Arizona State University
Deposits - Payment Card Processing
Best Practices

Background:

The major credit card companies (VISA, MasterCard, Discover, American Express and JCB International) have published a uniform set of data security standards that ALL merchants (i.e. ASU Departments) must comply with in connection with the acceptance of payment cards. These standards are called the Payment Card Industry Data Security Standard or PCI DSS, and the Payment Application Data Security Standard or PA-DSS. These standards place additional responsibilities on ASU departments in connection with the acceptance of payment cards. ASU must comply with these security standards in order to continue to accept payment cards.

Non- compliance with these standards puts ASU at risk for:

- Large monetary fines assessed to your department and/or Arizona State University
- Loss of merchant status for your department
- Possible loss of merchant status for all of Arizona State University
- Loss of faith by the community in the Arizona State University name

The PCI DSS is a multifaceted security standard that includes requirements for security management, policies, procedures, network architecture, software design and other critical protective measures. This comprehensive standard is intended to help organizations proactively protect customer account data.

The PA-DSS standards are to assist software vendors and others develop secure payment applications that do not store prohibited data, such as full magnetic stripe, CVV2 or PIN data, and ensure their payment applications support compliance with the PCI DSS. Payment applications that are sold, distributed or licensed to third parties are subject to the PA-DSS requirements.

Arizona State University (ASU) adheres to the highest standards for protecting sensitive data. Payment card data is highly sensitive and therefore must meet the security compliance standards established by the payment card industry. Departments should contact Financial Services, Payment Card Services prior to pursuing any services or applications that may involve accepting credit cards as a form of payment.

Services for processing payment cards, whether through Point of Sale (POS) terminals, mail/telephone order or over the Internet, and any specialized programs or services (e.g. shopping carts, electronic check payments) that link through an electronic bank card authorization system (payment gateway) will be contracted on an University wide level through the Financial Services office in conjunction with the Information Security office and Purchasing department.

Departments may only use the services of vendors which have been approved by ASU's Financial Services, Information Security office and Purchasing departments to process payment card transactions regardless of whether the transaction is point of sale (POS), mail/telephone order or internet based.

Approved merchant departments are to adhere to the Payment Card Data Security Standard, federal, bank and card association regulations and University polices. The merchant department's ability to accept payment cards is conditioned on complying with, and maintaining these standards and policies. If the merchant

department fails compliance, they are responsible for correcting any deficiencies immediately as directed by Financial Services, Payment Card Services and the Information Security Office to bring their merchant department into compliance. Failure to comply with PCI DSS or university policies may result in revocation of merchant department's privilege to accept payment cards. The merchant department is responsible for all costs associated with any security scans or reviews deemed necessary by the Information Security Office or the Payment Card Associations.

A merchant department that plans to receive revenue from external sales or services and provide taxable goods to customers outside of the University should contact their Financial Services Office accountant to discuss sales tax requirements.

Payment cards may not be accepted for University gifts and/or donations. All gifts and donations are processed through the ASU Foundation and departments should contact them for additional information on gift processing.

No University employee, contractor or agent who obtains access to payment card or other personal payment information in the course of conducting University business may sell, purchase, provide or exchange said information in any form including, but not limited to, imprinted sales slips, copies of imprinted sales slips, mailing lists, tapes or other media obtained by reason of a payment card transaction to any third party other than to the University's acquiring bank, depository bank, VISA, MasterCard or other payment card company or pursuant to a government request. All requests to provide information to any party outside of the merchant department must be coordinated with the Information Security Officer and Financial Services, Payment Card Services.

Best Practices:

Any ASU department ("Merchant") accepting payment cards on behalf of ASU for goods or services should designate a full time employee within that department who will have primary authority and responsibility for payment card and/or ecommerce transaction processing within that department. This individual will be referred to hereafter as the Merchant Responsible Person or "MRP". All MRP's will be responsible for the department complying with the security measures established by the payment card industry and university policies. In addition, the MRP is responsible to ensure any employee who processes transactions takes the Financial Services Cash Handling Online Training and if applicable have the appropriate background check completed before any access is granted to the employee.

Requests to accept payment cards by University departments are made by completing the ASU Merchant Account form and submitting it to the Financial Services, Payment Card Services office. Merchant departments may not accept payment cards, or authorize or complete settlement transactions for other University departments.

Responsibility	Action
Merchant Department	1. Select a Merchant Responsible Person (a designated individual within the department who will have primary authority and responsibility for payment card transaction processing and security compliance). 2. Complete the ASU Merchant Account request form. 3. Submit all completed and signed documents to Payment Card Services. 4. Follow security measures established by the payment card industry and university policies. 5. Notify Payment Card Services immediately when accounts are no longer needed and should be deactivated. 6. Follow the responsibilities and guidelines in the ASU Merchant Account request form.
Payment Card Services	1. Provide information and assistance to University departments that are analyzing the responsibilities and costs of accepting payment cards as a form of payment. 2. Review merchant account request form and accompanying documents submitted by departments to establish a merchant account and accept payment cards as a form of payment for services performed or for merchandise sold by department. 3. Establish the merchant account, order any required equipment and coordinate the implementation of payment card processing for the merchant department. 4. Ensure the appropriate and timely recording of deposits, processing fees and chargebacks to the university accounting system.

Cross References:

1. FIN 108, “Sales Tax”
2. FIN 307, “Departmental Cash and Check Receipting”
3. Payment Card Merchant Security Requirements:
    - Arizona Revised Statute (A.R.S.) 44-7501-Notification of Breach of Security System; enforcement; civil penalty; preemption; exceptions; definitions http://www.azleg.gov/FormatDocument.asp?inDoc=/ars/44/07501.htm&Title=44&DocType=ARS
    - Payment Card Industry Data Security Standard (PCI DSS) and Payment Application Data Security Standard (PA DSS) https://www.pcisecuritystandards.org/merchants/
    - Visa USA Cardholder Information Security Program (CISP) http://usa.visa.com/merchants/risk_management/cisp.html
    - MasterCard Worldwide http://www.mastercard.com/sdp
    - American Express: www.americanexpress.com/datasecurity
    - Discover Financial Services: http://www.discovernetwork.com/disc.html