POLICY ON INFORMATION SYSTEMS

DEFINITIONS

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

Term	Definition	Chapter

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	Information Security
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	Information Security
Assigned user	The specific individual to whom a mobile service device is issued	Mobile Service Devices
Business use	Use of a mobile service device to conduct official ASI business	Mobile Service Devices
Confidential Information	Information that is exempt from disclosure under the provisions of the California Public Records Act or other applicable state or federal laws.	Information Security
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.	Information Security
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.	Information Security
Data Owner	The individual with primary responsibility for determining the purpose and function of a record system	Information Security
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	Information Security
Electronic Computing Devices	Includes, but is not limited to, desktop computers, laptop computers, PDAs, tablet PCs, and smart phones.	Information Security
Electronic Storage Media	Includes, but is not limited to, floppy disks, ZIP disks, DVDs, CDs, external hard drives, and USB storage devices	Information Security
Emergency	A serious situation or occurrence threatening health, safety, or property that happens unexpectedly and demands immediate action	Mobile Service 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	Information Security
Extensive usage	Average monthly usage of the mobile device exceeds 250 minute of voice and 100 text messages.	Mobile Service Devices
First responder	A trained or certified individual who, upon arriving early to an incident or emergency, assumes immediate responsibility for the protection and preservation of life, property, evidence and environment.	Mobile Service Devices
Handled	The access, collection, distribution, process, protection, storage, use, transmittal, or disposal of information containing confidential data	Information Security
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.	Information Security

Information asset record	The contents of information assets created, sent, forwarded, replied to, transmitted, distributed, broadcast, stored, held, copied, downloaded, displayed, viewed, read, or printed by one or several electronic communications systems or services. This includes attachments to such records and transactional information associated with such records.	Information Assets
Information assets	Telecommunications equipment, transmission devices, electronic video and audio equipment; encoding or decoding equipment, computers and computer time, data processing or storage systems, computer systems, servers, networks, input/output and connecting devices, and related computer records, programs, software, and documentation that supports electronic communications systems and services.	Information Assets
Information systems and services	Any messaging, collaboration, publishing, broadcast, or distributions system that depends on electronic communications resources to create, send, forward, reply to, transmit, distribute, broadcast, store, hold, copy, download, display, view, read, or print electronic records for the purposes of communication across electronic communications network systems between or among individuals or groups, that is either explicitly denoted as a system for electronic communications or is implicitly used for such purposes.	Information Assets
Internal Use Information	Information which must be protected due to proprietary, ethical or privacy considerations.	Information Security
Level 1 – Confidential Information	Information that is exempt from disclosure under the provisions of the California Public Records Act or other applicable state or federal laws. Confidential information is information whose unauthorized use, access, disclosure acquisition, modification, loss, or deletion could result in severe damage to 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 is limited to those with a "business need-to-know". Statutes, regulations, or other legal obligations or mandates protect much of this information. Disclosure of Confidential information to persons outside of ASI is governed by specific standards and controls designed to protect the information.	Information Assets
Level 2- Internal Use Information	Information which must be protected due to proprietary, ethical or privacy considerations. Although not specifically protected by statute, regulations, or other legal obligations or mandates, unauthorized use, access, disclosure, acquisition, modification, loss or deletion of information at this level could cause financial loss, damage to ASI's reputation, violate an individual's privacy rights or legal action could occur.	Information Assets
Mobile service device	A device or an apparatus associated with a device that enables an employee to communicate wirelessly with another person. The term includes, without limitation, a cellular telephone, a laptop computer, , or a transmitting radio.	Mobile Service Devices
Occasional usage	Average monthly usage of the mobile device is below 100 minutes of voice and 25 text messages	Mobile Service Devices
Official ASI business	Conduct engaged in for the purpose of serving as an authorized representative of the Associated Students, Incorporated or for the purpose of acquiring knowledge, information, contacts, or intelligence that the corporation deems important to the operation of the organization, its programs, services, and facilities.	Mobile Service Devices
Personal device	A mobile service device that is the personal property of an ASI officer or employee	Mobile Service Devices
Personal use	Use of a mobile service device that is not related to the conduct of ASI business	Mobile Service Devices
Portable device	Portable computing devices including, but not limited to, laptops computers, PDAs, and tablet PCs	Information Assets
Record Custodian	The individual with responsibility for maintenance of a repository of records	Information Security
Red Flag	A pattern, practice or specific activity that indicates the possible existence of identity theft	Information Security
Regular usage	Average monthly usage of the mobile device ranges from 100 to 249 minutes of voice and 25 to 99 text messages	Mobile Service Devices
Removable media	Portable electronic storage media including but not limited to, CDs and USB storage devices	Information Assets

Security Breach	An unauthorized acquisition of computerized data that compromises the security, confidentiality or integrity of personal information maintained by ASI	Information Security
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.	Information Security
Security Incident	A collection of related activities or events which provide evidence that confidential information could have been acquired by an unauthorized person	Information Security
Service plan level	A contract or service agreement by a vendor to provide cellular communication service at a fixed monthly charge for a fixed number of minutes beyond which additional charges accrue	Mobile Service Devices
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	Information Security
System administrators	The Information Technology Manager and his/her designated staff	Information Assets
Third Party	Any individual (or individual on behalf of an organization) who is not an employee of ASI	Information Security
Workstation	An area provided to a user for the performance of tasks using an intelligent terminal or personal computer usually connected to a computer network	Information Assets

