Middlebury PCI DSS – Policy for Accepting Credit Card and eCommerce Payments V1.5 2017

http://go.middlebury.edu/PCIPOLICY http://go.middlebury.edu/PCIDSS http://go.middlebury.edu/PCIWISP

1.0 Purpose

This policy document provides information to ensure the College complies with the Payment Card Industry Data Security Standard (PCI DSS). The purpose of the PCI DSS is to protect cardholder data.

2.0 Scope

Any College employee, contractor, individual, entity (hereinafter referred to as agent), systems, and networks involved with the transmission, storage or processing of payment card data (includes systems that can impact the security of payment card data), in the course of doing business on behalf of the College, is subject to this policy, administrative and technical policies located on the Controller's website at http://go.middlebury.edu/pcipolicy.

3.0 Authority

The PCI DSS is a mandated set of requirements agreed upon by the five major credit card companies: VISA, MasterCard, Discover, American Express and Japanese Credit Bureau. These baseline security requirements apply to all transactions surrounding the payment card industry whether electronically driven or hard copy format. There is an annual reporting requirement, Self Assessment Questionnaire (SAQ) that must be completed by the holder of the merchant ID. Further details about this reporting requirement can be found at the PCI Security Standards Council Web site: https://www.pcisecuritystandards.org.

It is the policy of Middlebury that only departments who have been approved by the PCI Compliance Team may accept payment via payment card or contract with service providers to accept payment cards on behalf of Middlebury. Student Organizations and Clubs are prohibited from obtaining a merchant account. Please direct questions regarding the use of payment card services, by Student Organizations and Clubs, to the Student Activities office. Agents of the College are prohibited from accepting monies via PayPal, Venmo, Square or other methods which requires funds to flow through personal bank accounts.

PCI Compliance is an ongoing process, not a one-time event. The PCI DSS emphasizes "Business as Usual" (BAU); performing continuous compliance activities in an ongoing manner 24 hours a day, 7 days a week, 365 days a year.

Individuals found to have violated this policy, whether intentionally or unintentionally, may be subject to disciplinary action, termination and could limit a department's payment card acceptance privileges.

The PCI Compliance Team's purpose is to educate all entities in the College's payment environment and to enforce the PCI DSS Policies contained herein. Questions regarding this policy should be directed to the Middlebury PCI DSS Compliance Team.

4.0 Management

This policy was approved by Senior Finance Leadership, in October 2012. The PCI Compliance Team may modify this policy from time to time and as required annually. This policy is distributed annually in the *Middlebury College Handbook*. The most current version, V1.4, of this policy is to be readily available and accessible http://go.middlebury.edu/handbook.

5.0 Responsibility

Middlebury is committed to complying with the Payment Card Industry Data Security Standards. Compliance by Middlebury requires:

- ➢ Follow Middlebury's PCI DSS administrative and technical policies.
- ➢ Any department accepting payment card data, either at the College or through a Service Provider, on behalf of Middlebury ("Merchant Department") must designate an individual to serve as a Merchant Department Responsible Person (MDRP) within that department who will have primary authority and responsibility for payments made over the internet (eCommerce) and payment card transaction processing within that department.
- ➢ All Middlebury departments accepting payment cards and all agents of the College designated to accept payments cards will be trained upon hire and annually on this Middlebury PCI Policy, Physical Inspection and Skimming Prevention, and must electronically sign the PCI Security Awareness Training & Confidentiality Agreement prior to performing that work.
- ➢ Middlebury ITS staff will be trained upon hire and annually on the Middlebury PCI WISP and this Middlebury PCI policy. ITS staff will acknowledge and electronically sign the PCI Training & Confidentiality Agreement prior to that work.
- ➢ Middlebury will perform a background check on potential personnel who will handle payment card data (except agents of the College that handle one payment card at time; ex. Retail cashier) prior to hire to minimize the risk of attacks from internal sources.
- ➢ Any Middlebury department accepting payment cards will utilize only dedicated, PCI Compliance Team approved equipment to process card payments.
- ➢ Any Middlebury department accepting payment cards will not store cardholder data except as defined by this policy.
- ➢ Ensure that all credit card transactions are reviewed and reconciled to daily merchant reports. Upload daily reconciliation reports to a shared Finance folder.
- ➢ Cardholder data is classified as *Extremely Sensitive Data* as noted in the Data Classification policy.
- ➢ Cardholder data (Media) can be in hardcopy or electronic format.

