Lafayette College Policy for Credit Card and Electronic Payments
(Revised 9/22/2014)

Lafayette College acknowledges the importance of protecting our constituents by abiding by the applicable requirements of the Payment Card Industry (PCI) Security Standards Council, in particular their Data Security Standard commonly known as PCI-DSS. The PCI-DSS is a set of comprehensive requirements for credit card account data security, developed by the credit card industry (Visa, Mastercard, American Express, Discover and other credit card companies) to prevent identity theft and credit card fraud.

Any Lafayette College employee, student, contractor or agent who, in the course of doing business on behalf of the College, is involved in the acceptance of credit cards or electronic payments is subject to this Policy. Failure to comply with the terms of this Policy may result in disciplinary actions and could also limit a department's credit card and electronic payment acceptance privileges. Members of the community who are involved or interested in accepting credit card payments must understand the PCI standards and requirements (https://www.pcisecuritystandards.org/security_standards/) and pledge to adhere to them. In addition, they must also be familiar with this Policy, the College's Acceptable Use Policy, and its Data Stewardship Policy (http://its.lafayette.edu/policies/).

Background

In order to ensure that credit card activities are consistent, efficient and secure, the College has developed this Policy and supporting procedures for all types of credit card activity transacted in-person, over the phone, via mail service or the Internet. Security breaches, including vulnerability or release of confidential information, can result in serious consequences for the College such as the assessment of substantial fines, possible legal liability and the potential loss of the ability to accept credit card payments in addition to reputational damage. This Policy provides guidance so that credit card acceptance and electronic payments (eCommerce) processes comply with PCI-DSS and are appropriately integrated with the College's financial and other systems.

The Controller's Office is responsible for creating and managing all credit card merchant accounts. The Controller's Office and the Associate Vice President for Finance and Business Operations work jointly to oversee College-wide operational policies and procedures regarding payment processing. The Information Technology Services (ITS) division is responsible for the operation of the College's data networks including all merchant services systems. All three groups work together to help establish and ensure continued compliance with PCI-DSS policies and requirements.

Basic Requirements

Departments that wish to accept credit card and/or electronic payments on behalf of Lafayette for donations, goods or services must initially review the request with the Controller's Office to ensure that the credit card merchant account is properly established. Once an appropriate account is established, the department must designate an individual who will have primary authority and responsibility for compliance with applicable College policies within that department. This individual will be referred to in this Policy as the Merchant Department Responsible Person or "MDRP." Applicable departments must have a MDRP at all times. It is the responsibility of the MDRP and the MDRP's direct supervisor to ensure this role is filled. The direct supervisor must notify the Associate Vice President for Finance and Business Operations of the initial MDRP and any changes in the MDRP. The current list of the College's MDRP's is included as Appendix A.

All **MDRPs** must:

1. Ensure that all employees (including the MDRP and any student employees), contractors and agents with access to payment card data within their areas of responsibilities receive and acknowledge upon hire and at least on an annual basis that they have read, understand and agree to comply with this Policy, the College's Acceptable Use Policy and its Data Stewardship Policy. Such acknowledgement form is included as Appendix B. The MDRP should forward a copy of each executed acknowledgement to the Associate Vice President for Finance and Business Operations and keep the original within the department.
2. Ensure that all physical copies of credit card data and bank account data collected by the department is kept secured at all times. Such data to be secured includes but is not limited to account numbers, card imprints, and Terminal Identification Numbers (a unique number assigned and linked to a specific point-of-sale (POS) terminal or workstation that can be used to identify the merchant operating the terminal during credit card sales transaction processing).
3. Ensure all Point of Sale (POS) devices deploy anti-virus software by working with ITS and/or the appropriate vendor, if necessary. Ensure all anti-virus mechanisms are current, actively running and generating audit logs. Retain audit trail history for a minimum of one year.
4. Ensure all POS devices are updated and patched with the latest vendor-supplied security patches. Work with ITS and/or the appropriate vendor as necessary.
5. Ensure Point of Sale (POS) devices are physically secured. In addition, inspect all Point of Sale devices on a weekly basis for tampering or substitution.
6. Verify and collect PCI DSS Compliance Certificate or PA-DSS Validation Certificate (POS systems) from all service providers with whom your department works on at least an annual basis, but quarterly is recommended. The MDRP should retain a copy of the certificates and submit a copy to Associate Vice President for Finance and Business Operations upon receipt. Such service providers include but are not limited to CBS Interactive, Sequoia, Vendini, Harris Connect/iModules, University Tickets, TouchNet and any other companies which accept electronic payments on the College's behalf.

7. Assist in the completion of the PCI Self Assessment Questionnaire the College is required to file. The current version of the Self-Assessment Questionnaire the College is required to complete is attached as Appendix C.

Data is considered to be secured only if the following criteria are met.