INFORMATION SECURITY

BACKGROUND AND PURPOSE

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 STATEMENT

It is the policy of the ASI 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

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*, 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*

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:

PERSONAL INFORMATION

- Notice Triggering Personal Information*
    - 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:
        - Driver's license or California identification card number.
        - 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.
        - Medical information.
        - Health insurance information.
    - 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

**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.*

***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*

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

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 CSULB and ASI systems or services

LAW ENFORCEMENT INFORMATION

- Law enforcement records related to an individual

LEGAL INFORMATION

- Legal investigations conducted by ASI
- Attorney/Client communications

CONTRACT INFORMATION

- Sealed bids
- Third party proprietary information per contractual agreement

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, upon direction and approval from their 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:

IDENTITY VALIDATION KEYS

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

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

- Advising records
- ASI 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

ASI ALUMNI INFORMATION

- Same as Employee Information

JOB APPLICANT INFORMATION

- Same as Employee Information

ASI DONOR INFORMATION

- Same as Employee Information

OTHER

- Location of critical or protected assets
- 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:

STUDENT INFORMATION

- Directory Information
    - Name
    - Major field of study
    - Grade level
    - Enrollment status
    - Campus e-mail address
    - 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:

EMPLOYEE INFORMATION

- Directory Information
    - Title
    - Status as a student employee (such as Intern, Student Assistant, Graduate Assistant
    - 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

2.0 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.**

2.1 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.

2.1.1 PROHIBITED USES OF SOCIAL SECURITY NUMBERS

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.

2.1.2 SECURITY SAFEGUARDS

In addition to complying with the legal requirements concerning the use and display of Social Security Numbers (SSN), 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

- 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 SSN 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.

3.0 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.

3.1 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.

3.2 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.

3.3 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
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.

4.0 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:

4.1 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.

4.2 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.

5.0 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.

5.1 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.

5.2 IDENTIFICATION OF RED FLAGS

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

5.2.1 ALERTS, NOTIFICATIONS, OR WARNINGS FROM A CONSUMER REPORTING AGENCY

- 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.

5.2.2 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.

5.2.3 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.

5.2.4 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.

5.2.5 NOTICE FROM OTHERS INDICATING POSSIBLE IDENTITY 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.

5.3 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.

5.4 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.

5.5 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.

5.6 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.

6.0 SECURITY INCIDENT REPORTING AND BREACH NOTIFICATION PROCEDURES

ASI is required to disclose in a timely manner 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

6.1 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.

6.1.1 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.

6.1.2 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.

6.2 SECURITY BREACH NOTIFICATION PROTOCOL

6.2.1 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.

6.2.2 EXTERNAL NOTIFICATIONS

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.

6.2.3 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.

6.2.4 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.

6.2.5 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.

6.2.6 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.

6.2.7 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.

6.2.8 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.

6.2.9 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.

6.3 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.

7.0 TRAINING

All ASI directors, officers, and employees having access to confidential information will receive training regarding ASI's Policy on Information Security upon hiring. Employee training will be provided by the ASI Director of Administrative Services. Documentation of this training for review by the university internal auditor shall be kept in employee personnel files.

8.0 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

INFORMATION ASSETS

BACKGROUND AND PURPOSE

Information assets are essential to the ability of the Associated Students, Incorporated (ASI) to conduct business and carry out its mission. The continued and reliable availability of these resources are paramount to ASI's ability to fulfill its instructional, public service, campus support and other educationally related functions. To this end, ASI strives to provide its employees and volunteers with state-of-the-art information assets.

Nonetheless, the use of information assets is limited by restrictions that apply to all ASI property and by constraints necessary for the reliable operation of information systems and services. ASI reserves the right to deny use of its information assets, when necessary, to satisfy these restrictions and constraints.

The purposes of this policy are to:

- Ensure that ASI's information assets are used for purposes appropriate to the performance of ASI business;
- Ensure that User's privacy rights are protected;
- Inform User's about the applicability of laws and standards to information assets;
- Ensure that information assets are used in compliance with those laws and standards; and
- Prevent disruption to and misuse of ASI's electronic communication systems and services.

POLICY STATEMENT

It is the policy of the Associated Students, Incorporated (ASI) that the use and contents of all ASI information assets will conform to CSU and CSULB policies and standards, state law and federal law including the Copyright Act of 1976 and all subsequent amendments including, but not limited to, the Digital Millennium Copyright Act of 1998 and the Teach Act of 2002.

Access to information assets is a privilege, not a right. All users are required to act honestly and responsibly. All users must respect the integrity of the physical facilities, all pertinent license and contractual agreements, and the rights of other computer users.

In addition, all ASI information assets will be accessible to users with disabilities in compliance with law and University policies. Alternate accommodations will conform to law and University policies and standards.

Accepting any ASI account will constitute an agreement on behalf of the user to abide by and be bound by this and any other provisions concerning use of information assets. This agreement will be acknowledged and documented in writing by having each user complete an Acceptable Use Agreement. This agreement will be retained in the user's personnel file or volunteer file in the Human Resources Office.

This policy applies to:

- All information assets owned or managed by ASI;
- All information assets provided by ASI through contracts or other agreements;
- All users and uses of ASI information assets; and
- All electronic records in the possession of ASI employees or of other users of ASI information assets.

