



# CALIFORNIA STATE UNIVERSITY, LONG BEACH

Subject: <b>Information Security Policy</b>	
Department: <b>Information Security Management and Compliance</b>	Reference No.:
Division: <b>Administration and Finance</b>	Issue Date: <b>April 2007</b>
References:	Revision Date: <b>N/A</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. POLICY STATEMENT

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 appropriate administrative, technical and physical safeguards to protect university information assets. It is the policy of California State University, Long Beach (CSULB) 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, and CSU and CSULB policies, procedures, and standards regarding information security and privacy.

## II. SCOPE

The CSULB Information Security Policy 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 services.

## III. RESPONSIBILITIES

**A. University Information Security Officer** is an appropriate administrator designated by the President and delegated responsibility for implementing this policy; developing standards and communications regarding the acquisition, transmission, processing, maintenance, safeguarding, release and disposal of personal and confidential information and other CSULB sensitive data; developing appropriate 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.

**B. Division Information Security Officers** are management level employees appointed or designated by each Vice President, the Director of Athletics, and each auxiliary organization who serve as a conduit between the University Information Security Officer and their respective division/area and 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 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.

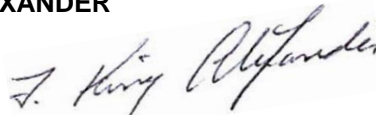
- C. Campus Information Technology Committee (CITC)** is responsible for developing the strategic plan for meeting campus information technology goals including information security. The CITC is also responsible for assisting the University Information Security Officer with developing and issuing information security policies, standards, procedures and guidelines to the campus community and providing assistance to the Division/Area Information Security Officers in their implementation of these policies, procedures, and standards within their respective division/area.
- D. Custodians of Records** are appropriate administrators designated by the Vice President, Administration and Finance who are responsible for accepting and responding to subpoenas, court orders, request for records under the California Public Records Act or other compulsory legal processes which involve the release of University records or personal information.
- E. Administrators** are supervisors or managers included in the Management Personnel Plan or equivalent in CSULB auxiliary organizations. Administrators are responsible for ensuring compliance with established information security policies, procedures, and standards within their respective college, department, or administrative area, or organization.
- F. CSULB Faculty, CSULB Staff Members, and employees of 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 confidential information or other CSULB sensitive data are responsible for following established information security policies, standards, and practices.

**FURTHER INFORMATION**

Information Security Management and Compliance  
iso@csulb.edu.  
(562) 985-2283

**APPROVED BY PRESIDENT ALEXANDER**

**APRIL 2007**

A handwritten signature in black ink, appearing to read "J. King Alexander", is written over a faint, light-colored rectangular stamp or watermark.