- Only those with a need-to-know are granted access to credit card, bank account and electronic payment data. When an employee no longer needs to know such information, their access to such information, POS terminals, secure locations, and files should be revoked.
- Email, text, instant messaging and fax must not be used to transmit credit card or personal payment information. If it should be necessary to transmit credit card information, only the last four digits of the credit card number can be displayed.
- Credit card or personal payment information is never stored electronically or downloaded onto a computer or network drive or to any portable devices such as USB flash drives, compact disks, laptop computers or personal digital assistants/cell phones.
- The processing and storage of personally identifiable credit card or payment information on College computers and servers is prohibited. Such information includes, but is not limited to credit card numbers, expiration dates, credit card validation codes, social security numbers, and bank account information.
- The three-digit card-validation code printed on the signature panel of a credit card (or four-digit card-validation code printed on the front of an American Express card) is never stored in any form. Elsewhere is this Policy, this code is referred to as the CSV code.
- The full contents of any track from the magnetic stripe (on the back of a credit card, in a chip, etc.) are never stored in any form.
- All but the last four digits of any credit card account number are always masked, should it be necessary to display credit card data.
- Credit card information received for manual processing must be processed in a credit card merchant account the same day it is received if possible; but absolutely no later than 1 business day.
- Upon successful entry into a POS/payment processor, all credit card data must be redacted from the documentation. Acceptable methods for credit card data redaction are: 1). Cut the credit card data out of the document and immediately shred it. 2). Completely mask the credit card data with a wide tip black marker, photocopy the document and immediately shred the original.
- Any credit card data (number, expiration date and CSV code) that has not been processed thru a credit card merchant account (pending entry in POS/payment processor) shall be housed in a secure/locked location and only authorized and essential staff shall have access to the keys/combination.
- All credit card receipts and credit card authorizations must be kept in a locked and secure area.
- Any credit card or bank account information that must be conveyed to the Controller's Office for entry into a POS/payment processor must be hand-delivered in a sealed envelope by someone within the department who is

authorized and has signed the PCI DSS Employee Acknowledgement Form. The campus mail system should never be used to transit credit card information to the Controller's Office.

- All media containing credit card and personal payment data that is no longer deemed necessary or appropriate to store must be destroyed or rendered unreadable. [Transactional records which must not contain credit card or bank account information should be retained per the College's document retention policy for a minimum of five (5) years.]

The processing of credit card or bank account data received by email, fax or other unsecured method of transmission is prohibited. If you should receive credit card or bank accounts data via email, the email must be purged from the email system. To appropriately purge please delete the email and then delete it from your deleted/trash folder immediately. Also, contact ITS to ensure that any back-up copies on any server are destroyed. If received via fax or other unsecure method of transmission, shred the document immediately. The customer/donor/constituent should be contacted and advised that we are unable to process the data received and request a more secure means for the payment.

College employees, contractors or agents who obtain access to payment card, bank account, or other personal payment information in the course of conducting business on behalf of the College may not sell, purchase, provide, or exchange said information in any form including but not limited to imprinted sales slips, carbon copies of imprinted sales slips, mailing lists, tapes, or other media obtained by reason of a card transaction to any third party other than to the College's acquiring bank, depository bank, Visa, MasterCard, American Express, Discover or other credit card company, or pursuant to a government request. All requests to provide information to any party outside of your department must be coordinated with the Associate Vice President for Finance and Business Operations.

Quarterly network scans will be facilitated by the ITS division.

Third-Party Partners

All agreements with third party entities (e.g., hardware or software providers - even software as a service (SaaS) providers, or other entities who will be accepting credit card payments on the Lafayette campus such as our Dining Services partner or vendors selling merchandise in Farinon) must comply with the PCI standards. Each department intending to utilize such a third party provider must designate a MDRP and applicable employees or contractors must execute the PCI DSS Employee Acknowledgement Form prior to the execution of any agreement or use of any such hardware, software or system.

Prior to execution of any agreement and use of any hardware, software or service, the department initiating the request must document that the proposed third-party partner is compliant with PCI standards by confirming that they are using systems that are verified PCI Compliant on the Visa Global Registry of Service Providers (http://www.visa.com/splisting/searchGrsp.do) and if purchasing a Point of Sale (POS) system; the system and specifications must be on the PA-DSS

Validated Payment Applications list on the PCI Security Standards Council website: (https://www.pcisecuritystandards.org/approved_companies_providers/vpa_agreement.php).