9.0 ACCESS TO INFORMATION ASSETS

ASI will grant access to information assets to its employees and volunteers when required for the performance of their essential duties and responsibilities. Each workstation will be equipped with the necessary hardware and software to enable the user to satisfactorily perform his/her assigned tasks. All users will be required to complete an Acceptable Use Agreement, which will be maintained in the employee's personnel file.

Access to specialized software such as the accounting or human resources information systems will be provided to users with a documented need. All such users will complete a user access request form and have it approved by their immediate supervisor prior to gaining access.

All ASI computers are also authenticated clients of the campus network. All ASI users must log into the campus domain using their valid CSULB email account.

9.1 PERMISSION GROUPS

Users will be placed in permission groups according to departmental design. All users will be placed in the "Users" group so as to protect computing systems from unapproved software installations that may damage or degrade the system, servers, or network and to safeguard against viruses, worms, Trojan horses, key loggers, spyware and malware. Only the Information Technology Manager will be allowed full access to the domain main server. Systems administrators will have administrative privileges on all local machines. Administrative control of a local workstation will be awarded to the individual user only as required by the nature of his/her position and level of authority.

9.2 SOFTWARE

ASI will install the necessary operating system and basic software applications on all workstations. In addition, ASI will install software purchased by various departments within ASI that is necessary for work-related purposes. It is the responsibility of the ASI Information Technology Office to ensure that applicable licensing requirements have been met.

9.2.1 PROHIBITED SOFTWARE

9.2.2 INSTANT MESSAGING SOFTWARE

Instant messaging is allowed, however the acceptance of attachments is not permitted regardless of the file type, extension, or originator.

9.2.3 DOWNLOADING SOFTWARE

Downloading of software is restricted to specific user groups. If applications are needed for day-to-day business, the User should contact the IT Department or submit a request on the IT Helpdesk.

10.0 PRIVACY

Although not legally required to do so, ASI respects the privacy of all users. System administrators will not log onto a user's account or view the user's files without explicit permission from the user. Only when a legitimate reason exists will a duly authorized ASI staff person access an individual's user files or data. Legitimate reasons include:

- Repair or maintenance of computing equipment ASI deems is reasonably necessary.
- Investigation of improper or illegal use of resources where there is reasonable cause to believe there is:
    - Use for unauthorized personal financial gain
    - Threatening, harassing, or illegal email
    - Copyright violations
    - Unlawful activity
    - Other misuse in violation of this Policy
    - Response to a public records request, administrative or judicial order, or request for discovery in the course of litigation.

Although ASI and the campus have enacted various security measures, ASI cautions that the system, like any other system, cannot be considered totally secured and user privacy cannot be guaranteed

The ASI network is on the CSULB campus hub. As such, it provides access to information available through electronic information resources including the Internet. At this time, the campus cannot block unwanted emails or pop-up ads. Consequently, the ASI cannot guarantee any individual that he/she will not be inadvertently exposed to material he/she deems offensive.

10.1 AUTOMATED MONITORING

The right to privacy does not preclude system administrators from maintaining and monitoring system logs of user activity. Automated searches for files and transmissions that endanger privacy, confidentiality of data, system security or integrity are performed regularly to protect all users and ensure the continued availability of information assets. System administrators may take appropriate actions in response to detection of such files or transmissions.

10.2 THIRD PARTY SERVICES

Contracts with outside vendors for information systems and services must explicitly reflect and be consistent with this policy and other University policies related to privacy. Any third party organization providing contractors to ASI will be provided access to this policy for review prior to commencing work.

11.0 ACCEPTABLE USE OF INFORMATION ASSETS

11.1 USER ACCESS

User access is granted to a specific individual and may not be transferred to or shared with another user. The password and user ID must not be shared with any other individual. This principle is intended to protect the integrity, security, and privacy of the user account as well as that of the entire system.

11.2 INCIDENTAL USE

Information assets, including access to the Internet and e-mail are resources provided for ASI- related business. Personal use will be permitted, provided it does not interfere with ASI operations and the user's performance of his/her duties. This privilege, however, must not be abused. Excessive usage of information assets for personal reasons is a work performance issue that is the responsibility of individual department managers to monitor.

11.3 DOWNLOADED MATERIAL

Any materials downloaded from the Internet must comply with all ASI regulations concerning print or other visual materials. Materials that constitute sexual or other discriminatory harassment and/or other offensive material are not permitted in the workplace. Employee rights to a safe workplace may not be endangered because of the inappropriate use of information assets.

11.4 PASSWORD STANDARDS

User access is contingent upon prudent and responsible use. Each user must have a password to access a workstation. Passwords are the front line of protection for user accounts. Passwords can preserve the confidentiality of password-protected data and are the sole property of account holders. As such, all ASI employees, including contractors and vendors with access to ASI systems, are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

This standard applies to all individuals who have or are responsible for an account or any form of access that supports or requires a password on any ASI or CSU system, has access to the CSULB network, or stores any non-public ASI information.

Hackers use sophisticated programs to crack passwords and illegally enter a system.

