Administrative Policy for Payment Card Industry (PCI) Date: 03/26/10
No.: C-13 Page: 1 of 6

POLICY:

It is the policy of the University of Alaska that all payment card transactions are to be executed in compliance with standards established by the Payment Card Industry Security Standards Council, which includes Visa, MasterCard, American Express, JCB International, and Discover. This policy does not apply to purchasing cards. Nothing in this policy is intended to create, extend, or support any cause of action or other claim for damages against the university or its employees acting within the scope of their employment.

Departments are not permitted to transmit, process, or store payment card (either credit or debit card) information on University computers, servers, workstations, or on other electronic media (Email, Internet, Fax Machines, CD/DVD media, or flash drives). When cardholders visit university online sites they must be redirected to a PCI compliant (University approved) third party site to transmit, process, or store the payment card information, or be processed with applications adopted and supported by the University of Alaska.

SCOPE/APPLICABLITY:

This policy applies to all payment card merchants at the University. It applies to merchants accepting payment card payments using a payment card terminal connected to a data phone line as well as merchants processing or sending transactions over the Internet. Internet transactions include links on UA websites (which are processing payment cards for UA) redirecting customers to another website, use of software including Point-of Sale software on a computer to transmit, process, or store cardholder data, use of third party vendors to transmit, process, or store cardholder data information and use of wireless equipment. Scope of PCI also applies to the networks and phone lines being used for transmission and connectivity between workstations and other devices. The University Credit Card Merchant Policy requires each department that accepts payment cards be approved by the designated MAU Office and where applicable approved by the Office of the Chief Information Officer.

BACKGROUND:

Accounting and Administrative Manual

Accounting and Administrative Manual

vii. If cardholder data is shared with service providers then obtain and examine all contracts with the company and any other affiliated third party providers that would handle the cardholder data (for example, backup tape storage facilities, managed service providers such as Web hosting companies or security service providers, or those that receive data for fraud modeling purposes)

1. Service providers must contain provisions requiring adherence to the PCI DSS requirements.

2. Confirm that the agreement includes an acknowledgement that the service provider is responsible for the security of cardholder data the provider possesses.

f. Submit to quarterly external vulnerability scans conducted by an Approved Scanning Vendor (ASV).[xii]

10. Each year employees handling cardholder data will be required to sign an agreement verifying their understanding of their responsibilities as it relates to security and PCI compliance.[xiii]

11. All merchants and third party vendors at the University must remain PCI Compliant at all times.

12. All third parties with access to cardholder data must comply with both PCI-DSS and university's policies.

13. All service providers must be Level 1 per the lists of validated service providers as maintained by Visa and MasterCard.[xiv]

14. All payment applications hosted on the University Systems must be on the PA-DSS list maintained by the PCI Council and an approved vendor by the University.[xv]

15. Annually, in October, all merchant account holders will submit a signed Self Assessment Questionnaire (SAQ).

NON-COMPLIANCE:

Merchants not complying with this administrative policy will lose the privilege to accept payment card payments until compliant. Additionally, fines may be imposed by the affected payment card brand in the case of a data breach; they could start at $50,000 for

the first offense and go higher depending on the decision made by the acquirer. Person in