Louisiana State University
Finance and Administration
Operating Procedure

**FASOP: AS-22**

# CREDIT CARD MERCHANT POLICY

**Scope:** All campuses served by Louisiana State University (LSU) Office of Accounting Services

**Effective:** August 22, 2013

## I. Introduction

Colleges and universities have traditionally had open networks of information that foster the exchange of ideas and information. However, this very openness frequently attracts criminal organizations and other groups with malicious intent that increase the risk of security breaches that can result in the disclosure of customers' credit card information. Refer to Section VII to review definitions and useful links related to the payment card industry.

## II. Purpose

To provide guidance regarding the responsibilities and procedures related to credit card handling. Additionally, to protect LSU's customers' credit card information, the University's reputation, and to reduce the financial costs associated with a breach of credit card information.

## III. Background

As a result of credit card breaches and the resulting customer distrust in using credit cards as a payment option, the credit card industry formed a council in 2006 called the Payment Card Industry (PCI) Security Standards Council which includes Visa, MasterCard, American Express, and Discover. This PCI Council has developed Data Security Standards (DSS) to assure consumers that their brands and using credit cards are reliable and secure. These standards include controls for handling and restricting credit card information, computer and Internet security, and reporting of a breach of credit card information.[1] These standards are mandated by the industry in order for a merchant to be approved to accept credit card payments. Failure to comply with these standards can result in significant fines to the University, increased investment in security measures over and above those already in place, and loss of the University's privilege to accept credit card payments.

A credit card merchant is a department or any other entity at the University that accepts credit cards for payment. All University merchants have always been required to use the University-approved merchant services provider to settle credit card transactions. However, some University merchants have operated in a decentralized manner in selecting third party vendors and software products to process credit card payments. Some University merchants have designed and developed their own e-commerce websites, purchased third party software, or have internally developed software to process credit card payments. In addition, University merchants have selected third party vendors to electronically transmit and store credit card payments. In 2005, TrustWave, a certified PCI network scanning vendor, determined that 60% of breaches were due to third party error. To reduce the number of credit card breaches, the PCI Council developed a list of approved third party software and a list of approved processing vendors.[2]

[1] *Please see the link for PCI DSS under Section VII.*
[2] *Please see the links for PCI Approved Software and Service Provider under Section VII.*

Although the primary focus of the PCI DSS is on computer equipment, networks, and software that enable Internet-based sales, there are other computer services that can make these systems vulnerable to attack through the Internet and result in an exposure of cardholder information. Basic functions such as e-mail can result in open Internet accessibility of a merchant’s network. Therefore, in order to combat these threats and maintain compliance with PCI DSS, all University credit card merchants, including those transmitting via a terminal on a dedicated phone line must complete an annual self-assessment survey and, if applicable, an internal scan and a remote external scan by the University PCI approved vendor.

The credit card companies in the PCI Council have determined there are four levels of merchants in the industry, with ratings based on the transaction volume. Louisiana State University is a Level 4 (the lowest level) which is based on the number of credit card transactions per year and a good record relative to security breaches affecting credit card data. The PCI Council has delegated to the University-approved merchant services provider the responsibility to ensure that organizations are complying with the assessment and scanning requirements to verify compliance with the Data Security Standards.

In the event of a breach by a University merchant, the University-approved merchant services provider is authorized on behalf of the credit card companies to assess the particular University merchant any fine levied by the card associations as well as the costs of investigation, remediation, customer notification, and customers’ card re-issuance. Further, one breach may result in the card association elevating the University to a Level 1 (the highest level) merchant which requires each University merchant to pay for and submit to an outside audit of their credit card operation. Ultimately, a refusal to pay fines or submit to elevated compliance measures can result in all or part of the University losing the privilege of accepting credit card payments.

Periodic reviews of University merchants will be coordinated by Bursar Operations and the Chief IT Security and Policy Officer. Credit card handling procedures are subject to review by internal audit or external audit. Departments not complying with approved safeguarding and processing procedures may lose the privilege to serve as a credit card merchant.