6.0 Policy

6.1 MDRP

Any department accepting payment card and/or electronic payments on behalf of Middlebury for gifts, goods or services ("Merchant Department") **must** designate an individual (staff or faculty member) **within that department** who will have primary authority and responsibility for eCommerce, payment card transaction processing, third party Service Providers accepting payment cards on behalf of Middlebury, within that department. This individual will be referred to in the remainder of this policy statement as the Merchant Department Responsible Person or "MDRP". MDRP responsibilities can be seen at http://go.middlebury.edu/MDRP.

Each Merchant Department 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 record and track any change in MDRP's.

MDRP Responsibilities include, but are not limited to, the following:

- Ensure agents of the College, with access to or whom can affect the security of payment card data, complete the PCI Security Awareness Training Computer Based Training program **upon hire** and **annually**.

- Ensure job descriptions, for agents of the College that will have access to more than one payment card at a time, include a background check prior to hire.
- Ensure only dedicated, approved hardware/software is utilized to process card payments. Payment solutions such as Paypal, Venmo, Square or other method which requires funds to flow through personal bank accounts are prohibited.
- Be aware of all payment processes and practices within their merchant department.
- Ensure all agents of the College receive, and are trained on, the Merchant Department specific Standard Operating Practice(s) upon hire and annually. Ensure these department specific Standard Operating Practices are adhered to.
- Ensure that all payment card transactions are reviewed and reconciled to daily merchant reports. Upload daily reconciliation reports to the shared folder at Orgs\Payment Gateways\Reconciliation.
- Ensure all Point of Sales (POS) devices, including cellular based stand-alone swipe terminals and point of sale systems, are maintained under a state of consistent control and supervision. **The Cashier's Office has a cellular card swipe terminal for loan to agents of the College that have completed the PCI Security Awareness and Confidentiality Statement.
- Ensure Point of Sale devices/terminals (cash registers, stand-alone swipe terminals etc.) are physically secured.
- Perform Monthly Physical Inspections, on payment card processing devices, as noted in section 6.9 Physical Security and Skimming Prevention. Systems not in use must be secured in a locked facility and regularly inventoried. Retain inspection log for a minimum of one year.
- Ensure that all agents of the College are trained on Physical Security and Skimming Prevention upon hire and at least annually.
- Ensure all Point of Sale (POS) devices have updated patches and antivirus with up to date logging. Retain logging and audit trail history for a minimum of one year.
- Service Provider Management - verify and collect PCI DSS Compliance Certificates or PA-DSS Validation certificate (POS systems) on all service providers within the relevant Merchant Department on an annual basis. The MDRP should retain a copy of the certificates and submit a copy to the PCI DSS Compliance Team upon receipt.
- Ensure user access to cardholder data environment, within the relevant Merchant Department, is revoked when the individual's job no longer requires access to the Cardholder Data Environment (CDE). Maintain an audit log of user access to cardholder data environment for a minimum of one year.
- Validate compliance for the merchant department on an annual basis, by completing the Self Assessment Questionnaire (SAQ) in collaboration with the PCI Compliance Team.

6.2 Authorization

- Limit access to system components and cardholder data to only those individuals whose job requires such access
- The level of access is determined by job requirements; based on the least privilege model
- *Sensitive areas* are physically secured and sign in logs are utilized.
- Sufficient controls are in place to identify individuals entering/exiting
- Each Merchant Department must retain the signed PCI Security Awareness Training & Confidentiality Agreements, maintain a current list of employees and review monthly to ensure that the list reflects the most current access needed and granted.
- Each Merchant Department must maintain a current list of equipment authorized to be used to process CHD. Each equipment item must be identified by make, model, serial number (or other method of unique identification) and location of device. The equipment list must be submitted to the PCI Compliance Team quarterly; January 15, April 15, July 15, October 15.

6.3 Credit Card Acceptance and Handling

- In the course of doing business at Middlebury it may be necessary for a department or other unit to accept payment cards. The opening of a new merchant account for the purpose of accepting and processing of payment cards is done on a case by case basis. Any fees associated with the acceptance of payment cards in that unit, will

be charged to the unit (including but not limited to; infrastructure, security and management, i.e firewall, switch, network cables). Student Organizations and Clubs are prohibited from obtaining a merchant account, please contact the Student Activities office for available options.

- See Transmitting for acceptable methods of payment card acceptance.
- Interested departments should contact the PCI Compliance Team to begin the process of accepting credit cards. Steps include:
    - Completion of an "Application to become a Merchant Department"
    - Completion of training
    - Read the Middlebury PCI Policy for Accepting Credit Card and eCommerce Payments and the Middlebury PCI WISP
    - Completion of PCI Security Awareness Training Program
- All payment card transactions must be reviewed daily (business days) and reconciled to daily merchant reports. Daily reconciliation reports are to be saved in the Orgs\Payment Gateways\Reconciliation shared folder. Failure to reconcile payment card transactions in a timely manner is cause for the merchant department payment card processing ability to be suspended.

