Payment Card Acceptance

Purpose

The purpose of this policy is to establish business processes and procedures for accepting payment cards that will minimize risk and provide the greatest value, security of data, and availability of services to each ASI merchant account. In response to increasing incidents of identity theft, the major payment card companies created the Payment Card Industry Data Security Standard (PCI DSS) to help prevent theft of customer data. PCI DSS applies to all businesses that accept payment cards to procure goods or services. Compliance with this Standard is enforced by the payment card companies and generally, non-compliance is discovered when an organization experiences a security breach that includes cardholder data.

Security breaches can result in serious consequences for Associated Students, Incorporated, including release of confidential information, damage to reputation, the assessment of substantial fines, possible legal liability and the potential loss of the ability to accept payment card and e-Commerce payments.

Policy Statement

It is the policy of the Associated Students, Incorporated (ASI) to observe and comply with the rules and regulations established by the Payment Card Industry (PCI) and articulated in the PCI Data Security Standards (DSS). Additionally, these regulations are intended to ensure that payment card acceptance procedures are appropriately integrated with the ASI's financial and other information systems. This policy applies to all ASI employees, contractors, consultants or agents who, in the course of doing business on behalf of ASI, accept, process, transmit, or otherwise handle cardholder information in physical or electronic format.

This policy applies to all ASI departments and administrative areas which accept payment cards regardless of whether revenue is deposited in an ASI or University account. Responsibility for the execution and monitoring of this policy has been delegated by the Executive Director to the Director, ASI Administrative Services.

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
A.S. Business Office	The ASI office that approves all third-party service providers and coordinates the policies and procedures for accepting payment cards at ASI (USU-229)
Cardholder	The customer to whom a payment card has been issued or the individual authorized to use the card
Cardholder Data	All personally identifiable data associated with the cardholder (i.e., account number, expiration date, cardholder name)
Encryption	The process of converting information into an unintelligible form to anyone except holders of a specific cryptographic key. Use of encryption protects information between the encryption process and the decryption process against unauthorized disclosure
Department Supervisor	A supervisory employee within a department who has primary authority and responsibility for payment card and e-Commerce transaction processing within that department
Department	Any ASI department or unit that accepts payment cards bearing the logos of any of the five members of the Payment Card Industry Security Standards Council (American Express, Discover, JCB, MasterCard or VISA) as payment for goods and/or services, or to accept donations
Payment Card	Any payment card/device that bears the logo of American Express, Discover Financial Services, JCB International, MasterCard Worldwide, or VISA, Inc.

Term	Definition
Payment Card Account Change	Any change in the payment account including, but not limited to: • the use of existing payment card accounts for new purposes; • the alteration of business processes that involve payment card processing activities; • the addition or alteration of payment systems; • the addition or alteration of relationships with third-party payment card service providers, and • the addition or alteration of payment card processing technologies or channels
Payment Card Industry (PCI) Data Security Standard (DSS)	A multi-faceted security standard that includes requirements for security management, policies, procedures, network architecture, software design and other critical protective measures.
Sensitive Authentication Data	Security-related information (card validation codes/values, full magnetic-stripe data, or personal identification number (PIN)) used to authenticate cardholders, appearing in plain-text or otherwise unprotected form.

Regulations

1.0 Acceptable Payment Cards

ASI currently accepts VISA and MasterCard and has negotiated contracts for processing payment card transactions. Individual ASI units may not use or negotiate individual contracts with these or other payment card companies or processors. All individual ASI departments must use the ASI-negotiated contracts.

2.0 Prohibited Payment Card Activities

Associated Students, Incorporated prohibits certain credit card activities that include, but are not limited to:

- Accepting payment cards for cash advances
- Discounting a good or service based on the method of payment
- Adding a surcharge or additional fee to payment card transactions
- Using a paper imprinting system unless prior approval is granted by the A.S. Business Office

3.0 Payment Card Fees

Each payment card transaction will have an associated fee charged by the credit card company. Payment card fees will be allocated to the corresponding general ledger account of the Department.

4.0 Refunds

When a good or service is purchased using a payment card and a refund is necessary, the refund must be credited back to the account that was originally charged. Refunds in excess of the original sale amount or cash refunds are prohibited.

5.0 Chargebacks

Occasionally a customer will dispute a payment card transaction, ultimately leading to a chargeback. In the case of a chargeback, the department initiating the transaction is responsible for notifying the A.S. Business Office and for providing appropriate supporting documentation.

6.0 Maintaining Security

- All departments and administrative areas accepting payment cards on behalf of ASI are subject to the Payment Card Industry Data Security Standards (PCI DSS).
- ASI prohibits the transmission of cardholder data or sensitive authentication data via e-mail or unsealed envelopes through campus mail as these are not secure.
- ASI requires that all external services providers that handle payment card information be PCI compliant.
- ASI restricts access to cardholder data to those with a business "need to know."
- For electronic media, cardholder data shall not be stored on servers, local hard drives, or external (removable) media including floppy discs, CD's or thumb (flash) drives unless encrypted and otherwise in full compliance with PCI DSS.
- For paper media, cardholder data shall not be stored unless approved for legitimate business purposes by the Director, ASI Administrative Services.

