



CALIFORNIA STATE UNIVERSITY, LONG BEACH

Subject: Records Management Standard		Reference No.:
Department: Information Security Management and Compliance		Issue Date: September 2008
Division: Administration and Finance		Revision Date: May 2009
References: <ul style="list-style-type: none"> • CSU Records Access Manual • CSU Subpoena Handbook • CSU Executive Order 1031, Systemwide Records/Information Retention Schedules • Government Code Section 6250-6270 • Fair and Accurate Credit Transactions Act of 2003 (FACTA); FCRA, 15 U.S.C. 1681 et seq. • California Civil Code §1798.81 		Expiration Date: N/A
Web Links: <ul style="list-style-type: none"> • http://daf.csulb.edu/offices/vp/information_security 		

STANDARD CONTENTS

- Information Classification
- Information Protection
- Information Retention
- Information Disposition
- Public Records Requests
- Record Subpoenas
- Definitions

I. INTRODUCTION

California State University, Long Beach is committed to effective records management which includes, but is not limited to, the appropriate classification and protection of records from unauthorized use, access, disclosure, modification, loss or deletion; the retention of records to meet legal and regulatory requirements; and the appropriate disposition of records when their retention is no longer necessary.

II. SCOPE

This Standard applies to all records, regardless of medium that are collected, generated, and/or maintained by California State University, Long Beach except where superseded by grant, contract, or federal copyright law and to all employees of CSULB and CSULB auxiliary organizations.

III. INFORMATION CLASSIFICATION

The California State University identifies three (3) classification levels of information based on the value, legal requirements, sensitivity and criticality assigned to them. These levels are:

- Level 1 - Confidential
- Level 2 - Internal Use or Enterprise
- Level 3 - Public

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

Level 1 – Confidential

This is information maintained by the University which is exempt from disclosure under the provisions of the California Public Records Act or other applicable state or federal laws. The unauthorized use, access, disclosure, acquisition, modification, loss, or deletion of confidential information could result in severe damage to CSULB, its students, employees, or customers. Financial loss, damage to CSULB's reputation, and legal action could occur. Confidential information is intended solely for use within CSULB and limited to those with a "business need-to-know." Disclosure of confidential information to persons outside of the University is governed by specific standards and controls designed to protect the information.

Level 2 – Internal Use

This is information which must be protected due to proprietary, ethical or privacy considerations. Although not specifically protected by statute, regulation, or other legal obligations or mandates, unauthorized use, access, disclosure, acquisition, modification, loss or deletion of information at this level could result in financial loss, damage to CSULB's reputation, violate an individual's privacy rights or legal action could occur.

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. Knowledge of this information does not expose CSULB to financial loss or jeopardize the security of CSULB's information assets. Prior to disclosure, public information may be subject to appropriate campus review or procedures to mitigate any potential risks of inappropriate disclosure.

Identification of information classified at each level is found in **Attachment A – Information Classification**.

Roles and Responsibilities

Roles and responsibilities associated with Information Classification are as follows:

The CSU Office of the Chancellor is responsible for identifying Level 1 – Confidential Information.

University Information Security Officer Is responsible for assisting Division Information Security Officers in the identification of information types within their respective area and determining classification levels. The University Information Security Officer is also responsible for conducting an annual review of this Standard and amending it as appropriate.

Division Information Security Officers are responsible for guiding compliance with this Standard within their respective college, department, administrative area, or organization.

IV. INFORMATION PROTECTION

Information must be protected when handled, transmitted, stored, and disposed based on its classification level. Safeguards to protect university information assets are found in **Attachment B – Information Protection Requirements**.

Roles and Responsibilities

Roles and responsibilities associated with information protection are as follows:

Information Custodians are responsible for ensuring that access to and protection of information and the file systems that host them are in compliance with this Standard.

V. INFORMATION RETENTION

Retention Period

Records shall be retained for the minimum time periods indicated in the CSU or CSULB *Records Retention and Disposition Schedules*. Retention periods are counted from the date of creation of the record, unless other instructions (e.g., "3 years from termination") are noted in the records retention schedule.

