UNIVERSITY of LOUISIANA LAFAYETTE

PAYMENT CARD POLICY

Payment Card Industry Data Security Standard (PCI DSS) Version 3.2

Policy #	AF.0011.1
Responsible Executive:	Vice President for Administration and Finance
Responsible Office:	Financial Services
Originally Issued:	12/6/2022
Latest Revision:	12/6/2022

I. Policy Statement

This Policy governs the process of handling and processing payment card data at the University of Louisiana at Lafayette ("University").

II. Purpose of Policy

The purpose of this Policy is to prevent loss or disclosure of sensitive customer information including payment card data. Failure to protect customer information may result in financial loss for customers, suspension of payment card processing privileges by University and/or the payment card industry, and fines imposed on University by the payment card industry, and damage to the reputation of the department and the University.

A. General Information

1. Payment Card Industry Data Security Standards ("PCI DSS")

   The PCI DSS is a mandated set of requirements agreed upon by the five major payment card companies: VISA, MasterCard, Discover, American Express, and JCB. These security requirements apply to all transactions surrounding the payment card industry and the merchants/organizations that accept these cards as forms of payment. Further details about PCI DSS can be found at the PCI Security Standards Council website: https://www.pcisecuritystandards.org.

   In order to accept payment card payments, the University must prove and maintain compliance with the PCI DSS. This Policy and additional supporting documents provide the requirements for processing, transmission, storage, and disposal of cardholder data transactions. This is done in order to reduce the institutional risk associated with the

administration of card payments by individual departments and to ensure proper internal control and compliance with the PCI DSS.

2. VISA Inc. Cardholder Information Security Plan ("CISP")

   VISA Inc. instituted the CISP in June 2001. CISP is intended to protect VISA cardholder data – wherever it resides – ensuring that members, merchants, and service providers maintain the highest information security standard. In 2004, the CISP requirements were incorporated into the PCI DSS.

3. MasterCard Site Data Protection ("SDP") Program

   The SDP Program, with the PCI DSS as its foundation, details the data security and compliance validation requirements in place to protect stored and transmitted MasterCard payment account data.

B. Audit

The University's Internal Audit Department, the Funds Handling Compliance Accountant, or the Louisiana Legislative Auditor may conduct audits of any Merchant Department at any time.

C. Training

All individuals employed in a Merchant Department will be assigned annual payment card industry training by the Office of Financial Services and the Office of Human Resources in Cornerstone. Student workers employed in a Merchant Department and students representing a student organization which processes payment cards will receive an email from the Office of Financial Services to complete such annual payment card industry training in Moodle.

III. Applicability

This Policy is applicable to all University areas, departments, offices, employees, 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 the University.

IV. Definitions

1. **Application to Become Merchant Department:** is the document used by areas and departments/offices to obtain authorization to receive and process transactions via payment cards.

2. **Cardholder:** someone who owns and benefits from the use of a membership card, particularly a credit card.

3. **Cardholder Data ("CHD"):** are those elements of credit card information that are required by PCI DSS to be protected including Primary Account Number (PAN), Cardholder Name, Expiration Date, and the Service Code.

4. **Cardholder Name:** is the name of the Cardholder to whom the card has been issued.

5. **CAV2, CVC2, CID, or CVV2 Data:** are the three or four digit value printed on or to the right of the signature panel or on the face of a payment card used to verify card-not-present transactions.

6. **Database:** is a structured electronic format for organizing and maintaining information that is accessible in various ways, for example tables or spreadsheets.

7. **Disposal:** is the disposal of CHD in a certain manner that renders all data un-recoverable. This includes paper documents and any electronic media including computers, hard drives, magnetic tapes, USB storage devices. Before disposal or repurposing, computer drives should be sanitized in accordance with the State of Louisiana's Data Sanitization Standards and Requirements. The approved methods are: cross-cut shredding, incineration, approved shredding or disposal service.

8. **Expiration Date:** is the date on which a card expires and is no longer valid. The expiration date is embossed, encoded, or printed on the card.

9. **Magnetic Stripe (i.e. track) Data:** is the data encoded in the magnetic stripe or equivalent data on a chip used for authorization during a card-present transaction. Entries may not retain full magnetic-stripe data after transaction authorization.

10. **Merchant Department:** is any department or unit (e.g., a group of departments or a subset of a department) which has been approved by the University to accept credit cards and has been assigned a Merchant identification number.

11. **Merchant Department Responsible Person ("MDRP"):** is an individual within the Merchant Department who has primary authority and responsibility within that Merchant Department for credit card transactions.

12. **Payment Card Industry Data Security Standards ("PCI DSS"):** are the security requirements defined by the Payment Card Industry Security Standards Council and the 5 major Credit Card Brands: Visa, MasterCard, American Express, Discover, and JCB.

13. **PIN/PIN Block:** is the personal identification number entered by cardholder during a card-present transaction, and/or encrypted PIN block present within the transaction message.

14. **Primary Account Number (""):** is the number code of 14 or 16 digits embossed on a bank or credit card and encoded in the card's magnetic stripe. PAN identifies the issuer of the card and the account and includes a check digit as an authentication device.

15. **Sensitive Authentication Data:** are additional elements of credit card information that are also required to be protected but never stored. These include Magnetic Stripe (i.e., track) data, CAV2, CVC2, CID, or CVV2 data, and PIN/PIN block.

16. **Service Code:** is the service codes that permits where the card is used and for what.