## IV. Policy Information

### A. Policy

In general, departments are not permitted to transmit, process, or store credit card information on University computer systems or unapproved Internet services. When cardholders visit University online sites, they must be redirected to a PCI approved third party payment processor site to transmit, process, or store the credit card information.

Alternatively, an LSU department may submit a request to transmit, process, or store credit card information on University-owned computer systems or subscribed services provided all software and third party vendors are PCI approved and additional internal requirements are met. The request must be submitted to and approved by Bursar Operations.

### B. To Whom This Policy Applies

This policy applies to all campus units that accept funds through credit card transactions. The policy applies to merchants accepting credit card payments using a credit card terminal connected to a data phone line as well as merchants processing or sending transactions over the Internet. Internet transactions include links on LSU websites redirecting customers to another website; use of software including Point of Sale software on a computer to transmit, process, or store credit card information; use of a third party vendor to transmit, process, or store credit card information; and use of a wireless device. Each department that accepts credit cards for payment must be approved by Bursar Operations and, where applicable, approved by the Chief IT Security and Policy Officer.

C. Who Should Know This Policy

Officials or administrators with the responsibility of managing University credit card transactions, employees entrusted with handling or processing credit card information, and employees who may come into contact with credit card information indirectly through their job duties should know this policy. This includes business managers, accountants, fiscal officers, systems managers, and network managers.

## V. General Responsibilities and Requirements

A. Responsibilities of Bursar Operations and the Chief IT Security and Policy Officer

Responsibilities include:

1. Administer the process of obtaining new merchant accounts.
2. Communicate the policy and PCI DSS to merchants.
3. Advise merchants wanting to accept credit card payments via wireless, the Internet, or transmit credit card information via the Internet for batch processing on achieving and maintaining compliance with all facets of PCI DSS.
4. Coordinate periodic reviews of existing merchants to include verification of procedures, computer scans, and other activities required at the institution level as appropriate.

B. Responsibilities of Credit Card Merchants

All University merchants must comply with the requirements listed in Section C below. These responsibilities include PCI requirements and University requirements. In addition, University merchants must refer to the specific requirements listed in “Credit Card Merchant Policy for Terminal and Internet-related processing” located in Section D of this document.

C. General Responsibilities for all Fiscal Officers and Systems Managers

Responsibilities include:

1. Comply with applicable sections of the PCI DSS.[3] Reference PCI DSS.3.
2. Obtain approval for new University merchants or new purchases of computer software or hardware containing payment transaction features – these items require approval by Bursar Operations, Procurement Services and, if applicable, the Chief IT Security and Policy Officer before entering into any contract, purchase, acquisition, or replacement of equipment, software, Internet provider, or wireless device.
3. Maintain a department information security policy – supervisors must establish and document policies and procedures for physically and electronically safeguarding cardholder information and satisfy the requirements of PCI DSS 12. Please complete the form AS539 “Responsibilities of Credit Card Handlers and Processors” according to your department’s credit card processing arrangement.
4. Prevent unauthorized access to cardholder data and secure the data – establish procedures to prevent access to cardholder data in physical or electronic form including but not limited to the following: hard copy or media containing credit card information must be stored in a locked drawer or office; department should establish password protection on computers; visitor sign-in logs, escorts and other means must be used to restrict access to documents, servers, computers, and storage media used to any extent in the handling of credit card payments. Reference PCI DSS 9.
5. Communicate policy to staff and obtain signatures – supervisors including Deans, fiscal officers, and systems managers must communicate this policy to their staff and submit appropriate forms (AS539) for all personnel involved in credit card transactions. Reference PCI DSS 12.6.

