Information Security

Background and Purpose

The Associated Students, Incorporated (ASI) recognizes its affirmative and continuing obligation 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 ASI's mission, violate individual privacy rights, and possibly constitute a criminal act.

The purpose of ASI's Policy on Information Security is to define the principles to which all directors, officers, agents, and employees of the Associated Students, Incorporated (ASI) must adhere when handling information owned by or entrusted to Associated Students, Incorporated in any form. These principles cover the following areas:

- Defining the confidentiality, integrity and availability requirements for information used to support ASI's operations,
- Ensuring that those requirements are effectively communicated to individuals who come in contact with such information, and
- Collecting, using, managing, and disposing of such information – whether electronically or physically - in a manner that is consistent with those requirements.

Policy

It is the policy of the Associated Students, Incorporated that all information gathered and maintained by directors, officers, agents and employees of Associated Students, Incorporated for the purpose of conducting ASI business is, by definition, corporate information. As such, each individual who uses, stores, processes, transfers, administers and/or maintains this information is responsible and will be held accountable for its appropriate use and disposal. In summary, anyone who handles such information must:

- Abstain from divulging, copying, releasing, selling, loaning, reviewing, altering or destroying any information except as properly authorized within the scope of one's professional activities and authority.
- Take appropriate measures to protect information wherever it is located, e.g., held on physical documents, stored on computer media, communicated over voice or data networks, exchanged in conversation, etc.

- Safeguard any physical key, ID card, or computer/network account that permits access to information. This includes creating computer passwords that satisfy the requirements of ASI's Policy on Information Assets, Password Standards.

- Render unusable any confidential information held on any physical document or computer storage medium (e.g., diskette, CD, magnetic tape, hard disk) that is being discarded.

- Report any activities that may compromise confidential information to Executive Director and the CSULB Office of Information Security Management and Compliance.

ASI's Information Security Policy applies to all of the following:

- Information assets that are acquired, transmitted, processed, transferred and/or maintained by ASI

- 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 management, staff, students, and consultants employed by ASI

- Personal electronic devices of ASI management and staff, which access ASI information technology resources

Who Should Know This Policy

☒ Budget Area Administrators	☒ Elected/Appointed Officers	☐ Grant Recipients
☒ Management Personnel	☒ Program Advisors	☒ Staff
☒ Supervisors	☒ Volunteers	

Definitions

For purposes of this policy, the terms used are defined as follows:

Term	Definition
Access	Personal inspection or review of confidential information or a copy of confidential information, or an oral or written description or communication of confidential information
Account	A continuing relationship established by a person with ASI to obtain a product or service for personal, family, household or business purpose. Accounts include an extension of credit, such as the purchase of property or services involving a deferred payment as well as a deposit account
Confidential Information	Information that is exempt from disclosure under the provisions of the California Public Records Act or other applicable state or federal laws.
Covered Account	A consumer account designed to permit multiple payments or transactions. These are accounts where payments are deferred and made by a borrower periodically over time such as a tuition or fee installment payment plan.
Creditor	A person or entity that regularly extends, renews, or continues credit and any person or entity that regularly arranges for the extension, renewal, or continuation of credit.

