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) without prior approval of the Chief Financial Officer. 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/APPLICABILITY:
This policy applies to all payment card merchants at the University. It applies to UA merchants accepting payment card payments using a payment card terminal connected to a data phone line as well as UA 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 approved vendor websites for payment processing 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 business 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. The PCI Council has developed Data Security Standards (DSS) to assure consumers that their brands and payment card processes are reliable and secure. These standards include controls for handling and restricting cardholder data, securing IT infrastructure, and reporting 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 PCI DSS compliance requirements. UA has approved vendors for banking and processing credit cards. If the business process requires non-approved vendors (termed as 3rd party service providers) for integration with/without existing card processors, then an exception can be requested by the MAU. Such requests must be presented to the PCI Advisory Team consisting of Controller, Financial Systems, Cash Management, IT Security, PCI Compliance Manager, Internal Audit and General Counsel. The contracts with 3rd party service providers must include the language adhering to the PCI DSS. 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. 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. MAU business offices will maintain and update the inventory of each merchant identification number (MID), address, contact person, IP addresses and related software version of the computer/laptop/mobile device. MAU business offices must maintain logs of authorized personnel having access to payment portals, and personnel must be trained on how to detect tampering of card processing terminals. Each department or unit will be responsible for achieving and maintaining compliance for their distinct MID. In case of card information received via mail and phone, orders must be processed within 1 business day and any written card/personal identifiers must be cross-shredded. In the event of a data breach, stolen computers/mobile devices used to process credit cards, the UA will adhere to the Information Security Incident & Breach Handling Procedure Please contact ua-security@alaska.edu.

REQUIRED PRACTICES by PCI Council:

1. Install and maintain a firewall configuration to protect cardholder data
2. Do not use vendor-supplied defaults for system passwords and other security parameters
3. Protect stored cardholder data
4. Encrypt transmission of cardholder data across open, public networks
5. Protect all systems against malware and regularly update anti-virus software or programs
6. Develop and maintain secure systems and applications
7. Restrict access to cardholder data by business need to know
8. Identify and authenticate access to system components
9. Restrict physical access to cardholder data
10. Track and monitor all access to network resources and cardholder data
11. Regularly test security systems and processes
12. Maintain a policy that addresses information security for all personnel

RESPONSIBILITIES

1. Define the PCI environment for each MID and establish controls that meet PCI compliance.
2. Each year employees and authorized volunteers handling cardholder data will be required to sign an agreement verifying their understanding responsibilities as it relates to security and PCI compliance.

3. When handling paper cardholder data, it must be locked in a secure device with authorized and restricted access.

4. When a business process requires handling of credit card holder data in paper form (for example, fundraising events, annual gala events etc.), the paper copies containing cardholder data will be destroyed within one business day.

5. Destruction of hard copy (paper) must be by cross cut shredder before disposal.

6. If a Primary Account Number (PAN) is necessary to be stored, it must be masked. (First 6 or last 4 digits may be maintained).

7. PANs must not be sent outside the PCI environment.

8. Access to cardholder data and PAN’s (whether on paper or electronically) is restricted to only those with a need to know. Remote access to cardholder data and PAN’s should be in accordance with the most current PCI standards.

9. Movement of media containing cardholder data must be classified as confidential, logged, and authorized by the University.

10. Systems responsible for transmission of cardholder data must be compliant with PCI standards.

11. All merchant account holders must submit to monthly/quarterly external vulnerability scans conducted by an Approved Scanning Vendor (ASV).

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

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

14. All service providers must be responsible for maintaining PCI compliance as mandated by the PCI Security Standards Council.

15. All payment applications hosted on the University System must be on the PCI DSS list maintained by the PCI Council and be a University-approved vendor.

16. Annually, in October, all merchant account holders must submit the applicable signed Self-Assessment Questionnaire (SAQ).

NON-COMPLIANCE:
Merchants not complying with this administrative policy may lose the privilege to accept payment card payments until compliant. Fines may be imposed by the affected payment card brand in the case of a data breach. There might be significant penalties. Persons 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.