6.4 Transmitting

- Employees must be discreet and use common sense when handling cardholder data.
- Payment cards may be accepted in the follow manner:
    - In person (card present)
    - Direct telephone contact (telephone order); the constituent on the telephone should verify the payment card information twice, agents of the College should not read the payment card data back to constituent
    - Through a PCI DSS compliant automated system that is entirely hosted by a PCI DSS compliant third party organization (eCommerce) and approved by the PCI Compliance Team
    - Physical mail
- Cardholder data must not be accepted or sent via end user messaging technologies; email, text message, SMS, chat etc. If an email is received containing cardholder data, a snapshot of the email header must be sent to the PCI Compliance Team at pcicomplianceteam@middlebury.edu for logging. DO NOT FORWARD or PRINT the cardholder data. Delete the email from Inbox and Deleted Items folder. It is also necessary to delete it from the "Recover Deleted Items" folder. Follow up with the constituent and advise this method of transmitting cardholder data is not secure. Advise the constituent we cannot process the payment and educate him/her on the appropriate methods of conveying a credit card payment. See above for appropriate acceptance methods.
- Constituent Cardholder data must not be accepted or sent via fax. If a fax is received with cardholder data, immediately shred in a crosscut shredder. Notify the PCI Compliance Team with the name, date, location the cardholder data was received. Follow up with the constituent and advise this method of transmitting cardholder data is not secure. Advise the constituent we cannot process the payment and educate him/her on the appropriate methods of conveying a credit card payment. See above for appropriate acceptance methods. **Middlebury Procurement Cards are exempt from this specific requirement- Procurement cards may be faxed**.
- Merchant departments must maintain strict control over the internal and external distribution of any kind of media that contain cardholder data. All media moved from a designated secure area (department the cardholder data is delivered to) must be marked confidential, documented on a triplicate copy media removal tracking log, and transported in a secure bag by Public Safety or a document service. No media containing cardholder data may leave the premises of the department that accepted it for processing. Materials sent to constituents, with a designated area for written cardholder data, to be returned to Middlebury must have the return address of the department that will process the cardholder data on the return vehicle. Every effort should be made to eliminate the area for written cardholder data on appeals, instead noting a secure means to make a credit card payment on a secure online forms, by check, or phone.
- In the rare instance that an agent of the College is offered payment card information during an off-site visit, the agent will provide the donor with a transmittal form or direct the constituent to an approved method of payment (i.e. online donation site, phone). The constituent may then fill out the form and mail it directly to the

appropriate office at Middlebury. For compliancy and security Middlebury employees must not store or take possession of cardholder data (CHD) while off-site.

6.5 Processing

- Cardholder Data received for manual processing (mail, hand delivered) 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 (excluding calendar and fiscal year end periods). Cardholder data in written form is redacted immediately following authorization in the payment gateway. Acceptable forms of redaction are crosscut shred, incinerate, or pulp hardcopy materials so that cardholder data cannot be reconstructed.
- Refunds for donations must be processed using the same credit card for the transaction. A different card may not be used.
- Mask the Primary Account Number (PAN) when displayed (the first six and last four digits are the maximum number of digits to be displayed), such that only personnel with a legitimate business need can see the full PAN.

6.6 Storage

- ****Middlebury does not store authorized cardholder data (media), in hardcopy or electronic form****
- Cardholder data that is collected but has not yet been processed (pending authorization in payment gateway), in addition to any USPS mail that hasn't been opened, must be stored in a secure location (locked safe, locked file cabinet), see Processing above. Only authorized staff shall have access to the keys/combination.
- Middlebury does not store Sensitive Authentication Data; including the primary account number (PAN), expiration date and service code (CVV).
- Cardholder data may not be stored on any portable devices including but not limited to USB flash drives, cellular phones, personal digital assistants and laptop computers.
- Cardholder data may not be stored in logs (for example, transaction, history, debugging, error), history files, trace files or database contents.
- Procurement cards may not be stored
- A quarterly process for identifying and securely deleting stored cardholder data is maintained in the Information Security - Auditing and Penetration Test - Standard Operating Procedures (SOP).

