Payment Card Services Policy

Policy 503.8

1 Introduction

1. Appalachian State University requires that campus units be formally authorized to accept payment cards based on their compliance with this policy and related standards.

2 Scope

2. This policy is binding and applies to all Appalachian State University employees and service providers who transmit or process payment card transactions.

3 Definitions

3.1 Payment Card

A card that can be used to make a payment for a purchase or in payment of some other obligation.

3.2 Customer

An individual or other entity that makes a payment to the University for goods or services.

3.3 ITS

Means the University’s Information Technology Services.

3.4 Merchant

A campus unit that accepts payment cards as a method of payment.

3.5 NCOSC

Means North Carolina Office of State Controller.

3.6 Payment Card Services

Services that enable a Merchant to accept a transaction payment by use of a customer's payment card.

3.7 Payment Card Industry Data Security Standard (PCI DSS)

A proprietary information security standard developed by the PCI Security Standards Council for organizations that handle cardholder information for the major debit, credit, prepaid, epurse, ATM, and POS cards.

3.8 Merchant ID (MID)

An account established for a campus unit to credit sales amounts and debit processing fees.

3.9 Service Providers

Companies that provide services to campus merchants or other services providers that control or could impact the security of cardholder data.

3.10 Primary Account Number

Payment card number (credit or debit) that identifies the issuer and the particular cardholder account.

3.11 Cardholder Data

Full magnetic stripe from a payment card or the Primary Account Number(PAN) plus any of the following:
Cardholder name
Expiration date
Service Code or other Authentication Data

3.12 University

Appalachian State University

4 Policy and Procedure Statements

4.1 Payment Card Oversight Committee

4.1.1 A Payment Card Oversight Committee shall be formed under the authority of Finance and Operations with ITS support to provide oversight of all University payment card processing.

4.1.2 Representation on this committee will include but not be limited to: Finance and Operations, Internal Audits, and the ITS - Office of Information Security. This committee is charged with providing review and advisement concerning:

1. Payment Card Services and Solutions
2. Changes To Authorized Payment Card Services and Solutions
3. Compliance Assessment and Reporting

4.2 Authorized Use of Payment Card Services

University units must be authorized to accept payment card receipts by the Office of the Controller. In order to be authorized, the following requirements must be met:

4.2.1 The merchant card services used must be approved by the Office of the Controller.

4.2.2 Payment card acceptance methods and solutions used must be approved by the Office of the Controller and the ITS - Office of Information Security.

4.2.3 Any third party service providers used to collect, transfer, or process payment card information on behalf of the University merchant must be approved by the Office of the Controller and the ITS Office of Information Security.

4.2.4 The use of payment card services must conform to all applicable procedures, standards, and regulatory requirements, including, but not limited to, the University Controller's Payment Card Processing Procedure Manual and the Payment Card Industry Data Security Standard (PCIDSS).

4.3 Payment Card Industry Data Security Standard (PCI-DSS)

All University units approved as Merchants must comply with the Payment Card Industry Data Security Standard before accepting payment card transactions. Failure to comply with this standard can result in significant fines and disruption of University payment card processing. Maintaining compliance with this standard will include, but not be limited to, the following requirements:

4.3.1 Successful completion of Annual PCIDSS Self Assessment Questionnaire

4.3.2 Collection and verification of PCI-DSS compliance documentation submitted by third party service providers.

4.3.3 Passing quarterly network scans and periodic security tests of IT systems associated with payment solutions.

4.3.4 Arranging and validating annual compliance training for all individuals involved in payment card acceptance.

4.3.5 Proactively advising the Payment Card Oversight Committee when payment solutions and services are significantly modified so that compliance can be re-verified for associated merchant accounts.

4.3.6 Accepting responsibility for any fines or expenses resulting from any breach of cardholder data accepted by the unit. These expenses may include, but not be limited to, notification of customers exposed by data breach, investigation expenses, and any costs associated with external audits.

4.4 Payment Card Fees

4.4.1 University Merchants are responsible for all costs associated with payment card processing. These costs include, but are

not limited to, merchant account setup & administrative fees, equipment purchases, recurring monthly costs, and fees based on a percentage of every transaction from each credit card brand.

4.4.2 The University Office of Controller retains the right to apply an additional one time or annual compliance fee to University units for any technical equipment, software licenses, or assessment services needed to support compliance needs or other requirements.

4.5 Establishment of Payment Card Services

4.5.1 Requests to accept credit card payments on behalf of the University must meet the following requirements:

1. The University unit must obtain receipt center approval from the University Controller's Office.
2. The University unit must select an approved payment solution or submit information concerning the requirements and justification for a new payment solution to be considered.
3. The University unit must submit information outlining the need to collect payment card receipts, including anticipated volume of transactions, income, fees, and expenses incurred to implement and administer the payment card acceptance solution.

4.6 Merchant Responsibilities

4.6.1 University Merchants must accept the following the responsibilities:

1. Follow all security requirements established by the Payment Card Industry Security Standards Council and the ITS Office of Information Security.
2. Perform periodic compliance activities that are requested by the Controller's Office in a timely manner.
3. Promptly notify Student Accounts and Treasury Services when Merchant accounts are no longer needed and should be deactivated.
4. Ensure that utilized payment solutions never store cardholder data.
5. Immediately report any confirmed or suspected loss or exposure of cardholder data to the ITS Office of Information Security without delay.

4.7 Exemptions

4.7.1 Exemptions to this policy may only be authorized by the Vice Chancellor of Finance and Operations and the Chief Information Officer.

4.8 Enforcement

4.8.1 The University Controller and Chief Information Security Officer have joint authority to enforce this policy. Failure to abide by the terms of this policy can result in the immediate revocation a unit's authorization to accept payment card transactions. Individuals who fail to comply with this policy shall be subject to discipline in accordance with applicable University policies, up to and including dismissal.

5 Additional References

1. NC OSC Policy 500.10 Merchant Cards Security Incident Plan
2. NC OSC Policy 500.11 Compliance with PCI Data Security Standards
3. Security and Privacy of Data
4. NC GS § 14-113.24. Credit, charge, or debit card numbers on receipts SunTrust Merchant Services Operating Procedures
5. Collection of Cash Outside University's Cashier's Office

6 Authority

NCGS 66-51.12(a)

7 Contact Information

Office of the Controller – 828-262-2110
ITS – Office of Information Services – 828-262-6277

8 Original Effective Date

June 30, 2015

9 Revision Dates