Term	Definition
Data Acquisition	Unencrypted electronic personal and/or notice-triggering information that has been acquired, or reasonably believed to have been acquired, by an unauthorized person in any of the following situations: • Equipment - Lost or stolen electronic equipment (including palm pilots, laptops, desktop computers, and USB storage devices) containing unencrypted personal information. • Hacking - A successful intrusion of computer systems via the network where it is indicated that unencrypted personal information has been downloaded, copied, or otherwise accessed. • Unauthorized Data Access - Includes situations where someone has received unauthorized access to data, such as sending non-public mail/e-mail to the wrong recipient, incorrect computer access settings, inadvertent posting of personal information in electronic format or other non-hacking incidents. Unauthorized data access also includes indications that the information was used by an unauthorized person, such as fraudulent accounts opened or instances of identity theft reported.
Data Owner	The individual with primary responsibility for determining the purpose and function of a record system
Disclosure	To permit access to or to release, transfer, disseminate, or otherwise communicate all or any part of confidential information by any means, orally, in writing, or by electronic or any other means to any person or entity
Electronic Computing Devices	Includes, but is not limited to, desktop computers, laptop computers, PDAs, tablet PCs, and smart phones.
Electronic Storage Media	Includes, but is not limited to, floppy disks, ZIP disks, DVDs, CDs, external hard drives, and USB storage devices
Encryption	All encryption algorithms, with the exception of trivial ciphers, meet the minimal campus requirements for encryption. If personal information stored on the compromised electronic equipment is encrypted, no University notification is required
Handled	The access, collection, distribution, process, protection, storage, use, transmittal, or disposal of information containing confidential data
Incident Report	An investigatory summation of a Security Incident completed by the CSULB Office of Information Security Management and Compliance to determine if ASI has incurred a Security Breach.
Internal Use Information	Information which must be protected due to proprietary, ethical or privacy considerations.
Record Custodian	The individual with responsibility for maintenance of a repository of records
Red Flag	A pattern, practice or specific activity that indicates the possible existence of identity theft
Security Breach	An unauthorized acquisition of computerized data that compromises the security, confidentiality or integrity of personal information maintained by ASI
Security Breach Response Planning Group	Individuals designated by the University to address Information Security issues. The group includes the Associate Vice President/Dean of Students, Student Services, Associate Vice President of Academic Technology, Associate Vice President, Vice Provost for Academic Affairs, Associate Vice President, Information Technology Services, Associate Vice President, University Relations, Associate Vice President, Academic Technology, Technology Strategist, Information Security Officer, Assistant Information Security Officer, and the Chief of Police.
Security Incident	A collection of related activities or events which provide evidence that confidential information could have been acquired by an unauthorized person
Service Provider	Any person or entity that receives, maintains, processes, or otherwise is permitted access to confidential information through its provision of service directly to ASI
Third Party	Any individual (or individual on behalf of an organization) who is not an employee of ASI

Standards and Procedures

1.0 Classification of Information

ASI 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

Collections 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[1], the entire file, document, etc. shall be classified at the most secure classification level.

1.1 Level 1 - Confidential Information

This classification represents information maintained by ASI that 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 ASI, its students, employees, or customers. Financial loss, damage to ASI's reputation, and legal action could occur. Confidential information is intended solely for use within ASI 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:

(1) Personal Information
  (a) Notice-triggering Personal Information[2]
    (i) 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:
      1. Social Security Number.
      2. Driver's license or California identification card number.
      3. 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.
      4. Medical information.
      5. Health insurance information.
    (ii) A user name or email address, in combination with a password or security question and answer that would permit access to an online account[3]
  (b) Biometric Information
  (c) Electronic or digitized signatures
  (d) Private Key (digital certificate)
  (e) Medical and Psychological counseling records
  (f) Forms of national or international identification (such as passports, visas, etc.), in combination with name
  (g) Criminal background check results

[1] 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

[2] 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.

[3] Added by Senate Bill No. 46, http://www.leginfo.ca.gov/pub/13-14/bill/sen/sb_0001-0050/sb_46_bill_20130927_chaptered.pdf

(h) Passwords or credentials

(2) 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

(3) Medical Information - Information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional

(4) 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

(5) 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

(6) 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

(7) Technical Security Information - Vulnerability/security information related to CSULB and ASI systems or services

(8) Law Enforcement Information - Law enforcement records related to an individual

(9) Legal Information
(a) Legal investigations conducted by ASI
(b) Attorney/Client communications

(10) Contract Information
(c) Sealed bids
(d) Third party proprietary information per contractual agreement

1.1.1 Collection of Confidential Information

Level 1 - Confidential Information must not be collected unless it is appropriate and relevant to the purpose for which it will be collected. It must be collected, to the extent possible, from the individual directly and not from other sources. Where information is obtained from other sources, a record must be maintained of those sources from which the confidential information was obtained.

Confidential information will not be collected or maintained unless approved by the ASI Director of Administrative Services. Confidential information will not be transferred outside the Associated Students, Incorporated unless the transfer is compatible with the disclosed purpose for which it was collected.

1.1.1.1 Personal Information Associated with "Identity Theft"
Collection of any Notice-triggering Personal Information must be limited to situations where there is legitimate business need and **no reasonable alternative exists**. Department

supervisors must ensure that their employees understand the need to safeguard this information, and that adequate procedures are in place to minimize this risk. Access to such information may only be granted to authorized individuals on a need to know basis.

1.1.1.2 Individuals' Rights

Individuals have the right to inquire and be notified about whatever confidential information ASI maintains concerning them. An opportunity to inspect any such confidential information must be afforded within 30 days of any request. If the record containing the confidential information also contains confidential information about another individual, that information must be deleted from the record before it is disclosed. Individuals may request copies of records containing any confidential information about them, and those copies must be provided within 15 days of the inspection. ASI may charge a reasonable per page cost for making any copies. Individuals may request that their personal information be amended and, if the request is denied, the individual may request a review of that decision by the Executive Director or designee.

