



## CALIFORNIA STATE UNIVERSITY, LONG BEACH

|   |                                    |
|---|------------------------------------|
| Subject: <b>Information Security and Privacy Program</b>  |                                    |
| Department: <b>Information Security Management and Compliance</b>   | Reference No.:                     |
| Division: <b>Administration and Finance</b>   | Issue Date: <b>May 2003</b>        |
| References: <ul style="list-style-type: none"><li>• <b>California Information Practices Act; California Civil Code §1798-1798.78</b></li><li>• <b>Employee Access to Information Pertaining to Themselves; California Education Code §89546</b></li><li>• <b>California Code of Regulations, Title V, § 42396-42396.5</b></li><li>• <b>Gramm-Leach-Bliley Act; FTC-15USC Subchapter I, §6801-6809 &amp; Subchapter II, §6821-6827</b></li></ul> | Revision Date: <b>October 2010</b> |
| Web Links: <a href="http://daf.csulb.edu/offices/vp/information_security">http://daf.csulb.edu/offices/vp/information_security</a>  | Expiration Date: <b>N/A</b>        |

### I. INTRODUCTION

California State University, Long Beach recognizes its affirmative and continuing obligation to protect the confidentiality, maintain the integrity, and ensure the availability of information about and used by CSULB faculty, staff, students and customers and to provide administrative, technical and physical safeguards to protect university information assets.

The California State University, Long Beach Information Security and Privacy Program provides the framework for assisting the University with meeting its responsibilities to:

- Safeguard personal and confidential information of CSULB faculty, staff, administrators, students and customers and other CSULB sensitive data regardless of format or medium;
- Protect against anticipated threats or hazards to the physical security or integrity of CSULB information assets;
- Protect the privacy of CSULB faculty, staff, administrators, students, and customers by preventing non-permitted disclosure of personal and confidential information; and
- Ensure campus compliance with federal and state law, regulations, CSU and CSULB policies, procedures, and standards regarding information security and privacy.

### II. PROGRAM SCOPE

The CSULB Information Security and Privacy Program applies to:

- Information that is acquired, transmitted, processed, transferred and/or maintained by CSU Long Beach and CSU Long Beach auxiliary organizations;
- All data systems and equipment including departmental, divisional and other ancillary systems and equipment as well as data residing on these systems and equipment;
- Home/personal electronic devices of CSULB faculty, staff, and administrators which access information technology resources; and
- Faculty, staff, administrators, students, and consultants employed by CSULB or CSULB auxiliary organizations and other persons having access to CSULB information technology resources.

### III. PROGRAM RESPONSIBILITY

#### University Information Security Officer

The University Information Security Officer is an appropriate administrator designated by the President and delegated responsibility for developing policies, procedures, and standards regarding the acquisition, transmission, processing, maintenance, safeguarding, release and disposal of personal and confidential information and other CSULB sensitive data; developing training and informational materials; and assessing and ensuring the University's compliance with applicable laws, regulations, and CSU and University policies, procedures, and standards regarding information retention, security and privacy.

#### Division/Area Information Security Officers

Division/Area Information Security Officers are management level employees appointed or designated by each Vice President, the Director of Athletics and each auxiliary organization and who serve as a conduit between the University Information Security Officer and their respective division/area. Division/Area Information Security Officers work closely with the University Information Security Officer to guide compliance with established campus policies, procedures, and standards within their respective division/area. Each Division/Area Information Security Officer shall provide periodic reporting including an annual report to their Vice President and the University Information Security Officer on the status of division/area compliance with the articulated information security policies, procedures and standards.

