



CALIFORNIA STATE UNIVERSITY, LONG BEACH

Subject: Information Classification and Protection Standard	
Department: Information Security Management and Compliance	Reference No.:
Division: Administration and Finance	Issue Date: December 2007
References: State of California State Administrative Manual § 4840.2 & 4841.3	Revision Date:
Web Links: Information Security and Compliance	Expiration Date:

I. INTRODUCTION

California State University, Long Beach’s databases and files, regardless of format, are essential public resources that must be protected from unauthorized use, access, disclosure, modification, loss, or deletion. However, the appropriate level of physical, technical and administrative safeguards necessary to provide protection is relative to the value, legal requirements, sensitivity and criticality of the information.

The California State University, Long Beach Information Classification and Protection Standard establishes information classification levels based on these factors; describes the types of information residing at each level; and prescribes the safeguards to protect university information assets.

II. SCOPE

The CSULB Information Classification and Protection Standard applies to all information in written format that is collected, generated, and/or maintained by CSU Long Beach and CSU Long Beach auxiliary organizations except where superseded by grant, contract, or federal copyright law

III. DEFINITIONS

Financial Information – Personal information which includes, but is not limited to, 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.

Health Insurance Information – An individual’s health insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the individual, or any information in an individual's application and claims history, including any appeals records.

Medical Information – Information regarding an individual’s medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional.

Notice-triggering Personal Information – Specific items of personal information identified in CA Civil Code Sections 1798.29 and 1798.3. This information includes an individual’s name in combination with Social Security Number, driver’s license/California identification card number, 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.

Payment Related Data – Information related to credit/debit card payments for goods or services offered by the University or its auxiliary organizations.

Protected Health Information – Individually identifiable information created, received, or maintained by health care providers or health plans 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.



CALIFORNIA STATE UNIVERSITY, LONG BEACH

Written format means any handwriting, typewriting, printing, photographing, photocopying, transmitting of electronic mail or facsimile, and every other means of recording upon any tangible thing, and any form of communication or representation, including letters, words, pictures, sounds, or symbols, or combinations thereof, and any record thereby created, regardless of the manner in which the record has been stored.

IV. ROLES AND RESPONSIBILITIES

- A. **The CSU Office of the Chancellor** is responsible for identifying Level 1 information and reviewing the requirements for the protection of Level 1 information on a periodic basis.
- B. **University Information Security Officer** is responsible for communicating the identity of Level 1 information to Division Information Security Officers and assisting in the identification of information types within their respective area and determining classification levels. The University Information Security Officer is also responsible for providing advice and guidance to Division Information Security Officers regarding the implementation of this Standard within their respective division or area. The University Information Security Officer is also responsible for conducting an annual review of this Standard and amending it as appropriate.
- C. **Division Information Security Officers** are responsible for guiding compliance with this Standard within their respective division or area.
- D. **Information Custodians** have operational responsibility for the physical and/or electronic security of the information and are generally responsible for granting access to and ensuring the appropriate use of the information. Information custodians are also responsible for ensuring that access to and protection of information and the file systems that host them are in compliance with all applicable information security policies and standards.
- E. **University Administrators** are university managers and supervisors in the Management Personnel Plan 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.
- F. **Information Owners** are CSULB Faculty and 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 University information assets. Information owners are responsible for following established information security policies, procedures, and standards.

V. INFORMATION CLASSIFICATION STANDARD

The California State University (CSU) has identified three (3) classification levels of University information referred to as Level 1, Level 2, and Level 3. Types of university information are assigned to each level based on the value, legal requirements, sensitivity and criticality assigned to them.

Aggregates of information shall be classified based upon the most secure classification level. That is, when information of mixed classifications exists in the same file, document or other written format, the entire file, document, etc. shall be classified at the most secure classification level.

Level 1: Confidential

Confidential Information is information maintained by the University that is exempt from disclosure under the provisions of the California Public Records Act or other applicable state or federal laws.