1.1.2 Access to Confidential Information

No ASI director, officer, or employee will be granted access to confidential information in ASI's custody without the review and written approval of the ASI Director of Administrative Services. The approval of access to confidential information will be based on several factors including the determination that access is required for the employee to perform a critical function that is part of the employee's job duties and responsibilities and assurance that all requirements designed to protect individual privacy and safeguard confidential information will be met.

Employees approved for security access must receive appropriate training and sign a "Protection of Confidential Information – Summary of Responsibilities document". A copy of the signed form will be retained in the individual's official personnel file. Additionally, copies of the signed form should be kept on file with the appropriate department supervisor.

1.2 Level 2 – Internal Use/Enterprise Information

This classification represents information that 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 ASI's reputation, violation of an individual's privacy rights or legal action.

Level 2 Internal Use/Enterprise Information includes, but is not limited to:

(1) Identity Validation Keys
   (a) Birth date (full: mm-dd-yy)
   (b) Birth date (partial: mm-dd only)

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

(3) Student Information
   (a) Advising records
   (b) ASI services received
   (c) Disciplinary actions

(d) Student photo

(4) Employee Information
(a) Net salary
(b) Employment history
(c) Home address
(d) Personal telephone numbers
(e) Personal email address
(f) Parents and other family members names
(g) Payment history
(h) Performance evaluations
(i) Background investigations
(j) Mother's maiden name
(k) Biometric information
(l) Electronic or digitized signatures
(m) Birthplace (City, State, Country)
(n) Race and Ethnicity
(o) Gender
(p) Marital Status
(q) Physical description
(r) Photograph

(5) ASI Alumni Information
(a) Same as Employee Information

(6) Job Applicant Information
(a) Same as Employee Information

(7) ASI Donor Information
(a) Same as Employee Information

(8) Other
(a) Location of critical or protected assets
(b) Licensed software

1.3 Level 3 – Public Information

This classification represents 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 ASI to financial loss or jeopardize the security of ASI'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:

(1) Student Information
(a) Directory Information
(i) Name
(ii) Major field of study
(iii) Grade level
(iv) Enrollment status
(v) Campus e-mail address
(vi) Personal telephone numbers

Note: ASI 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 **may** be released to ASI and CSULB personnel and units only **if it is 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:

(2) Employee Information (including student employees)
- (a) Title
- (b) Status as a student employee (such as Intern, Student Assistant, Graduate Assistant)
- (c) Campus e-mail address
- (d) Work location and telephone number
- (e) Employing department
- (f) Position classification
- (g) Gross salary
- (h) Name (first, middle, last)(except when associated with confidential information)
- (i) Signature

4.0 Protection of Information

Information must be protected when handled, transmitted, stored, and disposed based on its classification level. Safeguards to protect ASI information assets are found in Appendix 1.

4.1 Protection of Social Security Numbers

The Social Security number (SSN) represents a unique privacy risk. No other form of personal identification plays such a significant role in linking records that contain sensitive information that individuals generally wish to keep confidential. The need to significantly reduce the risks to individuals of the inappropriate disclosure and misuse of SSNs has led California to enact legislation to limit their use and display. California law is intended to deter public disclosure of social security numbers; however, it does not prohibit the use of social security numbers for internal verification, for administrative purpose, or as otherwise required by law.

4.1.1 Prohibited Use of Social Security Numbers (SSN)

In compliance with California Civil Code Sections 1798.85-1798.86 and California Labor Code Section 226 ASI is prohibited from doing the following:

- Publicly posting or displaying an individual's SSN;
- Printing an individual's social security number on identification cards or badges;
- Requiring persons to transmit a SSN over the Internet unless the connection is secure or the SSN is encrypted;
- Requiring persons to log on to a web site using a SSN without a password;
- Printing SSNs on anything mailed to an individual unless required by law or the document is a form or application. When sending applications, forms, or other documents required by law to carry SSNs through the mail, the SSN will be

placed in such a way that it will not be revealed by an envelope window. A SSN may not be printed on a postcard;

- Encoding or embedding a social security number in a card or document, including using a bar code, chip, magnetic strip, or any other technology;

- Printing more than the last four digits of an employee's SSN on employee pay stubs or itemized statements.

4.1.2 Security Safeguards

In addition to complying with the legal requirements concerning the use and display of SSNs, ASI will take the following measures to reduce the collection of SSNs, control access to SSNs, and protect SSNs.

Reduce the Collection of SSN's.

- ASI will collect SSNs preferably only where required to do so by federal or state law.

