Accounting and Administrative Manual

Title: E-commerce  
No.: C-14  
Effective Date: October 22, 2020

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 activities.

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 Bursar and/or Associate Vice Chancellor of Financial Services, or designee, and the Chief Finance Officer, or designee.

The Chief Finance Officer, 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 2-5 business days, unless exception.
D. Procurement standards
E. A contract is in development with third-party vendors
F. Use of the university’s approved payment card processor, unless exception as below
G. Existing E-commerce solutions within the UA System be used, to extent feasible
H. Identification of main departmental contact
I. Net economic benefit or efficiency in business processing described
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 contracted with Touchnet Market place and TSYS Bank to provide a PCI compliant e-commerce solution for university payment card transactions. (The UA centralized e-commerce software solution is Touchnet Marketplace. This system is configured and verified to meet current PCI DSS and university data security requirements.)

University organizations should receive approval before entering into any contracts for purchases of payment card services, software and/or equipment. Units should utilize Procurement & Contract Services for purchases and contracts must include the appropriate Payment Card Industry Data Security Standard (PCI DSS) language. 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 may not set up their own banking relationships. Payment card revenue must be deposited into designated University of Alaska bank accounts within xx days. The Office of Cash Management negotiates all banking and payment card processing relationships on behalf of the entire University System, thereby taking advantage of the volume discounts and internal controls not available to individual departments or business units.

If an organization wants to use a payment processing solution other than TouchNet, provide your campus PCI office with the vendor contact information, proof of vendor PCI compliance, and application documentation. Campus PCI Offices (i.e. Bursar’s Offices) will evaluate the vendor product for compliance with University’s e-commerce security guidelines. The university designee(s) will forward the information and their recommendations to the Controller’s Office to evaluate the vendor product for compliance with University’s e-commerce security guidelines.

Items needed to support an exception to using the University’s E-commerce application follows to be provided to CFO/Compliance Office:

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. What PCI DSS SAQ requirements are associated with this 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
8. Provide documentation for internal compatibility with UA’s payment processing, merchant bank, and
   a. Pass through authentication from customer’s application to Touchnet
   b. Receipt redirect from Touchnet to customer’s application
   c. Code examples of the pass-through authentication and receipt redirect
d. Generic test site URL

e. Nondisclosure agreements if applicable


The respective university and the controller’s office shall keep a perpetual inventory of approved and active E-commerce activities, to allow for awareness, coordination and communication.