PAYMENT CARD MERCHANT POLICY

Scope: Louisiana State University and A&M College, Pennington Biomedical Research Center, and LSU Agricultural Center

Effective: **July 1, 2019 (Revised)**
August 22, 2013 (Original)

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' payment card information.

II. Purpose

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

III. Background

As a result of payment card breaches and the resulting customer distrust in using payment cards as a payment option, in 2006, the payment card industry formed the Payment Card Industry (PCI) Security Standards Council which includes Visa, MasterCard, American Express, Discover, and JCB. This PCI Council has developed Data Security Standards (DSS) to act as baseline security controls to reduce the risk of payment card breaches. These standards include controls for handling and restricting payment card information, computer and Internet security, and reporting of payment card information breaches. These standards are mandated by the industry in order for a merchant to be approved to accept payment 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, loss of the University's privilege to accept payment card payments, and damage to the University's reputation.

A payment card merchant is a department or any other entity at the University that accepts payment cards as payment for goods and/or services. All University merchants have always been required to use the University-approved merchant services provider to settle payment card transactions. However, some University merchants have operated in a decentralized manner in selecting third party vendors and software

products to process payment card payments. Some University merchants have designed and developed their own ecommerce websites, purchased third party software, or have internally developed software to process payment card payments. In addition, University merchants have selected third party vendors to electronically transmit and store payment 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 payment card breaches, the PCI Council developed a list of approved third party software and a list of approved processing vendors.

The primary focus of the PCI DSS is to describe security controls for people, processes, and technologies that interact with or could affect the security of cardholder data. Although merchants often times direct their focus 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 email 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 payment 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 vulnerability scan and a remote external vulnerability scan by the University PCI approved vendor.

The payment 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 3 which is based on the number of payment card transactions per year. 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.

Periodic reviews of University merchants will be coordinated by Bursar Operations, the PCI Project Team, the LSU A&M Chief IT Security and Policy Officer, or by campus-level IT unit and/or IT security personnel at other campuses. Payment card handling procedures are subject to review by internal audit or external audit.

Failure to meet the requirements outlined in this policy will result in suspension of the physical, and if appropriate, electronic payment capability for the affected merchant(s). In the event of a breach or a PCI violation, the payment card brands may assess penalties to the institution's bank which will likely then be passed on to the institution. Any fines and assessments imposed will be the responsibility of the impacted merchant. A one-time penalty of up to $500,000 per card brand can be assessed as well as on-going monthly penalties.

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 payment 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 payment card payments.

IV. 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 payment card. In the case of American Express, this is a four (4) digit code on the front of the payment card.

B. eMarket – a service which enables university merchants to collect revenue for events, sales, and services through an approved online marketplace.

C. 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.

D. Merchant – a payment card merchant is a department or entity that accepts payment 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.

E. PAN (Primary Account Number) – the payment card number.

F. Payment Gateway – a type of service provider that transmits, processes, or stores payment card 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.

G. PCI (Payment Card Industry) Approved Software – shopping cart and/or payment processing software that is installed on an LSU computer and determined by the payment card industry to follow the industry's best practices for securing payment 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".

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

I. PCI DSS (Data Security Standards) – security standards for payment 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/

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

K. 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/

L. PCI Project Team – a group of representatives from various departments and campuses responsible for assisting the University in achieving and maintaining compliance with the PCI DSS and reducing the scope of items within the University that will need to be compliant with the PCI DSS by implementing changes set by the strategic direction of the University as it relates to the reduction or mitigation of risk.

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

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

O. P2PE Solution - A point-to-point encryption (P2PE) solution is provided by a third party solution provider, and is a combination of secure devices, applications and processes that encrypt data from the point of interaction (for example, at the point of swipe or dip) until the data reaches the solution provider's secure decryption environment. A PCI P2PE solution must include all of the following:

1. Secure encryption of payment card data at the point-of-interaction (POI)
2. P2PE-validated application(s) at the point-of-interaction
3. Secure management of encryption and decryption devices
4. Management of the decryption environment and all decrypted account data
5. Use of secure encryption methodologies and cryptographic key operations, including key generation, distribution, loading/injection, administration and usage.

