PCI Policies
2011

Appalachian State University

Table of Contents

Terms:

MSA	Master Service Agreement
PCI DSS	Payment Card Industry Data Security Standard
STMS	SunTrust Merchant Services
SAQ	Self Assessment Questionnaire
OSC	Office of State Controller
NCOSC	North Carolina Office of State Controller

CVV — Card Verification Code or Value

Also known as Card Validation Code or Value, or Card Security Code. Refers to either: (1) magnetic-stripe data, or (2) printed security features. (1) Data element on a card's magnetic stripe that uses secure cryptographic process to protect data integrity on the stripe, and reveals any alteration or counterfeiting. Referred to as CAV, CVC, CVV, or CSC depending on payment card brand. The following list provides the terms for each card brand:

_
_ CVC – Card Validation Code (MasterCard payment cards)
_ CVV – Card Verification Value (Visa and Discover payment cards)

_ CSC – Card Security Code (American Express)

(2) For Discover, JCB, MasterCard, and Visa payment cards, the second type of card verification value or code is the rightmost three-digit value printed in the signature panel area on the back of the card. For American Express payment cards, the code is a four-digit unembossed number printed above the PAN on the face of the payment cards. The code is uniquely associated with each individual piece of plastic and ties the PAN to the plastic. The following list provides the terms for each card brand:

_ CID – Card Identification Number (American Express and Discover payment cards)

_ CAV2 – Card Authentication Value 2 (JCB payment cards)

_ CVC2 – Card Validation Code 2 (MasterCard payment cards)

_ CVV2 – Card Verification Value 2 (Visa payment cards)

Section 1: State and Contractual Requirements Governing Campus Credit Cards

A. Cash Collection Point Approval for Departments

All departments must get approval from the University Controller to sell goods or services. A copy of this approval will be on file in the Office of Internal Audits. Furthermore, additional and separate approval must be obtained from the Credit Card Compliance Committee in order for the department to accept credit cards from its customers as a payment option. Approval is only given to departments that meet Payment Card Industry Data Security Standards, attend training and comply with University PCI policies, NCOSC Electronic Commerce Policies and State Cash Management Law.

B. State Requirements

Senate Bill 222 passed in 1999 amended several statutes that authorized the State Controller to issue policies relating to "electronic payments," which support the Statewide Electronic Commerce Program (SECP). All entities subject to the State's Cash Management Law, and all entities that participate in one or both of the Master Services Agreements (Electronic Funds Transfer and Merchant Cards) are subject to the policies. Entities are encouraged to be fully aware of the policies to ensure compliance.

As a prerequisite for participating under the MSA, Appalachian State University is required to comply with all card association rules. This includes the rules pertaining to the PCI Data Security Standard.

C. Contractual Requirements Concerning Fines

A department can be fined by a card association even if a security breach has not occurred. It is uncertain as to how aggressive the card associations will be in levying fines for such non-compliant merchants that might be detected. Visa has announced its fine structure. Effective September 30, 2007, Visa will levy a monthly fine of $25,000 to any level 1 merchant (department) detected as non-compliant. Effective December 31, 2007, Visa will levy a monthly fine of $5,000 to any level 2 merchant detected as non-compliant. Departments at Appalachian State University are considered level 2 merchants.

In the event of a breach, all fines and expenses associated with the breach will be borne by the department accepting the credit card that was compromised. Related expenses in addition to the fine could include but are not limited to labor and supply cost

associated with identifying and notifying the population exposed by the breach. All costs associated with any required external audits will also be paid by the department, which could be significant.

E. Statutory Requirements Governing Transaction Fees

University Policy on transaction fees:
The University does not allow transaction fees to be assessed on credit card transactions.

F. The Credit Card Compliance Committee

In an effort to ensure compliance with MSA, State's Cash Management Law and PCI DSS, the Credit Card Compliance Committee has been established. This committee is made up of members from Business Affairs, Internal Audits and Information Technology. This Committee has been charged to provide oversight of credit card activity, the University's participation in the MSA and compliance with PCI Standards. North Carolina State Controller's Office requires that each participant must participate in any security assessments and security scans required by the associations and/or OSC, in order to be and to remain compliant with Payment Card Industry (PCI) Security Standards, and be responsible for any fines levied as the result of not being compliant.

Section 2 - Payment Card Industry Data Security Standards (PCI-DSS)

PCI-DSS are national standards from the Card Association and apply to all organizations anywhere in the country that process, transmit or store credit cardholder information. The University and all departments that process payment card data have a contractual obligation to adhere to the PCI-DSS and for annually certifying their continued compliance by submitting the PCI-DSS Self Assessment Questionnaire (SAQ) appropriate to their credit card activities.

Any costs incurred by a participant to become and remain compliant with the PCI Data Security Standards, including but not limited to an annual penetration test (if applicable), shall be borne by the participant. Any costs incurred by the University associated with an onsite security audit or a forensic investigation that may be required shall be borne by the department.

