CALIFORNIA STATE UNIVERSITY, LONG BEACH

Subject: **Confidential Information Security Program**	
Department: **Administration & Finance**	Reference No.:
Division: **Administration & Finance**	Issue Date: **March 2003**
References: **NA**	Revision Date: **April 2004**
Web Links: **CSULB Information Security Program**	Expiration Date: **NA**

I. Introduction

California State University, Long Beach (CSULB) recognizes its affirmative and continuing responsibility to protect confidential employee and student data and maintain confidentiality of that data. The CSULB Confidential Information Security Program serves as the framework for assisting the University in meeting this responsibility.

The California State University Long Beach (CSULB) Confidential Information Security Program establishes appropriate and reasonable administrative, technical and physical safeguards designed to:

- ensure the security and protection of confidential information in its custody, whether in electronic, paper, or other forms;
- protect against any anticipated threats or hazards to the security or integrity of such confidential information; and
- protect against unauthorized access to or use of such confidential information.

The CSULB Confidential Information Security Program complies with CSU requirements for information security and the requirements of the following federal and state laws and regulations:

Gramm-Leach-Bliley Act of 1999

Federal Trade Commission Regulations (16 CFR, Part 314), Standards for Safeguarding Customer Information; Final Rule, May 23, 2002

California Information Practices Act of 1977

California Code of Regulations, Title 5, Sections 42396 through 42396.5

California Education Code, Section 89546, Employee Access to Information Pertaining to Themselves

Comprehensive Computer Data Access and Fraud Act (California Penal Code, Section 502)

Federal Trade Commission Regulations (16 CFR, Part 314), Standards for Safeguarding Customer Information; Final Rule, May 23, 2002

Health Care Portability and Accountability Act of 1996 (HIPAA)-Privacy Rule

California Civil Code, Sections 1798.80-1798.84 and Section 1798.29

The CSULB Confidential Information Security Program does **not** address procedures to protect the privacy of student education records. The procedures designed to protect the privacy of student education records required by the Family Education Rights and Privacy Act of 1974 (FERPA), are contained in the CSULB Student Records Procedures.

II. Scope

This program applies to all information that is processed and/or maintained by CSU Long Beach or any CSU Long Beach auxiliary organization that contains data deemed confidential.

This plan applies to all students, faculty and staff, consultants or any other person having access to CSULB confidential information employed by CSULB or any CSULB auxiliary organization.

The unauthorized modification, deletion, or disclosure of confidential information included in CSULB data files and data systems can compromise the integrity of CSULB programs, violate individual privacy rights, and is expressly forbidden. Careless, accidental or intentional disclosure of confidential information may result in disciplinary action against those involved in unauthorized disclosure and civil action against CSULB.

In certain limited circumstances as specified in the California Information Practices Act of 1977 and in conformance with procedures contained in this Program, CSULB may disclose confidential information. The more common exceptions which permit disclosure under the California Information Practices Act are provided in Appendix A.

III. Definitions

Access means a personal inspection or review of the confidential information or a copy of the confidential information, or an oral or written description or communication of the confidential information.

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 by electronic or any other means to any person or entity.

Confidential Information as used in this document means any information identified in governing law, regulation or policy as *personal information, individually identifiable health information, confidential information, education records, personally identifiable information, non-public information, non-public personal data, confidential personal information or sensitive information*. It is information that identifies or describes an individual, including, but not limited to, his or her social security number, physical description, home address, home telephone number, ethnicity, gender, telephone number, signature, passport number, bank account number, education, financial matters, medical or employment history, and performance evaluations. It includes statements made by, or attributed to, the individual. *Confidential Information* also includes computerized data 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: (1) Social Security number; (2) driver's license number or California Identification Card number; (3) account number (which could include a student or employee 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. *Confidential Information* does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records. *Confidential Information* does not include publicly available directories containing information an individual has voluntarily consented to have publicly disseminated or listed, such as name, address, or telephone number.

Confidential Information Security Program Coordinator is the individual responsible for implementing the provisions of this Plan.

