THE UNIVERSITY OF ARIZONA

Financial Services Office
Bursar's Office

888 North Euclid, Room 104
PO Box 3520
Tucson, Arizona 85722-3520
tel (520) 621-3232
fax (520) 621-4233
www.bursar.arizona.edu

CAMPUS MERCHANT BANK CARDS (CREDIT) ACCEPTANCE AGREEMENT

The University of Arizona provides a contract with Bank of America to supply the University units with the option to accept bank cards (credit) to sell goods, and services to its customers. With this service, the University merchants are subject to, must understand and must comply with all rules, regulations and contractual provisions regarding the handling of bank cards. The regulations include the University Information Security Policy, Payment Card Industry Standards and Card (MC, VISA, AMEX, DISCOVER) Association merchant requirements. These rules and regulations must be adhered to as the department/unit or the University may be subject to severe financial penalties for failure to comply.

In an effort to insure that University merchants understand and comply with the above, all University merchants must agree to and follow the following provisions. These provisions are not intended to be an exhaustive list of all applicable requirements. At a minimum, Campus Merchants should familiarize themselves with FRS Department Manual Policies 8.10 and 8.14, the PCI-DSS, PA-DSS (both located online at https://www.pcisecuritystandards.org), the University Information Security Policy (http://security.arizona.edu) and all supporting standards. The PCI-DSS Compliance Action Plan (located at http://security.arizona.edu/pci) offers additional guidance. Refer to the online glossary at https://www.pcisecuritystandards.org for definitions of certain terms used in this Agreement.

Please review and initial after each statement and sign the bottom of the agreement to indicate your intent to comply.

1. Receipt of Card Data:
    a. Point of Sale Terminals/Dial Pay:
        i. Bank card must be swiped and receipt signed for any goods or services. If the back of the card is not signed, picture identification of customer must be obtained before continuing transaction.
        ii. If the bank card is unable to be swiped electronically and the card number is "keyed" in, the bank card must be imprinted on the sales form provided by Bank of America.
        iii. All customer/merchant receipts must not display the Primary Account Number (payment card number) except for the last 4 digits.
        iv. It is prohibited to transmit bank card information (e.g. account numbers, expiration dates, etc) via email.
        v. If card numbers are obtained through the mail or on paper, the information containing the card numbers must be retained in a secure locked area and must be restricted and/or blocked from view of third party and others without the business need to know.

_____(initial)

    b. eCommerce:
        i. All electronically captured information must be in an encrypted secure socket layer (SSL) that meets the Card Industry Standards with minimum access to cardholder information.

ii. All eCommerce gateways must be PCI certified and compliant with The University of Arizona security requirements.
iii. All University merchants must utilize a "hosted order page" service of the gateway or any gateway that does not require that the cardholder information be entered on an order page residing on any University web page nor server. Thereby, insuring that the cardholder information is not obtained, stored nor passes through the University servers.

_____(initial)

c. Software Based Merchants:
   i. The third party vendor application is certified and validated and listed on the VISA Payment Application Best Practices (PABP) validated and certified secure application list or PCI SSC list of PA-DSS Validated Payment Applications which both can be accessed at http://usa.visa.com/merchants/risk_management/cisp_payment_applications.html

   ii. All customer/merchant receipts must not display the card number except for the last 4 digits (truncation).
   iii. Card numbers must not be transmitted via email.
   iv. If card numbers are obtained through the mail or on paper, the information containing the card numbers must be retained in a secure locked area and must be restricted and/or blocked from view of third party and others without the need to know.