In addition, all contracts with the vendor/service provider must contain the following language:

> *Lafayette College requires that [vendor] shall at all times maintain compliance with the most current Payment Card Industry Data Security Standards (PCI DSS). [Vendor] will be required to provide written confirmation of compliance annually. [Vendor] acknowledges responsibility for the security of cardholder data as defined within PCI DSS. [Vendor] acknowledges and agrees that cardholder data may only be used for completing the contracted services as described in the full text of this document, or as required by the PCI DSS, or as required by applicable law.*
>
> *In the event of a breach or intrusion or otherwise unauthorized access to cardholder data stored at or for [vendor], [vendor] shall immediately notify Lafayette's Office of the Vice President for Information Technology Systems to allow the proper PCI DSS compliant breach notification process to commence. [Vendor] shall provide appropriate payment card companies, acquiring financial institutions and their respective designees access to the [vendor]'s facilities and all pertinent records to conduct a review of the [vendor]'s compliance with the PCI DSS requirements.*
>
> *In the event of a breach or intrusion [vendor] acknowledges any/all costs related to breach or intrusion or unauthorized access to cardholder data entrusted to [vendor] deemed to be the fault of [vendor] shall be the liability of [vendor]. [Vendor] agrees to assume responsibility for informing all such individuals in accordance with applicable law and to indemnify and hold harmless Lafayette College, and its officers and employees from and against any claims, damages or other harm related to such breach.*

Mobile Devices

All credit card terminals remain connected to the Lafayette phone or network jack designated by ITS. These designated phone or network jacks are uniquely configured and periodically scanned to maintain the College's PCI compliance; therefore utilizing another jack without explicit written permission from ITS is prohibited.

If there is a need for the use of cellular phone, PDA, iPad and other tablet-based payment processing, please contact the Controller's Office to review options.

Process for Responding to a Security Breach

In the event of a breach, a suspected breach of security, or the suspected vulnerability of data that is required to be secured per this Policy, the applicable department must immediately:

1. Notify the Associate Vice President for Finance and Business Operations, the Controller, and the Director of Network and Systems in ITS. Email should be used for initial notification but **details of the breach should not be disclosed in the email correspondence.** The email should provide a phone number at which the MDRP or the individual reporting the incident can be reached.
2. Document all conditions, personnel and events related to the suspected breach and log all actions taken leading up to and after.
3. Be on high alert and monitor all payment systems to prevent further vulnerabilities.
4. Have available the files documenting the department's compliance with this Policy including but not limited to copies of the PCI DSS Employee Acknowledgement Forms, copies of contracts with Third Party Partners, and copies of compliance certifications from Third Party Partners.

ITS will manage the incidence response to mitigate the impact and alert any internal or external agencies or people as required and in accordance with its procedures. As part of managing the incidence response, ITS will:

1. Work with the College's legal counsel to analyze the legal requirements for reporting compromises.
2. Review critical systems and components to inform the College's response.
3. Coordinate with the incident response procedures of applicable vendors and partners.

Appendix A – Merchant Department Responsible Persons

(as of October, 2013)

Dave Blasic for Athletics

Stephanie Hayes for Development

Rachel Moeller for Alumni Relations

Scott Morse for Athletic Communications

Linda Arra for Career Services

Chuck Corsi for the College Store

Kari Fazio for Dining Services

Kristin Cothran for Student Activities

Linda Jroski for the purchasing credit card and travel card programs

Allison Quensen Blatt for Williams Center for the Arts

Judy Reed for Accounts Payable and Receivable

Appendix B – PCI DSS Employee Acknowledgement Form

As a member of the faculty or staff of Lafayette College or as a third-party contractor to Lafayette College, I acknowledge that in the course of my work I may have access to personal, proprietary, transaction-specific, and/or otherwise confidential data through the processing of credit card or electronic banking transactions. As an individual with responsibilities for processing, storing and/or transmitting credit card or bank account data, I may have direct access to sensitive and confidential information in paper or electronic format. To protect the integrity and the security of the systems and processes as well as the personal and proprietary data of those to whom the College provides service, and to preserve and maximize the effectiveness of College's resources, I agree to the following:

- I will maintain the confidentiality of my password and will not disclose it to anyone.
- I will utilize credit card and bank account data for College business purposes only.
- If I am a Lafayette College employee, I have viewed and understand the online training course on PCI made available by ITS. [To view the training, log into http://spaces.lafayette.edu/course/view.php?id=230, select "IT/Security Awareness" under "My Courses" in the left column and then select "PCI" under "Special Topics."]
- I have read, understand and agree to abide by the College's Acceptable Use Policy and Data Stewardship Policy published by ITS. I have also read ITS' Guidelines for Strong Passwords.
- I have read, understand and agree to abide by the College's Policy for Credit Card and Electronic Payments. I will properly store, protect, and dispose of confidential data in accordance with this Policy. Any violations to this Policy will be grounds for disciplinary action up to and including termination of employment.

Name (Print): _____

L #: _____

Signature:_____ Date: _____

Department:_____

MDRP Signature:_____ Date: _____

L # of MDRP: _____

MDRP should retain original and return a copy to the Associate Vice President for Finance and Business Operations.

Appendix C – PCI Self Assessment Questionnaire