- When collecting SSNs as allowed, but not required, ASI will do so only as reasonably necessary for the proper administration of lawful business activities.

- If a unique personal identifier is needed, ASI will use employee or student identification numbers, or otherwise develop a substitute for the SSN.

Control Access to SSN's.

- ASI will limit access to records containing SSNs only to those who need to see the numbers for the performance of their duties.

- ASI will protect records containing SSNs, including back-ups, during storage by encrypting the numbers in electronic records or storing records in other media in locked cabinets.

- ASI will not store records containing SSNs on computers or other electronic devices that are not secured against unauthorized access.

- ASI will not share SSNs with other organizations or persons except where required by law.

- ASI will prohibit third parties from using SSNs, except as required by law.

Protect SSNs with Security Safeguards

- ASI will comply fully with the CSULB Clean Desk and Clear Screen Standard.

- ASI will not leave voice mail messages containing SSNs.

- ASI will not fax documents containing SSNs to public FAX machines.

- ASI will promptly report any inappropriate disclosure or loss of records contains SSNs to the Executive Director and the campus office of Information Security Management and Compliance. See Security Incident Reporting and Breach Notification Procedures.

Discarding or destroying electronic documents containing SSN must be accomplished in accordance with the Electronic Media Sanitization Standard.

5.0 Disposal of Information

To protect the confidentiality of information and the related privacy rights of students, 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.

5.1 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 these cases, media should be destroyed.

5.2 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 the Associated Students Business Office for an approved document destruction vendor.

Appendix 2 describes the disposal methods for various media containing level 1 and level 2 data/records.

5.3 Electronic Media Sanitation Procedures

ASI departments will be fully responsible for ensuring that storage media (hard drives) have been sanitized or destroyed prior to asset disposition or internal reassignment. The following procedures are intended to guide ASI staff and information technology personnel through the use of CSULB's standardized tool and processes to securely sanitize hard disks of computers that are being:

- Disposed of;

- Reassigned to other individuals within ASI; or
- Transferred to another ASI department.

This is necessary to reduce the possibility of inappropriate exposure of data and unauthorized use.

When electronic computing devices or electronic storage media are to be transferred or disposed of, the ASI Director of Administrative Services will work with appropriate supervisors to complete the following steps:

1) All electronic computing devices or electronic storage media will be overwritten using university-approved and validated overwriting technologies/methods/tools without exception:

   Darik's Boot and Nuke (DBAN) http://dban.sourceforge.net (One pass is sufficient.)

   Apple Disk Utility http://support.apple.com

2) In instances involving an inoperable hard drive that cannot be cleared, ASI will require its removal from the electronic computing device in order to ensure proper destruction. Inoperable electronic computing devices and/or electronic storage media must be isolated and secured until properly destroyed. These devices will be destroyed using the degausser or by disposal with ASI's contracted e-waste disposal firm. Staff may contact the CSULB Information Security Management and Compliance department to make an appointment to use the degausser

3) The ASI Network Administrator must complete or obtain a signed Media Sanitization Certification form for the item(s) to be transferred or disposed of.

4) The Media Sanitization Certification must be submitted with the Property Transfer/Disposal Form to the ASI Director of Administrative Services for processing.

5) Upon approval from the ASI Director of Administrative Services, the item(s) may then be transferred to the new department/user or disposed of.

6.0 Service Provider Requirements

Due to the specialized expertise needed to design, implement, and service new technologies, vendors may be needed to provide resources that ASI is unable to provide on its own. Further, vendors may be needed to assist in the disposal of the volumes of hard-copy confidential information that is generated by ASI. In recognition of its responsibility for the performance and actions of these vendors, the following actions are required:

6.1 Due Diligence of Service-Providers

The adequacy of the service provider's system of safeguarding information shall be determined by the Controller prior to ASI entering into a contractual relationship with the service provider. ASI shall not contractually engage a service provider who cannot demonstrate that they have a system to safeguard student, employee, or donor information.

ASI shall not enter into a contractual agreement with any provider who is not capable of maintaining appropriate safeguards for confidential information.

6.2 Service Provider Agreements

All contracts with service providers must include a privacy clause that requires the service provider to implement appropriate measures to safeguard confidential information and to refrain from sharing any such information with any other party. In those cases where the service provider's contract does not include a privacy clause, a Confidential Information Addendum must be completed and appended to the service provider's contract.

Contracts must, when appropriate, include the requirement that in addition to the ASI insurance requirements for service agreements, the service provider be bonded and maintain personal liability insurance that protects against allegations of violations of privacy rights of individuals as a result of improper or insufficient care on the part of the service provider.