Confidential information is information whose unauthorized use, access, disclosure, acquisition, modification, loss, or deletion could result in severe damage to CSULB, its students, employees, or customers. Financial loss, damage to CSULB's reputation, and legal action could occur. Level 1 information is intended solely for use within CSULB and limited to those with a "business need-to know." Statutes, regulations, other legal obligations or mandates protect much of this information. Disclosure of Level 1 information to persons



CALIFORNIA STATE UNIVERSITY, LONG BEACH

outside of the University is governed by specific standards and controls designed to protect the information. Level 1 information includes, but is not limited to:

Personal Information

- Passwords or credentials
- Notice-triggering Personal Information (See Definition)

Payment Related Data

See Definition

Medical Information

See Definition

Health Insurance Information

See Definition

Financial Information

See Definition

Protected Health Information

See Definition

Technical Security Information

- Vulnerability/security information related to campus systems or services

Law Enforcement Information

- Law enforcement records related to an individual

Library Patron Information

- Library database for faculty, staff, students and community borrowers which may contain:
 - Home Address
 - Home Phone
 - Social Security Numbers

Level 2: Internal Use

Internal use information is information which must be protected due to proprietary, ethical or privacy considerations. Although not specifically protected by statute, regulations, or other legal obligations or mandates, unauthorized use, access, disclosure, acquisition, modification, loss or deletion of information at this level could cause financial loss, damage to CSULB's reputation, violate an individual's privacy rights or legal action could occur. Level 2 information includes, but is not limited to:

Identity Validation Keys

- Birth date (full: mm-dd-yy)
- Birth date (partial: mm-dd only)
- Mother's maiden name

Student Information

- Educational records (excludes directory information)
 - Home or mailing address
 - Personal telephone numbers
 - Personal email address
 - Ethnicity
 - Gender
 - Birthplace
 - Grades



CALIFORNIA STATE UNIVERSITY, LONG BEACH

- Courses taken
- Schedule
- Test Scores
- Advising records
- Educational services received
- Disciplinary actions
- Student identification number

Non-directory student information **may not be released except with Enrollment Services approval** under prescribed conditions.

Alumni Information

- Same as Student Information

Employee Information

- Net salary
- Employment history
- Home address
- Personal telephone numbers
- Personal email address
- Parents and other family members names
- Payment history
- Performance evaluations
- Background investigations
- Biometric information
- Electronic or digitized signatures
- Private key (digital certification)
- Birthplace (City, State, country)
- Ethnicity
- Gender
- Marital Status
- Personal characteristics
- Physical description
- Photograph
- Employee identification number

Job Applicant Information

- Same as Employee Information

University Donor Information

- Name
- Home or mailing address
- Personal telephone numbers
- Personal email address

Legal Information

- Legal investigations conducted by the University

Contract Information

- Sealed bids

University Research

- Trade secrets or intellectual property



CALIFORNIA STATE UNIVERSITY, LONG BEACH

Library Patron Information

- Information which links a library patron with a specific subject the patron has accessed or requested

Facilities Information

- Building plans and architectural drawings

Emergency Preparedness Information

- Locations of hazardous materials or similar assets
- Emergency Operations Plan

Level 3: Public

This is information that is generally regarded as publicly available. Information at this level is either explicitly defined as public information or intended to be available to individuals both on and off campus or not specifically classified elsewhere in this standard. Knowledge of this information does not expose CSULB to financial loss or jeopardize the security of CSULB's information assets. Level 3 information may be subject to appropriate campus review or disclosure procedures to mitigate potential risks of inappropriate disclosure. Level 3 information includes, but is not limited to:

Student Information

- Name
- Major field of study
- Grade level
- Enrollment status
- Participation in officially recognized sports/activities
- Weight and height of athletic team members
- Dates of attendance
- Degrees, honors and awards received
- E-mail address
- Most recent or previous college/university attended

Note: The University may disclose the above information without prior written consent, unless the student has requested that certain information not be released (non-disclosure).

Employee Information

- Title
- Public E-mail address
- Work location and telephone number
- Employing department
- Position classification
- Gross salary
- Name (first, middle, last)(except when associated with confidential information)

Financial Information

- Budget information

VI. INFORMATION PROTECTION STANDARD

This table describes the protection measures required for each information classification level.

