Date: Thu, 29 Apr 2004 11:42:20 -0700
To: sfsu_admins_and_chairs@sfsu.edu
From: "Robert A. Corrigan" <president@sfsu.edu>
Subject: San Francisco State University Confidentiality and Information Security Plan (UED #04-32)
Sender: owner-sfsu_admins_and_chairs@sfsu.edu

In March 2004, the President's Cabinet reviewed and approved a comprehensive *Confidentiality and Information Security Plan* (CISP) for San Francisco State University. This plan is the culmination of almost seven months of intensive committee work under the leadership of Co-Chairs Richard Giardina and Suzanne Dmytrenko. The committee's charge, provided by Vice President Leroy M. Morishita, was to formulate a campus CIS policy and implementation plan which would ensure full compliance with federal, state and CSU requirements for information security.

I hereby issue the SFSU *Confidentiality and Information Security Plan* as University Executive Directive (UED) #04-32, effective immediately.

Briefly, the SFSU *Confidentiality and Information Security Plan* establishes appropriate and reasonable administrative, technical, and physical safeguards designed to:

- Ensure the security and protection of confidential information in the University's custody, whether in electronic, paper, or other forms
- Protect against any threats or hazards to the security or integrity of such confidential information
- Protect against unauthorized access to or use of such confidential information.

It is important to note that maintenance of information confidentiality and security is a serious concern and will require full and active participation of the entire campus community - by all University employees and at all administrative levels. Please review this plan carefully in order to fulfill your campus responsibilities in securing and protecting confidential information.

Overall administration of this CISP is delegated by me to the Vice President for Administration & Finance as *Chief Administrator*. As *Custodians of Record*, the Associate Vice President for Human Resources, Safety & Risk Management, the Associate Vice President for Fiscal Affairs, and the University Registrar, within their areas of supervision, will be responsible for the campus implementation, definition and training required by this plan.

San Francisco State University *Confidentiality and Information Security Plan*

Prepared for the
Vice President for Administration and Finance
By the Confidentiality and Information Security Committee
February 2004, Revised June 2006

Richard Giardina, Associate Vice President, Academic Planning & Assessment; Co-Chair
Suzanne Dmytrenko, University Registrar; Co-Chair
Ron Beall, Associate Dean, College of Business
Paul Beckman, Information Security Officer, Associate Professor Information Systems
Caran Colvin, Vice Chair, Academic Senate, Professor Psychology
Denise Fox, Associate Vice President for Human Resources, Safety & Risk Management
Chess Kittredge, Director, Strategic Technology Architecture, Division of Information Technology
Phoebe Kwan, Executive Director, Division of Information Technology
Robert Maples, Director, Student Systems Support & Development
Willie Mullins, Clinical Director, Counseling Center
Laureen O'Brien, Executive Assistant to the Vice President, University Advancement
Jonathan Rood, Associate Vice President, Division of Information Technology
Donna Ryan, Manager, Employment/Compensation, Human Resources, Safety & Risk Management
Jo Volkert, Associate Vice President, Enrollment Planning & Management
Larry Ware, Associate Vice President for Fiscal Affairs & Controller
Cora Wong, Director, Student Financial Operations & Business Systems/Bursar
Bea Yorker, Director, School of Nursing

TABLE OF CONTENTS

San Francisco State University
Confidentiality & Information Security Plan

The SFSU *Confidentiality and Information Security Plan* establishes appropriate and reasonable administrative, technical, and physical safeguards designed to:

- Ensure the security and protection of confidential information in the University's custody, whether in electronic, paper, or other forms
- Protect against any threats or hazards to the security or integrity of such confidential information
- Protect against unauthorized access to or use of such confidential information. (See Appendix A for definitions used in this document.)