Custodian of Records are those individuals specifically designated by the Vice President, Administration and Finance to accept and respond to a subpoena, court order, request for records under the California Public Records Act, or other compulsory legal process which involves the release of University records or confidential information.

Financial Information includes but is not limited to information about an individual's number of tax exemptions, amount of taxes withheld, amount of OASDI withheld, amount and type of voluntary/involuntary deductions/reductions, survivor's amounts, net pay and designee for last payroll warrant.

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

Individually Identifiable Health Information means any information, including demographic information collected from an individual, that is created or received by a health care provider, health plan, employer or health care clearinghouse; and relates to the past, present, or future physical or mental health or condition of an individual, the provisions of health care to an individual, and identifies the individual; or with respect to which there is a reasonable basis to believe that the information can be used to identify the individual.

Information Security Officer is the individual or individuals responsible for protecting confidential information in the custody of the University; the security of the equipment and/or repository where this information is processed and/or maintained; and the related privacy rights of the University students, faculty and staff concerning this information.

Permitted Disclosures are disclosures of confidential information permitted under the California Information Practices Act of 1977.

Service Provider means any person or entity that receives, maintains, processes, or otherwise is permitted access to confidential information through its provision of service directly to the university.

Third Party means any individual (or individual on behalf of an organization) who is not an employee of California State University, Long Beach.

IV. Roles and Responsibilities

A. Vice President, Administration and Finance

The President has delegated responsibility to the Vice President, Administration and Finance for the overall administration of the CSULB *Confidential Information Security Program*.

To effectively implement and administer the CSULB *Confidential Information Security Program* the responsibility for protecting confidential information; the security of the equipment and/or repository where the information is processed and/or maintained; and, the related privacy of CSULB faculty, staff and students has been further delegated as follows:

B. Information Security Program Coordinator

The Information Security Program Coordinator designated by the Vice President, Administration and Finance is responsible for implementing the provisions of this Plan. The coordinator shall:

- Assist Information Security Officers in identifying reasonably foreseeable internal and external risks to the security and confidentiality of confidential information;
- Evaluate the effectiveness of the current safeguards for controlling these risks;
- Provide assistance to Information Security Officers regarding the requirements of the *Confidential Information Security Program*;
- Provide training to University Managers and assist University Managers as necessary in developing and delivering adequate training and education for all employees with access to confidential information;
- Provide recommendations for revisions to this Plan as appropriate;
- Prepare an annual report on the status of the *Confidential Information Security Program*;
- Prepare more frequent reports if necessary or requested;
- Update the *Confidential Information Security Program* as necessary;
- Maintain the *Confidential Information Security Program* and make the plan available to the University community;
- Provide assistance to Custodians of Records in responding to third party requests for confidential information permitted under the California Information Practices Act of 1977;
- Ensure that Custodians of Records designations are current and that appropriate training and assistance is provided;
- Ensure that, where appropriate, written delegations to release confidential information to third parties are current; and
- Consult with University Counsel before campus release of any confidential information to third parties

C. Information Security Officers

Individuals in the following positions have been identified as campus Information Security Officers:

- Associate Vice President, Information Management and Analysis is responsible for safeguarding the confidential information processes and is maintained by Information Technology Services;
- Common Management System (CMS) Project Director is responsible for safeguarding the confidential information in the CMS systems;
- Executive Director, CSULB Foundation is responsible for safeguarding the confidential information maintained in Foundation data systems or data files;
- General Manager/CEO, Forty-Niner Shops is responsible for safeguarding the confidential information maintained in Forty-Niner data systems or data files;
- Executive Director, Associated Students, Inc. (ASI) is responsible for safeguarding the confidential information maintained in ASI data systems or data files;
- Division Executives are responsible for safeguarding non-centralized confidential information maintained in divisional or other ancillary data systems, equipment, and records within their division.
- Executive Director of Athletics is responsible for safeguarding non-centralized confidential information maintained in SAR data systems or data files

Information Security Officers are responsible for:

