Payment card processing best practices

Major credit card companies — 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. They place additional responsibilities on ASU departments to accept payment cards.

These 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 for the following reasons:

- 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.

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 helps organizations proactively protect customer account data.

ASU adheres to the highest standards for protecting sensitive data. Payment card data is susceptible and must meet the security compliance standards established by the payment card industry. Departments should contact Merchant Services before pursuing any services or applications that may involve accepting credit cards as a payment method.

Services for processing payment cards, whether through point-of-sale terminals, mail or telephone order or over the internet — and any specialized programs or services linking through an electronic bank card authorization system — will be contracted on a university-wide level through Merchant Services in conjunction with the Information Security Office and Purchasing and Business Services.

Departments may only use the services of vendors approved by Merchant Services, the Information Security Office and Purchasing and Business Services to process payment card transactions regardless of whether the transaction is by point of sale, mail or telephone order or internet based.

Approved merchant departments must adhere to the payment card data security standard, federal, bank and card association regulations and university policies. The merchant department's ability to accept payment cards is conditioned on complying with and maintaining these standards and procedures. If the merchant department fails compliance, they are responsible for correcting any deficiencies immediately as directed by Financial Services, Merchant Services, and the Information Security Office to bring their merchant department into compliance.

Failure to comply with PCI DSS or university policies may revoke the merchant department's privilege to accept payment cards. The merchant department is responsible for all costs associated with security scans or reviews deemed necessary by the Information Security Office or the payment card associations.

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

Payment cards may not be accepted for university gifts or donations. The ASU Foundation processes all gifts and donations. Departments should contact the ASU Foundation for more information about gift processing.

No university employee, contractor or agent who obtains access to a payment card or other personal payment information while conducting university business may sell, purchase, provide or exchange said information in any form including, but not limited to:

- Copies of imprinted sales slips.
- Government requests.
- Imprinted sales slips.
- Mailing lists.
- Mastercard, Visa or other payment card companies.
- Tapes or other media obtained because of a payment card transaction to any third party other than the university's acquiring or depository bank.

Employees must coordinate all requests to provide information to any party outside the merchant department with the Information Security Office and Merchant Services.

Best practices

Any ASU department that accepts payment cards on behalf of ASU for goods or services should designate a full-time employee with primary authority and responsibility for payment card and e-commerce transaction processing within that department. This individual will be referred to hereafter as the Merchant Responsible Person (MRP).

All MRPs 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 for ensuring that any employee who processes transactions takes the Financial Services cash handling training available in Career EDGE and, if applicable, has the appropriate background check completed before the employee is granted access.

Requests to accept payment cards by university departments are made by completing the ASU Merchant Account Request and Agreement and submitting it to Merchant Services. Merchant departments may not accept payment cards or authorize or complete settlement transactions for other university departments.

Responsibilities and actions

Merchant department

Actions:

1. Select an MRP — a designated individual within the department with the primary authority and responsibility for payment card transaction processing and security compliance.
2. Complete the ASU Merchant Account Request and Agreement.
3. Submit all completed and signed documents to Merchant Services.
4. Follow security measures established by the payment card industry and university policies.
5. Notify Merchant Services immediately when accounts are no longer needed and should be deactivated.
6. Follow the responsibilities and guidelines in the ASU Merchant Account Request and Agreement form.

Merchant Services

Actions:

1. Provide information and assistance to university departments analyzing the responsibilities and costs of accepting payment cards as a form of payment.
2. Review the ASU Merchant Account Request and Agreement and accompanying documents submitted by departments to establish a merchant account and accept payment cards as payment for services performed or merchandise sold by the department.
3. Establish the merchant account, order 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.

Resources

- FIN 108: Sales tax.
- FIN 301-04: Deposits — payment card processing.
- FIN 305: Deposits at University Cashiering Services.
- Payment card merchant security requirements:
    - American Express PCI compliance.
    - ARS §44-7501.
    - Discover PCI compliance.
    - Mastercard SDP program.
    - PCI DSS compliance with Visa.
    - PCI security standard merchant resources.