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:

As a result of payment card breaches and the resulting customer distrust in using credit and debit cards as a payment option, the payment card industry has formed a council called the Payment Card Industry (PCI) Security Standards Council which includes Visa, MasterCard, American Express, JCB International, and Discover. This PCI Council has

developed Data Security Standards (DSS) to assure consumers that their brands and using payment cards are reliable and secure. These standards include controls for handling and restricting cardholder data, computer and Internet security, and reporting of a breach of cardholder data. These standards are mandated by the industry in order for a merchant to accept payment cards.

As a merchant, the University of Alaska must adhere to the security guidelines or face significant financial penalties. In addition to such penalties, any compromise of cardholder information undermines public confidence in the University's ability to maintain appropriate stewardship over confidential information entrusted to it. Lack of compliance in a single area of the University could result in fines and jeopardize the entire University's ability to accept payment cards in any area. Each department or unit will be responsible for achieving and maintaining compliance for their distinct merchant identification number (MID).

REQUIRED PRACTICES:

1. Store no electronic cardholder data anywhere.[i, ii]
2. Paper copies containing cardholder data will be destroyed within 1 business day at which point they will be cross-cut shred.[i]
3. If a Primary Account Number (PAN) is necessary to be stored, it must be truncated. The only acceptable display is no more than the first 6 and last 4 digits.[iii]
4. PANs must not be sent via any electronic means.[iv]
5. Access to cardholder data and PAN's (whether on paper or electronically) is restricted to only those with a need to know.[v] Remote access to cardholder data is strictly prohibited.[vi]
6. When storing paper cardholder data, it should be in a locked device (cabinet, safe, room, etc) with restricted access.[vii]
7. Destruction of hardcopy (paper) must be cross-cut shred before disposing of it.[ii]
8. Movement of media containing cardholder data must be classified as confidential, logged, and authorized by the University.[viii]
9. In order to transmit cardholder data, an electronic media must meet the following requirements:

a. Be isolated from all University software and University network resources (either through its own connection to the Internet, a virtual LAN, or a separate phone line).

b. Allowed to only access the University system wide authorized payment gateway, no other Internet resources should be accessible.

c. Anti-virus software must be installed and up to date, actively running, and capable of generating audit logs before any transactions are transmitted.[ix]

d. Current security patches must be applied to machines before any transactions are transmitted.[x]

e. Adhere to the Office of Information Technology Credit Card regulations which require the following:[xi]

    i. Establish, publish, maintain and disseminate a security policy.

        1. Annually, identify threats and vulnerabilities, and formal risk assessment.

        2. Annually, information security policy is reviewed and updated to reflect changes to business objectives or the risk environment.

    ii. Daily operational security procedures must provide specifications regarding account maintenance procedures and log review procedures.

    iii. Examine the critical employee facing technologies (such as modems and wireless).

        1. Explicit management approval (partial reference, R02.07.041)

        2. Authenticate devices with username and password or other authentication item (example token).

        3. List all devices and personnel access.

        4. Labeling of all devices with owner, contact information and purpose.

5. List acceptable uses of technology. (partial reference, P02.07.050)
6. Acceptable network locations for technologies.
7. List company-approved products.
8. Automatic disconnect of modem sessions after a period of inactivity.
9. Activation of modems for vendors only when needed by vendors, with immediate deactivation use.
10. When accessing cardholder data remotely via modem, prohibition of storage of cardholder data onto local hard drives, floppy disks, or other external media. Prohibition of cut-and-paste and print functions during remote access.

iv. Security policy must clearly define information security responsibilities for all employees and contractors.

v. Assignment of information security from a Chief Security Officer or other security-knowledgeable member of management.

1. Require employees to acknowledge in writing that they have read and understood the security procedures.
2. Monitor and analyze security alerts and information, and distribute to business management personnel.
3. Establish, document, and distribute security incident response and escalation procedures to ensure timely and effective handling of all situations.
4. Administer user accounts – account and authentication management
5. Monitor and control access to data.

vi. Require employees to acknowledge in writing that they have read and understood the University's PCI DSS related policies and procedures.

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 violation of this policy may be subject to a full range of sanctions, including the loss of computer or network access privileges, disciplinary actions, suspension, termination of employment and/or legal action. Some violations may constitute criminal offenses under local, state and federal laws. The University will carry out its responsibility to report such violations to the appropriate authorities.

---

[i] Requirement 3.1
[ii] Requirement 9.10
[iii] Requirement 3.3
[iv] Requirement 4.2
[v] Requirement 9.9
[vi] Requirement 7.1
[vii] Requirement 9.6
[viii] Requirement 9.7
[ix] Requirement 5.2
[x] Requirement 6.1
[xi] Requirement 12.1, 12.3, 12.4, 12.5, 12.6, 12.8,
[xii] Requirement 11.2
[xiii] Requirement 12.6.2
[xiv] Requirement 12.8
[xv] Requirement 12.8.1