- Protecting confidential information in custody of the University;
- Providing security of the equipment or repository where the information is processed and/or maintained;
- Protecting the privacy rights of University faculty, staff and students;
- Promoting and encouraging good security procedures and practices;
- Identifying and monitoring risks for which the University must be prepared;
- Developing plans and procedures to preserve the information in case of natural or man-made disasters;
- Ensuring that training is provided to employees on information security requirements and procedures;
- Ensuring compliance with the University *Confidential Information Security Program*; and
- Notifying the Information Security Program Coordinator when a request for confidential information has been made by a third party; and
- Approving requests for confidential information maintained in non-centralized data systems or files; and
- Preparing an annual report which critically evaluates the adequacy of existing safeguards, compliance with campus safeguarding policies and procedures and suggests the implementation of additional safeguards, if appropriate.

D. Custodians of Records

Custodians of Records are responsible for:

- Accepting all third party requests for University Records and information;
- Verifying that all subpoenas or other requested information is legally valid;
- Releasing requested records and information in response to legally valid subpoenas, Public Record Acts requests, etc.

E. University/Auxiliary Managers

With guidance and assistance of the appropriate Information Security Officer and Information Security Program Coordinator, University/Auxiliary Managers are responsible for:

- Protecting the confidentiality of information in their area;
- Providing security of the equipment or repository where the information is processed or maintained;
- Promoting and encouraging good security practices and procedures
- Identifying and monitoring risks to the security of confidential information in their area;
- Developing and implementing written department privacy and safeguarding plan to preserve confidential information in the event of natural or man-made disasters, protect the privacy rights of University faculty, staff and students, and safeguard confidential information (see section VI for additional information);

- Providing appropriate training to those employees who may have access to confidential information;
- Ensuring that those employees who may have access to confidential information have read and signed an Access and Compliance Form;
- Consulting with the Information Security Program Coordinator prior to releasing confidential information covered by the Information Practices Act; and
- Ensuring compliance with the University *Confidential Information Security Program*

F. Employees

Employees who have access to confidential information shall:

- Participate in training regarding access and use of confidential information;
- Sign a university Access and Compliance Form (Appendix B)
- Comply with University Confidential Information policies and procedures

V. Risk Assessment

Reasonable, foreseeable internal and external risks to the security and integrity of confidential information that could result in the unauthorized disclosure, misuse, alteration, destruction, or other compromise of such information have been identified. These risks may include, but are not limited to:

- Unauthorized access of confidential information by anyone not approved for access;
- Compromised system security as a result of system access by a computer hacker
- Interception of data during transmission
- Loss of data integrity
- Physical loss of data in a disaster
- Poor audit trails
- Errors introduced into the systems
- Lack of transaction completeness and documentation
- Unauthorized access of confidential information by employees
- Unauthorized telephone requests for confidential information
- Unauthorized access through hardcopy files or reports
- Unauthorized transfer of confidential information through third parties

It is recognized that this may not be a complete list of the risks associated with the protection of confidential information. Since technology growth is not static, new risks are created regularly.

VI. Management and Control of Risks

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

A. 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 from which the confidential information was obtained.

There shall be no confidential information collected or maintained which has not been approved by the appropriate Information Security Officer.

B. Access

No CSULB employee or CSULB auxiliary organization employee shall be granted access to centralized electronic data systems containing confidential information in the custody of CSULB without review and written approval of the appropriate Information Security Officer. The approval of access to confidential information will be based on several factors including the division

executive's determination that access is required for the employee to perform a critical university or auxiliary function that is part of the employee's job duties and responsibilities and assurance that all requirements contained in the Confidential Information Security Program designed to protect individual privacy and safeguard confidential information will be met.

Employees with approved CMS access are concurrently approved access to the campus administrative Legacy System. CSULB employees or CSULB 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 must receive appropriate training and sign an Access and Compliance Form (Appendix B). A copy of the signed Form will be retained in the individual's official personnel file. Additionally, copies of Access and Compliance Forms should be kept on file with the appropriate University/Auxiliary Manager.

Employees with approved access to electronic information will be assigned an account by the appropriate Information Security Officer or University Manager. Accounts will be immediately deactivated upon the separation of the employee. An employee approved for access to electronic information does not need to complete an additional Access and Compliance Form for access to non-electronic information.

