Standard Administrative Policy and Procedure

Subject: Payment Card Industry Compliance
Number:

I. PURPOSE

The purpose of this policy is to prevent credit card fraud, hacking, and various other security vulnerabilities and threats, and minimize the possibility of a breach of account data by adhering to the Payment Card Industry Data Security Standard (PCI DSS). The PCI DSS was developed by the founding members of the Payment Card Industry Security Standards Council (PCI SSC). The PCI SSC is responsible for managing the security standards, while compliance is enforced by the card brands, namely American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa Inc.

II. POLICY

The University of Wyoming will take all reasonable efforts to ensure compliance with the current version of the PCI DSS and will remediate any non-compliance with due diligence. All card handling activities and related technologies must comply with the PCI DSS in its entirety. No activity will be conducted nor any technology employed that might obstruct compliance with any portion of the PCI DSS.

Card handling activities must be conducted as described herein and in accordance with the standards and procedures listed in the Related Documents section of this Policy. The University will not process credit card information received via network fax machines, email, or other end-user messaging technologies. The University prohibits the storage of electronic credit card information, in any format, on any system. All new or changed card activities and handling technologies and non-electronic storage of credit card information must be pre-approved by the PCI Chair.

This Policy will be reviewed at least annually and updated as needed to reflect changes to business objectives or the risk environment.

III. APPLICABILITY

This Policy applies to all personnel who store, process, transmit, have access to, or affect the security of account data, including all faculty, staff, contractors, and students who are employed by the University. This policy also applies to any employee who contracts with a third party vendor to handle and/or process account data on behalf of the University. All vendors, contractors, and business partners who store, process, transmit, have access to, or affect the security of account data

on behalf of the University will state in their contract that they are and will remain compliant with the current version of the PCI DSS at all times.

The most current version of this policy is available at http://www.uwyo.edu/fsbo/pci.html or through the Financial Services Business Office.

If any requirements of the PCI DSS conflict with local, state, and federal laws or regulations, then the applicable local, state or federal law shall control.

IV. TRAINING

All personnel in positions that store, process, transmit, have access to, or affect the security of account data will complete PCI DSS training upon hire and at least annually. All personnel will acknowledge, in writing or electronically, that they have read and understand these security policies and procedures, and that they will comply with these policies. These acknowledgements will be kept in the employee's personnel file.

V. SUPPORTING DOCUMENTS

All supporting documentation can be found at http://www.uwyo.edu/fsbo/pci.html.

Responsible Division/Unit: Division of Administration and Division of Information Technology
Source: Payment Card Industry Data Security Standards
Links: http://www.uwyo.edu/regs-policies
Associated Regulations, Policies, and Forms: None
Approved: 8/7/2018