Individual credit card information is confidential. Failure to maintain strict controls over this data could result in unauthorized use of credit card data. Credit card information is confidential information and should be treated with great care.

Key Data Control Items

1. Under no circumstances should a department store sensitive authentication data (track data from the magnetic stripe, card-validation code CVV2 data,) after authorization (not even if encrypted).

2. Never send or request cardholder information to be sent via email. Departmental forms (web and mail order forms) should be designed so that credit card information can be easily and completely removed from the registration information. You should never ask for the CVV2 code to be mailed to you unless you have a strong business case for the number i.e. shipping a product. Just having the CVV2 code increases the department's liability. Once the credit card has been processed, all credit card information must be destroyed immediately via a cross shredder. It is not sufficient to simply mark out the credit card information. Websites and forms should state that credit card information should never be emailed to the department.

3. Customer records located within a department should be stored only if there is a documented business need and in a locked non-portable cabinet dedicated solely to these records. The Controller's Office will approve each department's business need, a proper retention schedule and method of disposing or deleting sensitive card holder information.

4. Access to these records should be limited to only those employees who need this information to perform approved duties.

5. Under no circumstances should a department retain electronically (including Excel files, thumb drives, shadow databases, etc.) the card numbers and expiration dates of the customer credit cards.

6. Make sure all access to storage areas is secure and that all visitors are authorized to enter areas that cardholder data is processed or maintained.

7. Use appropriate facility entry controls to limit and monitor physical access to systems that store, process, or transmit cardholder data.

8. Do not use wireless PCs for processing credit card data unless approved in writing by the Credit Card Compliance Committee.

9. All personnel who have direct access to on-line credit card information are required to attend the PCI Security Training and to have read the University Credit Card Policy.

10. All credit card information temporarily recorded on paper should be processed immediately and then the paper document should be properly destroyed in cross cut shredder.

11. The customer copy of the credit card receipt can only contain the last 4 digits of the credit card number. It is required that departments use double truncation which permits only the last 4 digits to be printed on both the merchant and customer receipt.

12. Never send credit card information to the University Archives. Receipts should be destroyed via cross cut shredder immediately after the approved business need has expired.

13. Departments must assure that all university computers have installed the most recent updated versions of the University recommended antivirus, spyware detection software and other recommended security software. All general purpose (desktop) computers that handle credit card data must run an approved university build and be configured as a "sensitive data" workstation. Exceptions to this policy must be documented with compensating controls to replace the protections provided by the university build and "sensitive data" workstation configuration.

Section 3 - Campus Operating Policies

A. Merchant Accounts and Credit Card Transactions

Departments cannot negotiate their own contracts with credit card processing companies. All merchant accounts for accepting credit cards must be approved by the Credit Card Compliance Committee and participate in the State's MSA.

Each Department is responsible for all expenses associated with credit card merchant accounts and it cannot adjust the price of goods or services based on the method of payment.

B. Accepted Methods for Processing Credit Card Transactions

There are 2 accepted methods for processing transactions: (1) First Data Connect, and (2) card swipe terminal. Other methods of processing credit cards and other gateways

are not permitted unless authorized in writing by the Credit Card Compliance Committee and North Carolina State Controller's Office.

A department planning to allow its customers to use credit cards over the web will be responsible for designing the departmental website. This website will serve as the "window" to the approved gateway. Credit card information must not be stored directly on the department's webpage nor entered into the website. The website and its connection to the approved gateway will be reviewed by the Credit Card Compliance Committee to ensure that it meets Payment Card Industry Data Security Standards.

C. Financial Controls

When an item or service is purchased using a credit card, and a refund is necessary, the refund must be credited to the same credit card account from which the purchase was made.

All transactions must be settled and recorded daily in the University's financial system via proper reporting to The Cashier's Office.

The department's (merchant's) copy of the receipt should not contain the full card number and expiration date. The merchant's copy of the receipt should only contain the full number and expiration date *if there is a business reason* for doing so. The merchant copy of the receipts must be kept in a secure place (i.e. locked cabinet with minimal access) for no more than 90 days. At the end of 90 days, the receipts should be destroyed in a secure manner, via cross cut shredder.

Departments must assure that all university computers have installed the most recent updated versions of the University recommended antivirus, spyware detection software and other recommended security software. All general purpose (desktop) computers that handle credit card data must run an approved university build and be configured as a "sensitive data" workstation. Exceptions to this policy must be documented with compensating controls to replace the protections provided by the university build and "sensitive data" workstation configuration.

D. Reporting Requirements for Actual or Suspected Security Incidents

Departments must report any actual or suspected security incident in which cardholder information may have been compromised. The incident should be reported to Credit Card Compliance Committee and the University Controller. If the incident involved the loss or suspected compromise of stored or processed electronic data, it must also be reported to the IT Security Officer**. THIS MUST BE DONE IMMEDIATELY. The University must report all breaches to the State Controller's Office within 24 HOURS OF DECTECTION.**