THE CALIFORNIA STATE UNIVERSITY
Office of the Chancellor
401 Golden Shore
Long Beach, CA 90802-4210
(562) 951-4411

Date: April 8, 2005 **Code: HR 2005-16**

Reference: HR 2005-01

To: CSU Presidents

Supersedes: HR 2004-08

From: Jackie R. McClain
Vice Chancellor
Human Resources

Subject: **Requirements for Protecting Confidential Personal Data: Updated to Include Information Practices Act Web Site and Security Breach Disclosure Requirements**

The California State University (CSU) has responsibility to protect sensitive personal data and maintain confidentiality of that data under the Information Practices Act (IPA) and Title 5. In light of rapidly changing technology and increased Internet use, this memorandum is written to highlight the importance of the CSU's responsibility. The Information Practices Act, California Civil Code §1798, et seq., requires the Chancellor's Office and campuses to collect, use, maintain, and disseminate information relating to individuals in accordance with its provisions. Additionally, §42396 through §42396.5 of Title 5 of the California Code of Regulations address privacy and the principles of personnel information management. For campus reference, summaries of the IPA and §42396.2 of Title 5 are provided in Attachments A and B, respectively. Additional documents on protecting confidential data are available at Human Resources' Policy Web site at http://www.calstate.edu/HRAdm/policies.shtml (under Confidentiality/Protection of Personal Data).

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.

The CSU is obligated under IPA to disclose any breach of system security to California residents whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. General Counsel's Records Access Manual located at http://www.calstate.edu/gc/Docs/Records_Access_Manual.doc addresses the IPA disclosure requirements.

Distribution:

Executive Vice Chancellors
General Counsel
Vice Presidents, Administration
Vice Presidents, Academic Affairs
Vice Presidents, Student Affairs
Vice Presidents, Information Technology
Asst. Vice Chancellor, Information Technology
Information Technology Advisory Committee
Associate Vice Presidents/Deans of Faculty Affairs
Human Resources Directors
Benefits Officers
Payroll Managers
CMS Executive Director

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

1. 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.

2. 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 the CMS baseline system or any other computerized information system sign a data confidentiality agreement acknowledging that the employee understands requirements for protecting confidential personal data. A sample form for non-faculty employees is included for reference in Attachment C. Campuses may use an existing campus form or a revised campus form, consistent with existing campus policies and forms, to meet this confidentiality agreement requirement.

As a result of the Agreement between the California Faculty Association (CFA) and the CSU, campuses must use the Human Resources Information System Access and Compliance Faculty confidentiality form provided in Attachment D when faculty (Unit 3) employees are required to sign a form dealing with the confidentiality of campus records. **The faculty employee portion of the form cannot be modified.** The MPP Administrator section can be altered. Campuses do not need to have faculty employees sign new forms if they previously signed a similar confidentiality agreement with their respective campus.

For information on the required technical security measures for each campus and the Chancellor's Office, refer to the CSU Information Technology Security Policy issued by Executive Vice Chancellor and Chief Financial Officer West on September 13, 2002. The policy is posted at:

http://its.calstate.edu/systemwide_it_advisory/ITAC_keydocuments/IT_Security_Policy_092002.doc.

Questions regarding the faculty confidentiality form should be directed to Academic Human Resources at (562) 951-4503. Questions regarding a campus' technical requirements should be directed to the campus Chief Information Officer and/or Information Technology Advisory Committee (ITAC) Designee, as appropriate. Other questions can be directed to Human Resources at (562) 951-4411 or campus counsel, as appropriate. This HR Letter is available on the Web at: http://www.calstate.edu/HRAdm/memos.shtml.

JRMcC/gc

Attachments

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.

HUMAN RESOURCE INFORMATION SYSTEM ACCESS AND COMPLIANCE FORM

MPP ADMINISTRATOR

My signature below certifies that _____, an employee under my supervision, requires access to data in the Human Resource Information System because such data is relevant and necessary in the ordinary course of performing his/her job duties as a _____ (job title) in the _____ _____ (unit) at California State University, _____. I understand my obligation to provide training to this employee to ensure that he/she understands 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.

_____	_____	_____
Name (please print)	Signature	Date

_____
Title

EMPLOYEE

I certify that I have received training regarding 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 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.
- 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 the Human Resource Information System when I am not actively using it.
- 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 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 understand that if I 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.

_____	_____	_____
Name (please print)	Signature	Date

_____
Title

HUMAN RESOURCE INFORMATION SYSTEM ACCESS AND COMPLIANCE FORM

FACULTY

MPP ADMINISTRATOR:

My signature below certifies that _____, an employee under my supervision, requires access to data in the Human Resource Information System because such data is relevant and necessary in the ordinary course of performing his/her job duties as a _____ (job title) in the _____ _____ (unit) at California State University, _____. I understand my obligation to provide training to this employee to ensure that he/she understands 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.

_____	_____	_____
Name (please print)	Signature	Date

_____
Title

FACULTY EMPLOYEE:

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.

_____	_____	_____
Name (please print)	Signature	Date

_____
Title