I. PURPOSE
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.

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of medium that are collected, generated, and/or maintained by California State University, Long Beach except where superseded by grant, contract, or federal copyright law and to all employees of CSULB and CSULB auxiliary organizations.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

*Written form is defined as 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.
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 1 Confidential Information includes but is not limited to:

Personal Information

Notice-triggering Personal Information
1. 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:
   a. Social Security Number.
   b. Driver’s license or California identification card number.
   c. Account 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.
   d. Medical information.
   e. Health insurance information.
   f. Information or data collected through the use or operation of an automated license plate recognition system, as defined in CA Civil Code §1798.90.5.

2. A user name or email address, in combination with a password or security question and answer that would permit access to an online account
   - Biometric Information
   - Electronic or digitized signatures
   - Private Key (digital certificate)
   - Medical and Psychological counseling records
   - Forms of national or international identification (such as passports, visas, etc.), in combination with name
   - Criminal background check results
   - Passwords or credentials

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.

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

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.

1 California State Law and other legal statutes, such as the Health Information Portability and Accountability Act (HIPAA), require notification to individuals in the event of a security breach of certain personal information. The campus refers to this as Notice-triggering Personal Information
**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.

**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.

**Technical Security Information**
Vulnerability/security information related to campus systems or services.

**Law Enforcement Information**
- Law enforcement records related to an individual
- Law enforcement home address information

**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**
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 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)

**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/Alumni Information
- Educational records (excludes Directory Information as defined by FERPA)
  - Grades
  - Courses taken
  - Schedule
  - Test Scores
  - Advising records
  - Educational services received
  - Disciplinary actions
  - Student photo

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
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.

Level 3 Public Information includes, but is not limited to:

Student Information
Educational Directory Information (as defined by 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
V. INFORMATION PROTECTION REQUIREMENTS

Information must be protected when handled, transmitted, stored, and disposed based on its classification level. Safeguards to protect university information assets are found in the below matrix.

This matrix describes the protection measures required for each information classification level:

<table>
<thead>
<tr>
<th></th>
<th>Confidential Level 1</th>
<th>Internal Use Level 2</th>
<th>Public Level 3</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Handling</strong></td>
<td>Please refer to the Clean Desk and Clear Screen Standard.</td>
<td>Same as Level 1</td>
<td>No restrictions</td>
</tr>
<tr>
<td><strong>Transmitting</strong></td>
<td>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.</td>
<td>Distribution: Transmission only to CSULB employees and those individuals with a business need-to-know.</td>
<td>No restrictions</td>
</tr>
<tr>
<td><strong>Electronic Mail (email or attachments to email):</strong></td>
<td>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.”</td>
<td>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.</td>
<td></td>
</tr>
<tr>
<td><strong>Mail (hard copy):</strong></td>
<td>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”.</td>
<td>Mail (hard copy): Printed information may be sent through intercampus or U.S. mail with no special markings or handling.</td>
<td></td>
</tr>
<tr>
<td><strong>FAX:</strong></td>
<td>Authorized only from and to CSULB FAX machines. Information may not be sent to public FAX machines.</td>
<td>FAX: May be sent within the CSULB email system (@csulb.edu) or over a public network to persons with a business need-to-know.</td>
<td></td>
</tr>
<tr>
<td><strong>Telephone:</strong></td>
<td>Authorized, but only to CSU employees and others with a business need-to-know.</td>
<td>Telephone: Same as Level 1.</td>
<td></td>
</tr>
<tr>
<td><strong>Storage</strong></td>
<td>Must be stored on secured databases or file servers. When access to a secure server is not available and when approved by the appropriate administrator, Level 1-Confidential Information may be stored on University owned laptops, desktops or portable electronic storage media. In such cases, laptops, desktops and portable electronic storage media storing level 1 data must be <strong>encrypted</strong> and <strong>tagged</strong> according to the university’s Property Management procedures. If desktops used to process Level 1 data (not store) are in a secured campus office that only allows authorized access, the appropriate administrator may choose not to encrypt the desktop. This decision needs to be documented and approved in</td>
<td>Storage on secured databases or file servers strongly recommended. May be stored on University owned laptops, desktops or portable electronic storage media. Password protection required. Please refer to the <strong>Password Standard</strong>.</td>
<td>No restrictions</td>
</tr>
</tbody>
</table>

No restrictions
Confidential
Level 1

writing by the employee’s Appropriate Administrator and the University Information Security Officer. See Note 2.