C. Training

The Information Security Program Coordinator shall provide training to all University/Auxiliary Managers concerning Program requirements and their responsibilities.

All CSULB employees and CSULB auxiliary organization employees having access to confidential information will receive training regarding the University's Confidential Information Security Program and the Privacy and Safeguarding Plan for their department or administrative unit. Employee training shall be provided by the employee's manager or the appropriate Information Security Officer and include information regarding the campus Confidential Information Security Program and the Department Privacy and Safeguarding Plan. Information Security Officers and University/Auxiliary Managers shall keep documentation of this training for review by the campus internal auditor.

D. Physical Security of Records

All printed material containing confidential information must be protected against destruction, loss, or damage from potential environmental hazards such as fire, or water damage, to the extent possible and as determined by the appropriate University/Auxiliary Manager.

E. Record Retention

The maintenance of records beyond the retention requirements set forth in the CSU Records Disposition Schedule which can be accessed at http://daf.csulb.edu/offices/bhr/safetyrisk/index.html presents a significant risk to the security and integrity of confidential information. Due to space limitations, "historic records" are sometimes stored in remote campus locations and periodic inspections to ensure record security must be conducted and documented. Unless longer retention is specifically approved by the appropriate Information Security Officer, records containing confidential information shall be destroyed within 3 months following the required period of retention.

F. Record Destruction

Record destruction is the responsibility of University/Auxiliary Managers. All printed material containing confidential information shall be destroyed when retention is no longer required. Destruction must prevent unauthorized access to confidential information (i.e., shredding).

Prior to the survey and disposal of a campus computer or the transfer of a computer from one campus user to another user, the computer's hard drive shall be wiped clean using a low level formal utility to remove the operating system, software applications installed on the computer and any personal files which were stored on the computer.

Questions regarding desk top security procedures may be directed to the campus office of Information Technology Services.

G. Department Privacy and Safeguarding Plan

The development and implementation of written department privacy and safeguarding plan is the responsibility of each University/Auxiliary Manager. While there is no prescribed document format, at a minimum, the plan must be dated and signed by the appropriate University/Auxiliary Manager and must include:

1. name of the office, department, or operation where confidential information is handled;
2. identification of confidential information handled;
3. number of individuals with access to confidential information;
4. administrative controls implemented to minimize the number of individuals with access to confidential information;
5. description of physical security of records methods;
6. discussion of records retention and destruction methods; and
7. discussion of training content, frequency, delivery method, etc.

H. Service Provider Requirements

Due to the specialized expertise needed to design, implement, and service new technologies, vendors may be needed to provide resources that the University is unable to provide on its own. Further, vendors may be needed to assist in the disposal of the volumes of hard-copy confidential information that is generated by the University and its' auxiliaries. In recognition of its responsibility for the performance and actions of these vendors, the following actions are required:

Due Diligence of Service-Providers – The adequacy of the service provider's system of safeguarding information shall be determined prior to the University or its auxiliaries entering into a contractual relationship with the service provider. The University shall not contractually engage a service provider who cannot demonstrate that they have a system to safeguard student information. Depending on the service provider, the University Auxiliary may wish to review the service provider's audits, summaries of its test results for security, or other internal and external evaluations. The University/Auxiliary shall not enter into contractual agreement with any provider who is not capable of maintaining appropriate safeguards for confidential information.

Service Provider Agreements – All contracts with service providers must include a privacy clause which requires the service provider to implement appropriate measures to safeguard confidential information and to refrain from sharing any such information with any other party. Current provider contracts without a privacy clause are valid until May 24, 2004.

Contracts must, when appropriate, include the requirement that in addition to the CSU insurance requirements for service agreements, the service provider be bonded and maintain personal liability insurance which protects against allegations of violation s of privacy rights of individuals as a result of improper or insufficient care on the part of the service provider.