The SFSU *Confidentiality and Information Security Plan* complies with CSU requirements for information security and the requirements of federal and state laws and regulations identified in Appendix B**.**

Purpose

The purpose of this Plan is to enhance the management of personal information to prevent loss of privacy and/or financial damage. Colleges and departments should follow this Plan to reduce to a minimum the collection, distribution, and retention of personally-identifying electronic and printed data. Practices should embrace the following principles:

- Collect and retain only data essential to the performance of the assigned tasks
- Delete personal data in a secure manner when no longer needed or required
- Provide staff access to sensitive data only as needed to perform assigned duties
- Design computer and manual systems so that data considered confidential may be identified and controlled
- When confidential and personally-identifying information is distributed to any users, include notification of the rights and responsibilities of data users and data providers
- Restrict personal and confidential data not critical to the task when distributing full data sets to users
- Whenever possible, configure electronic applications that check authorizing or authenticating databases to return confirming responses rather than personal or confidential data
- Review and update agreements with external service providers to ensure compliance with federal and state legislation and CSU and SFSU policy
- Have procedures in the event that notification is required to individuals whose personal or confidential data, retained on computer systems, have been compromised
- Develop mechanisms to ensure that confidential information is not left exposed or unattended on computer screens or on paper for unauthorized viewing

Scope

This Plan covers electronic and paper-based data defined as confidential in Appendix A. This includes all information maintained, processed, or distributed by SFSU on primary computer systems or any subsidiary systems that contain data defined by law or policy as confidential. This includes, but is not limited to, SFSU mainframe data bases and subsidiary systems within the following areas: Academic Affairs, Administration and Finance, Advancement, Student Affairs, and the officially

recognized auxiliary and affiliate organizations: SFSU Foundation, Student Center, Franciscan Shops Bookstore, Associated Students and Alumni Association. This Plan also applies to all faculty, staff, administrators, students, consultants, and any person or agency employed or contracted by SFSU or any of its auxiliary organizations who have a legitimate need to have access to SFSU confidential information as part of their required job responsibilities.

The unauthorized addition, modification, deletion, or disclosure of confidential information included in SFSU data files and data systems can compromise the integrity of SFSU programs and violate individual privacy rights and is expressly forbidden. In certain limited circumstances, as specified in federal and state legislation, SFSU may disclose confidential information. Refer to the *CSU Records Access Manual*. See Appendix B for web site.

Where provisions of this Plan are in conflict with the Collective Bargaining Agreements reached pursuant to Chapter 12 (commencing with Section 3560) of Division I of the Government code, the Collective Bargaining Agreements shall take precedence.

The Plan does not address the policy and procedures for protecting the privacy of SFSU student education records. The regulations and procedures governing SFSU student education records are covered in *SFSU Procedures on Management of Student Records*. See Appendix B for web site.

Roles and Responsibilities

*Chief Administrato*r – This individual is the Vice President for Administration and Finance, delegated by the President with responsibility for the overall administration of the SFSU *Confidentiality and Information Security Plan.* To effectively implement and administer the Plan, the Vice President for Administration and Finance has designated the management of confidential information as follows:

Custodians of Records – These individuals are the Associate Vice President for Human Resources, Safety & Risk Management, the Associate Vice President for Fiscal Affairs, and the University Registrar. Within their areas of supervision, they will:

- Implement and administer the Plan in order to protect the privacy rights of University faculty, staff, and students and to comply with legal and policy requirements
- Protect confidentiality and security of electronic and paper data maintained in their area
- Define functions and staff authorized to access confidential data and approve authorization (see Appendix C)
- Ensure that all employees receive employee/student confidentiality training as directed by the Associate Vice President for Human Resources, Safety & Risk Management and the University Registrar. The primary method will be to develop, implement, and maintain a web-based employee/student confidential tutorial
- Develop and implement appropriate campus-wide, electronic mechanisms to ensure that all employees comply with the required training
- Provide appropriate confidentiality training for employees with authorized access to confidential financial data as designated by the Associate Vice President for Fiscal Affairs
- Develop, implement, and communicate the expectations and means for the safeguarding of confidential information to appropriate persons and organizations
- Ensure that risk assessments are conducted when necessary or recommended by the Internal

Auditor
- Maintain appropriate and timely documentation for employees with access to confidential data
- Report to the Vice President for Administration and Finance on the status of the Plan bi annually
- Provide recommendations for revisions to this Plan as appropriate.

Administrators/College Deans- These individuals, including managers of campus auxiliary organizations, shall be responsible for oversight of their employees authorized to handle confidential information in their areas of supervision. They will:
- Ensure that the management and control of risks outlined in the Plan are adhered to by employees in their unit
- Grant permission to their employees to the appropriate level of access to confidential data
- Provide their employees with resources and methods for the security of the equipment or repository where confidential information is processed, stored, or handled.

