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 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.

Who Should Know This Policy

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

Definitions

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

Term	Definition
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	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 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.
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.

Term	Definition
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.
Portable device	Portable computing devices including, but not limited to, laptops computers, PDAs, and tablet PCs
Removable media	Portable electronic storage media including but not limited to, CDs and USB storage devices
System administrators	The Information Technology Manager and his/her designated staff
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

Standards and Procedures

1.0 Access to Information Assets

The Associated Students, Inc. (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.

1.1 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.

1.2 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.

1.2.1 Prohibited Software

Some applications are not permitted, such as peer-to-peer file sharing programs, spyware programs including toolbar add-ons to Internet Explorer, Netscape or other web browsers, internet phone programs including Skype, and programs where the end user license agreement is not concurrent with the policies listed in this document. These programs pose a substantial risk of hacker intrusion, virus transmission, and overall degradation of the ASI network systems. ASI will not install any application that could possibly result in harm to a workstation and/or the server systems.

1.2.2 Instant Messaging Software

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

1.2.3 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.

2.0 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.

2.1 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.

2.2 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.

3.0 Acceptable Use of Information Assets

3.1 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.

3.2 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.

3.3 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.

3.4 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. The following password standards are intended to thwart hacker attacks.

3.4.1 Minimum Password Length

All passwords must have a minimum of 8 characters.

3.4.2 Password History

The number of unique, new passwords that have to be associated with a user account before an old password can be re-used is 5.

3.4.3 Password Complexity Requirements

A password must meet the following requirements:

- It cannot be based on the user's name. The password cannot contain all or part of the user's first or last name.
- It must be case sensitive
- It must contain no spaces
- 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)
  - Non-alphanumeric characters (for example, # ! $ % %)

Following are some examples of passwords that meet these requirements: GoB3ach!, EduK8tr

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)

3.4.4 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.

3.4.5 Password Change Frequency

System	Frequency
SAGE MAS 200 Accounting	Every 90 days
Human Resources Information Systems (ABRA, Empower, ADP)	Every 90 days
BeachID	Annually

For systems not named above, a generally recommended change interval for passwords is at least annually.

3.5 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 the end of the workday.
- 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.

3.6 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.

3.6.1 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.
- Portable devices must be 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.

3.6.2 Portable Electronic Storage Media

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

- 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.

3.6.3 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.

3.6.4 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.

4.0 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.

4.1 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.

4.2 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.

4.2.1 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.

4.2.2 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.

5.0 ASI Websites

ASI Communications manages and operates all websites for the corporation. 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.

6.0 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.

7.0 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.

8.0 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 Information Technology Manager. 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.

9.0 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.

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.

Forms

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

Form Name	Purpose	Responsible Office	Approved By	Timeline for Submission
Acceptable Use Agreement	To gain access to ASI information assets by acknowledging receipt of and agreeing to abide by ASI's Policy on Information Assets	Human Resources Office	N/A	Must be completed upon hire or desired date of access. Allow 3 business days for processing.
MAS Access Level Request Form	To apply for user access to one or more modules of the accounting information system,	Information Technology	Information Technology Manager	Must be completed upon hire and updated whenever a change to access level is desired. Allow 3 business days for processing.