[3] *Please see the link for PCI DSS under Section VII.*

6. Restrict access based on a business need-to-know – Access to physical or electronic cardholder data must be restricted to individuals whose job absolutely requires access. Reference PCI DSS 7.1.
7. Assign a unique ID to each person with computer access – A unique ID must be assigned to each person with computer access to credit card information. User names and passwords shall not be shared. Reference PCI DSS 8.1.
8. Transmitting credit card information by e-mail or fax is prohibited – Full or partial credit card numbers and three or four digit validation codes (usually on the back of credit cards) may not be faxed or e-mailed. Reference PCI DSS 4.2.
9. Storing electronically the CVV, CVV2 validation code, or PIN number is prohibited – Do not store the three or four digit CVV or CVV2 validation code from the credit card or the PIN, personal identification number. Reference PCI DSS 3.2.
10. Segregation of duties – Establish appropriate segregation of duties between personnel handling credit card processing, the processing of refunds, and the reconciliation function.
11. Background checks – Perform applicable background checks on potential employees who have access to systems, networks, or cardholder data in accordance with LSU's policy on performing background checks and local law. If employees have access to one card number at a time to facilitate a transaction, such as store cashiers in a supervised setting, background checks are not required by PCI DSS. However, LSU's policy regarding background checks on employees must be followed. Reference PCI DSS 12.7.
12. Mask 12 of the 16 digits of the credit card number – Terminals and computers must mask the first 6 digits and the last 4 digits of the credit card number. Reference PCI DSS 3.3.
13. Imprint machines are not permitted – Do not use imprint machines to process credit card payments as they display the full 16 digit credit card number on the customer copy. Reference PCI DSS 3.4
14. Report security incidents to Bursar Operations and the Chief IT Security and Policy Officer – If you know or suspect that credit card information has been exposed, stolen, or misused this incident must be reported immediately to the following departments:

    a. Supervisor in writing
    b. Bursar Operations via e-mail to bursar@lsu.edu and via phone to (225) 578-3357
    b. Chief IT Security and Policy Officer via e-mail to security@lsu.edu and via phone to (225) 578-3700

    This report must not disclose via fax or e-mail credit card numbers, three or four digit validation codes, or PINs. The report must include a department name and contact number. Reference PCI DSS 12.9.

D. Specific Responsibilities for all Fiscal Officers and Systems Managers

The table below lists responsibilities for University merchants accepting credit card payments using the following methods:

1. Credit Card Terminal Merchants – connected to a data line
2. Internet-related Merchants – see the four cases described below:

Case A Redirecting customers using a link from an LSU web page to a PCI approved payment processing service provider or to another company's site.

Case B Point of Sale (POS) software that is PCI approved and approved by Bursar Operations, Procurement Services, and if applicable, the Chief IT Security and Policy Officer.

Case C Software that is PCI approved and approved by Bursar Operations, Procurement Services, and, if applicable, the Chief IT Security and Policy Officer.

Case D Wireless device and software that is PCI approved and approved by Bursar Operations, Procurement Services, and, if applicable, the Chief IT Security and Policy Officer.

### Credit Card Merchant Policy for Terminal and Internet-related Merchants

This includes Internet, Internet-related, software, Point of Sale, and wireless systems. In general, departments are not permitted to transmit, process, or store credit card data on University computer systems or the Internet. When cardholders visit university online sites, they must be redirected to a PCI approved third party payment processing site to transmit, process, or store the credit card data. See

Case A below. Alternatively, an LSU department may submit a request to transmit, process, or store the credit card data provided all third party vendors are PCI approved and additional internal requirements are met. The request must be submitted to the Office of Accounting Services, Bursar Operations and will be reviewed by a technical committee (See Case B, C, or D below):

Credit Card Terminal Merchants

| *Merchants using credit card terminals connected to a data phone line.* | |
|---|---|
| Fiscal Requirements | 1. Use terminals that do not print on the customer copy the full 16 digit credit card number.<br>2. Background checks may be required. Reference PCI DSS 12.7.<br>3. Secure storage of credit card information. PCI Provisions applicable: Reference PCI DSS 3, 7, 9 & 12 |