P. Qualified Security Assessor (QSA) - a designation conferred by the PCI Security Standards Council to those individuals that meet specific information security education requirements, have taken the appropriate training from the PCI Security Standards Council, are employees of a Qualified Security Assessor (QSA) company approved PCI security and auditing firm, and will be performing PCI compliance assessments as they relate to the protection of payment card data.

Q. Self-Assessment Questionnaire (SAQ) - a validation tool intended to assist merchants and service providers who are permitted by the payment brands to **self**-evaluate their compliance with the Payment Card Industry Data Security Standard (PCI DSS).

R. Service Provider – a vendor that provides access to the Internet and applications that facilitates the transfer and/or storage of payment 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.

V. Policy Information

A. Policy

Departments are not permitted to transmit, process, or store payment 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 payment card information.

B. To Whom This Policy Applies

This policy applies to all faculty, staff, students, organizations, third-party vendors, individuals, systems, and networks involved with payment card handling. This includes transmission, storage, and/or processing of payment card data, in any form (electronic or paper), on behalf of Louisiana State University.

The policy applies to merchants accepting payment card payments using a payment 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 or process payment card information; use of a third party vendor to transmit or process payment card information; and use of a wireless device. Each department that accepts payment cards for payment must be approved by Bursar Operations.

C. Who Should Know This Policy

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

VI. General Responsibilities and Requirements

A. Responsibilities of Bursar Operations and the LSU A&M Chief IT Security and Policy Officer or campus-level IT unit and/or security personnel

1. Administer the process of obtaining new merchant accounts.
2. Communicate the policy and PCI DSS to merchants, business offices, and campus-level IT.
3. Advise merchants wanting to accept payment card payments via wireless, the Internet, or transmit payment card information via the Internet for batch processing on approved eMarket and/or P2PE solutions.
4. Coordinate periodic reviews of existing merchants to include verification of procedures, vulnerability scans, and other activities required at the institutional level.

B. Responsibilities of Payment Card Merchants

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

C. Responsibilities of PCI Project Team

The PCI Project Team is responsible for developing strategies for remediation of non-compliant items, addressing issues and findings, and monitoring merchant areas to ensure any and all corrective actions are applied.

D. General Responsibilities for all Fiscal Officers and Systems Managers

1. Comply with applicable sections of the current version of PCI DSS.
2. Obtain approval for new University merchants or new purchases of computer software or hardware containing payment transaction features – requests for new merchants require approval by Bursar Operations. Approval from Procurement Services and Bursar Operations is required before entering into any contract, purchase, acquisition, or replacement of equipment, software, or wireless device, in relation to payment processing.
3. Maintain a departmental PCI policy – supervisors must establish and document policies and procedures for physically and electronically safeguarding cardholder information and satisfy the requirements of the current version of PCI DSS. Please complete the form AS539 "Responsibilities of Payment Card Handlers and Processors" according to your department's payment card processing arrangement.
4. Ensure cardholder data is not stored in physical or electronic form. Handling of physical payment cards should be restricted to those individuals working in the capacity of their job responsibilities. All

employees involved in payment card handling must be trained on an annual basis.

5. Communicate policy to staff and obtain signatures – supervisors including Deans/Directors, fiscal officers, and systems managers must communicate this policy to their staff and submit appropriate forms (AS539) for all personnel involved in payment card transactions.
6. Assign a unique ID to each person with computer access – A unique ID must be assigned to each person with computer access to payment card information. User names and passwords shall not be shared.
7. Transmitting payment card information by email or fax is prohibited – Full or partial payment card numbers and three or four digit validation codes (usually on the back of payment cards) may not be faxed or e- mailed.
8. 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 payment card or the PIN, personal identification number.
9. Segregation of duties – Establish appropriate segregation of duties between personnel handling payment card processing, the processing of refunds, and the reconciliation function.
10. Complete an annual SAQ.
11. Background checks – In accordance with University policies, ensure background checks are performed on potential employees who have access to systems, networks, or cardholder data. 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.
12. If necessary for receipts, reporting, or reconciliation, show only the last four digits (suffix) of the payment card number.
13. Imprint machines are not permitted – Do not use imprint machines to process payment card payments as they display the full payment card number on the customer copy.
14. Collect and maintain annual Attestation of Compliance (AOC) documents from third party vendors providing payment services, where applicable.
15. Report security incidents to Bursar Operations, the Chief IT Security and Policy Officer, and campus-level IT and/or IT security units – If you know or suspect that payment 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 email to bursar@lsu.edu and via phone to (225) 578-3357
    c. Chief IT Security and Policy Officer via email to security@lsu.edu and via phone to (225) 578-3700 for LSU A&M or
    d. Campus-level IT units for other campuses