7.0 Identity Theft Prevention Program

In 2003, the U.S. Congress enacted the Fair and Accurate Credit Transaction Act of 2003 (FACTA) which required "creditors" to adopt policies and procedures to prevent identify theft. These requirements are described in Section 114 of FACTA and are known as the "Red Flags Rule".

The Red Flags Rule requires "creditors" holding "covered accounts" to develop and implement a written identity theft prevention program designed to identify, detect and respond to "Red Flags."

The purpose of the Identity Theft Prevention Program is to detect, prevent, and mitigate identity theft in connection with the opening of a "covered account" or the management of any existing covered account.

7.1 Covered Accounts

Covered Accounts include, but may not be limited to:

- Accounts that are created for ongoing services and allow the student or customer to remit payment to ASI when billed over a period of time.
- Any type of collection account.

7.2 Identification of Red Flags

Broad categories of "Red Flags" include the following examples:

7.2.1 Alerts, Notifications, or Warnings from a Consumer Reporting Agencies

- A fraud or active duty alert is included with a consumer report.
- A consumer reporting agency provides a notice of credit freeze in response to a request for a consumer report.
- A consumer reporting agency provides a notice of address discrepancy.
- A consumer report indicates a pattern of activity that is inconsistent with the history and usual pattern of activity of an applicant or consumer, such as:

- A recent and significant increase in the volume of inquires;
- An unusual number of recently established credit relationships;
- A material change in the use of credit, especially with respect to recently established credit relationships; or

- An account that was closed for cause or identified for abuse of account privileges by ASI or CSULB.

7.2.2 Suspicious Documents

- Documents provided for identification appear to have been altered or forged.
- The photograph or physical description on the identification is not consistent with the appearance of the applicant or customer presenting the identification.
- Other information on the identification is not consistent with information provided by the person opening a new covered account or customer presenting the identification.
- An application appears to have been altered or forged, or gives the appearance of having been destroyed and reassembled.

7.2.3 Suspicious Personal Identifying Information

- Personal identifying information provided is inconsistent when compared against external information sources used by the campus. For example:
  - The address does not match any address in the consumer report; or
  - The Social Security Number (SSN) has not been issued, or is listed on the Social Security Administration's Death Master File
- Personal identifying information provided by the customer is not consistent with other personal identifying information provided by the customer. For example, there is a lack of correlation between the SSN range and date of birth.
- Personal identifying information provided is associated with known fraudulent activity as indicated by internal or third-party sources used by ASI. For example:
  - The address on an application is the same as the address provided on a fraudulent application; or
  - The phone number on an application is the same as the number provided on a fraudulent application.
- Personal identifying information provided is of a type commonly associated with fraudulent activity as indicated by internal or third-party sources used by the campus.
  - The address on an application is fictitious, a mail drop, or a prison; or

- The phone number is invalid, or is associated with a pager or answering service.

- The SSN provided is the same as that submitted by other persons opening an account or other customers.

- The address or telephone number provided is the same as or similar to the address number or telephone number submitted by an unusually large number of other persons opening accounts or other customers.

- The person opening the covered account or the customer fails to provide all required personal identifying information on an application or in response to notification that the application is incomplete.

- Personal identifying information provided is not consistent with personal identifying information that is on file with the ASI.

- The person opening the covered account or the customer cannot provide authenticating information beyond that which generally would be available from a wallet or consumer report.

7.2.4 Unusual Use or Suspicious Account Activity

- The customer fails to make the first payment or makes an initial payment but no subsequent payments.

- A covered account is used in a manner that is not consistent with established patterns of activity on the account. There is, for example:

  - Nonpayment when there is no history of late or missed payments;

  - A material change in electronic fund transfer patterns in connection with a deposit account; or

- Mail sent to the customer is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the customer's covered account.

- ASI is notified that the customer is not receiving paper account statements.

- ASI is notified of unauthorized charges or transactions in connection with a customer's covered account.

7.2.5 Notice from Others Indicating Possible Identify Theft

- The campus is notified by a customer, a victim of identity theft, a law enforcement authority, or any other person that it has opened a fraudulent account for a person engaged in identity theft.

7.3 Detection of Red Flags

Detection of Red Flags in connection with the opening of covered accounts as well as existing covered accounts can be made through such methods as:

- Obtaining and verifying identity;
- Authenticating customers;
- Monitoring transactions
- Verifying the validity of change of address requests in the case of existing covered accounts.