Employees, including department chairs, faculty, staff, and student workers – These individuals:
- Shall not disclose confidential information to unauthorized individuals
- Shall not modify or delete confidential information unless authorized to do so
- Shall maintain confidential data in a secure manner
- Shall complete the employee/student confidentiality training
- Shall be required to certify that confidential data they have received will be maintained in a secure manner and will not be shared with unauthorized users
- In addition, all employees with job related responsibilities that require access to confidential financial information must complete specific confidentiality training as designated by the Associate Vice President for Fiscal Affairs.

Data Security Manager - This individual, the Associate Vice President for Information Technology, will:
- Develop plans and procedures to preserve confidential information in the event of natural or man-made disasters
- Implement adequate security measures for computing systems containing protected data within his/her jurisdiction
- Implement appropriate security strategies for both the transmission and the storage of protected data
- Notify appropriate units of possible security infringements
- Report any security breach as outlined in the Plan
- Disseminate guidelines related to security to departmental data managers.

Information Security Officer – This individual, appointed by the Vice President for Administration and Finance, will:
- Provide oversight of confidential information in the custody of the University
- Provide oversight of security of the equipment or repository where the information is processed and/or maintained
- Promote and encourage good security procedures and practices

- Provide oversight of plans and procedures to preserve the information in case of natural or man-made disasters.

Internal Auditor -This individual will:

- Assist the campus in identifying reasonably foreseeable internal and external risks to the security and confidentiality of information
- Evaluate the effectiveness of the current safeguards for controlling these risks
- Provide recommendations for revisions to this Plan as appropriate
- Develop and perform random audits of departments and individuals as deemed necessary.

Management and Control of Risks

The University has developed the following general policies and practices necessary to reasonably safeguard confidential information:

Collection
Confidential information shall not be collected unless it is appropriate and relevant to the purpose for which it will be collected. It must be collected, to the extent practicable, from the individual directly and not from other sources. Where information is obtained from other sources, a record must be maintained of those sources.

Access
No employee of the University or any of its auxiliaries shall be granted access to centralized computer systems containing confidential information in the custody of SFSU without the review and written approval of the Vice President for Administration and Finance ~~or his/her designee~~. No SFSU or auxiliary organization employee shall be granted access to non-centralized data files or data systems containing confidential information without the review and written approval by the appropriate Custodian of Records. Such approval will only be granted in cases where the access is required for the employee to perform a critical university or auxiliary function that is part of the employee's job duties. SFSU employees or auxiliary organization employees who currently have such access to information are subject to this review and written approval process in order to continue their access capability.

Employees approved for security access to electronic systems with confidential data shall receive training and complete any forms as established by the appropriate Custodian of Records. Additional training may be required when determined as necessary by the Custodian of Records.

Employees with approved access to electronic information will be assigned a secured computer account and must comply with the terms defined by the appropriate Custodian of Records. Accounts will be deactivated upon the separation or transfer of the employee or when use is no longer necessary or approved.

For authorized extracts of confidential student data, requestors shall complete the *Authorization to Access Confidential Employee/Student Information Agreement Form*, located in Appendix C, and be instructed on the appropriate use and disposal of confidential data.

Software should be designed or installed, where feasible, to prevent data from being accessed by

unauthorized persons. This can include, but is not limited to, screen savers, timeouts for idleness, and password protection on applications housing confidential data.

Unauthorized Access
Any person who knowingly accesses and, without permission, alters, damages, adds, deletes, destroys, or otherwise uses any data, computer, computer system, or computer network in order to either devise or execute any scheme or artifice to defraud, deceive, extort, or wrongfully control or obtain money, property, or data is subject to campus sanctions and penalties defined by law. See Penalties section below.

The goal of the University is to assign each authorized user his/her own account to access confidential data. It is recognized that unauthorized employees may be assigned tasks that involve viewing and working with confidential data. In these circumstances, it is the responsibility of the employee's supervisor for any breaches of confidential data.