    This report must not disclose via fax or email payment card numbers, three or four digit validation codes, or PINs. The report must include a department name and contact number.

E. Specific Responsibilities for all Fiscal Officers and Systems Managers

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

1. Payment 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 and Procurement Services. Approval from the LSU A&M Chief IT Security and Policy Officer or by campus-level IT unit and/or IT security personnel at other campuses will be coordinated by Bursar Operations.

Case C Software that is PCI approved and approved by Bursar Operations and Procurement Services. Approval from the LSU A&M Chief IT Security and Policy Officer or by campus-level IT unit and/or IT security personnel at other campuses will be coordinated by Bursar Operations.

Case D Wireless device and software that is PCI approved and approved by Bursar Operations and Procurement Services. Approval from the LSU A&M Chief IT Security and Policy Officer or by campus-level IT unit and/or IT security personnel at other campuses will be coordinated by Bursar Operations.

Payment 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 payment 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 payment card data.

See Case A below. Alternatively, an LSU department may submit a request to transmit or process the payment 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 member of the PCI Project Team (See Case B, C, or D below):

Payment Card Terminal Merchants

Merchants using payment card terminals connected to a data phone line. ***The university will begin migrating to P2PE solutions in FY 2020.***	
Fiscal Requirements	• Use terminals that do not print on the customer copy the full payment card number. • Background checks should be performed in accordance with university and PCI-DSS guidelines. • Migrate to P2PE solution in accordance with the university's migration timeline.

Internet-related Merchants

Case A – Merchants Redirecting *Redirecting customers to PCI approved service providers or to another company's website using a link from an LSU computer. Merchants do NOT transmit, process, or store payment card data on any computer located on a University IP address.*	
Examples	• LSU hosted web page collects all information except payment card information (i.e. LSU web page is linked to RegOnline product). • LSU hosted web page is linked to another PCI approved company's site.

Questions	• Is the service provider PCI approved? • Is the service provider linked to another service provider? If yes, is that provider PCI approved? • Does the merchant have access to payment card number? If yes, this is not permitted.
Fiscal Requirements	• All service providers are PCI approved. • Third party contract language applies to all vendors. No access to payment card numbers.
System Requirements	• Successful external vulnerability scan by Approved Scanning Vendor. • Successful internal vulnerability scan performed by campus IT. Department must coordinate with campus IT team to schedule such scans. • Implement technical controls to provide a secure computing environment, including all applicable controls required by PCI DSS. • There should be no access to payment card numbers at the redirected site.

Case B – Point of Sale (POS) Merchants *Using terminal connected to a computer to transmit or process payment card information and using PCI approved service providers. POS software must be PCI approved and approved by the university PCI Project Team. Merchants must submit a request to Bursar Operations.*	
Examples	• Using POS software to transmit or process payment card information. • Using a terminal connected to a computer to swipe payment card transactions that are "batched" daily and sent via the Internet.
Questions	• Is the POS software on the PCI list? • Is the service provider on the PCI approved list? • Is the service provider linked to another service provider? If yes, is that provider PCI approved? • Does the merchant have access to payment card numbers? If yes, this is not permitted.
Fiscal Requirements	• Software is on the PCI list. • All service providers are PCI approved. • Third party contract language applies to all vendors. • No access to payment card numbers. • Background checks should be performed in accordance with university and PCI-DSS guidelines. • Annual Attestation of Compliance (AOC) required by service providers.
System Requirements	• Successful external vulnerability scan by Approved Scanning Vendor. • Successful quarterly vulnerability internal scan performed by campus IT. Department must coordinate with campus IT team to schedule such scans. • Implement technical controls to provide a secure computing environment, including all applicable controls required by PCI DSS.