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®).

See Note 1 for prohibitions regarding the storage of specific Payment Related Data.

Printed level 1 information must be secured in a locked enclosure.

Internal Use
Level 2

personal desktops, personal digital assistants (PDAs) iPods® or cell phones (such as BlackBerry®, Treo®, and iPhones®).

Public
Level 3

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.

Disposal

Proper Media Sanitization Methods are described, below.

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

Note 2:
If an unencrypted computer or hard drive with level 1 data is missing (stolen or lost), the University is required by law to activate security breach protocol/procedure. The department will have to bear the costs related to the breach notification requirements.

VI. INFORMATION DISPOSAL REQUIREMENTS
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.
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.

For additional information regarding the disposal of electronic storage media, please refer to the CSULB Electronic Media Sanitization Process.

The matrix below describes the disposal methods for various media containing level 1 and level 2 data/records:

<table>
<thead>
<tr>
<th>Media Type</th>
<th>Method</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Hard Copy Storages</strong></td>
<td></td>
</tr>
</tbody>
</table>
| Paper                             | Physically destroy by shredding (cross-cut shredder) or campus authorized document destruction service contractor.  
                                             *Please refer to Purchasing for the current document destruction service contractor. Purchasing Front Desk 5-4296.* |
| Microforms                        | Physically destroy by shredding (cross-cut shredder) or campus authorized document destruction service contractor.  
                                             *Please refer to Purchasing for the current document destruction service contractor. Purchasing Front Desk 5-4296.* |
| **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 Memory Storage**       |                                                                        |
| Floppies                          | Overwrite by using university-approved and validated overwriting technologies/methods/tools, or degauss.  
                                             For more information refer to the CSULB Electronic Media Sanitization Process. |
| IDE (Integrated Drive Electronics) Hard Drives | Overwrite by using university-approved and validated overwriting technologies/methods/tools, or degauss.  
                                             For more information refer to the CSULB Electronic Media Sanitization Process. |
| Serial ATA (Advanced Technology Attachment) Drives | Overwrite by using university-approved and validated overwriting technologies/methods/tools, or degauss.  
                                             For more information refer to the CSULB Electronic Media Sanitization Process. |
<table>
<thead>
<tr>
<th>Media Type</th>
<th>Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>Zip Disks</td>
<td>Overwrite by using university-approved and validated overwriting technologies/methods/tools, or degauss.</td>
</tr>
<tr>
<td></td>
<td>For more information refer to the CSULB Electronic Media Sanitization Process.</td>
</tr>
<tr>
<td>SCSI (Small Computer System Interface) Drives</td>
<td>Overwrite by using university-approved and validated overwriting technologies/methods/tools, or degauss.</td>
</tr>
<tr>
<td></td>
<td>For more information refer to the CSULB Electronic Media Sanitization Process.</td>
</tr>
<tr>
<td>Reel and Cassette Format Magnetic Tapes</td>
<td>Clear magnetic tapes by either re-recording (overwriting) or degaussing.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td>Magnetic Cards</td>
<td>Overwrite media by using university-approved and validated overwriting technologies/methods/tools, or physically destroy by shredding.</td>
</tr>
<tr>
<td>Optical Disks</td>
<td></td>
</tr>
<tr>
<td>CDs</td>
<td>Physically destroy by shredding.</td>
</tr>
<tr>
<td>DVDs</td>
<td>Physically destroy by shredding.</td>
</tr>
<tr>
<td>Static Memory Storage</td>
<td></td>
</tr>
<tr>
<td>Compact Flash Drives or USB/Memory Sticks</td>
<td>Overwrite media by using university approved and validated overwriting technologies/methods/tools.</td>
</tr>
<tr>
<td>Flash Cards</td>
<td>Perform a full chip purge as per manufacturer’s data sheets.</td>
</tr>
<tr>
<td>Smart Cards</td>
<td>Overwrite media by using university-approved and validated overwriting technologies/methods/tools.</td>
</tr>
<tr>
<td>PCMCIA (Personal Computer Memory Card International Association Cards)</td>
<td>Overwrite media by using university-approved and validated overwriting technologies/methods/tools.</td>
</tr>
<tr>
<td>RFID (Radio-Frequency Identification)</td>
<td>Overwrite media by using university-approved and validated overwriting technologies/methods/tools.</td>
</tr>
<tr>
<td>Items Not Listed Above</td>
<td></td>
</tr>
<tr>
<td>Other Memory Devices</td>
<td>Contact your area computer technician or the campus Assistant Information Security Officer at 5-4862 for the best method of sanitization.</td>
</tr>
<tr>
<td>Unlisted Technologies</td>
<td>For electronic technologies not listed in the above table, please contact the campus Assistant Information Security Officer at 5-4862.</td>
</tr>
</tbody>
</table>

