapidly changing technology and increased Internet use, this form is written to highlight the importance of CSUSB's responsibility for the confidentiality of personal information. The Information Practices Act, California Civil Code Section 1798, et seq. protects individuals' privacy rights in "personal information" contained in state agency records. Additionally, Sections 42396 through 42396.5 of Title 5 of the California Code of Regulations address privacy and the principles of personnel information management. The Family Educational Rights and Privacy Act of 1974 (FERPA) affords student certain rights with respect to their education record. One of which is the right to consent to the disclosure of personally identifiable information except to the extent that FERPA authorizes disclosure without consent. CSUSB's Records, Registration, and Evaluations Office provide campus guidelines for complying with FERPA. Furthermore, CSUSB's Acceptable Use Policy for Electronic Communications provides general principles regarding respect for privacy and sharing of account passwords. Further information on these state and federal laws as well as CSUSB's policies, can be obtained at the following web site locations:

- Information Practices Act of 1977
<http://www.privacy.ca.gov/code/ipa.htm>
- California Code of Regulations-Title V
<http://ccr.oal.ca.gov>
- Family Educational Rights and Privacy Act (FERPA)
<http://www.ed.gov/offices/OM/fpco/ferpa/>
- Requirements for Protecting Confidential Employee Data: Updated to Reflect Faculty Unit Confidentiality Agreement Requirement
<http://www.calstate.edu/HRAAdm/pdf2004/HR2004-08.pdf>.
- CSU Coded Memorandum HR2002-27 – Requirements for Protecting Confidential Data
<http://www.calstate.edu/HRAAdm/pdf2002/HR2002-27.pdf>
- CSU Coded Memorandum HR2003-5 – Req. for Protecting Confidential Data - Updated
<http://www.calstate.edu/HRAAdm/pdf2003/HR2003-05.pdf>
- CSU Records Access Manual (February 2003)
http://www.calstate.edu/Gc/Docs/Records_Access_Manual.doc
- Policy and Procedures for Student Records Administration
http://policies.csusb.edu/student_records_administration.htm
- Acceptable Use Policy for Electronic Communications
<http://policies.csusb.edu/eleccomm.htm>

INFORMATION PRACTICES ACT OF 1977

To ensure employees understanding of the Information Privacy Act (IPA) and to prevent inappropriate disclosure of information, the University had provided a summary of key components below.

A. General Provisions and Legislative Findings

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. All individuals have a right of privacy in information pertaining to them. The California's Legislature has found that:

1. 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.
2. 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.
3. In order to protect the privacy of individuals, it is necessary that the maintenance and dissemination of personal information be subject to strict limits.

B. Definitions

1. The term "personal information" means any information maintained by the campus 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.
2. 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.

C. Penalties

1. "The intentional violation of any provision of this chapter or any rules or regulations adopted there under by an employee of any campus shall constitute a cause for discipline, including termination of employment."
2. Any person who willfully requests or obtains any record containing personal information from a campus under false pretenses shall be guilty of a misdemeanor or fined not more than five thousand dollars (\$5,000), or imprisoned not more than one year, or both.

**INFORMATION ON PAGES 1 & 2 SHOULD BE KEPT BY THE EMPLOYEE
FOR FUTURE REFERENCE.**

California State University San Bernardino
CONFIDENTIALITY COMPLIANCE FORM
Unit 4 Employees

EMPLOYEE NAME

I certify that I have received the appended state and federal laws and University policies (list also attached) that govern access to and use of information contained in employee, applicant, and student records, including data that is accessible through the Management Information 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 Management Information System. While copies of current state and federal laws are attached, these laws may be revised necessitating 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 storing and disposing of the information so it remains confidential.
- I will secure access to confidential/sensitive data by taking appropriate actions, which may include, but are not limited to, locking the data in cabinets, locking my office, signing off the system when not actively using it, not leaving data open on the computer screen or my desk, etc.
- 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 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 the normal and reasonable duties of my position require compliance with the above.

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

Name (please print)

Signature

Date

Title