_____(initial)

2. Transmission of Bankcard Information:
   a. In addition to restrictions on methods of transmittal in the PCI-DSS, bankcard information must **not** be transmitted through the following devices:
      i. Email
      ii. Network connected fax machine
      iii. Non-encrypted network components and servers
      iv. Cell phones
      v. Lap top computers

_____(initial)

3. Storage and Disposal:
   a. Cardholder Information must not be stored on any system, computer, technology device, server, or point of sale device after authorization.
   b. Department point of sale terminals must be settled daily and cleared after settlement.
   c. Any cardholder information in paper format must be stored in a secure (locked) limited access area for a period of time no longer than is necessary to meet document retention of the individual units.
   d. Access to the area which is used to process, transmit or store cardholder data must be restricted to authorized University personnel on a need to know basis. All card holder information must not be physically present at workstations when the employee is not physically present.
   e. If possible, merchant receipt must be truncated. If terminal is unable to truncate or the unit utilizes mail in or phone order printed forms that includes cardholder information, the personal account number (cc#) and expiration date must be rendered unreadable and unrecoverable except the last four digits after authorization.

f. Storage of the Card validation code (the three digit value printed on the signature line of the card) is strictly prohibited.

_____(initial)

4. Network and Systems:
    a. All network components, servers and purchased and custom applications that are part of the payment card system must conform to all current PCI-DSS requirements. For more information, visit www.pcicomplianceguide.org. An outline of the primary principles and requirements follows. Refer to the PCI-DSS (located online at https://www.pcisecuritystandards.org) for the detailed elements of each.
        i. Building and Maintaining a secure network
            1. Install and maintain a firewall configuration to protect data
            2. Do not use vendor supplied defaults for system passwords and other security parameters
        ii. Protecting Cardholder Data
            1. Protect stored data
            2. Encrypt transmission of cardholder data and sensitive information across public networks.
        iii. Maintaining a Vulnerability Management Program
            1. Use and regularly updated anti-virus software
            2. Develop and maintain secure systems and applications.
        iv. Implementing Strong Access Control Measures
            1. Restrict access to data by business need to know
            2. Assign an unique ID to each person with computer access
            3. Restrict physical access to cardholder data
        v. Regularly Monitoring and Testing Networks
            1. Track and monitor all access to network resources and cardholder data
            2. Regularly test security systems and processes
        vi. Maintain a Department Information Security Departmental Policy that addresses information security standards which follows and meets all University Information Security Standards and PCI-DSS requirements.

_____(initial)

5. Payment Card Industry Standards Program:
    a. Annually, upon direction of FSO-Bursar Campus Banking & Merchant Services all merchants must complete the PCI-DSS Self-Assessment Questionnaire appropriate to their operation. All questionnaire assessment fees will be the responsibility of the department. Services will be available to assist Units with completing the questionnaire.
    b. All eCommerce merchants will work with their payment eCommerce gateway providers to perform the appropriate network (external and internal) scans quarterly, semi-annually or annually.

_____(initial)

6. Reconciliation:
    a. The merchant is responsible to review monthly merchant statements for accuracy and report any adjustments needed within 60 days of statement date to FSO-Bursar Campus Banking & Merchant Services.

_____(initial)

7. Security Compromise:
    a. To meet the Arizona Revised Statute (A.R.S). 44-7501 (Notification of Breach of Security System), University Information Security Policy and PCI-DSS Bank Card industry provision and requirements, all suspected and/or confirmed security compromises will be reported immediately to FSO-Bursar Campus Banking & Merchant Services and the University Information Security Office.
    b. Any questions regarding compromise can be directed to FSO-Bursar Campus Banking & Merchant Services or the Information Security Office.

_____(initial)

8. Merchant Services:
    a. FSO-Bursar Campus Banking & Merchant Services will be notified of any department merchant service changes.
    b. FSO-Bursar Campus Banking & Merchant Services will facilitate all equipment leasing/purchasing and return of equipment.

_____(initial)

9. Applicable Requirements:
    a. I have reviewed FRS Department Manual 8.10 & 8.14
    b. I have reviewed the Payment Card Industry Data Security Standards (located online at https://www.pcisecuritystandards.org).
    c. I have reviewed the University Information Security Policy and related standards.

_____(initial)

I understand and agree to comply with the above:

Merchant Name: _____

Merchant Responsible Person Name: _____

Contact Phone and Email: _____

Signature: _____ Date: _____

Department/Unit Head Name: _____

Department: _____

Title: _____

Signature: _____ Date: _____