For further information or assistance, contact your designated computer technician or the campus Assistant Information Security Officer at 562-985-4862 or iso@csulb.edu.
**Revision History**

<table>
<thead>
<tr>
<th>Revision Date</th>
<th>Revised By</th>
<th>Summary of Revisions</th>
<th>Section(s) Revised</th>
</tr>
</thead>
</table>
| January 16, 2014 | Aysu Spruill, Director of Internal Auditing Services/Campus Information Security Officer | Added new item to notice-triggering information, as amended by CA senate bill 46:  
2) A user name or email address, in combination with a password or security question and answer that would permit access to an online account  
See SB 46 Senate Floor Analysis, dated 9/3/2013.  
This bill expands the scope of personal information subject to existing security breach disclosure requirements to include a user name or email address, in combination with a password or security question and answer that permits access to an online account. This bill also imposes additional requirements on the disclosure of a breach of the security of the system or data in situations where the breach involves personal information that permits access to an online or email account. | Level 1 - confidential list |
“In such cases, laptops, desktops and portable electronic storage media storing level 1 data must be encrypted and tagged according to the university’s Property Management procedures.”  
Added revised language to Level 2 Storage. “Storage on secured databases or file servers strongly recommended.  
May be stored on University owned laptops, desktops or portable electronic storage media. Password protection required. Please refer to the Password Standard.”  
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®).” |
<table>
<thead>
<tr>
<th>Revision Date</th>
<th>Revised By</th>
<th>Summary of Revisions</th>
<th>Section(s) Revised</th>
</tr>
</thead>
<tbody>
<tr>
<td>September 28, 2016</td>
<td>Gene Wohlgezogen, Asst. Information Security Officer</td>
<td>Added part “f” addressing License Plate Recognition to “Notice-triggering Personal Information,” per Senate Bill No. 34, enacted October 6, 2015.</td>
<td>Section IV</td>
</tr>
</tbody>
</table>

**Review/Approval History**

<table>
<thead>
<tr>
<th>Review Date</th>
<th>Reviewed By</th>
<th>Action (Reviewed, Recommended or Approved)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/17/2014</td>
<td>Mary Stephens, VP Administration and Finance</td>
<td>Approved</td>
</tr>
<tr>
<td>12/11/15</td>
<td>Ted Kadowaki, AVP Budget And University Services</td>
<td>Approved</td>
</tr>
</tbody>
</table>