7.0 Responsibilities

7.1 Department Supervisor

Department Supervisors are responsible for:

- Executing on behalf of the relevant Department, the Application for Payment Card Account Acquisition or Change.
- Ensuring that all employees (including Department Supervisor), contractors, and agents with access to payment card data within the relative Department acknowledge on an annual basis and in writing that they have read and understood this Policy. These acknowledgements should be submitted to the Director, ASI Administrative Services.
- Ensuring that all payment card data collected by the relevant Department in the course of performing ASI business, regardless of whether the data is stored physically or electronically is secured. Data is considered to be secured only if all of the following criteria are met:
    - Only those with a "need to know" are granted access to payment card and electronic payment data;
    - Email is not to be used to transmit credit card or personal payment information. If it should be necessary to transmit credit card information via email only the last four digits of the credit card number can be displayed;

- Credit card or personal information is never downloaded onto any portable devices or media such as USB flash drives, compact disks, laptop computers or personal digital assistants;

- Fax transmissions (both sending and receiving) of credit card and electronic payment information occurs using only fax machines that are attended by those individuals who must have contact with payment card data to do their jobs;

- The processing and storage of personally identifiable credit card or payment information on ASI computers and servers is prohibited;

- Only secure communication protocols and/or encrypted connections to the authorized vendor are used during the processing of e-Commerce transactions;

- The three or four digit validation code printed on the payment card is never stored in any form;

- The full contents of any track data from the magnetic stripe are never stored in any form;

- The personal identification number (PIN) or encrypted PIN block are never stored in any form;

- The primary account number (PAN) is rendered unreadable anywhere it is stored;

- All but the last four digits of any credit card account number are masked when it is necessary to display credit card data;

- All media containing payment card or personal payment data is retained no longer than a maximum of six (6) months and then destroyed or rendered unreadable; and

- Notifying the CSULB Director, Information Security Management and Compliance (562)985-8260 in the event of suspected or confirmed loss of cardholder data. Details of any suspected or confirmed breach should not be disclosed in any email correspondence. After normal business hours, notification shall be made to the University Police, (562) 985-4101.

7.2 Information Technology Manager

The ASI Information Technology Manager shall regularly monitor and test ASI's network and coordinate ASI's compliance with the PCI Standard's technical requirements and verify the security controls of systems authorized to process credit cards.

7.3 CSULB Director, Information Security Management and Compliance

The CSULB Director, Information Security Management and Compliance shall maintain currency with the requirements of the PCI DSS and related requirements and communicate these to ASI to help ASI ensure that this policy remains current. She/He shall coordinate and lead any campus response to a security breach involving cardholder data.

7.4 Director, ASI Administrative Services

The Director, ASI Administrative Services shall:

- Provide training to ensure that applicable ASI departments are trained in accepting and processing payment cards in compliance with this policy;
- Work with external vendors and coordinate payment card policies, standards, and procedures;
- Serve as liaison between the A.S. Business Office, Information Technology Manager, and ASI department for Payment Card account acquisition or change procedures; and
- Review and modify the Application for Payment Card Account Acquisition or Change as necessary.
- When required, conduct the ASI PCI DSS Self-Assessment and complete the ASI's Attestation of Compliance.

7.5 CSULB Internal Auditing Services

CSULB Internal Auditing Services shall:

- Periodically review ASI compliance with this policy and the Payment Card Industry (PCI) Data Security Standards (DSS); and
- Identify unapproved payment applications or external vendors that collect payment card data on behalf of ASI and notify the A.S. Business Office

8.0 Payment Card Account Acquisition or Change Procedures

To acquire or change a payment card account, the Department Supervisor must submit an Application for Payment Card Account Acquisition or Change to the A.S. Business Office (USU-229). The application must be signed by the Department Supervisor and appropriate ASI Director. Applications that request e-Commerce activities must also be signed by the ASI Information Technology Manager. All e-Commerce activities shall be processed by a third-party vendor authorized by ASI.

All requests shall be reviewed by the Director, ASI Administrative Services, the CSULB Director of Information Security Management and Compliance, and the CSULB Director, Network Services. The Director, ASI Administrative Services shall respond to all applications. When an application to acquire a payment card account is approved, the Director, ASI Administrative Services will assist the Department Supervisor in establishing the new merchant account activity. All card processing terminals shall be obtained through the A.S. Business Office.

The Department Supervisor may appeal a decision to deny an application to acquire or change a payment card account to the ASI Executive Director and the CSULB Associate Vice President, Financial Management.

9.0 Wireless Technology

ASI discourages the use of wireless technology to process or transmit cardholder data. Requests for Payment Card Account Acquisition or Change that include the use of wireless technology will be reviewed on a case by case basis and shall carefully consider the need for the technology against the risk of a non-secure payment environment.

If the use of wireless technology is approved, the storage of cardholder data on local hard drives, floppy disks or other external media is prohibited. It is also prohibited to use cut-and-paste and print functions during remote access. Activation of modems for vendors will be permitted only when no other alternative is available and will be immediately deactivated after use.

10.0 Sanctions

The Executive Director and/or the CSULB Associate Vice President, Financial Management may suspend credit card account privileges of any department or administrative unit not in compliance with this policy or that places ASI and the University at risk.

Any department or administrative unit engaged in payment card activities will be responsible for any financial loss due to inadequate internal controls or negligence in adhering to the PCI Data Security Standard.

11.0 Training

Employees who are expected to be given access to cardholder data shall be required to complete upon hire, and at least annually thereafter, security awareness training focused on cardholder data security. Employees shall be required to acknowledge at least annually that they have received training, understand cardholder security requirements, and agree to comply with these requirements.

Forms

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

Form Name	Purpose	Responsible Office	Approved By	Timeline for Submission
Application for Payment Card Account Acquisition or Change	To acquire or change a payment card account	A.S. Business Office	Director, ASI Administrative Services	Submit at least two weeks before desired date of payment card acceptance