11.4.1 PASSWORD COMPOSITION

A password must meet the following requirements:

A password must meet the following requirements:

- It must be case sensitive
- It must be at least ten characters in length
- It must contain no spaces
- Not match an of a person's previous passwords
- It must not contain any non-English language characters
- It must contain characters from three of the following four categories:

    - Uppercase alphabet characters (A – Z)
    - Lowercase alphabet characters (a – z)
    - Arabic numerals (0 – 9)
    - Special characters (` ~ ! @ # $ % ^ & * ( ) _ + - = { } | [ ] \ : " ; ' < > ? , . /)

To the extent that password complexity is supported by respective devices and/or systems, passwords should also:

- Not contain personal information such as user name or CSULB ID number
- Not contain a complete dictionary word from English or another language
- Be significantly different from previous passwords
- Not be incremental with every password change (Example: Password 1, Password 2, Password 3…)
- Be difficult to crack, but easy to remember (Example: make up a sentence, and then use the first letter of each word or sound, adding a couple of digits or symbols and uppercase letters. For instance, "Tennis anyone??" becomes the password: "10Sne1??" or "I love 8 hot fudge sundaes best," becomes "iL8hfsB!"
- Not have more than two characters repeated consecutively
- Not use adjacent keyboard characters (Example: asdfghjkl,qwertyu,12345678)

11.4.2 PASSWORD PROTECTION

Passwords must be treated as confidential information. To protect confidential information, users should take the following measures:

- Do not use the same password for CSULB accounts as for your personal accounts.
- Do not reveal a password over the phone to ANYONE.
- Do not reveal a password in an email message.
- Do not talk about your password in front of others.
- Do not hint at the format of your password (e.g., "my dog's name").
- Do not reveal a password on questionnaires or forms.
- Do not reveal a password to co-workers while on vacation.
- Do not write passwords down and store them anywhere in your office.

- Do not store passwords in a file on ANY computer systems without encryption.
- Do not use the "Remember Password" feature of applications or web browsers.

11.4.3 PASSWORD CHANGE FREQUENCY

System	Frequency
SAGE MAS 200 Accounting	Annually
Human Resources Information Systems (ADP)	Annually
BeachID/campus LDAP, AD-based systems	Annually

11.5 CLEAR SCREEN STANDARDS

All workstations must be clear of ASI information classified as Level 1 – Confidential or Level 2 – Internal Use when a workstation is unattended.

- Users must "log off" their computers when their workspace is unattended.
- Users must "shut down" their computers at least weekly, no later than the close of business on Friday.
- 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.

11.6 PORTABLE DEVICE AND REMOVABLE MEDIA STANDARDS

Portable computing devices (including but not limited to laptops computers, PDAs, tablet PCs) and portable electronic storage media (including but not limited to CD's and USB storage devices) are vulnerable to loss or theft. In the event of loss or theft, information stored on these devices or media may result in identity theft or unauthorized access to secure systems, networks, and resources.

Level 1 - Confidential information stored on portable computing devices and portable electronic storage media must be encrypted or otherwise rendered unreadable and unusable by unauthorized persons.

11.6.1 PORTABLE COMPUTING DEVICES

The following requirements apply to all ASI owned portable computing devices containing confidential or internal use data/information:

- Level 1 - Confidential information must not be stored on portable computing devices unless absolutely necessary and must be removed when the business reason for storage is no longer required. **Level 1 or Level 2 information may not be stored on non-ASI owned portable computing devices.**
- Physically secured when not in use.

- Encryption software must be loaded and correctly configured.
- Strong password protection rules must be observed for all user profiles.
- Operating system software must be kept current and antivirus software must be kept current on devices capable of running such software.

11.6.2 PORTABLE ELECTRONIC STORAGE MEDIA

The following requirements apply to all ASI owned portable electronic storage media containing confidential or internal use data/information:

The following requirements apply to all ASI owned portable electronic storage media containing confidential or internal use data/information:

- Level 1 - Confidential information must not be stored on portable electronic storage media unless absolutely necessary and removed when the business reason for storage is no longer required. The method for removal is outlined in the CSULB Records Management Standard. Level 1 or Level 2 information may not be stored on personally owned portable electronic storage media.

- All files must be encrypted.

11.6.3 DISPOSAL REQUIREMENTS

All confidential or internal use information stored on portable computing devices or portable electronic storage media must be sanitized prior to disposal in accordance with the CSULB Records Management Standard.

11.6.4 REPORTING LOSS OR THEFT

The loss or theft of a portable computing device or portable electronic storage media within the scope of this standard must be reported to the ASI Executive Director, ASI Information Technology Manager, University Police and the Office of Information Security Management and Compliance. If lost or stolen off-campus, local law enforcement must be notified and a police report obtained.

12.0 PROHIBITED USES OF INFORMATION ASSETS

Misuse of ASI's information assets is prohibited. Users are prohibited from utilizing information systems and services for any unlawful, unethical or unprofessional purpose or activity. Examples of prohibited use include but are not limited to:

- Attempting to modify or remove computer equipment, software, or peripherals
- Attempting to load software without the Information Technology Manager's approval
- Transmission of threats, harassment, or defamation
- Downloading or distributing material or programs that could be deemed harmful to information systems or services
- Violating any state or federal laws or any applicable ASI, CSU, or CSULB policy or regulation
- Intentionally accessing, viewing, downloading or disseminating materials containing obscene matter

- Intentionally damaging equipment, software, or data
- Accessing without proper authorization computers, software, information or networks to which the ASI belongs, regardless of whether the resource used is owned by the ASI or the access takes place from a non-ASI site
- Taking actions that interfere with the access of others to information assets
- Circumventing logon or other security measures
- Using information assets for purposes other than those for which they were intended or authorized
- Using information assets for unauthorized personal financial gain or for illegal purposes
- Sending any fraudulent electronic transmissions
- Violating any software license or copyright, including copying or redistributing copyrighted software
- Unauthorized sharing of peer-to-peer file copyrighted works, including music, pictures, and movies. Such actions are illegal and may carry significant financial and/or criminal sanctions.
- Using information resources, technology, or networks to harass or threaten users in such a way as to create a hostile workplace
- Disclosing proprietary information without the explicit permission of the owner
- Reading other users' information or files without the users' permission
- Leaving an unsecured work area while the workstation while is still logged-on to the computer. The user must be vigilant against illegal access by another party.