Modification of CSU Records Retention and Disposition Schedules

The campus may modify the *CSU Records Retention and Disposition Schedules*, as needed, by incorporating records unique to the campus. The CSU Schedules may not be otherwise abridged or altered.

Information concerning campus specific records shall be provided to the Director, Information Security Management and Compliance and shall include the record title and the records series to which the record shall be added (e.g., University Police, Personnel/Payroll). Information shall also include the identification of the custodian of record, record value, retention source authority, and the retention period.

Roles and Responsibilities

The roles and responsibilities associated with records retention are as follows:

Custodian of Records are responsible for identifying records unique to the campus which are not included in the *CSU Records Retention and Disposition Schedules* and for ensuring appropriate and timely disposal of records in accordance with CSU or campus retention and disposition schedule timeframes.

The **Director, Information Security Management and Compliance** is responsible for “publishing” the *CSULB Records Retention and Disposition Schedules* and for providing copies to the Office of the Chancellor upon request.

VI. RECORDS DISPOSITION

Disposition of records shall be conducted in a timely manner following the retention period and based on their information classification level.

Failure to adhere to disposition schedules can lead to the unnecessary expenditure of resources to store, maintain, search for, and produce records. Records not disposed of at the end of their retention period remain subject to records requests under statute or legal proceedings.

Determining Disposition Date

Retention periods are counted from the date of creation of the record, unless other instructions (e.g., “3 years from termination”) are noted in the Records Retention Schedule. Disposition would normally occur following the end of the month of year that marks the end of the retention period; thus, disposition of a record for which the retention period ends on July 10 would take place as soon after July 31 as practicable.

Cautions Regarding Disposition

There may be conditions under which records destruction **must** be deferred even if they have reached or exceeded the end of their retention period. These conditions include:

1. External requirements under state and federal laws or regulation or when grants or contracts retention periods override University retention periods;
2. Records that have been requested pursuant to statute or legal proceedings (e.g., California Public Records Act, Subpoena);
3. Records that have not been requested but are deemed likely to be requested pursuant to statute or legal proceedings including potential litigation must be retained following notification by the campus Risk Manager.
4. Records related to on ongoing investigation must not be disposed of without prior consultation with campus counsel.

Disposition Based on Classification Level

To protect the confidentiality of information and the related privacy rights of CSULB students, faculty, staff, donors, patrons, vendors, and others, Level 1 and Level 2 information contained in all software and/or computer files, storage media devices and hard copy must be sanitized prior to disposal. The sanitization process ensures that recovery of information is not possible. Several methods can be used to sanitize media; however, the two major types of sanitization are clearing and destroying.

Clearing – Clearing information is a level of media sanitization that protects the confidentiality of information against a robust keyboard attack. Simple deletion of items does not suffice for clearing. Clearing must not allow information to be retrieved by data, disk, or file recovery utilities and must be resistant to keystroke recovery attempts executed from standard input devices and from data scavenging tools. Overwriting is an acceptable method for clearing media. The security goal of overwriting is to replace written data with random data.

There are several overwriting software products to overwrite storage space on media. CSULB Network Services provides software tools and instructions to securely clean the data from ATA based hard drives and other storage media. Overwriting cannot be used for media that are damaged or not rewritable. In such cases, media should be destroyed.

Destroying – Destruction of media is the ultimate form of sanitization. After media are destroyed, they cannot be reused as originally intended. Physical destruction can be accomplished using a variety of methods. Hard copy destruction can be accomplished using a variety of methods, with cross-cut shredding being the most common practice. Straight cut shredding is not a compliant destruction method. Departments may shred media on site or contact Procurement and Support Services for a listing of approved document destruction vendors.

Recommendations for sanitizing media types are found in **Attachment C – Media Sanitization Methods**.

VII. PUBLIC RECORDS REQUESTS RESPONSE PROCEDURES

The purpose of the California Public Records Act (Act)s to promote “access to information concerning the conduct of the people’s business which is a fundamental and necessary right of every person in this state.” Further, the California constitution makes clear that the public’s rights of access must be broadly construed and all exceptions narrowly construed.

