ASU Merchant Account Request

Please complete this request and email it to Merchant Services at merchants@asu.edu.

Merchant name: This is the name that will be displayed on the cardholder's statement. Please be descriptive and remain under 25 characters, including spaces. Begin at space five.

A	S	U	—																					
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Visa and MasterCard merchant accounts will be established. If you have a business need to accept payment cards other than Visa and MasterCard, please explain and list card type(s):

_____

Department's physical address: _____

Department's financial contact name: _____ Email: _____

Department contact's phone number: _____ Fax: _____

Department phone number to appear on the cardholder's statement — required: _____

What percentage of sales will be card present and not present? **Note**: It must equal 100 percent.

- Present: _____
- Not present: _____

Product or service to be sold: _____

Is the business seasonal?

☐ Yes. List the active months: _____

☐ No.

Estimated average ticket amount: $_____

Annual Visa and MasterCard volume: $_____

Workday account to record revenue

Cost center and program or grant: _____ Revenue code: _____

Optional Workday worktags: _____

Approval

_____

Cost center, project or grant manager signature Date

By signing this form, the cost center, program or grant manager approves establishing this merchant account for the business purpose stated and assumes responsibility for compliance with the Payment Card Industry Data Security Standard as outlined in the merchant responsibilities acknowledgment.

PCI DSS and merchant responsibilities acknowledgment

Major credit card companies, such as American Express, Discover, JCB International, Mastercard and Visa, have published a uniform set of data security standards that all merchants must comply with regarding accepting payment cards. The standards place additional responsibilities on ASU departments to accept payment cards.

The standards are called the Payment Card Industry Data Security Standard and the Payment Application Data Security Standard. ASU must comply with these security standards to accept payment cards. Non-compliance with these standards puts ASU at risk of the following:

- Loss of faith by the ASU community.
- Loss of merchant status for your department.
- Possible loss of merchant status for all of ASU.
- Significant monetary fines assessed to your department or ASU.

Compliance is required from all merchants and service providers that store, process or transmit cardholder data. The program applies to all payment channels, including retail, mail or telephone order and e-commerce. Before becoming a merchant site, you must review your security for credit card and other sensitive data relating to the PCI Security Standards Council requirements.

General rules, regulations and guidelines

Security

- ASU merchants are required to review the Payment Card Industry Data Security Standard.
- E-commerce gateways must be PCI DSS certified and compliant with ASU's security requirements.
- Electronically captured information must be in an encrypted secure socket layer meeting the PCI DSS requirements with minimum need-to-know basis access to cardholder information.
- Vendor technical documents provided to the merchant must be kept in a secure location and not shared with anyone without prior approval from Merchant Services.
- If you process credit card data in any form — face-to-face or electronically — you must comply with PCI DSS.
- It is prohibited to store card information and card validation codes on any ASU computer, database or server. You must protect cardholder data by keeping it secure and confidential.
- To comply with ARS §44-7501, the PCI DSS payment card industry provisions and requirements, all suspected or confirmed security compromises must be reported immediately by completing the following steps:
    - Contact the ASU Experience Center online or call 855-278-5080.
    - Email the ASU Information Security Office or submit a ticket in My ASU.
    - Email PCI Merchant Services at pci@asu.edu.
- If a breach has occurred with the data you are storing, you may be responsible for all externally imposed fines and costs associated with bringing your location into compliance. Treat the following as high-risk transactions:
    - Shipping addresses from:
        - Hospitals.
        - Mail drops.
        - Overseas.
        - Prisons.
    - Use of an anonymous email address.
- You agree not to disclose or acquire information concerning a cardholder's account without the cardholder's consent.
- You will not sell, purchase, provide, disclose or exchange card account information or other details.

- You agree to maintain all card documentation containing card account numbers in a secure environment, restricting user access to payment card account numbers on a need-to-know basis. Credit card receipts and documentation must be treated the same way you would treat large cash sums. Your department is responsible for any losses due to inadequate internal controls. Secure environments include:
    - File cabinets in a locked office.
    - Locked drawers.
    - Safes.
- You must keep all original, imaged or microfilmed copies of card documentation for no less than 180 days and no longer than two years, depending on the retained documentation. After this period, cardholder data must be deleted or shredded before it is physically disposed of.
- You must not collect card numbers and card information via email, unsecured or network fax machines or cell phones, as they are not secure formats.

The department must agree to comply with the latest PCI DSS Standards and ASU PCI best practices.

Contact Merchant Services at merchants@asu.edu for questions or more information.