12.1 WEB BROWSING

Web Browsing represents a threat to the security of the workstation as well as to the whole organization. Being exposed to the dangers of web browsing is very easy as hostile scripts can be downloaded and executed automatically.

The following types of web browsing are specifically prohibited:

- Visiting online gambling websites
- Visiting pornographic websites
- Visiting hacking/cracking websites
- Visiting of Warez sites
- Visiting of gaming websites such as Flash-based games or other "profile based" installable games designed to circumvent applied security controls by IT staff.

12.2 COPYRIGHT AND FAIR USE

Federal copyright law applies to all forms of intellectual works, which include, but are not limited to, text in any format, graphics, art, photographs, music and software. No copyrighted material may be copied, reproduced, republished, uploaded, posted, transmitted, or distributed in any way, without explicit permission of the owner of the material, except as provided by the fair use provisions of the digital Millennium Copyright Act. Use of any ASI information assets to circumvent legitimate copyright protections is prohibited.

Prohibited electronic use of copyrighted materials includes, but is not limited to:

1. Reproduction of copyrighted materials, trademarks, or other protected materials without express written permission from the material's owner.
2. Usage of materials that enjoy protected status under current intellectual property laws in their own publications.
3. Distribution or duplication of copyrighted software without appropriate licensing agreements or use of software in a manner inconsistent with its license.
4. Distribution or reproduction, in any digital form, of copyrighted music, video, or other multimedia content without the express written permission of the material's rightful owner.

The "fair use" provisions of copyright law allow for the limited reproduction and distribution of published works without permission for such purposes as criticism, news reporting, teaching (including multiple copies for classroom use), scholarship, or research. The CSU document, "Fundamentals of Copyright and Fair Use" provides additional information on the Fair Use exception to copyright law.

Copyright infringements are a violation of Title 5 of the California Code of Regulations.

12.2.1 RESPONSIBILITIES

ASI has a legal duty to ensure that official websites, official email, and other official communication and expressions do not violate copyright law. Official web sites and communications include those that are funded or otherwise sponsored by ASI for an ASI purpose, or which are created by an employee, who is acting within the course and scope of employment.

Individual users/account holders/web content authors are responsible for assuring that their use of ASI information assets is in compliance with the copyright law, as well as CSU and CSULB policies on copyrighted materials.

ASI employees, who in the course and scope of employment, edit or publish other's content are not responsible for assuring compliance with governing law or policy and are not liable for copyright violations.

The University's Designated Agent is responsible for receipt, investigation and response to notices of copyright infringement.

12.2.2 RESPONSE TO POLICY VIOLATIONS

When there is reason to believe that a violation of this policy has occurred, an investigation will be conducted. User access to information assets may be temporarily suspended while an investigation is being conducted.

If the investigation involves an ASI staff member and warrants University action, an explanation of the causal events will be reported to the Executive Director and the Vice President for Student Services. In cases involving students, the Office of Judicial Affairs and the Dean of Students Office will be notified. Investigating officials will examine charges of violations with due respect for individual privacy, the security of other users, and the rights of due process.

Violations of ASI and/or University policy may result in sanctions, including but not limited to, limitation or revocation of access rights and/or reimbursement to ASI and/or the University for any expenses incurred related to the violation, including costs associated with the detection and investigation of the violation, as well as from the violation itself.

Violations of applicable statutes may result in criminal prosecution.

13.0 ASI WEBSITES

ASI Communications manages and operates all websites for the organization. Access to websites is restricted to authorized individuals trained by ASI Communications to properly operate the website according to current standards including, but not limited to, ADA (Americans with Disabilities Act), ATI (CSU Accessibility Technology Initiative), and W3C Standards.

The following uses of ASI websites are specifically prohibited:

- Circumventing ASI Communications in the creation, development, purchase, or any other acquisition of a website for any purpose not approved by ASI. Such sites are considered "Shadow" sites and are not permitted under any circumstance.
- Misrepresenting ASI or any of its departments
- Using ASI logos, graphics, and media created by ASI outside of an approved ASI website without express permission from ASI Communications and the Executive Director. These items are property of ASI.
- Linking to sites that contain viruses, malware, threatening or hateful speech, pornography, stolen goods, or other material that may be deemed offensive to visitors is strictly prohibited.

14.0 DISCLAIMERS

The use and operation of ASI information assets is subject to the following disclaimers:

- ASI accepts no responsibility for any damage or loss of data arising directly or indirectly from the use of those resources.
- Regular backups of files stored on servers are made to protect data in the event of hardware or software failure. However, ASI makes no warranty that all data can or will be restored, and accepts no responsibility for any damage or loss arising directly or indirectly from hardware or software failure, or human error.
- ASI accepts no responsibility for files that are not stored on network servers.
- Because the ASI network is part of the CSULB network and educational in nature, security measures may not provide adequate protection. Although every effort is made to maintain adequate security, ASI accepts no responsibility for any loss of privacy, theft or loss of information, or loss of data arising directly or indirectly from the absence or failure of security measures.

