



CALIFORNIA STATE UNIVERSITY, LONG BEACH

Subject: Information Security Policy	
Department: Information Security Management and Compliance	Reference No.:
Division: Administration and Finance	Issue Date: April 2007
References:	Revision Date: May 2009
Web Links: • http://daf.csulb.edu/office s/vp/information_security	Expiration Date: N/A

I. POLICY STATEMENT

California State University, Long Beach (CSULB) recognizes its affirmative and continuing responsibility to protect the confidentiality, maintain the integrity, and ensure the availability of its information assets. Unauthorized modification, deletion, or disclosure of information assets can compromise the integrity of the mission of CSULB, violate individual privacy rights, and possible constitute a criminal act. It is the policy of California State University, Long Beach to ensure:

- confidentiality of personally identifiable information;
- integrity of data stored on or processed by CSULB information systems;
- availability of information stored or processed by CSULB information systems;
- maintenance and currency of applications installed on CSULB information systems; and
- compliance with applicable laws, regulations, and CSU/CSULB policies, standards, and procedures governing information security and privacy protection.

II. SCOPE

The CSULB Information Security Policy applies to:

- Information assets that are acquired, transmitted, processed, transferred and/or maintained by CSU Long Beach or CSU Long Beach auxiliary organizations;
- All media in which the information asset is held (e.g., paper, electronic, oral, etc.)
- All data systems and equipment including departmental, divisional or other ancillary systems and equipment as well as data residing on these systems and equipment;
- All faculty, staff, administrators, students, and consultants employed by CSULB or CSULB auxiliary organizations having access to CSU information assets; and
- Personal electronic devices of CSULB faculty, staff, and administrators which access information technology resources.

III. RESPONSIBILITIES

Information security roles and responsibilities are intended to support the University's information security program. These roles and responsibilities include, but may not be limited to the following:

- University Information Security Officer** is an appropriate administrator designated by the President and delegated authority for implementing this policy; developing standards and procedures to support this policy; developing appropriate training and informational materials; and assessing and ensuring the University's compliance with applicable laws, regulations, and CSU and University policies, standards and procedures regarding information security.
- Division Information Security Officers** are management employees designated by each Vice President, the director Athletics, and each CSULB auxiliary organization who serves as a conduit between the University Information Security Officer and their respective division/area and who work closely with the University Information Security Officer to guide compliance with established CSULB information security policies, standards and procedures.

- C. Custodians of Records** are appropriate administrators designated by the Vice President, Administration and Finance who are responsible for 1) accepting and responding to subpoenas, court orders or other compulsory legal processes involving the release of University records; 2) accepting and responding to requests for records made pursuant to the California Public Records Act; or 3) ensuring compliance with the CSU records/information retention and disposition schedules.
- D. University Administrators** are managers or supervisors included in the Management Personnel Plan or equivalent in CSULB auxiliary organizations who are responsible for ensuring compliance with established information security policies, standards and procedures within their respective college, department, administrative area or organization.
- E. Faculty, Staff and Employees of CSULB Auxiliary Organizations** who in the course and scope of their duties and responsibilities access, collect, distribute, process, store, use, transmit or dispose of CSULB information assets are responsible for following established information security policies, standard and procedures.

IV. POLICY COMPLIANCE

The University reserves the right to temporarily or permanently suspend, block, or restrict access to information assets when it reasonably appears necessary to do so to protect the confidentiality, integrity, availability, or functionality of those assets.

Any disciplinary action resulting from violations of this policy or program supporting policies, standards or procedures shall be administered in a manner consistent with the terms of the applicable collective bargaining agreement and/or the applicable provisions of the California Education Code. Student infractions of this policy or supporting policies, standards or procedures may be referred to the Office of Student Judicial Affairs. Third party service providers who do not comply with established information security policies, standards or procedures may be subject to appropriate actions as defined in contractual agreements.

V. POLICY MANAGEMENT

This policy shall be reviewed and if necessary updated annually by the University Information Security Officer.

FURTHER INFORMATION

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

APPROVED BY PRESIDENT ALEXANDER
May 2009