

California State University, Long Beach
Confidentiality of Human Resource Records and Information Requirements

The California State University (CSU) has responsibility to protect sensitive employee data and maintain confidentiality of that data under the Information Practices Act (IPA) and Title 5. The Information Practices Act, California Civil Code Section 1798, et seq. requires the campus to collect, use, maintain and disseminate information relating to individuals in accordance with its provisions. Additionally, Sections 42396 through 42396.5 of Title 5 of the California Code of Regulations address privacy and the principles of personnel information management. Summaries of the IPA and Section 42396.2 of Title 5 are provided in Attachments A and B of this document, respectively. Attachment C contains Education Code Section 89546 relating to employee records.

INTRODUCTION

Pursuant to CSU HR Technical letter HR 2003-05 issued March 13, 2003, the campus must take necessary measures to protect confidential employee 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 information, the following measures must be followed:

1. *The campus must ensure that all employees with access to confidential 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 employee data.*
2. *Confidential employee 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 employee data include the requirement that employees with access to confidential employee data in PeopleSoft or any other computerized information system sign a confidentiality agreement acknowledging that the employee understands requirements for protecting confidential employee data.

ACCESS TO EMPLOYEE RECORDS

This section establishes campus procedures to be followed when requests for access involve records concerning University employees/applicants. All requests for employment verification should be referred to *Payroll and Benefit Services* at extension 5-4164. All requests for faculty employee and/or faculty applicant information shall be forwarded to the *Associate Vice President for Academic Personnel*. All requests for staff employee and/or staff applicant information shall be forwarded to the *Director of Staff Personnel Services*. If the format of the request is a report or Excel file, a special form

has been developed to formalize your request. The HR Report Authorization form is found on the campus website: http://www.csulb.edu/divisions/af/cms/end_user/HR/forms/index.html If you have questions about completing the form, please contact the HR Coordinator at 5-8716, or the Director of HR Technical Resources at 5-5365.

REQUIREMENTS FOR HANDLING CONFIDENTIAL EMPLOYEE/APPLICANT INFORMATION

Due to the need to safeguard the privacy of individuals, efforts must be made to prevent the inadvertent release of information that would constitute an unwarranted invasion of personal privacy. University managers/supervisors must establish procedures that will assure that the confidential information is available only to those persons whose work requires access to such information. This information is not to be released to anyone other than users whose University duties require access. The only exceptions are by written permission of the employee whose information is being requested or pursuant to a valid subpoena or other court order. Reasonable precautions must be taken to prevent unauthorized persons from casually observing confidential information in work areas during normal business hours. The information must then be returned to locked files during non-business hours.

PROCEDURES FOR DISCLOSING REQUIRED INFORMATION CONCERNING EMPLOYEES

When the requested information concerns an employee/applicant and when disclosure is determined to be required by the Associate Vice President for Academic Personnel or the Director of Staff Personnel Services, they will be responsible for compiling and providing the information to the requestor. Current CSU policy requires the Associate Vice President for Academic Personnel and the Director of Staff Personnel Services to FAX the request (often a subpoena for *employee* records) to the CSU Office of General Counsel for prior approval to release the requested information.

It should be noted that the California Public Records Act, Government Code, Section 625 makes certain employment information a matter of public record. In disclosing the information listed in the next section (**EMPLOYEE INFORMATION FOR DISCLOSURE/PROTECTION**), any personal items such as home address and/or home phone number, Social Security number, etc., should be deleted before disclosure is made.

When requests are received concerning general classes or categories of employee, e.g., a listing of all academic employees, these requests must be referred to the Associate Vice President for Academic Personnel or the Director of Staff Personnel Services.

EMPLOYEE INFORMATION FOR DISCLOSURE/PROTECTION

EMPLOYEE INFORMATION THAT MAY BE DISCLOSED

The following information concerning CSU employees is a matter of public record and must be made available in response to any bona fide request:

- Name
- Department (Organizational Unit)
- Funding Source
- (Attendance) Unit
- County of employment
- Gross Salary
- Frequency of Pay
- Pay Rate
- Time worked
- Shift differential eligibility based on work assignments (but not actual payroll details)
- Pay period
- Job classification/range
- Time base/FTE
- Retirement system
- Job description, duties and responsibilities
- Dates of appointment and separation

EMPLOYEE INFORMATION THAT MUST NOT BE DISCLOSED

The following information is identified as personal or confidential and is not subject to mandatory public disclosure. If the information requested is not listed here it shall be considered *confidential* and not subject to disclosure.