Internet-related Merchants

| Case A – Merchants Redirecting<br>*Redirecting customers to PCI approved service providers[4] or to another company's website using a link from an LSU computer. Merchants do NOT transmit, process, or store credit card data on any computer located on a University IP address.* | |
|---|---|
| Examples | 1. LSU hosted web page collects all information except credit card information. (i.e. LSU web page is linked to RegOnline product.<br>2. LSU hosted web page is linked to another PCI approved company's site. |
| Questions | 1. Is the service provider PCI approved?<br>2. Is the service provider linked to another service provider? If yes, is that provider PCI approved?<br>3. Does the merchant have access to 16 digit credit card numbers? If yes, this is not permitted. |
| Fiscal Requirements | 1. All service providers are PCI approved.<br>2. Third party contract language applies to all vendors.[5]<br>3. No access to 16 digit credit card numbers. |
| System Requirements | 1. Successful external scan.<br>2. Successful internal scan using CIO approved software.<br>3. Comply with university Computing Security Standards.<br>4. No access to 16 digit credit card numbers. |

| Case B – Point of Sale (POS) Merchants<br>*Using terminal connected to a computer to transmit, process or store credit card information and using PCI approved service providers[4]. POS software must be PCI approved and approved by the university PCI technical committee. Merchants must submit a request to Bursar Operations.* | |
|---|---|
| Examples | 1. Using POS software to transmit, process, or stored credit card information.<br>2. Using a terminal connected to a computer to swipe credit card transactions that are "batched" daily and sent via the Internet. |
| Questions | 1. Is the POS software on the PCI list?<br>2. Is the service provider on the PCI approved list?<br>3. Is the service provider linked to another service provider? If yes, is that provider PCI approved?<br>4. Does the merchant have access to 16 digit credit card numbers? If yes, this is not permitted. |
| Fiscal Requirements | 1. Software is on the PCI list.<br>2. All service providers are PCI approved.<br>3. Third party contract language applies to all vendors.[5]<br>4. No access to 16 digit credit card numbers.<br>5. Background checks may be required. Reference PCI DSS 12.7. |
| System Requirements | 1. Successful quarterly external scan.<br>2. Successful quarterly internal scan using CIO approved software.<br>3. Comply with university Computing Security Standards. |

| | |
|---|---|
| | 4. No password access to 16 digit credit card numbers.<br>5. Background checks may be required. Reference PCI DSS 12.7. |

| Case C – Merchants Using Software<br>*Using software that is PCI approved[5] to transmit, process, or store credit card information and using PCI approved service providers[4]. Merchant must submit a request to Bursar Operations.* | |
|---|---|
| Examples | 1. Purchased software installed on a university computer that transmits to a PCI approved service provider. |
| Questions | 1. Is software on the PCI list?<br>2. Is the service provider on the PCI approved list?<br>3. Is the service provider linked to another service provider? If yes, is that provider PCI approved?<br>4. Does the merchant have access to 16 digit credit card numbers? If yes, see the Fiscal and System Requirements below. |
| Fiscal Requirements | 1. All service providers are PCI approved.<br>2. Third party contract vetted through Procurement Services.<br>3. Merchant policy regarding access to 16 digit credit card numbers approved to in writing by Bursar Operations.<br>4. Background checks may be required. Reference PCI DSS 12.5. |
| System Requirements | 1. Pass system's architecture review by LSU technical committee.<br>2. Survey successfully completed.<br>3. Successful quarterly external scan.<br>4. Successful quarterly internal scan using CIO approved software.<br>5. Merchant policy regarding access to 16 digit credit card numbers approved in writing by Financial Systems Services.<br>6. Background checks may be required. Reference PCI DSS 12.5. |

| Case D – Wireless Merchants<br>*Using wireless terminals via 1) direct transmission of credit card information to a PCI approved service provider, or 2) indirect transmission via an OSU server to a PCI approved service provider[4]. Merchant must submit a request to Bursar Operations.* | |
|---|---|
| Examples | 1. Wireless transmission of credit card data using a PCI approved wireless device.<br>2. Wireless transmission using a PCI approved wireless device and transmitting via an LSU server to a PCI service provider or LSU approved cellular provider. |
| Questions | 1. Is wireless device and cellular service on the PCI and LSU approved list?[5]<br>2. Is the service provider on the PCI approved list?<br>3. Is the service provider linked to another service provider? If yes, is that provider PCI compliant?<br>4. If transmitting to an LSU server, does the merchant have access to 16 digit credit card numbers? If yes, see the Fiscal/System Requirements below. |
| Fiscal Requirements | 1. Wireless device and software is on the PCI list.[5]<br>2. All service providers are PCI approved.[4]<br>3. Third party contract language applies to all vendors.[5]<br>4. If transmitting to an LSU server, a merchant policy regarding access to 16 digit credit card numbers must be approved in writing by Bursar Operations.<br>5. Background checks may be required. Reference PCI DSS 12.5. |
| System Requirements | 1. Pass systems architecture review by LSU technical committee.<br>2. If transmitting via an LSU server to a PCI approved service provider, the following system requirements must be met:<br>a. Survey successfully completed.<br>b. Successful quarterly external scan.<br>c. Successful quarterly internal scan using CIO approved software.<br>d. Comply with University Computing Standards. |