Physical Security of Records
The appropriate level of physical security must be followed in order to protect confidential records and data. The following guidelines give examples of common practices that will ensure good business practices for the security of SFSU confidential data:

Department Guidelines - Areas where confidential information is processed and/or stored, and areas housing utilities or service facilities supporting university information equipment, including air conditioning, telephone terminal, and electrical distribution rooms, should be designated as secure areas. In addition, the following practices should be ensured:

- Access to secure areas should be authorized and controlled
- Access control methods should be provided for all secure areas, e.g., locked doors with keypad or card swipe mechanisms or staffed reception areas
- Provision should be made for prohibiting unauthorized access to secure areas when the area is unattended and unoccupied
- Unauthorized personnel and visitors who require access to secure areas should be escorted by authorized personnel at all times
- Signs indicating "Authorized Personnel Only" or a similar message should be prominently posted at all entrances to secure areas
- Surveillance methods should be installed in all secure areas as funding becomes available
- Control logs should be kept of access to secure areas for visitors, external maintenance and support personnel, and authorized personnel outside of normal business hours or assigned hours of work. Access control logs should record the following information:
    - Identification of the person entering
    - Employer or affiliation
    - Reason for access
    - Identification of the individual authorizing entry
    - Secure area to be entered
    - Date and time of entry
    - Date and time of departure

Individual Guidelines - All confidential information on any personal computer or storage device, e.g., microfilm/fiche, hard drive, backup floppy disk, email, optical, or paper, must be protected by the appropriate level of physical security. Confidential information held in electronic form with suitable

backups is less vulnerable to loss than a paper copy. Employees should follow these guidelines whenever possible:

- Protect the system from unauthorized use, loss, or damage, e.g., lock doors when out of the office
- Take measures to guard access from ground floor windows
- Keep portable equipment secure, e.g., do not leave equipment in a car
- Position monitors and printers so that others cannot see confidential or sensitive data
- Install screen savers
- Keep external storage media such as zip disks, tapes, floppy drives, USB drives in a secure place
- Seek advice on disposing of equipment and data
- Report any loss to the appropriate person
- Take particular care at home to keep the system and sensitive data secure from other persons
- Take care not to spill food or drinks over the equipment
- Get appropriate authorization before taking University equipment off-site
- Log out, shut down, or lock the system when leaving the office
- Turn power off overnight
- Ensure that confidential, sensitive, or personal data are deleted from internal disks prior to disposal or transfer of desktop equipment.

Record Retention

A significant risk to the security and integrity of confidential information may occur when records are retained beyond the requirements noted in the CSU Records Disposition Schedule. (See Appendix B for web site.) Unless longer retention is specifically approved, records containing confidential information shall be destroyed within 3 months following the required period of retention. The appropriate Custodian of Records is responsible for ensuring that records are retained for the length of time specified in legislation and CSU policies. Confidential data may be stored in remote campus locations or off campus in State Archive facilities. Periodic inspections to ensure record security should be conducted by the appropriate Custodian of Records.

Record Destruction

All electronic and printed material containing confidential information shall be destroyed when retention is no longer necessary. Confidential information should be destroyed in an appropriate manner, e.g., confidential shredding. Confidential information awaiting destruction must be stored in a secure manner, e.g., locked shredding bin. Campus officials should ensure shredding bins and access to other methods to dispose of confidential information are available to employees.

Service Provider Requirements
Due to the specialized expertise needed to design, implement, and service new technologies, service providers may be needed to provide resources that the University is unable to provide on its own. Other service providers may be needed to assist in the disposal of hard-copy, confidential information that is generated by the University. In recognition of its responsibility for the performance and actions of these independent contractors, the University shall undertake the following actions with respect to contracts with entities that, by nature of the services provided, have or may have access to confidential information:

Due Diligence in regard to Service Providers – The adequacy of the service provider's system of safeguarding information shall be assessed prior to the University entering into a contractual relationship with the service provider. The University shall contractually engage only those service providers who can demonstrate that they have a sufficient system to safeguard confidential information. The providers shall demonstrate or provide assurances that entities to which they subcontract portions of the services shall also have systems to safeguard information. Depending on the nature of the services, the University may elect to review the service provider's audits; summaries of its test results for security; internal and external evaluations of its security systems; and methods for ensuring subcontractor protection of confidential information.

Service Provider Agreements – All contracts with providers whose services are covered by this policy shall include a privacy clause requiring the contractor to certify that the contractor and all its subcontractors have in place appropriate measures to safeguard confidential information, and that the contractor and all its subcontractors shall refrain from sharing any such information with any other party. As of the effective date of this policy, no contract subject to the provisions herein shall be executed or extension option exercised unless the contract complies with this policy.

Contract Insurance and Risk Transfer Requirements – All contracts and agreements with providers whose services are covered under this policy shall include insurance and risk transfer provisions as prescribed in current Chancellor's Office Executive Orders. Furthermore, the provisions shall include, as appropriate, requirements that service providers be bonded and maintain adequate personal injury and other insurance coverage, in order to protect against allegations of violations of privacy rights of individuals as a result of improper or insufficient care on the part of service providers.