15.0 OWNERSHIP OF ASI INFORMATION ASSET RECORDS

All information asset records created through the use of ASI owned information assets are deemed property of ASI. ASI reserves the right to protect these files by placing them in a secure location on the file server. Proper access will be granted to those who need to use these files and restricted from those who do not.

16.0 ENFORCEMENT

Enforcement of ASI's Policy on Information Assets will be the responsibility of the supervisor of the department utilizing them. Compliance with this policy will be monitored by the ASI Network Administrator. Instances of non-compliance or violations of this policy will be reported to the appropriate division Director and Executive Director. Indication of any prohibited use will result in the immediate disabling of the computer account and/or user account until the situation is resolved with the appropriate division Director and Executive Director.

17.0 DISCIPLINE

Violation of this policy may result in disciplinary action, up to and including separation. Disciplinary action involving employees will be coordinated with the Human Resources Manager. The overall seriousness of the matter will be considered in setting the disciplinary action to be taken against the individual. Such action may include:

- Employee counseling
- Suspension of computing privileges
- Combination of the above
- Dismissal

Violations involving students who are not employees or volunteers of ASI will be reported to the Dean of Students.

18.0 ADMINISTRATION

The ASI Director of Administrative Services is responsible for the administration, revision, interpretation, and application of this policy. The policy will be reviewed triennially and revised as needed, unless earlier revisions are necessitated by changes in regulations of CSULB or the California State University Office of the Chancellor.

MOBILE SERVICE DEVICES

BACKGROUND AND PURPOSE

ASSOCIATED STUDENTS, INCORPORATED (ASI) RECOGNIZES THAT THE PERFORMANCE OF CERTAIN JOB RESPONSIBILITIES MAY BE ENHANCED BY, OR REQUIRE, THE USE OF A MOBILE SERVICE DEVICE. THE PURPOSE OF THIS POLICY IS TO ESTABLISH GUIDELINES FOR THE PROCUREMENT, POSSESSION, AND APPROPRIATE BUSINESS USE OF MOBILE SERVICE DEVICES BY OFFICERS AND EMPLOYEES OF THE ASI, AS WELL AS THE INTENT OF MOBILE SERVICE REIMBURSEMENTS. . POLICY STATEMENT

It is the policy of the ASI to facilitate access to efficient, cost effective telecommunication equipment and services when necessary for the fulfillment of an officer's or employee's essential duties and responsibilities. In cases where it is warranted, ASI will provide a mobile service device and plan to qualified employes, or reimburse an employee for par their use of a personal device. When provided by ASI, mobile service devices may be used for business purposes only. In addition, employees should only use mobile service devices when a less costly alternative does not exist. This policy and related procedures apply to all ASI departments.

19.0 ELIGIBILITY FOR MOBILE SERVICE DEVICES

Eligibility for mobile service devices or monthly usage reimbursements shall be limited to those officers or employees who have a legitimate business need to communicate via mobile phone during their work hours and in some cases, when not engaged in normal work hours. The following are the basic criteria for establishing "legitimate business need."

- The job function of the officer or employee requires considerable time outside of their assigned office or work area and it is important to ASI that he/she remain accessible during those times;
- The job function of the officer or employee requires them to be accessible outside of scheduled or normal working hours;
- The job function of the officer or employee requires them to have wireless data and internet access; and/or

- The employee is designated as a "first responder" to emergencies on campus.
- The corporation has concerns for the personal safety of an officer or employee who travels, works evening hours, works in isolated areas, or works in high crime areas

If an individual meets one or more of these criteria, they shall be considered a viable candidate for a mobile service device or monthly usage reimbursement. The assignment of mobile service devices or reimbursements shall be authorized only when there is a demonstrated need.

ASI-provided devices may only be assigned to employees who have been informed of ASI guidelines on the use of mobile service devices.

The purchase of mobile service equipment and plans by ASI shall be subject to approval by the ASI Executive Director or designee and will be processed through the ASI Business Office.

20.0 USE OF ASI-PROVIDED MOBILE SERVICE DEVICES

The following regulations govern the care and use of mobile service devices provided to officers and employees by ASI.

20.1 PHYSICAL SECURITY

Officers and employees shall take reasonable precautions to prevent theft and vandalism of any ASI-provided mobile service device. In the event that an ASI-provided mobile service device is lost, stolen, or vandalized due to one's failure to use reasonable precautions, ASI may require the officer or employee to reimburse ASI for the reasonable cost of replacing the equipment.

20.2 PERSONAL USE

The use of ASI-provided mobile service devices for personal business is prohibited except in cases of emergency. The employee shall reimburse ASI for any detectable charges for personal use.