There can be confusion about what constitutes a request under the Act. Obviously, something in writing that formally references the Act constitutes such a request. However, something less formal, which does not reference the Act constitutes a request. A Public Records Act request does not have to be in writing and may be made orally. However, for purposes of clarity, an individual should be asked to make the request in writing. When necessary, the record owner may be required to assist the requestor in making a focused and effective request that reasonably identifies a record or records.

All records maintained by the University are potentially subject to disclosure under this Act, including those in electronic and hard copy. There are numerous exceptions established by the Act and it is extremely important that records which are excluded from disclosure are not disclosed to the public.

A person who has been denied access to a public record may file a lawsuit to enforce his/her right to inspect or receive a copy of the public record. If the court finds that refusal to disclose the record was unjustified, the court may enter an order requiring its disclosure. The court may also order the University to pay reasonable attorneys’ fees and court costs.

To ensure that the University produces records in accordance with the Act and does not produce records which are excluded from disclosure under the Act, University procedures which comply with both the Act and CSU policy have been established.

Procedures

These procedures are provided in general terms as the appropriate University response may vary based on the request. The Office of Information Security Management and Compliance will work closely with the records owner to ensure that the University response is made in accordance with the Act.

1. All requests for University Records requested under the California Public Records Act received by a University office or employee must promptly be forwarded to the Office of Information Security Management and Compliance. Since the University has a legal obligation to acknowledge the request in writing within ten days from receipt, it is extremely important to avoid any delay in providing the request to the Office of Information Security Management and Compliance.

2. The Office of Information Security Management and Compliance will take necessary action to ensure that the University meets all legal requirements of the Act including, but not limited to,
 - determining whether or not the records requested are subject to the Act;
 - providing written response to the requester within 10 days*;
 - providing notice to the Office of General Counsel; and
 - providing additional written notifications to the requestor as required by the Act.

*Note: It is not necessary to provide the actual requested records with the ten-day initial response time. If records are available for disclosure, they must be made available for inspection or copying within a **reasonable** amount of time based on their volume and complexity.

3. When a determination has been made that the records requested are subject to the Act, the Office of Information Security Management and Compliance will work with the record's owner to produce and provide the record or to make the record available for inspection.

VIII. RECORD SUBPOENAS

The University has instituted the following procedures for handling "Records Only" and "Appearance and Records" subpoenas. These procedures are intended to avoid the release of information in response to an invalid subpoena. The release of personal information in response to an invalid subpoena is a violation of the privacy of the person or persons whose personal information is released and may subject the University to legal liability.

Process servers attempting to serve a "Records Only" or "Appearance and Records" subpoena should be directed to the appropriate University Records Custodian. Only these individuals/positions are authorized to accept, respond to, or release University records / information.

Student Records/Information

Director of Judicial Affairs
Office of the Vice President for Student Services, BH 377

Faculty Personnel (includes librarians and coaches) Records/Information

Associate Vice President for Academic Personnel
Office of the Vice President for Academic Affairs, BH 303

Staff Personnel Records/Information (including payroll records for all employees)

Director, Staff Human Resources and Employee Relations
Human Resources Management, BH 335

Non-Personnel Records or where it is not possible to determine the specific subject of the request

Director, Information Security Management and Compliance
FM/SRM

IX. DEFINITIONS

Appearance and Records Subpoena – A legal document which requires the University to produce documents and provide personal attendance of a witness.

Cardholder Data – Information contained on a credit card including the cardholder name, the primary account number (PAN), service code, expiration date, full magnetic stripe data, CAV/CVC2/CVV2/CID, and PIN/PIN blocks.

CSU Records Retention Schedule – A CSU document lists and governs the retention period of identified records that are common within the CSU. The *CSU Records Retention Schedules* are published on line and can be found at the CSU Records/Information Retention and Disposition website, www.calstate.edu/recordsretention.

CSU Long Beach Records Retention Schedule – A document that identifies records unique to CSULB.

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 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.

Media – A general term referring to the material on which business information has been recorded and may subsequently be used for business purposes.

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, 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.

Protected Health Information – Individually identifiable information created, received, or maintained by health care providers or health plans sufficient to allow identification of the individuals 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.