7.4 Response to Red Flags

The detection of a Red Flag by an employee must be reported to the ASI Executive Director, ASI Director of Administrative Services, and the CSULB Office of Information Security Management and Compliance. Based on the type of red flag, the Director of ASI Administrative Services and the Director, Information Security Management and Compliance together with the employee will determine the appropriate response.

Appropriate responses may include:

- Monitoring a covered account for evidence of identity theft;
- Contacting the individual;
- Changing any passwords, security codes, or other security devices that permit access to a covered account;
- Reopening a covered account with a new account number;
- Not opening a new covered account;
- Closing an existing covered account;
- Not attempting to collect on a covered account or not selling a covered account to a debt collector;
- Notifying law enforcement; or
- Determining that no response is warranted under the particular circumstances.

7.5 Service Providers

ASI remains responsible for compliance with the Red Flag Rules even if it outsources operations to a third party service provider. The written agreement between ASI and the third party service provider shall require the third party to have reasonable policies and procedures designed to detect relevant Red Flags that may arise in the performance of their service provider's activities. The written agreement must also indicate whether the service provider is responsible for notifying only

ASI of the detection of a Red Flag or if the service provider is responsible for implementing appropriate steps to prevent or mitigate identity theft.

7.6 Training

All ASI employees who process any information related to a covered account shall receive training to understand their responsibilities associated with the Identity Theft Prevention Program.

8.0 Security Incident Reporting and Breach Notification Procedures

ASI is required to disclose any breach of system security to individuals whose unencrypted personal information was, or is reasonably believed to have been acquired by an unauthorized person. Any student, staff, or other agent having access to ASI confidential information will immediately notify the CSULB Office of Information Security Management and Compliance and the Executive Director

8.1 Security Incident Reporting & Investigation Protocol

The following outlines procedures and protocols for notification of and response to a security breach involving unencrypted electronic personal information processed and/or maintained by ASI.

8.1.1 Security Incident Reporting

Any employee or data owner who believes that a security incident has occurred, shall immediately notify the Vice President, Administration and Finance and the CSULB Office of Information Security Management and Compliance. After business hours, notification shall be made to University Police (562) 985-4101.

Upon notification by an employee, Information Technology Services, or University Police of a suspected unauthorized acquisition of confidential information the CSULB Office of Information Security Management and Compliance shall promptly notify with the Security Breach Response Planning Group.

8.1.2 Security Incident Investigation

The CSULB Office of Information Security Management and Compliance will conduct an investigation into the security incident to determine whether there has been a security breach. As part of the investigation, and when applicable, the ASI Director of Administrative Services will require the data owner to complete and submit an Employee Identification of Stored Data statement to the CSULB Office of Information Security Management and Compliance. All investigatory work will be documented within an Incident Report.

Upon completion of the investigation, the CSULB Office of Information Security Management and Compliance will inform the Security Breach Response Planning Group of the result of the investigation.

8.2 Security Breach Notification Protocol

8.2.1 Internal Notifications

If it is determined after investigation that a security breach involving notice triggering information has occurred, the CSULB Office of Information Security Management and Compliance shall notify the Vice President of Administration and Finance and Office of General Counsel.

If it is determined that a breach is of the appropriate magnitude and may require a press release, the CSULB Office of Information Security Management and Compliance shall notify the Senior Director, Information Security Management, Associate Vice President, University Relations, Office of the Chancellor and copy the CIO/Assistant Vice Chancellor.

The CSULB Office of Information Security Management and Compliance will notify the responsible department, confirming the security breach of notice triggering information and provide advice and guidance. The CSULB Office of Information Security Management and Compliance will also initiate the campus breach notification process and work closely with the Executive Director or designee responsible for controlling access to, and security of, the breached electronic equipment to ensure the appropriate handling of the breach response and inquiries. The CSULB Office of Information Security Management and Compliance will provide guidance to designated employees responsible for responding to breach notification inquiries.

8.2.2 External Notification

If it is determined after investigation that a security breach involving credit/debit card information has occurred, the CSULB Office of Information Security Management and Compliance will direct notification to the appropriate merchant bank(s). Within three (3) business days of a confirmed breach, the CSULB Office of Information Security Management and Compliance shall provide an Incident Report to the appropriate merchant bank(s). Within ten (10) business days, the CSULB Office of Information Security Management and Compliance shall provide to the appropriate merchant bank(s) a list of all potentially compromised accounts.

8.2.3 Notification of Affected Individuals

The department or office responsible for controlling access to, and security of, the breached electronic equipment will compile the list of the names of persons whose personal information was, or is reasonably believed to have been, acquired by an unauthorized person. In consultation with the CSULB Office of Information Security Management, a list of individuals to notify shall be compiled based on the following criteria:

- Residents of California.
- All individuals who are likely to have been affected, such as all whose information had been stored in the files involved, when identification of specific individuals cannot be made.