| | |
|---|---|
| | e. Merchant policy regarding access to 16 digit credit card numbers approved in writing by Bursar Operations.<br>f. Background checks may be required. Reference PC DSS 12.5. |

[4] *Service Provider – a vendor that provides access to the Internet and applications that facilitates the transmission and/or storage of credit card information. See link under Service Provider in Section VII.*

[5] *PCI Approved Software – software installed on an LSU computer and determined by the credit card industry to follow the industry's standards for securing credit card information. See link under PCI Approved Software in Section VII.*

## VI. Miscellaneous Topics

These guidelines should be followed when needing assistance on the following miscellaneous topics:

A. Establishing New University Credit Card Merchant

In order to accept credit cards a department must complete an AS537 "Credit Card Merchant Agreement and Request" form and return it to Bursar Operations. Upon approval, Bursar Operations will establish a new University merchant account. If at any time there is a question or concern about accepting credit cards, please contact Bursar Operations for assistance at bursar@lsu.edu or (225) 578-3357.

B. Changes to an Existing Account

Changes to an existing merchant account must be approved by Bursar Operations, Procurement Services and the Chief IT Security and Policy Officer. Examples of changes are: purchasing, selling, surplusing, or discarding a terminal; purchasing software; selecting a new service provider. Signing a contract with any third party vendor related to credit card payment processing must be approved by the Office of Procurement Services.

C. Training

It will take approximately four weeks for University merchant numbers to be set up and to obtain the equipment as needed. A "Welcome Kit" will be sent to you by the University-approved merchant services provider. The contact number for the current merchant services provider for the University can be obtained by contacting Bursar Operations at bursar@lsu.edu or (225) 578-3357.

D. Accounting for Transactions

After daily closeout and batching, the University merchant will prepare an entry in the CARD using Method of Payment (MOP) codes provided by Bursar Operations. Appropriate backup should be attached to the CARD entry from the Point of Sale system/terminal and merchant services provider. The CARD entry should be delivered to the University Cashier in Bursar Operations for processing. It is the University merchant's responsibility to reconcile their CARD entries to the University-approved merchant services provider at least monthly.

E. Fees

Each transaction is subject to assessment fees, discount fees, and per item fees charged by Visa, MasterCard, American Express, and Discover. Additional fees for transaction processing are assessed by the University-approved merchant services provider based on a competitive bid process. Each month, Bursar Operations prepares a CARD entry to charge these fees to the merchant's expenditure account. A copy of the CARD entry along with a copy of the merchant services statement is sent to each merchant.

## VII. Definitions and Payment Card Industry (PCI) Links

A. CVV Card Verification Value Code (CVV2, CID) – a three (3) digit number on the back of a credit card. In the case of American Express, this is a four (4) digit code on the front of the credit card.

B. IP (Internet Protocol) Address – a unique number used to represent every computer in a network. The format of an IP address is typically four sets of numbers separated by dots (e.g. 198.123.123.5), although some newer systems may use an IP address containing eight sets of numbers.

C. Merchant – a credit card merchant is a department or entity that accepts credit cards for payment. An LSU merchant is assigned a merchant account number by the merchant services provider. This number is also the merchant account number for Visa, MasterCard, and Discover transactions. A separate merchant account number is assigned for American Express.

D. PAN (Primary Account Number) – the 16 digit credit card number.

E. Payment Gateway – a type of service provider that transmits, processes, or stores credit cardholder data as part of a payment transaction. They facilitate payment transactions such as authorizations and settlement between merchants or processors, also called endpoints. Merchants may send transactions directly to an endpoint or indirectly using a payment gateway.