	Confidential	Internal Use	Public
	Level 1	Level 2	Level 3



CALIFORNIA STATE UNIVERSITY, LONG BEACH

	Confidential Level 1	Internal Use Level 2	Public Level 3
Handling	<p>Visual Disclosure: Ensure that documents and screens are positioned to prevent inadvertent disclosure. Do not leave documents and screens unattended.</p> <p>Paper or removable media must be stored in a locked enclosure when not in use.</p> <p>Computer Printing: Remove printouts immediately if using an internal shared printer.</p>	Same as Level 1	No restrictions
Transmitting	<p>Distribution: Limited to those employees with an established business need-to-know and are either CSULB employees or who someone who has signed a confidentiality agreement.</p> <p>Electronic Mail (email or attachments to email): May be sent within the CSULB email system (@csulb.edu) but not over a public network unless password protected or encrypted.</p> <p>All email transmissions of confidential information must contain the follow statement: "The information contained in this email message or its attachment is confidential. Dissemination or copying of this email is strictly prohibited. If you think that you have received this email in error, please email the sender."</p>	<p>Distribution: Transmission only to CSULB employees and those individuals with a business need-to-know.</p> <p>Electronic Mail (email or attachments to email): May be sent within the CSULB email system (@csulb.edu) or over a public network to persons with a business need-to-know.</p>	No restrictions



CALIFORNIA STATE UNIVERSITY, LONG BEACH

	Confidential Level 1	Internal Use Level 2	Public Level 3
	<p>Mail (hard copy): Printed information may be sent through intercampus or U.S. mail but must be sealed in a plain envelope clearly marked, "To be Opened by Addressee Only".</p> <p>FAX: Authorized only from and to CSULB FAX machines. Information may not be sent to public FAX machines.</p> <p>Telephone: Authorized, but only to CSU employees and others with a business need-to-know.</p>	<p>Mail (hard copy): Printed information may be sent through intercampus or U.S. mail with no special markings or handling.</p> <p>FAX: Same as Level 1.</p> <p>Telephone: Same as Level 1.</p>	
Storage	<p>Must be stored on secured databases or file servers. When access to a secure server is not available and when approved by the employee's Appropriate Administrator, Level 1-Confidential Information may be stored on laptops, desktops or portable electronic storage media, including but not limited to, CD-ROMs, DVD-ROMs, external hard drives, zip disks, floppy disks, reel and cassette format magnetic tapes, flash-memory cards, magnetic cards and USB flash drives (a.k.a. Memory Sticks, Thumb or Jump Drives).</p> <p>Laptops, desktops and portable electronic storage media must be encrypted or otherwise rendered unreadable and unusable by unauthorized persons</p>	<p>When stored on CSULB property, no special requirements. If transported off-campus, appropriate care must be taken to prevent disclosure or theft.</p>	<p>No restrictions</p>



CALIFORNIA STATE UNIVERSITY, LONG BEACH

	Confidential Level 1	Internal Use Level 2	Public Level 3
	<p>and must be located in a secure location at the University or another site approved by ITS management (including off-site backup services).</p> <p>Level 1 information may not be stored on personal equipment such as personal laptops, personal desktops, personal digital assistants (PDAs) iPods® or cell phones (such as BlackBerry®, Treo®, and iPhones®).</p> <p>See <i>Note 1</i> for prohibitions regarding the storage of specific Payment Related Data.</p> <p>Printed information must be stored in a locked enclosure.</p>		
Retention	Records of any type of medium, such as paper, microfiche, magnetic, or optical, shall not be retained beyond the minimum retention period identified in the CSU Record Retention Schedule.	Same as Level 1	Same as level 1
Destruction	Destroy in accordance with CSULB Media Sanitation Standard, August 2006.	Same as Level 1	Normal waste disposal

Note 1: Payment Related Data

The Primary Account Number (PAN) may not be stored unless encrypted.

The following types of payment related data may not be stored even if encrypted:

- (1) Sensitive authentication data, which includes, but is not limited to, all of the following:
 - a. The full contents of any data track from a payment card or other payment device
 - b. The card verification code or any value used to verify transaction when the payment device is not present
 - c. The personal identification number (PIN) or the encrypted PIN block
- (2) Any payment related data that is not needed for business purposes.
- (3) Any of the following data elements:
 - a. Payment verification code
 - b. Payment verification value
 - c. PIN verification value