20.3 RESPONSIBILITIES FOR ASI-PROVIDED DEVICES

20.3.1 PROCUREMENT AND COORDINATION OF EQUIPMENT

ASI shall designate a staff member to oversee all ASI-provided mobile service devices, with the following responsibilities:

- Receiving and reviewing proposals for services plans and making recommendations to management regarding selection of service plans
- Placing orders for equipment and service with the appropriate vendor
- Receiving and processing billing statements for ASI-provided mobile service devices and allocating costs to the appropriate departmental budgets
- Periodically distributing billing detail statements to assigned users for the identification of personal use
- Terminating service at the direction of an assigned user's supervisor or the Human Resources Department

20.3.2 DEPARTMENT SUPERVISORS

Department supervisors or their designees shall be responsible for the following:

- Receiving individual requests for mobile service devices and service plans and providing supervisor authorization to the ASI Business Office
- Assigning each mobile service device to one specific individual (Assigned User)
- Ensuring appropriate controls are in place for the security and maintenance of the equipment assigned to their staff
- Ensuring that all Assigned Users have received read the Policy on Mobile Service DevicesTo periodically audit the billing detail of assigned users under their supervision to detect any personal use

20.3.3 ASSIGNED USER

The Assigned User shall control and monitor the use and return of the mobile service device and shall be responsible for reimbursing the ASI for any personal use of their assigned mobile services device as indicated on the billing detail.

21.0 USE OF PERSONAL DEVICES

If an officer or employee meets the eligibility requirements for a mobile service device, as outlined above, but does not require an ASI-provided device, he or she may be entitled to a monthly reimbursement to cover the business-related use of their personal devices.

21.1 CELLULAR SERVICE REIMBURSEMENT

The Cellular Service Reimbursement must be requested by the employee to their direct supervisor. Approval to authorize a reimbursement and the amount of said reimbursement is required by the supervisor and division director.

The reimbursement will be paid as a flat rate per pay period, based on the selected service(s) and usage level(s) outlined below. ASI will pay only the agreed upon amount, even if monthly costs exceed the stipend. This flat rate will be reimbursed to employees as a fringe benefit in recognition of them providing ASI the use of their person mobile device. The Cellular Service Reimbursement, therefore, is not considered wages and is not a taxable benefit to the employee.

This reimbursement does not constitute an increase to base pay, and will not be included in the calculation of percentage increases to base pay due to merit increases, cost of living adjustments, reclassifications, or in-range progressions or to any benefits based on a percentage of salary.

The reimbursement is neither permanent nor guaranteed. ASI reserves the right to remove a participant from this reimburesement plan and/or cancel the reimbursement plan if there is insufficient funding to meet the plan costs, the employee's position no longer requires access to a mobile service device, or this policy is revised or terminated.

21.2 REIMBURSEMENT OPTIONS

The amount of the reimbursement will be determined based on the business use required of the officer's or employee's position and the minutes or data needed to perform their job responsibilities. A tiered model based on the current market rates* includes the following options:

Service type	Usage		
	Occasional	**Regular**	**Extensive**
Voice/Data/Text	$25	$45	Device and service plan provided by ASI

The amounts indicated above are per month. The reimbursement amount selected should cover all reasonable and appropriate business use, and may be comprised of one or more cellular services each with its own usage level.

An officer or employee receiving a monthly usage reimbursement must be able to show, if requested by their supervisor, a copy of the monthly access plan charges and business-related use to determine if the reimbursement amount is appropriate.

**The reimbursement rates will be evaluated, and if appropriate, adjusted annually to align to current market rates.*

21.3 RIGHTS & RESPONSIBILITIES OF PERSONAL DEVICE USERS

21.3.1 PROCUREMENT

The officer or employee is responsible for purchasing the mobile service device and establishing a service contract with the service provider of their choice. The service contract is in the name of the officer or employee, who is solely responsible for all payments to the service provider. The officer or employee will; determine plan choices, service levels, calling areas, service and phone features; and accepts termination clauses and payment terms.

ASI does not accept any liability for claims, charges or disputes between the service provider and the officer or employee. If the officer or employee terminates a service contract at any point, they must notify their supervisor within three business days to terminate the reimbursement.

21.3.2 PHYSICAL SECURITY

ASI assumes no responsibility for the loss, theft, or damage of an officer's or employee's personal device. Such devices are considered the personal property and responsibility of the officer or employee.

21.3.3 INFORMATION TECHNOLOGY SUPPORT

21.3.4 HTTPS://CSULB-MY.SHAREPOINT.COM/:F:/G/PERSONAL/JORDAN_ERES_CSULB_EDU/EUHLYNI513PBHBWKYRMCPOQBLMP9WOGMRXWW4LFUVC2BSW?E=QCZFJVDATA SECURITY AND MAINTENANCE

Mobile service devices covered by this policy are used in part to conduct ASI business and/or to create, receive, send, or store non-confidential ASI data. As a result, information contained on devices covered by this policy are also subject to Federal and State data maintenance laws (e.g., public records requirements, records retention requirements), as well as all ASI policies, including those pertaining to acceptable computing use and email. An officer or employee receiving an ASI monthly usage reimbursement must comply with Federal, State, and ASI requirements, and assist ASI in providing access to information about or contained on the mobile service device covered by this policy in response to requests for such information by third parties as required by Federal and/or State law.

Any mobile service device that has data capabilities must be password protected. If a mobile service device with data capabilities is stolen or missing, it must be reported to the employee's supervisor, the service provider, and to ASI Information Technology immediately

Officers and employees are expected to delete all ASI data from their mobile service devices when their employment with ASI is severed, except when required to maintain that data in compliance with a litigation hold notice.