Public Record – Any writing containing information relating to the conduct of the public's business which has been prepared, owned, used, or retained by the University regardless of physical form or characteristics.

Record – Any recording upon any tangible thing in any form of communication or presentation, including letters, words, pictures, sounds, or symbols, or any combination of these or other means to engage in business, regardless of media.

Records Disposition – The discarding or abandonment of information or the sale, donation, or transfer of any medium, including computer equipment, upon which information which has reached the end of its retention period is stored.

Records Only Subpoena – A legal document which requires the university to produce documents.

Record Retention – The maintenance of records for prescribed time periods.

Retention Period – The minimum period of time that a record must be kept.

Record Value – The importance or usefulness of a record to the University. Records may have value in one or more of the following areas:

Operational – Required by a campus/department to perform its primary function

Legal – Required to be kept y law or many be needed for litigation or investigation

Fiscal – Related to the financial transactions of the campus, especially those required for audit or tax purposes.

Historical - Long term value to document past events.

Vital – Critical to maintain or ensure operational continuity for the campus after a disruption or disaster. Vital records or information may fall into any one of the above value categories.

Subpoena –A legal document that directs the University or an employee of the University to attend at a specific time and place to testify as a witness, and/or to produce documents or other tangible objects in a legal proceeding.

Writing – Any handwriting, typewriting, printing, photostating, photographing, photocopying, transmitting by electronic mail or facsimile, and every other means or recording upon any tangible thing and 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.

FURTHER INFORMATION

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

The CSU classification level identifies the following records and their classifications.

LEVEL 1: CONFIDENTIAL

Information includes but is not limited to:

Personal Information

- Passwords or credentials
- Notice-triggering Personal Information
- Biometric Information
- Electronic or digitized signatures
- Private Key (digital certificate)
- Psychological counsel records
- Forms of national or international identification (such as passports, visas, etc.), in combination with name

Cardholder Data

Medical Information

Health Insurance Information

Financial Information

Protected Health Information

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

Legal Information

- Legal investigations conducted by the University
- Attorney/Client communications

Contract Information

- Sealed bids
- Third party proprietary information per contractual agreement

LEVEL 2: INTERNAL USE

Information includes, but is not limited to:

Identity Validation Keys

- Birth date (full: mm-dd-yy)
- Birth date (partial: mm-dd only)

Student/Alumni Information

- Educational records (excludes directory information)
 - Grades
 - Courses taken
 - Schedule
 - Test Scores
 - Advising records
 - Educational services received
 - Disciplinary actions

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
- Mother's maiden name
- Biometric information
- Electronic or digitized signatures
- Birthplace (City, State, country)
- Race and Ethnicity
- Gender
- Marital Status
- Physical description
- Photograph

Alumni Information

- Same as Employee Information

Job Applicant Information

- Same as Employee Information

University Donor Information

- Same as Employee Information

University Research

- Trade secrets or intellectual property

Library Patron Information

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

Other

- Location of critical or protected assets
- Licensed software

LEVEL 3: PUBLIC

Information includes, but is not limited to:

Campus Identification Keys

- Campus identification number
- User ID (do not list in a public or an aggregate list when it is not the same as the student email address)

Student Information

Educational directory Information (FERPA)

- Name
- Major field of study
- Grade level
- Enrollment status
- Dates of attendance
- Degrees, honors and awards received
- E-mail address
- Home or mailing address
- Personal telephone numbers

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).

Addresses and telephone numbers for currently enrolled students will be released to CSULB personnel and units solely for the purpose of conducting legitimate University business. They may not be shared with individuals or organizations outside the University except in accordance with the provisions immediately below:

Addresses and telephone numbers may be released for non-commercial use by individuals or organizations outside the University provided the request for such information has been reviewed and approved by the appropriate University personnel. Requests from the academic offices of accredited educational institutions shall be reviewed by the Provost and Senior Vice President for Academic Affairs or designee. All other requests shall be reviewed by the Vice President for Student Services or designee.

In addition to the above, the Director of Athletics may provide information concerning participation of students in athletic events including the height and weight of athletes.