The following positions have delegated authority to serve as Division/Area Information Security Officer:

| Division/Area                      | Division/Area Information Security Officer                       |
|------------------------------------|--|
| Academic Affairs                   | Associate Vice President, Academic Technology                    |
| Administration and Finance         | University Information Security Officer                          |
| Associated Students, Inc           | Executive Director, Associated Students, Inc.                    |
| Athletics                          | Senior Associate Athletics Director/SWA                          |
| Forty-Niner Shops, Inc.            | Manager, ID Card Services  |
| Foundation                         | Chief Operating Officer  |
| President's Office                 | Executive Assistant to the President                             |
| Student Services                   | Associate Vice President , Student Services/<br>Dean of Students |
| University Relations & Development | Director of Advancement Services                                 |

#### Custodians of Records

Custodians of Records are appropriate administrators designated by the President and division Vice Presidents to maintain the official/original copy of the record/information. Custodians of records are responsible for a) Assuring that the campus is operating in compliance with the portion of the CSU Records Retention and Disposition Schedules for which they have been delegated authority; b) Identifying records/information that may have historic or vital value for the campus, and; c) reporting to the University Information Security Officer any university specific records that have not been cited within the CSU Records Retention and Disposition Schedule.

In addition, the following positions have been delegated authority to accept and respond to subpoenas:

| Type of Records Subpoenaed   | Custodian of Record                          |
|--|--|
| Student Records/Information  | Director, Office of Judicial Affairs         |
| Staff Personnel Records/Information<br>(including payroll records for all employees)               | Director, Staff Human Resources              |
| Faculty Personnel Records/Information<br>(including Librarians and Coaches)                        | Senior Director, Academic Employee Relations |
| Non-Personnel Records or where it is not possible to determine the specific subject of the request | Risk Manager                                 |

**University Administrators**

University Administrators are managers and supervisors included in the Management Personnel Plan (MPP) or equivalent in CSULB auxiliary organizations. University Administrators are responsible for ensuring compliance with established information security policies, procedures and standards within their respective college, department, administrative area, or organization.

**CSULB Faculty, CSULB Staff Members and employees of Auxiliary Organizations**

CSULB Faculty, CSULB Staff Members and employees or Auxiliary Organizations who, in the course and scope of their duties and responsibilities, access, collect, distribute, process, store, use, transmit or dispose of personal or other CSULB sensitive data are responsible for following established information security policies, procedures, and standards.

#### IV. DEFINITIONS

|   |  |
|---|--|
| <b>Access</b>                                       | A personal inspection or review of the personal information or a copy of the personal information, or an oral or written description or communication of the personal information.   |
| <b>Disclosure</b>                                   | To permit access to or to release, transfer, disseminate, or otherwise communication all or any part of the personal information by any means, orally, in writing, or by electronic or any other means to any person or entity.  |
| <b>Personal Information</b>                         | Specific items of personal information identified in CA Civil Code Sections 1798.29 and 1798.3. This information includes an individual's first name or first initial and his or her 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 or redacted: Social Security Number, driver's license/California identification card number, health insurance information, medical information, or financial account number such as credit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account. |
| <b>Directory Information</b>                        | Any student information that is not generally considered to be harmful to or an invasion of a student's privacy. CSULB designated Directory Information includes student name, address and telephone number, major field of study, dates of attendance, degrees and awards received, and email address.  |
| <b>Education Record</b>                             | Any record (in handwriting, print, tape, film, computer or other medium which is directly related to a student.  |
| <b>Financial Information</b>                        | Includes but is not limited to information about an individual's number of tax exemptions, amount of taxes or OASDI withheld, amount and type of voluntary/involuntary deductions/reductions, survivor's amounts, net pay and designee for last payroll warrant.   |
| <b>Handled</b>                                      | The access, collection, distribution, process, protection, storage, use, transmittal or disposal of information containing personal data.  |
| <b>Individually Identifiable Health Information</b> | Medical information which includes or contains any element of personal identifying information sufficient to allow identification of the individual such as the individual's name, address, electronic mail address, telephone number, or social security number, or other information that, alone or in combination with other publicly available information, reveals the individual's identity.   |
| <b>Permitted Disclosures</b>                        | Disclosures of personal information permitted under the California Information Practices Act of 1977. (See Appendix A)   |
| <b>Service Provider</b>                             | Any person or entity that receives, maintains, processes, or otherwise is permitted access to personal information through is provision of service directly to the University.   |
| <b>Student</b>                                      | Any person who is attending or has previously attended California State University, Long Beach. This includes any person who has been enrolled in the regular, extension or special (i.e., summer or winter), regardless of the physical location of the program.  |
| <b>Third Party</b>                                  | Any individual or individual on behalf of an organization who is <u>not</u> any employee of California State University, Long Beach.   |