Training

All SFSU and auxiliary organization employees will receive employee/student confidentiality training as directed by the Associate Vice President for Human Resources, Safety & Risk Management and the University Registrar when feasible and deemed necessary. The appropriate Custodian of Records will provide training for employees approved for additional security access to employee, student, and/or financial confidential data. Training shall include controls and procedures to prevent employees from providing confidential information to an unauthorized individual or entity and how to properly handle, store, and dispose of documents that contain personal identifying information. Training shall also include information to protect against destruction, loss, or damage to confidential information from potential environmental hazards such as fire, water, acts of nature, or technological failures. Custodians of Records shall document employees who have received training. Information on the University's *Confidentiality and Information Security Plan* shall be

presented at New Employee Orientation for staff, Management Orientation sessions for administrators, and New Faculty Orientation for faculty. Additional training methods include:

- Web and email instructions to employees on a periodic basis, reference cards, posters for department offices, in-person training for new and current employees
- Web site with the Plan, FAQ, web tutorial, and alerts when any changes occur
- Meetings with relevant College groups and councils, administrators, and new and continuing faculty and staff to publicize the Plan and address any questions or concerns
- Special training for office coordinators who will have to train and monitor student assistants
- On an annual basis, reminders to employees of the confidentiality guidelines outlined in the Plan.

Compliance

The Associate Vice President for Human Resources, Safety & Risk Management and the University Registrar shall develop comprehensive mechanisms for employee/student confidentiality training. These shall include, but are not limited to, the development, implementation, and maintenance of a web-based tutorial. They will also develop mechanisms for ensuring campus-wide electronic or other methods for compliance with the requirements of confidentiality training.

Security of Administrative Systems

The Division of Information Technology (DoIT) *Security Guide* identifies the policies and practices specific to safeguarding of information operated and maintained by DoIT. The Plan is updated regularly to reflect changes in practices and procedures. See Appendix B for web site.

It is the responsibility of DoIT to ensure the physical security of computer-stored information on centralized computer systems, including but not limited to delivery of output, disposal of waste material, and on-site access as required by the appropriate Custodian of Records. DoIT is also responsible for providing the means of controlling access to the confidential information by remote access and programs as required by the Custodian of Records.

Administrative control of the access to and use of computer-stored information on the centralized computer systems is the responsibility of DoIT. Any authorized user who collects or receives and maintains confidential information is responsible for the security of the data in his/her keeping. All confidential files shall have access restricted by the appropriate Custodian of Records through appropriate passwords or other similar means. The Custodian of Records of confidential data must also establish and periodically disseminate the rules of access.

Required Disclosure of Security Breach

The University is required 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.

Incident Response Process
Unencrypted confidential data, whether stored on a centralized or a non-centralized computer system, or data stored on a computer system which is transferred to a hardcopy format (computer print out, microfilm/fiche, or disk/tape media), are subject to the Incident Response Process. If the Data Security Manager (the Associate Vice President for Information Technology) is informed that there has been a security breach of data acquired or divulged in an unauthorized manner, he/she shall immediately:

- Block access to the affected computing system
- Notify the appropriate Custodian of Records, Administrator/College Dean, or Department Chair
- Ask the appropriate department to conduct an analysis of the breach and inform the Data Security Manager
- Assess the nature of the breach, including a description of the incident, the response process, the notification process, and the actions taken to prevent further breaches of security
- Consult with University Counsel as appropriate
- Report the breach to the Vice President for Administration and Finance

The appropriate Custodian of Records, Administrator/College Dean, or Department Chair will:

- Examine the evidence of a breach to assess the possibility that protected information has been obtained
  If it is suspected that there is criminal activity involved in the breach, file a police report with the Department of Public Safety
  Identify the number of individuals whose protected data may have been acquired
- Submit a report to the Data Security Manager describing the nature of the security breach and report the number of individuals affected, including contact information
- Notify the affected individuals of the security breach (via e-mail, web site notice, postal mail) if required. A sample notification is located in Appendix D.