6.7 Disposal

- Cardholder data must be disposed of in a certain manner that renders all data unrecoverable. This includes hard copy (paper) documents and any electronic media including computers, hard drives, magnetic tapes and USB storage devices.
- The approved methods of disposal for hardcopy media are:
    - Cross-cut shredding
    - Incineration
- The approved method of disposal, rendered unrecoverable, for electronic media:
    - Secure wipe program
    - In accordance with industry-accepted standards for secure deletion
    - Physically destroying the media is rendered unrecoverable

6.8 Merchant Account Request

The MDRP must follow the process noted in Appendix A: Checklist for Process for Merchant Account Request or Service Provider Change, Appendix B: Merchant Account Request Form or Service Provider Change and Appendix C: PROJECT PLAN (PCI Related), located at the end of this policy, to implement payment card processing and ecommerce at

Middlebury. These steps must also be completed in the event of a **significant system** or **Service Provider** change in payment card and ecommerce processing systems.

6.9 Physical Security and Skimming Prevention of Payment Card Processing Devices

Middlebury will maintain an up-to-date inventory of all devices that capture payment card data. Middlebury will protect card present processing devices from tampering or substitution in adherence to the below requirements:

The MDRP, or designee, is to conduct the following:

- Maintain a list of all devices that capture payment card data, for which the list is to include the following:
    - Make, model, serial number (or other method of unique identification) and location of device
    - Ensure that the list of devices is updated when devices are added, relocated, decommissioned
    - Physically secure all devices that capture payment card data
    - Portable payment card processing devices must be stored securely in a locked area when not in use.
    - Cashiers must perform a daily visual inspection of devices that capture payment card data
    - Train employees, in their department, upon hire and at least annually on *Physical Security of Point of Sale Devices – Skimming Best Practices*.
    - Attendance logs for the Physical Inspection-Skimming Prevention training, must be kept by the MDRP and provided to the PCI Compliance Team upon request.
    - A Terminal Characteristics form must be completed for each terminal annually and upon any significant change
    - A monthly physical inspection must be performed, documented and retained.

The Terminal Characteristics and Monthly Physical Inspection forms must be retained for a period of one year. MDRP or designated staff are to submit the Monthly Physical Inspection forms to the PCI Compliance Team on a quarterly basis; January 15, April 15, July 15, October 15.

6.10 Security Awareness Program

In accordance with Middlebury's Standard Operating Practice Req 12.6 Formal PCI Security Awareness Program:

All persons with physical and logical access to Middlebury's environment, whether employees, third-parties, service providers, contractors, temporary employees, and/or other staff members, must be trained on their role in protecting Middlebury from threats to help safeguard Middlebury's finances, operations, and brand name.

- Upon hire and at least annually, all users connected to Middlebury's cardholder data environment (in any way), are to complete the Middlebury's PCI DSS Security Awareness Training program.
- Read the Middlebury PCI Policy for Accepting Credit Card and eCommerce Payment
- ITS staff are required to read the Middlebury PCI WISP and acknowledge their role in safeguarding Middlebury's environment, by electronically signing the ITS version of the PCI Training and Confidentiality Agreement upon hire and on an annual basis.
- Employees entering payment card data into a card-present device must read and adhere to the Skimming Prevention and Physical Security training material.
- Attendance logs for those who attend Security Awareness and Physical Inspection-Skimming Prevention training, must be kept by Information Security and provided to the PCI Compliance Team upon request.
- All agents of the College must read and electronically sign the Confidentiality agreement in agreement with Middlebury's terms and conditions and acknowledgment of their role in safeguarding Middlebury's environment on an annual basis.

6.10.1 Technical Training

In addition to the above, those who have admin or privileged access (ITS staff) or roles with systems which transmit, process, and store cardholder data must receive additional technical training to further reinforce and supplement their knowledge of security practices.

6.11 Security Breach

In the event of a breach or suspected breach of security, the department must immediately execute each of the relevant steps detailed below:

- The MDRP or any individual suspecting a security breach must immediately notify the Incident Response Team at infosec@middlebury.edu, in accordance with the Technical Incident Response Policy, of an actual breach or suspected breach of payment card information. Email should be used for the initial notification and to provide a telephone number for the Incident Response Team to respond to. Details of the breach should not be disclosed in email correspondence.
- Notify the MDRP and the department head of the unit experiencing the suspected breach.
- The MDRP or any individual suspecting a security breach involving ecommerce also must immediately ensure that the following steps, where relevant, are taken to contain and limit the exposure of the breach:
    - Prevent any further access to or alteration of the compromised system(s). (i.e., do not log on at all to the machine and/or change passwords)
    - Do not switch off the compromised machine; instead, isolate the compromised system(s) from the network by unplugging the network connection cable.
    - Preserve logs and electronic evidence.
    - Document every action you take from the point of suspected breach forward, preserving any logs or electronic evidence available. Include in the documentation:
        - Date and time
        - Action taken
        - Location
        - Person performing action
        - Person performing documentation
        - All personnel involved
    - Be on HIGH alert and monitor all ecommerce applications
    - Log all actions taken