Employee Information (including student employees)

- Title
- Status as a student employee (such as TA, GA, ISA)
- Campus e-mail address
- Work location and telephone number
- Employing department
- Position classification
- Gross salary
- Name (first, middle, last)(except when associated with confidential information)
- Signature

Attachment B
Information Protection Requirements

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

	Confidential Level 1	Internal Use Level 2	Public Level 3
Handling	Please refer to the Clean Desk and Clear Screen Standard .	Same as Level 1	No restrictions
Transmitting	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.	Distribution: Transmission only to CSULB employees and those individuals with a business need-to-know.	No restrictions
	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. 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."	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.	
	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".	Mail (hard copy): Printed information may be sent through intercampus or U.S. mail with no special markings or handling.	
	FAX: Authorized only from and to CSULB FAX machines. Information may not be sent to public FAX machines.	FAX: Same as Level 1.	
	Telephone: Authorized, but only to CSU employees and others with a business need-to-know.	Telephone: Same as Level 1.	

	Confidential Level 1	Internal Use Level 2	Public Level 3
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 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 Note 1 for prohibitions regarding the storage of specific Payment Related Data.</p> <p>Printed information must be stored in a locked enclosure.</p>	Same as Level 1.	No restrictions
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
Disposition	Dispose in accordance with the Attachment C – Media Sanitization Methods.	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

Media Type	Method
Hard Copy Storages	
Paper	Destroy.
Microforms	Destroy.
Hand-Held Devices	
Cell Phones	Manually delete all information, then perform a full manufacturer's reset to reset the cell phone back to its factory default settings.
Personal Digital Assistant (PDA) (Palm, PocketPC, other)	Manually delete all information, then perform a manufacturer's hard reset to reset the PDA to factory state.
Equipment	
Copy Machines	Perform a full manufacturer's reset to reset the copy machine back to its factory default settings
Fax Machines	Perform a full manufacturer's reset to reset the fax machine back to its factory default settings
Magnetic Disks	
Floppies	Overwrite media by using university-approved and validated overwriting technologies/methods/tools.
IDE Hard Drives	Overwrite media by using university-approved and validated overwriting technologies/methods/tools.
Serial ATA Drives	Overwrite media by using university-approved and validated overwriting technologies/methods/tools.
Zip Disks	Overwrite media by using university-approved and validated overwriting technologies/methods/tools.
SCSI Drives	Overwrite media by using university-approved and validated overwriting technologies/methods/tools.
Reel and Cassette Format Magnetic Tapes	<p>Clear magnetic tapes by either re-recording (overwriting) or degaussing. Clearing a magnetic tape by re-recording (overwriting) may be impractical for most applications since the process occupies the tape transport for excessive time periods.</p> <p>Clearing by Overwriting: Overwriting should be performed on a system similar to the one that originally recorded the data. For example, overwrite previously recorded classified or sensitive VHS format video signals on a comparable VHS format recorder. All portions of the magnetic tape should be overwritten one time with known nonsensitive signals.</p>

Media Type	Method
Optical Disks	
CDs	Destroy.
DVDs	Destroy.
Memory	
Compact Flash Drives or USB/Memory Sticks	Overwrite media by using university approved and validated overwriting technologies/methods/tools.
Other Memory Devices	Contact your area computer technician or the campus Assistant Information Security Officer at 985-4862 for the best method of sanitization.
Magnetic Cards	
Flash Cards	Perform a full chip purge as per manufacturer's data sheets.
Magnetic Cards	Overwrite media by using university-approved and validated overwriting technologies/methods/tools.
Personal Computer Memory Card International Association (PCMCIA) Cards	Overwrite media by using university-approved and validated overwriting technologies/methods/tools.
Smart Cards	Overwrite media by using university-approved and validated overwriting technologies/methods/tools.
RFID	Overwrite media by using university-approved and validated overwriting technologies/methods/tools.
Items Not Listed Above	
Unlisted Technologies	For electronic technologies not listed in the above table, please contact the campus Assistant Information Security Officer at 985-4862.

For further information or assistance, contact your designated computer technician or the campus Assistant Information Security Officer at 562-985-4862.