VII. Common Management System (CMS)

CMS security contains components that are managed locally by campuses as well as components that are managed centrally by the Chancellor's Office CMS staff. Campus CMS security responsibilities are managed by security designees in the CMS functional areas and ITS department. CMS security at the Chancellors Office is managed by Software Operations Support Services (SOSS), Hardware Operations Support Services (HOSS), Network Services (4CNet / CENIC), and the outsourced data center service provider (Unisys).

Detailed CMS security requirements and management responsibilities have been identified by responsible area and are documented in *CMS Security Requirements*, a document developed and maintained by HOSS that can be accessed at: http://cms.calstate.edu/T3_Documents/TechnicalOverview/CMS%20Security%20Requirements%2011062001.doc

This document outlines security requirements and management responsibilities for the following:

1. CMS Application Security
2. CMS Logon Security
3. Network Security
4. CMS Database Security
5. CMS Web Server Security
6. CMS Unix Security

VIII. Campus Legacy (mainframe) System

The Campus Information Technology Services Security Manual which can be accessed at: http://daftest.csulb.edu/offices/ima/its/index.html details the policies and practices specific to the safeguarding of information

operated and maintained by Information Technology Services (ITS). Such policies and practices will be observed until such time they are replaced or revised by CMS information security procedures.

It is the responsibility of ITS to ensure the physical security of computer stored information of the Legacy (mainframe) computer installation holding such information and includes but is not limited to delivery of output, disposal of waste material and on-site access as required by the Owner of the data/Custodian of Record. The computer installation is also responsible for providing the means of controlling access to the confidential information by remote access and programs as required by the Owner/Custodian of Record.

Administrative control of the access to and use of computer-stored information on the Legacy System is the responsibility of the user who collects or receives and maintains that information. All confidential files shall have access restricted by such Owner/Custodian of Record through passwords or other similar means. The Owner/Custodian of Record of confidential data must also establish and periodically disseminate the rules of access.

IX. Permitted Disclosures of Confidential Information

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. The more common exceptions which permit disclosure are contained in Appendix A. Some of these disclosures may impose requirements not included in this document. Consultation with the Information Security Program Coordinator is required before releasing personal information covered by the Information Practices Act.

X. Required Disclosure of Security Breach

The University is required to disclose any breach of system security to individuals whose unencrypted personal information was, or is reasonably believed to have been acquired by
an unauthorized person. Any university student, faculty, staff, consultant or any other person having access to CSULB confidential information employed by CSULB or any CSULB auxiliary organization shall immediately notify the appropriate Information Security Officer **and** Vice President for Administration and Finance **or** the Information Security Program Coordinator **or** the campus Internal Auditor. The Vice President for Administration and Finance or the Information Security Program Coordinator or the campus Internal Auditor shall, without unreasonable delay, notify the CSU Office of General Counsel.

XI. Individuals' Rights

Individuals have the right to inquire and be notified about whatever confidential information 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 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/Auxiliary may charge a reasonable per page cost for making any copies. Individuals may request that their personal information be amended and, if the request is denied, the individual may request a review of that decision by the Vice President, Administration and Finance or his designee.

XII. Periodic Evaluation and Revision

The University shall periodically evaluate, test, and adjust the *Confidential Information Security Program* to validate that equipment and systems function properly and produce the desired results. Each Information Security Officer and University/Auxiliary Manager shall perform ongoing assessments to ensure that employees follow written procedures for information security. Information security shall be included in all internal audits. The campus shall conduct an annual review of the *Confidential Information Security Program* to ensure that it remains appropriate and relevant. An annual report to critically evaluate the adequacy of existing safeguards, compliance with campus safeguarding policies and procedures and

recommendations for implementation of additional safeguards shall be completed by the Confidential Information Security Program Coordinator and reviewed by the Vice President for Administration and Finance.

Appendix A
Permitted Disclosures

The University may not disclose confidential information except in certain limited circumstances. The more common exceptions permit disclosure in the following circumstances:

- 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 (unless the Public Records Act provides an exception);
- 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 disclosure does not conflict with other state or federal laws;
- pursuant to a subpoena, court order, or other compulsory legal process it, 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.

FORMS: NA