Individuals' Rights

Individuals have the right to inquire and be notified about whatever confidential information SFSU has on file concerning them. An opportunity to inspect any such confidential information must be afforded within 30 days of any request. If the record containing the confidential information also contains confidential information about another individual, that information must be deleted from the record before it is disclosed. Individuals may request copies of records containing any confidential information about them, and those copies must be provided within 15 days of the inspection. The University may charge a reasonable per page cost for making any copies. Individuals may request that their personal information be amended. If the request is denied, the individual may request a review of that decision by the appropriate Custodian of Records.

Penalties

Employees are subject to disciplinary and/or civil action if they are involved in unauthorized disclosure through careless, accidental, or intentional disclosure of information to unauthorized individuals; unauthorized modification, addition, or deletion of information; or violation of any provisions of this Plan.

Appendix A

Definitions

Access means a personal inspection, review, or communication of confidential or restricted information. This includes records or data which are oral, written, or electronic.

Centralized computer systems means those computer hardware and software systems housed in and maintained by DoIT.

Non-centralized computer systems means those computer hardware and software systems housed in departments other than DoIT or by individual employees on their computer system.

Confidential Information means any information not exempted in specific legislation and identified as personal or confidential, such as personally-identifiable information, individually-identifiable health information, education records, and non-public information, as specified in federal or state law or CSU or SFSU policy. Confidential information includes, but is not limited to, the following examples:

- social security number
- physical description
- home address
- home telephone number
- ethnicity
- gender
- education (except student records which are exempted by FERPA)
- financial matters
- performance evaluations
- verbal or written statements made by or attributed to the individual
- medical or employment history

Confidential information may include individually-identifiable health information. This includes any information, including demographic information collected from an individual, created or received by a health care provider, health plan, employer, or health care clearinghouse. This includes information that relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to the individual, or the identification of the individual.

In addition, electronic confidential information that includes an individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted:

- Social Security number
- education
- driver's license number or California Identification Card number
- account number, e.g., identification number, credit or debit card number in combination with any required security code, access code, or password that would permit access to an individual's financial account.

There is some Public Information for employees and students that may be released to the public and is not considered confidential. This information includes the following:

SFSU Employees - Public Information not considered confidential. The following information is considered public for SFSU employees and may be released to the public:

- Name
- Classification Title
- Department and location where employed
- Email address
- Work phone number

For verifications concerning employees, Human Resources must have a signed release before the following information may be verified:

- Dates of Employment as provided by employee on form
- Salary noted by employee on verification form

SFSU Students - Public Information not considered confidential. The following information is considered public for SFSU students and may be released to the public unless the student has requested that their record be restricted:

- Name
- Email address
- Major field(s) of study
- Dates of attendance
- Class or Student Level
- Enrollment status (e.g., undergraduate or graduate, full-time or part-time)
- Degrees awarded
- Honors and awards received

Disclosure means to permit access to or to release, transfer, disseminate, or otherwise communicate all or any part of confidential information by any means, orally, in writing, or electronic.

Handle means the access, collection, distribution, process, protection, storage, use, transmittal, or disposal of information containing confidential data.

APPENDIX B

References/Web Addresses

The San Francisco State University *Confidentiality and Information Security Plan* complies with federal and state regulations and California State University policy specified in the following documents:

Federal and State Regulations:

- Gramm-Leach-Bliley Act of 1999: Federal Trade Commission Regulations. The Act includes two regulations: *The Financial Privacy Rule* and *The Safeguards Rule*. http://www.ftc.gov/privacy/glbact/.
- Health Care Portability and Accountability Act of 1996 (HIPAA)-Final Rule http://www.hhs.gov/ocr/hipaa/privruletxt.txt
- Family Education and Privacy Act of 1974 (FERPA), http://www.ed.gov/policy/gen/guid/fpco/ferpa/index.html
- California Information Practices Act of 1977 http://www.privacy.ca.gov/code/ipa.htm
- California Code of Regulations, Title V, Sections 42396 through 42396.5 Privacy and Personal Information Management, http://ccr.oal.ca.gov/cgi-bin/om_isapi.dll?clientID=365532&advquery=42396&infobase=ccr&record={125BC}&softpage=Browse_Frame_Pg42&x=37&y=8&zz=
- California Education Code, Section 89546, *Employee Access to Information Pertaining to Themselves,* http://www.leginfo.ca.gov/cgi-bin/displaycode?section=edc&group=89001-90000&file=89530-89546
- California Penal Code, Section 502, *Comprehensive Computer Data Access and Fraud Act,* http://www.leginfo.ca.gov/cgi-bin/displaycode?section=pen&group=00001-01000&file=484-502.9
- California Civil Code Sections 1798-1798.78 Information Practices Act 1977, http://www.leginfo.ca.gov/cgi-bin/displaycode?section=civ&group=01001-02000&file=1798.80-1798.84