## **V. INFORMATION SECURITY RISKS**

There are several reasonable and foreseeable internal and external risks to the security and integrity of personal information that could result in the unauthorized disclosure, misuse, alteration, destruction, or other compromise of the security and confidentiality of personal and confidential information. These risks may include, but are not limited to:

- Unauthorized access of personal information by individuals not approved for access;
- Compromised system security
- Interception of data during transmission
- Loss of data integrity
- Physical loss of data
- Poor audit trails
- Unauthorized access of personal information by employees
- Unauthorized transfer of personal information to third parties or employees not approved for access
- Unauthorized transfer of personal information by third parties

## **VI. MANAGEMENT AND CONTROL OF RISKS**

The management and control of risks shall be accomplished by 1) the development of policies, procedures, and standards which address identified risks; 2) the development of training opportunities and informational materials to assist in the implementation of these policies, procedures and standards; and 3) monitoring, auditing and otherwise evaluating campus divisions/area/ auxiliary organizations for compliance with information policies, procedures, and standards.

The University Information Security Officer will work closely with the each Division/Area Information Security Officer to ensure that each division complies with the University's information security policies, procedures, and standards. The Division Information Security Officers will ensure that all new policies, procedures and standards are distributed within their own divisions/areas through the appropriate reporting and communication channels. Compliance with policies, procedures and standards will be monitored on an ongoing basis.

## **VII. INDIVIDUAL RIGHTS**

Individuals have the right to inquire and to be notified about the personal information that CSULB maintains concerning them. An opportunity to inspect any such confidential information must be afforded within 30 days of any request. If the record containing the personal information also contains personal information about another individual, that information must be deleted from the record before it is disclosed. Individuals may request copies of records containing personal information about them, and those copies must be provided within 15 days of the request. The University/Auxiliary may charge a reasonable per page cost for making any copies. Individuals may request that their personal information be amended, and if that request is denied, the individual may request a review of that decision by the Vice President, Administration and Finance or designee.

## **VIII. PERIODIC REVIEW**

The University Information Security Officer shall conduct an annual review of the Information Security and Privacy Program to ensure that it remains appropriate and relevant.

## **FURTHER INFORMATION**

Information Security Management and Compliance  
iso@csulb.edu.  
(562) 985-4862

## APPENDIX A PERMITTED DISCLOSURES

The California Information Practices Act was enacted in 1977 to protect individual's privacy rights in "personal information" contained in state agency records. The Act reflects the Legislature's determination that the right to privacy is in jeopardy and that the maintenance and dissemination of private information should be subject to strict limits. The Act prohibits disclosure of personal information except in certain limited circumstances. Some of these disclosures may impose requirements not included in this document. Consultation with the University Information Security Officer is required before releasing personal information covered by the Information Practices Act.

The following disclosures are permitted under the Information Practices Act:

- to the individual to whom the information pertains;
- where the individual to whom the information pertains has given voluntary written consent to disclose the information to an identified third party no more than 30 days before the third party requested it, or within the time limit agreed to by the individual in the written consent;
- to an appointed guardian or conservator of a person representing the individual provided it can be proven with reasonable certainty through CSU forms, documents or correspondence that the person is the authorized representative of the individual to whom the information pertains;
- to persons within the CSU who need the information to perform their functions;
- to another government agency when required by law;
- in response to a request for records under the California Public Records Act;
- where there is advance written assurance that the information is to be used for purposes of statistical research only and where the information will be redisclosed in a form that does not identify any individual;
- where the CSU has determined that compelling circumstances exist which affect the health or safety of the individual to whom the information pertains, and notification is transmitted to the individual at his or her last known address, and the disclosure does not conflict with other state or federal laws;
- pursuant to a subpoena, court order, or other compulsory legal process if, before disclosure, the CSU notifies the individual to whom the record pertains, and if the notification is not prohibited by law;
- pursuant to a search warrant;
- to a law enforcement or regulatory agency when required for an investigation of unlawful activity of or for licensing, certification, or regulatory purposes, unless the disclosure is otherwise prohibited by law.