POLICY CONCERNING INFORMATION SECURITY AND DATA GOVERNANCE

PURPOSE

The following policy is intended to establish a comprehensive framework for the protection of Information Assets and the fulfillment of fiduciary duties by the Board of Directors of Associated Students Inc., California State University, Fullerton (ASI). Adherence to these regulations is necessary to ensure the organization remains in "Good Standing" with the University, protects student and donor privacy, and complies with all applicable California and Federal statutes.

Contents

WHO SHOULD KNOW THIS POLICY

- ☒ Budget Area Administrators
- ☒ Management Personnel
- ☒ Supervisors
- ☒ Elected/Appointed Officials
- ☒ Volunteers
- ☒ Grant Recipients
- ☒ Staff
- ☒ Students

DEFINITIONS

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

Terms	Definitions
Auxiliary Organization	A nonprofit entity, legally separate from the CSU, organized to provide essential services to the campus and governed by California Education Code §89900 et seq..
CSU Data Level 1	Confidential information where unauthorized disclosure could result in severe damage to the CSU or individuals (e.g., SSNs, medical records, credit card data).
CSU Data Level 2	Internal Use information that is not public but carries moderate risk if disclosed (e.g., student IDs, employee home addresses).
CSU Data Level 3	Information intended for public disclosure or designated as publicly available.
Fiduciary Duty	The legal obligation of Directors to act with “Duty of Care" (prudence) and "Duty of Loyalty" (in the organization's best interest).
Education Records	Records directly related to a student and maintained by an institution or a party acting for the institution (FERPA).
Information Assets	Any technical resource, including hardware, software, network systems, and the data contained therein, owned or managed by the CSU or the Auxiliary.

STANDARDS

1. GOVERNANCE AND OVERSIGHT

a. Board of Directors Authority:

The Board of Directors is the governing body responsible for the ultimate direction of the organization’s affairs. While management is delegated to professional staff under Corporations Code §5210, the Board retains ultimate legal responsibility for the organization’s actions and inactions

b. Board Responsibility:

In performing their duties, directors are entitled to rely on information, opinions, reports, or statements prepared by ASI officers, employees, legal counsel, or independent accountants, provided the director acts in good faith and without knowledge that would cause such reliance to be unwarranted.

c. Duty of Inquiry:

Directors are required to make reasonable inquiries when circumstances indicate a need, such as following up on security audit findings or technical vulnerabilities.

d. Administration

The ASI System Administrator is responsible for the administration, revision, interpretation, and application of this policy. They will periodically evaluate, test, and adjust the information security and data governance program to validate that equipment and systems function properly and produce the desired results. The ASI System Administrator will perform ongoing assessments to ensure that employees follow written procedures for information security and data governance.

2. INFORMATION SECURITY STANDARDS (CSU Information Security Policy and Standards)

a. Adoption of Standards:

ASI has adopted the CSU Information Security Policy and Standards (formerly ICSUAM 8000) and its associated ISO-aligned domains as its primary security framework.

b. Asset Management:

All ASI data must be classified according to the CSU Data Classification Standard. Inventories of assets containing Level 1 or Level 2 data must be maintained throughout their lifecycle.

c. Access Control:

1. User Access Control

ASI will grant access to information assets to its employees, student leaders, and volunteers when required for the performance of their essential duties and responsibilities. Access to specialized software such as accounting or human resources information systems will be provided to users with a documented need. All such users will complete an ASI Help Desk ticket regarding access. The IT Department will get the approval of the department head before granting access. All ASI computers must be authenticated clients of the campus network. All ASI users must log into the campus domain using their valid CSUF email account.

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 Department to ensure that applicable licensing requirements have been met.

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

3. LEGAL AND NON-PROFIT COMPLIANCE

a. Privacy of Information:

ASI shall implement "reasonable security procedures" to protect personal information from unauthorized access, as required by California Civil Code §1798.81.5.

b. Records Retention:

ASI shall follow the CSU Systemwide Records Retention and Disposition Schedules. Electronic and paper files must be properly handled during leadership transitions to prevent unauthorized destruction. ASI is a nonprofit public benefit corporation and must comply with restrictions on transactions involving directors with material financial interests. ASI maintains its Record Retention and Document Management through the ASI Policy Concerning Corporate Management.

4. PERSONNEL AND WORKPLACE SECURITY

a. Background Checks:

Background checks are mandatory for any position (staff, student leader, or volunteer) with access to Level 1 Data or sensitive Information Assets.

b. Security Training:

All users with access to ASI/CSU Information Assets must complete annual Information Security Awareness training.

c. Separation of Duties:

Management shall ensure a proper separation of duties to prevent any single individual from having unchecked authority over sensitive financial or data.

5. MOBILE DEVICES AND REMOTE ACCESS ELIGIBILITY

a. Data Security:

All mobile devices provided to employees for ASI business are handled through CSUF Information Technology and follow the CSUF IT rules and regulations. The devices must be password protected. Confidential information (Level 1) must not be stored on personal devices or transmitted via unencrypted email.

b. Remote Access Eligibility

If the participating employee’s job activities require access to campus via Virtual Private Network (VPN), the participating employee is required to use ASI-owned computer equipment, in order to protect the integrity of the campus network. Level 1 or Level 2 information may not be stored on non-ASI owned portable computing devices.

Equipment used by the participating employee to connect via VPN must be reviewed by the ASI Information Technology department and approved in writing by ASI System Administrator. ASI Employees must take reasonable precautions to ensure that their devices (e.g., computers, tablets, smart phones, etc.) are secure before connecting remotely to ASI information assets and must close or secure connections to campus desktop or system resources (i.e., remote desktop, virtual private network connections, etc.) once they have completed ASI-related activities or when the asset is left unattended.

c. Severance of Service:

Upon separation or end of an elected term, all organization-owned hardware must be returned to the Information Technology department.

6. ENFORCEMENT

Failure to comply with this policy may result in disciplinary action, personal liability for Directors under the Corporations Code in cases of gross negligence, or the removal of the Auxiliary's "Good Standing" status.

DATE APPROVED: **04/21/2026**
DATE REVISED: