The U of A Mel and Enid Zuckerman College of Public Health Department Merchant (Credit Card) Payment Card Acceptance Security Policy - Center for Rural Health

PURPOSE: This Policy is to provide guidance and establish compliance with Payment Card Industry (PCI-DSS) (https://www.pcisecuritystandards.org) standards and requirements. The policy will be adhered to by all areas that handle credit card payments processes within this College. Each procedure that processes or transmits cardholder data (CHD) will be required to follow this policy.

POLICY:

1) All ecommerce solutions utilized to process customer credit card purchases will utilize gateways/applications that are designed to host the customer's order credit card payment through a third party PCI compliant system using a hosted order page. The MEZCOPH E-store will not store/retain customer credit card personal account numbers or magnetic strip information electronically on any servers, systems or paper. At no time will the department utilize any software applications, services, nor create procedures, processes that stores/retains customer credit card personal account numbers after credit authorization. All credit card software applications used to authorize credit card transactions will utilize transaction numbers, tokenization, or other method that renders the credit card personal account information unreadable/unavailable to the department staff. All ecommerce solutions utilized to process customer credit card purchases will utilize gateways/applications that are designed to host the customer's order credit card payment through a third party PCI compliant system using a hosted order page.

   NOTE: The management staff does not physically handle or have access to cardholder Data. Therefore, PCI-DDS V1.2, Section #9 (9.6-9.9) is not applicable to our unit.

2) Each year, a management staff person(s) will be designated the Merchant Responsible Person (MRP) that is assigned the responsibility of upholding and meeting all PCI-DSS compliance, University of Arizona Information Security and FRS Policy 8.14-Merchant BankCard/Credit Card Acceptance Policy and Procedure standards. In addition the Merchant Responsible Person will be responsible for the following:
   a. A Campus Merchant Bank Cards (Credit) Acceptance Agreement (www.bursars.arizona.edu) has been completed and sent to the FSO-Department Services Merchant Liaison in the Bursars office. This agreement outlines the responsibilities and awareness requirements of accepting credit cards.
   b. Review with the assigned *Department Information Security Liaison*, personnel that all applicable configurations, equipment, processes have been approved and meet

all PCI-DSS requirements, Campus Information Security Policies and UITS Security Operation Guidelines.

c. Assures the Self Assessment Questionnaire A is completed annually.
d. Attend the mandatory Annual Campus Merchant Security Awareness meeting held in October and semi-annual meeting in February.
e. Annually review PCI-DSS standards to insure that all new/changed standards have been reviewed and addressed by the department.
f. Maintain a PCI compliant folder (paper or electronically) of all PCI compliance supporting documentation.
g. No new credit card merchant services may be established without the approval of the assistant dean of finance.

3) Maintain an Information Security Policy (*PCI–DSS V2.0 Req. Sec. 12*): This department security policy addresses Merchant (CHD) information security for employees and contractors and is maintained, published and disseminated to all relevant system users. This policy addresses all PCI-DSS requirements, required annual processes to identify threats and vulnerabilities and yearly risk assessments and annual review.

i. No employee will input to the software applications, gateways etc. customer credit card information on any personal or department technology. Examples include: remote access technologies, wireless technologies, removable electronic media, laptops, PDAs, email and internet usage. Employee facing technology can represent a threat to the security of confidential data.
ii. All gateways, software applications that are contracted to process and authorize credit card information must verify that they are PCI-DSS compliant. The department will verify annually that the applications/gateway compliance is current by reviewing the latest VISA list of CISP compliant service providers.
iii. Information Security Responsibilities stated in this document will be adhered to at all times. It is the responsibility of each employee to acknowledge, agree, and authenticate electronically that they have read and understood The University of Arizona information security policy http://security.arizona.edu/files/IS100.pdf regarding non-disclosure of personal information of students and customers. The personal information includes, but is not limited to credit card, banking, and social security information. This authentication occurs upon accepting UACCESS and FERPA regulations.
iv. All employees will complete the mandatory Campus Information Security Awareness program.

4) Third Party Contracts/Service providers that have access to cardholder data are required to adhere to Payment Card Industry Security requirements. Per Campus Procurement and Contracting, any Agreement must contain the acknowledgement from the third party/ service provider that they understand and are responsible for the security of the cardholder data. The service providers must supply an annual letter of compliance to the department (o*n file at Bursar's Office Campus Banking & Merchant Services)*.

5) Management staff is responsible to assign a Department Information Security person. This person has direct responsibility for or must assign the responsibility for the following:
    a. Establish, document, distribute security policies and procedures, and require all employees to acknowledge in writing that they have read and understand the established security policy required by Campus Information Security Office and FSO-Bursars by performing mandatory security awareness training.
    b. Monitor and analyze security alerts and information, and distribute to appropriate personnel.
    c. Sets-up merchant accounts as sales accounts.
    d. Review and monitor all procedures and process that address access to credit card processing/authorizing.
    e. Employee security awareness program to train all employees via multiple communication methods.
    f. Follow campus processes that all potential employees who will have access to systems, networks, or cardholder data have been screened in accordance to Campus Human Resource guidelines.
    g. Understand the Incident response plan/procedures outlined by the Campus Information Security Office and FSO Bursar Merchant Services (http://utis.arizona.edu/services/security/report_incident) and develop a departmental incident response procedure. The plan includes the following:
        i) Training of all staff the proper protocol to follow in case of a suspected or known breach.
        ii) Maintain a list of roles, responsibilities and communication strategies in the event of a compromise.
        iii) Lessons learned review and remediation action after all breaches
        iv) Annual test the plan
        v) Outline specific personnel that are designated to be available on a 24/7 basis
        vi) Insure that all alerts from intrusion-detection, intrusion-prevention and file integrity monitoring systems are included.
    h. Establish, document, and distribute security incident response and escalation procedures to ensure timely and effective handling of all situations.

Credit Card (CHD) Security Policy Resource Links and Appendices

FSO-Bursar Department Services:
http://www.bursar.arizona.edu/departments/bankcard/index.asp
Campus Information Security Office: http://security.arizona.edu/
Payment Card Industry Standards: https://www.pcisecuritystandards.org/