F. PCI (Payment Card Industry) Approved Software – shopping card and/or credit payment processing software that is installed on an LSU computer and determined by the credit card industry to follow the industry's best practices for securing credit card information. This includes customized, pre-installed, and "off-the-shelf" software and wireless devices. The following link provides a complete list of PCI approved Payment Application vendors: https://www.pcisecuritystandards.org/. See the tab marked "Quick Link".

G. PCI Council – the credit card industry, Visa, MasterCard, American Express, and Discover, has formed a Council to establish Data Security Standards (DSS) and Payment Application (PA) standards for the industry. https://www.pcisecuritystandards.org/

H. PCI DSS (Data Security Standards) – security standards for credit card data that is established by the PCI Council. Merchants at Louisiana State University must refer to the current and applicable provisions of the DSS. https://www.pcisecuritystandards.org/

I. PCI PA-DSS (Payment Application Data Security Standard) – data security standards for software used to process credit card payments. These are the standards card transaction processing services (third party firms) must meet to do business.

J. PCI Self-Assessment Questionnaire – survey to be completed annually by LSU merchants. The DSS should be referred to for clarification of the questionnaire. https://www.pcisecuritystandards.org/

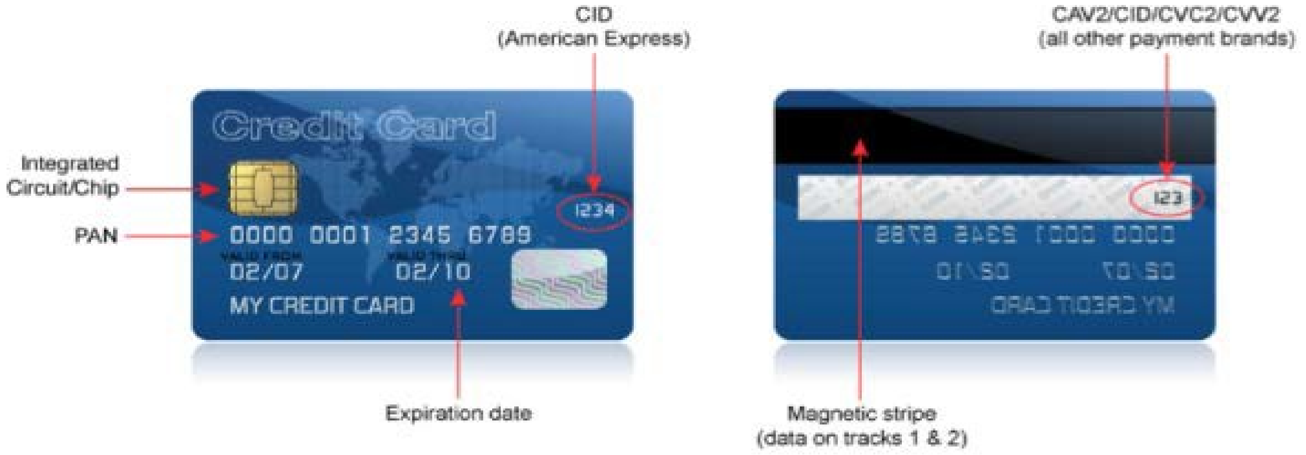
K. PED (Pin Entry Device) – terminal that allows entry of a customer's PIN (Personal Identification Number).

L. PIN (Personal Identification Number) – personal number used in debit card transactions.

M. Service Provider – a vendor that provides access to the Internet and applications that facilitates the transfer and/or storage of credit card information. The following link provides a complete list of PCI compliant service providers: http://www.visa.com/splisting/index.html. Note: this list is maintained on Visa's website.

## VIII. Credit Card Data Guide

The below is a graphic representation of the front and back of a standard credit card and its various parts.


CID
(American Express)
Credit Card
Integrated
Circuit/Chip
PAN
1234
0000 0001 2345 6789
VALID FROM
02/07
VALID THRU
02/10
MY CREDIT CARD
Expiration date
CAV2/CID/CVC2/CVV2
(all other payment brands)
123
Magnetic stripe
(data on tracks 1 & 2)