Accounting and Administrative Manual

Title: E-commerce
No.: C-14 Effective
Date: August 25, 2021
Review Date: June 7, 2022

I. Introduction

E-commerce refers to monetary transactions using an electronic medium, including activities that involve the buying and selling of goods and services over the Internet.

This procedure concerns the approval process for E-commerce products and services.

The university encourages the use of E-commerce as a means to efficiently conduct business and seeks effective internal controls surrounding E-commerce activity.

II. Approval Process

E-commerce activities must be approved in advance by the respective Vice Chancellor of Administrative Services, or designee, and the Vice President of Finance/CFO, or designee.

The Vice President of Finance/CFO, or designee, has authorization to provide exceptions as described in this procedure.

III. Guidelines

The following shall be satisfied in the approval process:

A. Payment Card Industry Data Security Standards (PCI DSS). See also Accounting and Administrative Policy No. C-13 Administrative Policy for PCI Compliance
B. Banking standards, including internal Cash Management procedures
C. Cash remittance to university within 48 hours, unless exception is approved by Chief Finance Officer
D. Procurement standards
E. A contract is in place with third-party vendors
F. Use of the university's approved payment card processor
G. Existing E-commerce solutions within the UA System be used
H. Identification of main departmental contact
I. Net economic benefit
J. Other standards, as applicable

The first payment card processing solution that departments should utilize is the University's centrally hosted E-commerce system, as it is Payment Card Industry and NACHA compliant.

UA has approved payment gateway, acquirer bank, and Point-of-Sale equipment to provide a PCI compliant E-commerce solutions for university payment card transactions. University organizations should receive approval before entering into any contracts for purchases of payment card services, software and/or equipment. Units should utilize University Contract Services for purchases and contracts must include the appropriate Payment Card Industry Data Security Standard (PCI DSS) language. Board of Regents -Corporate Authority Resolution authorizes UA's Chief Finance Officer to enter into finance related contracts and agreements. Only University approved equipment, payment gateways, and processes may be utilized – unless a written request for exemption is provided and approved. This requirement applies regardless of the transaction method or technology used (e.g. E-commerce, Point of Sales device, etc.).

Units should not set up their own banking relationships. Payment card revenue must be deposited into designated University of Alaska bank accounts within two days. The Office of UA Finance Units negotiate all banking and payment card processing relationships on behalf of the entire University System, thereby taking advantage of the volume discounts, reviewing internal controls and competitive pricing, etc.

If an organization wants to use a payment processing solution other than TouchNet or the approved payment gateway, provide your campus PCI office with the vendor contact information, proof of vendor PCI compliance, and application documentation. The CFO/FinSys will evaluate the vendor product for compliance with University's E-commerce security guidelines. The Campus PCI Office will forward the information and their recommendations to the Controller's Office and E-commerce team to evaluate the vendor product for compliance with University's E-commerce security guidelines.

Items needed before approving an exception to using the University's E-commerce application follows:

1. Provide a justification for use of a non-contracted vendor
2. Type-of-Point of Sales (POS) system (terminal, card processing terminals, related hardware and software)
3. State PCI DSS SAQ requirements associated with requested vendor/POS
4. Document that the vendor and POS system is PCI DSS compliant
5. Provide vendor attestation of compliance with PCI DSS standards
6. Document vendor POS is compatible with UA systems network

7. Provide vendor's encryption capabilities for campus IT/OIT security review
8. Provide documentation for internal compatibility with UA's payment processing, merchant bank, and
    a. Pass through authentication from customer's application to TouchNet or approved payment gateway
    b. Receipt redirect from TouchNet or approved payment gateway to customer's application
    c. Code examples of the pass-through authentication and receipt redirect
    d. Touchnet or approved payment gateway generic test site URL
    e. Nondisclosure agreements
9. Document procedures for working with Merchant Bank, ACH, and Money transfer process.
10. Additional forms/documentation may be requested.

The respective university and the PCI Advisory Committee shall keep a perpetual inventory of approved and active E-commerce activities, to allow for oversight, coordination and communication.