If notices are sent to more than 10,000 individuals, the CSULB Office of Information Security Management and Compliance shall notify the following consumer credit reporting agencies:

- Experian: E-mail to BusinessRecordsVictimAssistance@experian.com

- Equifax: E-mail to lanette.fullwood@equifax.com
- TransUnion: E-mail to fvad@transunion.com, with “Database Compromise” as subject.

The process for determining inclusion in the notification group shall be included in the Incident Report.

8.2.4 Notification Timing

Individuals whose notice-triggering information has been compromised shall be notified in the most expedient time possible, and without unreasonable delay, consistent with the legitimate needs of law enforcement or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

The information considered when determining the notification date shall be included within the Incident Report.

8.2.5 Content of Notice

The breach notification will provide a brief description of the security breach, a contact for inquiries, and helpful references to individuals regarding identity theft and fraud. The content of the breach notification, and when appropriate, the content of both the web site page and the press release will be reviewed and approved by the CSULB Office of Information Security Management.

8.2.6 Communications with Outside Agencies

With the exception of the Office of Public Affairs, University Police, and CSULB Office of Information Security Management and Compliance, ASI personnel are not authorized to speak on behalf of the university or ASI to media personnel or representatives of other outside agencies. All media inquiries or other public affairs inquiries should be directed to the Office of Public Affairs at (562) 985-4134. All other inquiries should be directed to CSULB Office of Information Security Management and Compliance at (562) 985-4862 or to the University Police at (562) 985-4101.

8.2.7 Method of Notification

A letter shall be printed with official ASI letterhead, addressed to the individual at the last recorded home address, or if only an email address is known, the last recorded email address on file with the University and/or ASI. Any notices returned with address forwarding information will be re-sent by the responsible department.

If less than 500,000 individuals were affected, or if the cost of disseminating individual notices is less than $250,000, notices shall be sent by first class mail or email address.

If more than 500,000 individuals were affected or if the cost of giving individual notices to affected individuals is greater than $250,000 or if there is insufficient contact information, the following substitute notification procedures shall be followed:

- Notices by e-mail shall be sent to all affected individuals whose e-mails are known.

- The University shall issue a press release to the media as appropriate.
- A "Notice of Breach" shall be conspicuously posted on the campus web site*.

*After a six month period of time the Office of General Council, Associate Vice President, University Relations, and the CSULB Office of Information Security Management and Compliance will determine if additional website posting time is necessary.

8.2.8 Breach Notification Inquiry Response

Subsequent to a security breach notification, the University can expect several inquiries from notified users, their parents/spouse, and security vendors. The CSULB Office of Information Security Management and Compliance will provide a written Inquiry Response Guide to be used by the ASI Executive Director, or designee(s), to respond to any phone calls/emails/letters/walk in traffic with inquiries regarding the breach.

8.2.9 Department Responsibility

The department responsible for controlling access to, and security of, the breached electronic information is responsible for financial and human resources used to notify and respond to the affected individuals.

8.3 Legal or Civil Actions

Subsequent to a breach, ASI may be reviewed by a governing state or federal agency or a civil action could be brought against ASI. The CSULB Office of Information Security Management and Compliance will represent all complaints and agency inquiries submitted to the University as a result of the security breach. Legal counsel will be solicited as needed to respond to complaints or actions. ASI is responsible for the payment of fines, penalties, or retributions levied by agencies or the courts.

8.0 Training

All ASI directors, officers, and employees having access to confidential information will receive training regarding ASI's Policy on Information Security. Employee training will be provided by the ASI Director of Administrative Services. Record Custodians must keep documentation of this training for review by the university internal auditor.

Administration

The ASI Director of Administrative Services is responsible for the administration, revision, interpretation, and application of this policy. He/she will periodically evaluate, test, and adjust the information security program to validate that equipment and systems function properly and produce the desired results. The ASI Director of Administrative Services will perform ongoing assessments to ensure that employees follow written procedures for information security. Information security will be included in all internal audits. This policy will be reviewed triennially and revised as needed, unless earlier revisions are necessitated by changes in the regulations of the IRS, CSULB, or the California State University Office of the Chancellor

Forms

The following forms and procedures are to be used in the execution of this policy.