If a suspected or confirmed intrusion / breach of a system has occurred, the Incident Response Team will alert Beazley Insurance, the merchant bank, the payment card associations, Internal Risk Department, General Counsel, and Senior Finance Leadership. A detailed incident response plan will be maintained by ITS Information Security. This incident response plan shall be in accordance with the parameters set forth by the Card Brands.

6.12 Service Provider Management

In accordance with Middlebury's Standard Operating Practice Req 12.8 Management of Service Providers:

Service Providers (third parties) are contractually required to adhere to the PCI DSS requirements. Due diligence must be exercised before engaging with any service providers that may affect or have a relationship or function associated with Middlebury's cardholder data environment. The written agreement shall include an acknowledgement by the service providers of their responsibility for securing cardholder data and breach liability language, see Data Privacy and Breach Notification .

Note: This also includes companies that provide services that control or could impact the security of cardholder data. Examples include managed service providers that provide managed firewalls, IDS and other services as well as hosting providers and other entities.

- Each Merchant Department must obtain the appropriate PCI Compliance documentation, from Service Providers, on an annual basis (prior to expiration date of the current documentation). The Service Provider Responsibility Matrix and AOC Tracker is viewable by MDRP's at https://docs.google.com/spreadsheets/d/1hwN2pc6D8iAQipDqMl-xxLqLT3eMl5qxHClGpUlUSS4/edit#gid=0.
- The MDRP is responsible for sending the updated PCI Compliance documentation to the PCI Compliance Team upon receipt from the Service Provider.
- Information Technology Services is responsible for obtaining the appropriate PCI Compliance documentation from managed service providers that provide managed firewalls, IDS and other services as well as hosting providers and other entities.
- Service Providers must provide either an SAQD-Service Provider AOC or an On-Site Assessment AOC for Service Providers. AOC's must note specific requirements Service Provider is attesting to.
- Service Providers must provide a current quarterly vulnerability scan from their ASV.
- Verify Payment Applications are validated on the PA DSS List of Validated Payment Applications at https://www.pcisecuritystandards.org/approved_companies_providers/vpa_agreement.php .

The PCI Compliance Team will maintain a collective, current and accurate list of Service Providers, at https://docs.google.com/spreadsheets/d/1hwN2pc6D8iAQipDqMl-xxLqLT3eMl5qxHClGpUlUSS4/edit#gid=0, with the following information:

- Service Provider Name
- Service being provided - description
- PCI Validation Required
- Validation Date
- Expiration Date
- Assessor
- Functional Area
- MDRP Responsible

6.13 Student Organizations

Student Organizations are NOT ALLOWED to accept monies via Paypal, Venmo, Square or other method which requires funds to flow through personal bank accounts.

All money collected from fundraisers or dues must be deposited directly into the organization's university account. No organizational money should ever be deposited into a personal banking account.

6.14 Student Vendors

Student Vendors must contact Business Services to complete the Student Vendor Authorization and Contract to obtain approval to act as a student vendor. Student Vendors are prohibited from using the College's payment card processes and systems. Student Vendors are not agents of the College.

7.0 Definitions

BAU - Business as Usual - The normal execution of standard functional operations within an organization

Breach - Any payment card data exposed by negligence or malice constitutes a reportable breach

CDE - Cardholder data environment - Area of computer system network that possesses cardholder data or sensitive authentication data and those systems and segments that directly attach or support cardholder processing, storage, or transmission.

CHD – Cardholder Data - payment card components that are required to be protected. These include: Primary Account Number, Cardholder Name, Expiration Date, Service Code, and Card Verification Code

Ecommerce - The buying and selling of products or services over the Internet

Managed Service Providers*:* A managed services provider (MSP) is most often an information technology (IT) services provider that manages and assumes responsibility for providing a defined set of services to its clients either proactively or as the MSP (not the client) determines that services are needed. Managed Services can include, but are not limited to: Backup, Data Recovery, Storage, Security, Network Management, Management Information Systems, Systems Management and Data Management.

MDRP – Merchant Department Responsible Person - Any department accepting payment card payments on behalf of the College for gifts, goods, or services ("Merchant Department") must designate an individual within that department who will have primary authority and responsibility for ecommerce and payment card transaction processing within that department.