21.4 CANCELLATION OF MONTHLY USAGE REIMBURSEMENT

Any reimbursement agreement will be immediately cancelled if an employee receiving a monthly usage reimbursement terminates employment with ASI. Any such reimbursement will also be cancelled if an employee changes job positions. In case of a change in job position, a new employee request for a device or reimbursement must be made to the new supervisor and division director, to establish the continued business need for a mobile service device.

If a personal decision by the employee, employee misconduct, or misuse of the device results in the need to end or change the service contract prior to the end of the contract period, the employee will bear the cost of any fees associated with that change or cancellation.

If a department decision (unrelated to employee misconduct) results in the need to end or change the service contract prior to the end of the contract period, the department will bear the cost of any fees associated with that change or cancellation. The original billing statement indicating the early termination charge must be submitted in order to be reimbursed in these circumstances.

Use of a device in any manner contrary to local, state, or federal laws will constitute misuse, and will result in immediate termination of the monthly usage reimbursement.

22.0 PROHIBITED USES

Regardless of whether an ASI-provided device or a personal device is used to conduct ASI business, the following practices are prohibited.

22.1 TRANSMITTING CONFIDENTIAL INFORMATION

Cellular transmissions are not secure. Employees shall refrain from using mobile service devices to relay confidential information.

22.2 DRIVING

An employee who uses a mobile service device is prohibited from using that device while driving, regardless of whether the business conducted is personal or ASI-related. This prohibition includes receiving or placing calls, text messaging, browsing the Internet, receiving or responding to email, checking for phone messages, or any other purpose related to their employment; ASI business; ASI customers; ASI vendors; volunteer activities, meetings, or civic responsibilities performed for or attended in the name of ASI; or any other personal or business-related activities not named here while driving. This prohibition includes the use of hands-free devices ("Bluetooth devices").

Except for emergency purposes, such as emergency calls to law enforcement, a health care provider, or the fire department, employees are expected to pull over and cease driving prior to using any mobile service device.

If an employee receives a citation(s) for violating the California Wireless Telephone Automobile Safety Act, the fines and penalties are solely the responsibility of the employee.

FORMS

The following forms 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	ASI Business Office	Executive Director	Must be completed and fully executed prior to the exchange of any confidential information
Cellular Service Reimbursement Request	To request a monthly reimbursement to compensate for the recurring use of a personal device for business use.	Human Resources Department	Employee Supervisor and Division Director	Must be submitted two weeks prior to beginning of the pay period in which the reimbursement becomes effective
Mobile Service Devices Usage Acknowledgement	To articulate and document assigned users understanding and agreement to abide by the California Wireless Telephone Automobile Safety Act, as well as ASI policy on device use	Human Resources Department	Assigned User	Must be submitted prior to the release of mobile service device to the assigned user

APPENDIX 1. PROTECTION MEASURES

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

Action	Level 1 – Confidential
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 drawer or file cabinet when the workstation is unattended and at the end of the w • All Confidential and Internal Use information must be stored in lockable drawers o • File cabinets containing Confidential or Internal Use information must be locked w when not attended. • Keys used to access Confidential or Internal Use information must not be left at an area. • Laptops must be either locked with a locking cable or locked away in a drawer or c 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 l • Copies of documents containing Confidential or Internal Use information must be removed from printers. • Documents containing Confidential or Internal Use information must be immediat facsimile machines.
Transmitting	**Distribution** Limited to those employees with an established business need-to-know and ar employees or someone who has signed a confidentiality agreement.
	Electronic Mail (email or attachments to email): May be sent within the CSULB email system (@csulb.edu) but not over a public network unl protected or encrypted.

	All email transmissions of confidential information must contain the follow statement: "The contained in this email message or its attachment is confidential. Dissemination or copying strictly prohibited. If you think that you have received this email in error, please email the se
	Mail (hard copy): Printed information may be sent through intercampus or U.S. mail but must be sealed in a p clearly marked, "To be Opened by Addressee Only".
	FAX: Authorized only from and to CSULB FAX machines. Information may not be sent to public FA
	Mail (hard copy): Printed information may be sent through intercampus or U.S. mail but must be sealed in a p clearly marked, "To be Opened by Addressee Only".
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 A Administrator, Level 1-Confidential Information may be stored on University owned lap portable electronic storage media, including but not limited to, CD-ROMs, DVD-ROMs, e drives, zip disks, flash-memory cards, magnetic cards and USB flash drives (a.k.a. Memo or Jump Drives). In such cases, laptops, desktops and portable electronic storage media data must be encrypted. If desktops used to process Level 1 data (not store) are in a secured campus office that authorized access, the appropriate administrator may choose not to encrypt the desktop. But this decision needs to be documented and approved in writ employee's Appropriate Administrator and the University CSULB Office of Information S Management and Compliance.* Level 1 information may not be stored on personal equipment such as personal laptops desktops, personal digital assistants (PDAs) iPods® or cell phones (such as BlackBerry®, iPhones®. See below for prohibitions regarding the storage of specific Payment Related Data**.
Retention	Records of any type of medium, such as paper, microfiche, magnetic, or optical, sha beyond the minimum retention period identified in the ASI Record Retention Schedule.

Disposition	Proper Media Sanitization Methods are described below.

**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.*

** *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:*
3. *Any of the following data elements:*
    a. *Payment verification code*
    b. *Payment verification value*

APPENDIX 2. DISPOSITION METHODS

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.
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.
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.