Financial Services Manual (FIN)

FIN 301–04: Deposits—Payment Card Processing

Effective: 3/12/2015 **Revised**:

Purpose

To set standards for payment card processing by departments and establish responsibility for overall management of the university's payment card programs.

Sources

Arizona Revised Statutes (ARS) § 44-7501
Arizona Board of Regents Policy Manual -3-101
Arizona Board of Regents Policy Manual - 3-102
University policy

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 that act, or will act, in the capacity of a "merchant" by accepting credit or payment card payments) must comply with in order to accept payment card payments. These standards are called the Payment Card Industry Data Security Standard (PCI DSS), and the Payment Application Data Security Standard (PA DSS). 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.

These standards place additional responsibilities on ASU merchant departments in connection with the acceptance of payment cards and ASU must comply with these security standards to continue to accept payment cards. Non-compliance with these standards puts ASU at
risk for:

- large monetary fines assessed to a department and/or to Arizona State University
- loss of merchant status for a department
- possible loss of merchant status for all of Arizona State University
  and/or
- loss of faith by the community in the Arizona State University name.

For more information on PCI DSS specifications and how they apply see the "PCI SSC Data Security Standards Overview" at: https://www.pcisecuritystandards.org/security_standards/index.php.

Policy

Payment card data is highly sensitive information. Therefore, ASU must adhere to the security compliance standards established by the payment card industry. ASU Payment Card Services, in coordination with ASU's Information Security Office, is responsible for the overall management and ongoing oversight of the university's payment card acceptance

program. This includes management of the relationship with the university's acquiring bank and coordination of compliance efforts. Furthermore, departments involved in payment card processing must adhere to all of the following:

1. Prior to pursuing any services or applications that may involve accepting payment cards as a form of payment, departments must contact ASU Payment Card Services for guidance with security reviews and contracts. Departments must only use the services of vendors to process payment card transactions that have been approved by ASU Payment Card Services, ASU's Information Security Office, and Purchasing and Business Services.
2. Each merchant department must maintain procedures that identify the roles and responsibilities for oversight of payment card activities for their departmental unit, and maintain compliance with the PCI DSS and other relevant standards and requirements for processing and securing card holder data.
3. Each merchant department is responsible for its costs and accountability with payment card acceptance including, but not limited to, merchant discounts, fees, costs of processing services, equipment, software maintenance, incident investigations, fines, remediation, and notification to customers. Each merchant department is also responsible for the privacy and security of any card holder data that it obtains, as well as the security and integrity of any Web site or Web application through which it processes online payments.
4. A merchant department that plans to receive revenue from external sales or services and provide taxable goods or services to customers outside of the university should contact its Financial Services accountant to discuss sales tax requirements.
5. Departments **must not** accept payment card payments for university gifts and/or donations because all gifts and donations are processed through the ASU Foundation. Departments should contact the ASU Foundation for additional information on gift processing.
6. Merchant departments **must not** accept payment cards, or authorize or complete transactions, for other university departments.

Procedures

Permission for Payment Card Payment Processing

University departments that wish to accept payment cards must complete the ASU PCI DSS Merchant Responsibilities Acknowledgement agreement and submit it to ASU Payment Card Services. See also the PCI Best Practices for information about using a third-party vendor to process payment card transactions.

Departmental Controls

Any ASU merchant department accepting payment cards on behalf of ASU for goods or services must designate a full-time employee within that department who will have primary authority and responsibility for payment card and e-commerce transaction processing within that department. This designee will be responsible for departmental compliance with all security measures established by the payment-card industry, the Information Security Office, the ASU PCI DSS Merchant Responsibilities Acknowledgement agreement, and this policy. In addition, before any merchant services access is granted to any employee who will process transactions, the departmental designee is responsible for ensuring that:

1. the employee completes the Financial Services Online Cash Handling Training

   and

2. if applicable, the department has performed/requested the appropriate background check for the employee.

Data Breach Notifications

In the event of a breach or suspected breach of security, the individual who, or merchant department that, suspects a security breach must immediately notify ASU's information security officer and Payment Card Services. E-mail and a verbal confirmation should be used for the initial notification but details of the breach, including sensitive data, should not be disclosed in any correspondence.

Additional Information

For additional information about security standards and practices, see:

1. *Arizona Revised Statutes (ARS)* § 44-7501
2. Merchant security requirements for payment cards:
    - Payment Card Industry Security Standards Council, https://www.pcisecuritystandards.org
    - PCI SSC Data Security Standards Overview, https://www.pcisecuritystandards.org/security_standards/index.php
3. ASU permission requests and best practices for payment cards

    and

4. ASU information security overview, policies, and standards.

Cross-References

For more information on ASU's security standards and background check processes, see the *Academic Affairs Policies and Procedures Manual*:

1. ACD 125, "Computer, Internet, and Electronic Communications Information Management Policy,"

    and

2. ACD 126, "Reference Check and Background Verification."

For more information on financial considerations and procedures, see:

1. FIN 103, "Departmental Record Keeping"
2. FIN 108, "Sales Tax"

    and

3. FIN 305, "Deposits at University Cashiering Services."