Media - refers to all paper and electronic media containing cardholder data.

Merchant - Any entity that accepts payment cards bearing the logos of any of the five members of PCI SSC (American Express, Discover, JCB, MasterCard, or Visa) as payment for goods and/or services. Note that a merchant that accepts payment cards as payment for goods and/or services can also be a service provider, if the services sold result in storing, processing, or transmitting cardholder data on behalf of other merchants or service providers.

Merchant Account/ID - A bank account that allows businesses to accept payments by payment cards. A merchant account is established under an agreement between an acceptor and a merchant acquiring bank for the settlement of payment card transactions.

Merchant of Record -

Payment Gateway - An e-commerce application service provider service that authorizes payment card payments

Payment Processor - A company, often third party, appointed by a merchant to handle payment card transactions for merchant acquiring banks.

PCI DSS COMPLIANCE - The Payment Card Industry Data Security Standard (PCI DSS) is mandated set of policies and procedures intended to optimize the security of credit, debit, and cash card transactions and protect cardholder against misuse of their personal information.

Point of Sale (POS) - The location where a payment card transaction occurs through a terminal or register.

SaaS Survey - Middlebury Security and Compliance Survey; required for all new Service Providers.

Self-Assessment Questionnaire (SAQ) - A validation tool to help merchants validate their compliance with PCI-DSS

Sensitive Area - refers to any data center, server room or any area that houses systems that store, process, or transmit cardholder data. This excludes public-facing areas where only point-of sale terminals are present, such as the cashier areas in a retail store.

Service Provider - Business entity that is not a payment brand, directly involved in the processing, storage, or transmission of cardholder data on behalf of another entity. This also includes companies that provide services that control or could impact the security of cardholder data. Examples include managed service providers that provide managed firewalls, IDS and other services as well as hosting providers and other entities. If an entity provides a service that involves only the provision of public network access—such as a telecommunications company providing just the

communication link—the entity would not be considered a service provider for that service (although they may be considered a service provider for other services).

Third Party - payment card transactions are processed through an external party to Middlebury. Software may or may not be owned by Middlebury.

8.0 Related Documents/Links

- Middlebury's PCI DSS Policy for Accepting Credit Card and ecommerce Payments http://go.middlebury.edu/pcipolicy
- Middlebury PCI Written Information Security Policy http://go.middlebury.edu/PCIWISP
- Middlebury PCI DSS Information Pages http://go.middlebury.edu/pcidss
- The web site for the PCI DSS Security Standards Council https://www.pcisecuritystandards.org/
- PCI DSS Overview https://www.pcisecuritystandards.org/security_standards/index.php http://www.compliance101.com/
- PCI DSS Self-Assessment Questionnaire Overview and instructions https://www.pcisecuritystandards.org/merchants/self_assessment_form.php
- For a list of Visa validated service providers see http://usa.visa.com/merchants/risk_management/cisp_service_providers.html
- For a list of validated P2PE (Point to Point Encryption) Solutions see https://www.pcisecuritystandards.org/assessors_and_solutions/point_to_point_encryption_solutions
- For a list of validated Payment Applications see https://www.pcisecuritystandards.org/approved_companies_providers/vpa_agreement.php
- https://www.pcisecuritystandards.org/document library PCI DSS V3.2

9.0 Revisions

V1.0 October 2012
V1.1 September 2013
V1.2 August 2014
V1.3 August 2015
V1.4 August 2016
V1.5 September 2017

10.0 Key Dates

- April 28, 2016 – PCI DSS Version 3.2 released
- June 30, 2016 – Sunset date for all service providers to migrate to secure versions of TLS in their service offerings
- October 31, 2016 – PCI DSS Version 3.1 expires, making PCI DSS Version 3.2 fully in force
- January 31, 2018 – Sunset date for all new requirements to be treated as best practices instead of requirements
- June 30, 2018 – Sunset date for all merchants to migrate to secure versions of TLS in their PCI related operations (certain exceptions for POS systems apply)

11.0 Appendices

Appendix A: Checklist for Process for Merchant Account Request or Service Provider Change
Appendix B: Merchant Account Request Form or Service Provider Change
Appendix C: Project Plan (PCI Related)

Appendix A: Procedure for Merchant Account Request and/or Service Provider Change

SUBMIT TO THE PCI COMPLIANCE Team @ PCIComplianceTeam@middlebury.edu

Project Name:
Description of services being utilized/contracted for:

Third parties, with whom cardholder data is shared, are contractually required to adhere to the PCI DSS requirements and to acknowledge that they are responsible for the security of the cardholder data which they transmit, process, store or can affect the security thereof.