Form Name	Purpose	Responsible Office	Approved By	Timeline for Submission
Confidential Information Addendum	To amend a service provider's contract to include a privacy clause requiring the service provider to implement appropriate measures to safeguard confidential information and to refrain from sharing any such information with any other party	A.S. Business Office	Executive Director	Must be completed and fully executed prior to the exchange of any confidential information
Protection of Confidential Information – Summary of Responsibilities	To request approval for employee access to confidential information maintained by ASI and to document their training in and understanding of security requirements	Office of the Executive Director	ASI Director of Administrative Services	Must be completed and fully executed prior to providing access to the employee.
Acceptable Use Agreement	To gain access to ASI information assets by acknowledging receipt of and agreeing to abide by ASI's Policy on Information Assets	Human Resources Office	N/A	Must be completed upon hire or desired date of access. Allow 3 business days for processing.

Appendix 1. Protection Measures

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

	Level 1 - Confidential	Level 2 - Internal Use	Level 3 - Public
Handling	• Users must "log off" their computers when their workspace is unattended. • Users must "shut down" their computers at the end of the workday. • All Confidential and Internal Use information must be removed from the desk and locked in a drawer or file cabinet when the workstation is unattended and at the end of the workday. • All Confidential and Internal Use information must be stored in lockable drawers or cabinets. • File cabinets containing Confidential or Internal Use information must be locked when not in use or when not attended. • Keys used to access Confidential or Internal Use information must not be left at an unattended work area. • Laptops must be either locked with a locking cable or locked away in a drawer or cabinet when the work area is unattended or at the end of the workday. • Passwords must not be posted on or under a computer or in any other accessible location. • Copies of documents containing Confidential or Internal Use information must be immediately removed from printers. • Documents containing Confidential or Internal Use information must be immediately removed from facsimile machines.	Same as Level 1	No restrictions
Transmitting	**Distribution**: Limited to those employees with an established business need-to-know and are either ASI employees or 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.	

	Level 1 - Confidential	Level 2 - Internal Use	Level 3 - Public
	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.	
Storage	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 University owned laptops, desktops or portable electronic storage media, including but not limited to, CD-ROMs, DVD-ROMs, external hard drives, zip disks, flash-memory cards, magnetic cards and USB flash drives (a.k.a. Memory Sticks, Thumb or Jump Drives). In such cases, laptops, desktops and portable electronic storage media storing level 1 data must be encrypted. 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. But this decision needs to be documented and approved in writing by the employee's Appropriate Administrator and the University CSULB Office of Information Security Management and Compliance.[4] 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 below for prohibitions regarding the storage of specific Payment Related Data.[5]	Same as Level 1.	No restrictions

[4] 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.

[5] 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

	Level 1 - Confidential	Level 2 - Internal Use	Level 3 - Public
	Printed level 1 information must be secured in a locked enclosure.		
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 ASI Record Retention Schedule.	Same as Level 1	Same as level 1
Disposition	Proper Media Sanitization Methods are described below.	Same as Level 1	Normal waste disposal

(c) PIN verification value

Appendix 2. Disposition Methods

The matrix below describes the disposal methods for various media containing Level 1 – Confidential and Level 2 – Internal Use data/records:

Media Type	Method
Hard Copy Storages	
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.
Zip Disks	Overwrite by using university-approved and validated overwriting technologies/methods/tools, or degauss. For more information refer to the CSULB Electronic Media Sanitization Process.
SCSI (Small Computer System Interface) 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.
Reel and Cassette Format Magnetic Tapes	Clear magnetic tapes by either re-recording (overwriting) or degaussing. 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.
Magnetic Cards	Overwrite media by using university-approved and validated overwriting technologies/methods/tools, or physically destroy by shredding.

Media Type	Method
Optical Disks	
CDs	Physically destroy by shredding.
DVDs	Physically destroy by shredding.
Static Memory Storage	
Compact Flash Drives or USB/Memory Sticks	Overwrite media by using university approved and validated overwriting technologies/methods/tools.
Flash Cards	Perform a full chip purge as per manufacturer's data sheets.
Smart Cards	Overwrite media by using university-approved and validated overwriting technologies/methods/tools.
PCMCIA (Personal Computer Memory Card International Association Cards)	Overwrite media by using university-approved and validated overwriting technologies/methods/tools.
RFID (Radio-Frequency Identification)	Overwrite media by using university-approved and validated overwriting technologies/methods/tools.
Items Not Listed Above	
Other Memory Devices	Contact your area computer technician or the campus Assistant CSULB Office of Information Security Management and Compliance at 5-4862 for the best method of sanitization.
Unlisted Technologies	For electronic technologies not listed in the above table, please contact the campus Assistant CSULB Office of Information Security Management and Compliance at 5-4862.