California State University Policies and Procedures:

- CSU Coded Memo: HR 2005-16, April 8, 2005, *Requirements for Protecting Confidential Personal Data: Updated to Include Information Practices Act Web Site and Security Breach Disclosure Requirement* http://www.calstate.edu/HRAdm/2005pages/2005hrmemo.shtml
- CSU Coded Memo: HR 2003-23, November 19, 2003, New *Legislation Regarding Use of Social Security Numbers,* http://www.calstate.edu/HRAdm/pdf2003/HR2003-23.pdf
- CSU Memo, *Increased Security Measures for CMS, March 26, 2003,* http://cms.calstate.edu/T6_Documents/NewsAndPublications/CMSWebsiteNews/2003/CMS%20NEWS%2003262003.doc
- CSU HR 2003-14, *HIPAA Regulations – Privacy Compliance, July 15, 2003,* http://www.calstate.edu/HRAdm/pdf2003/HR2003-14.pdf
- CSU *Information Security Policy, August 2002,* http://its.calstate.edu/systemwide_it_advisory/ITAC_keydocuments/IT_Security_Policy_092002.doc
- CSU *Records Access Manual, February 2003,* http://www.calstate.edu/gc/Docs/Records_Access_Manual.doc.
- *CSU Records Disposition Schedule* http://csuco.calstate.edu/Operations/archive_info.shtml

- CSU Memo, *Information Security Clarification, March 28, 2003*
- CSU Memo, *Compliance with the Gramm-Leach-Bliley Act-Safeguarding Confidential Personal Data, May 21, 2003,*

San Francisco State University Policies and Procedures:

- *SFSU Procedures on Management of Student Records, May 2002* http://www.sfsu.edu/~admisrec/reg/sfsu_policy.html
- Human Resources Practice Directive P202, *Protecting Confidential Data – Guidelines* http://www.sfsu.edu/~hrwww/emp_relations/hr_Directives/P202.html
- Division of Information Technology *Security Guide, March, 2003,* http://www.sfsu.edu/~helpdesk/docs/rules/security.htm

APPENDIX C

San Francisco State University
Authorization to Access Confidential Employee/Student Information
Agreement Form

The purpose of this form is to grant access to confidential data. In order to receive access, the requestor must complete the information requested below.

Certification – The requestor of this information must certify that data will be used for authorized purposes only. In addition, the guidelines noted in the SFSU Confidential and Information Security Plan must be followed. Failure to follow these guidelines may result in disciplinary and or civil action.

Purpose of request:

Population to be selected:

Frequency of data extraction:

I have received appropriate training on the use and disposal of confidential data. I understand I am responsible for the data that I receive and must ensure against any breaches of confidential data by myself or by other employees under my supervision (if applicable), who have been assigned tasks which involve viewing and working with confidential data.

Name of Requestor _____

Signature of Requestor_____ Date_____

Authorization:
Dean/Director_____Date_____

Authorization:
Custodian of
Records_____Date_____
To be filed with appropriate Custodian of Records

APPENDIX D

San Francisco State University
Draft Notification for Security Breach

California Senate Bill 1386 requires any state agency, including San Francisco State University, that has computerized data containing personal information, to disclose any security breach of a system containing such data to any California resident whose unencrypted personal information was, or is reasonably believed to have been acquired by an unauthorized person.

This notice is to inform you that on [date], personal information regarding University [employees/students], including yourself, was acquired by an unauthorized person. The personal information in the SFSU database contains names, [Social Security numbers], and [data listed in 1386]. Although there is no evidence that any personal data was acquired, this is being brought to your attention with the suggestion that you be aware of any possible access or possible misuse of your personal information.

The Federal Trade Commission website on identify theft (http://www.consumer.gov/idtheft/) offers additional information. Contacts are listed below for more information:

Social Security Administration fraud line at 1-800-269-0271

Credit Bureau Numbers: Equifax
1-800-525-6285 Experian 1-
888-397-3742 Trans Union 1-
800-680-7289

For further information regarding this matter please contact [name of contact].

Signed [appropriate Custodian of Records].