Written agreement with Service Providers must include the Data Privacy and Breach Notification language and a minimum liability insurance coverage.

Proposed Service Providers with a payment card component, or that can impact the security of payment card data, must provide the following documentation, and meet the below requirements, to be considered a Service Provider for Middlebury:

- Provide either an SAQ D-Service Provider Attestation of Compliance (AOC) or an On-Site Assessment AOC for Service Providers. Any other SAQ is not applicable. The AOC must be for the Service Provider we are contracting with, the Service Provider cannot rely on third party service provider's compliance.
- The AOC must specifically note assessment of the service being provided.
- Provide a recent quarterly vulnerability scan by their ASV.
- Complete the http://go.middlebury.edu/saas.
- Submit a card flow diagram, also known as a data flow diagram, noting all third party Service Providers involved in the process.
- Matrix of PCI Responsibilities Service Provider is responsible for.
- Service Provider Level 1, listed on the Visa Global Registry, is preferable
- Card present solutions should be Payment Card Industry Security Standards Council (PCI SSC) validated Point to Point Encryption (P2PE) solution. Service Provider must provide the PCI SSC Validation number.
- If a non-P2PE Payment Application is being considered, it must be listed on the PA DSS Validated Application List. NOTE- NON-P2PE VALIDATED SOLUTIONS REQUIRE ADDITIONAL REQUIREMENTS AND SIGNIFICANT COST TO THE MERCHANT DEPARTMENT.
- Must use only Payment Card Industry (PCI)-certified Qualified Integrators and Reseller (QIR) professionals for point-of-sale (POS) application and terminal Installation and integration.
- Encryption protocol must be TLS 1.1 or greater. TLS 1.2 is preferred, SSL and TLS 1.0 are no longer considered secure or compliant.

MDRP's must perform Service Provider "due diligence" on an annual basis or upon significant changes with the Service Provider. The MDRP should collaborate with the Service Provider to receive the current compliance document prior to the expiration of the documentation on file. The following documentation is to be forwarded to the PCI Compliance Team annually:

- Service Providers must provide either an SAQ D-Service Provider AOC or an On-Site Assessment AOC for Service Providers.
- The AOC submitted must specifically note assessment for the services being provided.
- Verify PCI SSC P2PE validation.
- Verify Payment Applications are listed PA DSS Applications and current version is being utilized.

Note: All Service Providers must complete **either** an SAQD-Service Provider AOC or an On-Site Assessment AOC for Service Providers. Any other SAQ is not applicable to a Service Provider.

Checklist:

1. ____ Functional area determines a need for a credit card/ecommerce account or new Service Provider for an existing process/merchant account.
2. ____ Functional area submits a request for above to the PCI Compliance Team by completing Appendix B: Merchant Account Request Form or Service Provider Change , Project Plan, the proposed contract, a point of access payment card diagram (obtained from the Service Provider), network configuration document (showing firewall configurations, Ports, IP addresses if this is a POS system) and Service Providers PCI Compliance documentation.
3. ____ Functional area sends the Service Provider the SaaS and Compliance Survey to complete. Service Provider must provide a firewall configuration document showing the requested firewall, ports, and IP configuration. Network Security submits findings to PCI Compliance Team.
4. ____ PCI Compliance Team gives conditional approval for the new solution. Functional area sends Project Plan to Information Technology Services for review and priority.
5. ____ Information Technology Services department(s) sends approval/non-approval to the functional area and PCI Compliance Team.
6. ____ PCI Compliance Team FINAL approval/non-approval for project request.
7. ____ Contract is approved in accordance with the College Contract Policy and includes the Data Privacy and Breach Notification clause.
8. ____ Functional area, PCI Compliance Team and Information Technology Services to collaborate on prioritization and scheduling of project implementation.
9. ____ PCI Compliance Team trains the MDRP on responsibilities.
10. ____ Functional area works with Finance to ensure the transactions are properly recorded in the general ledger and reconciliation reports are saved in the shared reconciliation file.

The comprehensive list of Service Providers is maintained at Service Provider Matrix and AOC Tracker. All MDRP's have been granted read access to the spreadsheet.

****Please note: the MDRP is responsible for managing the Service Provider's) utilized in their department.**

PCI Compliance Team Final Approval:

_____

Finance Representative Date
Kim Downs-Burns, AVP for Student Financial Services

_____

Information Technology Services Representative Date
Chris Norris, ITS Director, Information Security & Systems and Infrastructure

Appendix B: Merchant Account Request Form or Service Provider Change

SUBMIT TO THE PCI Compliance Team @ PCIComplianceTeam@middlebury.edu

Date: Requesting Department: Name:

Title: Email: Extension:

Describe the goods, services, and/or gifts for which you will receive payments. Please be specific:

Is this an existing or new source of revenue?