V. Policy Procedure

It is the policy of the University to allow acceptance of payment cards as a form of payment for goods and services upon written approval from the Office of the Vice President for Administration and Finance. The University requires all Merchant Departments or areas that accept payment cards to do so only in compliance with the PCI DSS and in accordance with this Policy, the University's departmental payment card procedures, and other supporting documents.

All areas or departments/offices that receive or expect to receive payments electronically must comply with the guidelines and procedures issued by the Office of the Vice President for Administration and Finance.

A. Request and Approval to Become a Merchant Department of the University

Any area or department/office who wishes to take payments via payment cards must obtain written approval from the appropriate Vice President over the respective area or department/office and the Office of Financial Services via the Application to Become a Merchant Department Form. In order to be a Merchant Department, the area or department/office must be an approved collection point of the University. See the Funds Handling Policy for additional information concerning approved collection points.

To begin the process of becoming a Merchant Department, an Application to Become a Merchant Department Form must be completed and submitted to the Funds Handling Compliance Accountant per the directions on the Form.

B. Merchant Department Requirements and Responsibilities

1. Merchant Departments are required to sign the Office of Financial Services' Payment Card Policy Agreement ("Agreement") which details their responsibilities, as well as security requirements (PCI DSS) that must be followed. This Agreement may be updated from time to time as requirements change. Failure to follow the requirements of the Agreement may result in the revocation of the Merchant Department's ability to accept card payments.

2. Merchant Department's must accept only payment cards authorized by the Office of Financial Services and agree to operate in accordance with the contract(s) the University holds with its service provider(s) and the card brands. This is to ensure that all transactions are in compliance with PCI DSS, federal regulations, NACHA rules, service provider contracts, and University policies regarding security and privacy that pertain to electronic transactions. Merchant Departments shall adhere to the Payment CARD Best Practices. Such Payment Card Best Practices, include, but are not limited to requiring Merchant Departments to keep CHD storage to a minimum by implementing data retention and disposal policies, procedures and processes that include at least the following for all CHD storage as follows:

    - CHD storage amount and retention time shall be limited to that which is required for legal, regulatory, and/or business requirements.

    - CHD that is not absolutely necessary in order to conduct business will not be retained in any format. All CHD will be treated as confidential.

    - Specific retention requirements for CHD must be developed per the University's Record's Management Policy.

    - Develop processes for secure deletion of CHD when it is no longer needed per the University's Record's Management Policy.

    - Develop a quarterly process for identifying and securely deleting stored CHD that exceeds defined retention per the University's Record's Management Policy.

    - Ensure that physical access to CHD records is restricted to staff with a need to know.

3. CHD received via end-user messaging technologies (e.g., email, instant messaging, SMS, chat, etc.) is never to be used to process a payment. Follow approved departmental procedures for the appropriate method of responding to and securely destroying the CHD.

4. All processing equipment is to be obtained through the Office of Financial Services by submitting the Merchant Department Equipment Request per the directions on the Request. Exceptions to this will be limited and will require a business plan (including reason why the available central processing systems will not work for your area) to be submitted attached to the Merchant Department Equipment Request and approved by the Office of Financial Services in advance of any equipment or system purchase.

5. All payments received must be deposited and reconciled in accordance with the University's Funds Handling Policy.

6. The Merchant Department will be responsible for collecting the funds and corresponding fees from the customer for any payment card chargebacks and/or disputed transactions.

7. In the case of a loss of funds or if a MDRP suspects irregularities in the handling of funds, the University of Louisiana at Lafayette Police Department (337-482-6447) and the Office of Internal Audit (337-482-5337) must be contacted immediately.

VI. Enforcement

The University's Office of Financial Services is responsible for enforcement of this Policy.

With respect to Employees, the University's Office of Financial Services, as well as individual MDRPs, are responsible for the enforcement of this Policy. MDRPs are responsible for ensuring adherence to this Policy and are required to take immediate action to ensure compliance.

With respect to students, the University's Office of Financial Services, as well as the Dean of Students, are responsible for the enforcement of this Policy.

Sanctions imposed pursuant to violations of this Policy will be commensurate with the severity of the offense and may include disciplinary action up to and including termination of employment or dismissal of a student or student organization.

VII. Policy Management

Upon adoption, the Vice President of Administration and Finance shall be the Responsible Executive for this Policy. The Assistant Vice President of Financial Services shall be the Responsible Officer for this Policy. The Office of Financial Services is the Responsible Office for this Policy.

VIII. Exclusions

This Policy shall have no exclusions.

IX. Effective Date

This Policy shall be effective as of the date of adoption of this Policy.

X. Adoption

This Policy is hereby adopted on this 12/6/2022.

DocuSigned by:
Joseph Savoie
1405E1487C93461...

Dr. E. Joseph Savoie
President

XI. Appendices, References and Related Materials

- The Office of Financial Services
- Funds Handling Policy
- Record's Management Policy
- Application to Become a Merchant Department
- Merchant Department Equipment Request
- CampusGuard Central Library Templates
- PCI Security Standards
- Payment Card Policy Agreement
- Payment Card PCI Best Practices
- State of Louisiana's Data Sanitization Standard and Requirements
- NACHA Rules
- VISA Inc. Cardholder Information Security Plan ("CISP")
- MasterCard Site Data Protection ("SDP") Program

XII. Revision History

- Original adoption date: 12/6/2022.