Case C – Merchants Using Software *Using software that is PCI approved to transmit or process payment card information and using PCI approved service providers. Merchant must submit a request to Bursar Operations.*

Examples	• Purchased software installed on university computer that transmits to a PCI approved service provider.
Questions	• Is software on the PCI list? • Is the service provider on the PCI approved list? • Is the service provider linked to another service provider? If yes, is that provider PCI approved? • Does the merchant have access to payment card numbers? If yes, this is not permitted.
Fiscal Requirements	• All service providers are PCI approved. • Third party contract vetted through Procurement Services. • Background checks should be performed in accordance with university and PCI-DSS guidelines. • Annual AOC required for service providers.
System Requirements	• Successful external vulnerability scan by Approved Scanning Vendor. • Successful internal vulnerability scan performed by campus IT. Department must coordinate with campus IT team to schedule such scans. • Implement technical controls to provide a secure computing environment, including all applicable controls required by PCI DSS.

Case D – Wireless Merchants *Using wireless terminals via direct transmission of payment card information to a PCI approved service provider. Merchant must submit a request to Bursar Operations.*	
Examples	• Wireless transmission of payment card data using a PCI approved wireless device.
Questions	• Is wireless device and cellular service on the PCI and LSU approved list? • Is the service provider on the PCI approved list? • Is the service provider linked to another service provider? If yes, is that provider PCI compliant?
Fiscal Requirements	• Wireless device and software is on the PCI list. • All service providers are PCI approved. • Third party contract language applies to all vendors. • Background checks should be performed in accordance with university and PCI-DSS guidelines. • Annual AOC required for service providers.
System Requirements	• Implement technical controls to provide a secure computing environment, including all applicable controls required by PCI DSS.

VII. Miscellaneous Topics

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

A. Establishing New University Payment Card Merchant

Departments requesting to accept payment cards must contact Bursar Operations to determine the best solution to meet their business needs while also minimizing the university's PCI scope and exposure, to the greatest extent possible.

eMarkets, where LSU is not the merchant of record, or P2PE solutions are the preferred methods by which the university accepts payment cards.

If it is determined that LSU will be the merchant of record, in order to accept payment cards, a department must complete an AS537 "Payment 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 payment cards, please contact Bursar Operations for assistance at bursar@lsu.edu or (225) 578-3357.

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.

B. Changes to an Existing Account

Changes to an existing merchant account must be approved by Bursar Operations, Procurement Services, and LSU A&M Chief IT Security and Policy Officer or campus-level IT unit and/or IT security personnel. Examples of changes are: purchasing, selling, surplus, or discarding a terminal; purchasing software; selecting a new service provider. Signing a contract with any third party vendor related to payment card payment processing must be approved by Procurement Services.

C. Training

Annual training is required for all individuals involved in the acceptance of payment cards.

D. Accounting for Transactions

Depending on the method by which payment cards are accepted (i.e. eMarket, POS, etc.), the process for recording transactions can differ. Bursar Operations will provide guidance and direction to merchants on the appropriate method for recording accounting transactions. Merchants should consult with Bursar Operations prior to recording deposits to ensure the proper method is used. The primary tool for recording account transactions for merchants is the Customer Accounts Receivable & Deposits (CARD).

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 payment card 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 may be assessed by the University-approved providers. Entries are prepared by Accounting Services to charge these fees to the merchant's expenditure account. A copy of the entry along with a copy of the merchant

services statement is sent to each merchant.

F. Procurement Services

Contracts involving the acceptance of payment cards and/or service providers must be reviewed by Procurement Services if they have terms and conditions and/or require signature. As part of the terms of the contract, all service providers must be PCI compliant throughout the entirety of the contract and should provide an annual AOC.

VIII. Payment Card Data Guide

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