- Social Security number
- Number of tax exemptions
- Amount of taxes withheld
- Amount of OASDI withheld
- Marital status
- All voluntary/involuntary deduction/reductions (amount and types)
- Survivor's amounts
- Net pay of an employee
- Home address
- Home telephone number
- Birth Date
- Ethnic data
- Designee for last payroll warrant
- Gender data
- Veteran status
- Performance evaluations
- Education
- Disciplines
- Financial matters
- Medical history
- Employment history

HR CONFIDENTIALITY/SECURITY AGREEMENT

In addition to completing an HR System Access form, all employees that wish to receive a CMS-PeopleSoft HRSA system log in/user ID/account will be required to sign an HR Confidentiality Form. As appropriate, other employees may also be required to sign the HR Confidentiality Form before HR data can be released. Everyone utilizing/accessing the CMS-PeopleSoft HRSA system and HR data shares the responsibility for the security, integrity and confidentiality of information. A copy of the signed HR Confidentiality Form will be retained in the individual's official personnel file.

STORAGE AND DISPOSAL OF CONFIDENTIAL INFORMATION

Employees should use caution in storing or disposing of confidential information. This includes shredding any paper that contains information described herein as personal or confidential. In addition, any personal or confidential data contained on computer media must be erased before disposing of the tape, diskette, CD-ROM, zip disk, or other type of medium. Questions regarding storage or disposal of faculty employee and/or faculty applicant confidential information should be directed to the Associate Vice President for Academic Personnel. For staff employee and /or staff applicant confidential information, questions should be directed to the Director of Staff Personnel Services.

Attachment A – Summary Information Practices Act of 1977

To view the entire code: <http://www.leginfo.ca.gov/calaw.html> (Select Civil Code/check box and then go to the bottom of the page and search for Section 1798 and or applicable subsections.)

As outlined in CSU Human Resources technical letters labeled as HR/PR 93-01 and Supplement 1, each campus has the legal responsibility to administer and comply with provisions of the Information Practices Act (IPA.) These documents are available at Human Resources Administration Web page at <http://www.calstate.edu/HRAdm/policies.shtml>. Additionally, the IPA is contained in Sections 1798 – 1798.78, of the California Civil Code. 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 (Section 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

Section 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 to 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

Section 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.*
- b) ...*
- 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

Section 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.

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

Section 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 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.

Section 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.

Section 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

Section 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 10: Penalties

Section 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.

Section 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.

Attachment B – California Code of Regulations

Sections 42396 through 42396.5 of Title 3 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:

Section 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 of 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 of 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 user of personal

information, including but not limited to Education Code Section 89546. See Attachment C.

Attachment C – Education Code Section 89546 relating to employee records.

89546. (a) Every employee of a state university or college shall have the right to access to all reports, documents, correspondence, and other material which pertain to the employee which are kept by the university or college. Each employee shall also have the right to have another person of the employee's choosing accompany the employee to inspect the employee's records.

(b) Upon written request, the employee shall, within 10 calendar days of the request, be provided an exact copy of all or any portion the employee desires of any of the items specified in subdivision (a). The employee shall bear the cost of duplicating such items.

(c) If, after examination of the records pertaining to the employee, an employee believes that any portion of the material is not accurate, relevant, timely, or complete, the employee may request in writing correction of the record or deletion of the offending portion, or both. Such request shall include a written statement by the employee as to the corrections and deletions that the employee believes need to be made and the reasons therefor. This statement shall become part of the employee's personnel file.

(d) Within 21 calendar days of the request for correction of the record or deletion of the portion of the record objected to, or both, the president of the state university or college shall either accede to the employee's request or notify the employee in writing of the president's refusal to grant the request. If the president refuses to grant the request, the president shall state the reasons for the refusal in writing, and the written statement shall become part of the employee's personnel file.

(e) The remedies authorized by this section shall be in addition to any other remedy provided by law.

(f) Personnel recommendations or decisions relating to the promotion, retention, termination, or any other personnel action shall be based primarily on material contained in the employee's personnel file and open to the employee's inspection. If a personnel recommendation or decision is based on any reasons not contained in the employee's personnel file, the party making the recommendation or decision shall commit those reasons to writing, and the written statement of those reasons shall become part of the employee's personnel file.

(g) Preemployment materials shall be excluded from the requirements of this section, except as they may be considered in subsequent personnel actions.

(h) If the provisions of this section are in conflict with the provisions of a memorandum of understanding reached pursuant to Chapter 12 (commencing with Section 3560) of Division 4 of Title 1 of the Government Code, the memorandum of understanding shall be controlling without further legislative action, except that if such provisions of a memorandum of understanding require the expenditure of funds, the provisions shall not become effective unless approved by the Legislature in the annual Budget Act.