Provide the Banner FOAPAL(s) where funds will be deposited and related fees will be assessed:

Explain why your department wants to accept payment card payments.

What economic benefits do you expect to gain by accepting credit cards? Please quantify and/or provide additional documentation to support this application.

Describe the frequency of payment card payments. Is this a one-time event? Are payments for seasonal or year-round activity? Provide detailed timeframes.

Will payment card be the sole method of payment? If not, what other methods of payment do you anticipate accepting for this specific purpose?

How do you plan to process these payments? (Check all that apply)

In-person (card present) Mail/phone Internet

**Note: Cardholder data should never be transmitted via email or fax correspondence.*

If you are planning to accept payment card payments via the Internet, do you have a website?

If so, please provide the URL:

Please indicate the estimated annual dollar volume and number of transactions for each applicable payment card acceptance process:

In-person	$	# transactions
Mail/phone	$	# transactions
Internet	$	# transactions

Who will be the Merchant Department Responsible Person (MDRP)? The MDRP, as referenced in the Middlebury (PCI) Policy for Accepting payment card and ecommerce Payments, is responsible for managing payment card and/or ecommerce transaction processing. Include name, job title, phone extension, and describe duties.

Please identify any additional staff who will be involved in processing payment card payments. Include name, job title, phone extension, and describe duties.

Will any other departments, software packages or outside Service Providers be involved in the processing of payment card payments? If so, please identify all parties and describe their roles and responsibilities.

Signatures: _____ Employee ID:
, MDRP

Signatures: _____ Employee ID:
, Departmental Budget Director

By signing this form, the Merchant Department Responsible Person acknowledges that he/she understands his/her role as outlined in the "Middlebury (PCI) Policy for Accepting Credit Card and ecommerce Payments" and accepts the responsibility of that role.

By signing this form, the Budget Director approves of the business case presented for the department to become a Merchant Department, the Banner information provided and the designated Merchant Department Responsible Person.

Appendix C: Project Plan (PCI Related)

SUBMIT TO: Applicable ITS Workgroup and the PCI Compliance Team @ PCIComplianceTeam@middlebury.edu

Name of the Project:	
Functional Area:	
Submitted by:	
Date Submitted:	
Proposed Start Date:	
Proposed Completion Date:	
Priority	Critical High Medium Low
VP of the Functional area: Are they aware of this project?	
Sponsor: (Functional Area Representative)	
Functional Lead: (if different from sponsor)	
Technical Lead:	
Project Manager: (may be one of the above)	
Stakeholders involved:	
Service Provider Technical Contact:	

Project Objective:

In just a sentence or two, what is the outcome we are trying to achieve – think outcome.

Project Scope:

Describe in detail the requirements of this project:

- *Middlebury Owned Merchant Account or Service Provider Merchant Account?*
- *If Middlebury Merchant Account- what Payment Processing Gateways does the Service Provider integrate with?*
- *Will your project require Banner modification or enhancement?*
- *Will your project require a Web development?*
- *If this is a Point-of-Sales system, please provide PA DSS Validation from PCI SSC.*
- *Provide firewall configuration document showing the requested firewall, ports, IP Configurations, server requirements (will Information Technology Services manage the server?).*
- *Will you need a network jack installed for the payment processing equipment?*
- *Who is responsible for the System Administration; management, administration, patching, operations (incl. antivirus) of the system?*
- *Include reporting requirements.*
- *Have the stakeholders involved been consulted?*

Project timeline and key milestone (please note the latest acceptable completion date):

Project Justification:

- *Why are we doing this project?*
- *How hard will it be to support this on an on-going basis?*

- *Does it require deep technical knowledge?*
- *Will the solution grow with our needs?*
- *Does it help promote administrative efficiency?*
- *Will it remove complex paper-based processes?*
- *Does it keep us in compliance with the law or with campus policy?*

Costs (List all hardware, software, network, staff, facilities, and other costs):

SIGN OFF

Project Sponsor: _____ *Date:* _____
This project specification is complete and accurate to the best of my understanding, and I authorize appropriate staff to begin development based upon this specification.

Project Team

Project Manager: _____ *Date:* _____

Functional Lead(s): _____ *Date:* _____

Technical Lead(s): _____ *Date:* _____