New York University
University Policies

Title:	Payment Card Industry (PCI) Data Security Standard Policy
Effective Date:	May 1, 2016
Date Last Revision:	April 29, 2016
Issuing Authority:	Executive Vice President for Finance and Information Technology
Responsible Officer:	Executive Vice President for Finance and Information Technology
Office Name:	Office of the Bursar

Policy

The University is committed to safeguarding personal and account information conveyed in processing debit and credit card payments. Also, the privilege of accepting payment cards from the leading card brands depends upon compliance with specified security standards. To comply with these standards, it is the policy of the University that security standards relating to payment card transactions be specified and applied.

Any questions on the Payment Card Industry (PCI) Data Security Standard Policy should be directed to the PCI team at pci.compliance@nyu.edu.

Purpose of this Policy

The purpose of this policy is to establish a framework for processing payment cards, to safeguard against the exposure and possible theft of cardholder data transacted through NYU, and to comply with the current Payment Card Industry Data Security Standard (PCI DSS) requirements. This policy does not address New York State laws or the laws of other states or jurisdictions that may apply to payment card transactions.

Scope of this Policy

This policy applies to the NYU schools and units that have access to cardholder data and to the people, processes and technology that handle cardholder data at or on behalf of NYU: any NYU school, unit, employee (full-time, part-time and temporary), student, volunteer, contractor, consultant, vendor, or other person or entity that processes, transmits, or stores cardholder data in a physical or electronic format for NYU or using NYU resources or that has access to the NYU cardholder data environment. All technical and operational system components, including software, computers and wired or wireless electronic devices, involved in processing cardholder data, whether owned or leased by NYU, are subject to PCI DSS and this policy.

Background

The Payment Card Industry Security Standards Council, which was founded by American Express, Discover, JCB International, MasterCard and Visa, has established stringent security requirements to safeguard credit or debit payment cardholder data called the Payment Card Industry Data Security Standard (PCI DSS). PCI DSS applies pursuant to contract to all entities that store, process or transmit cardholder data, including information printed on a card or stored on its magnetic stripe or chip and personal identification numbers entered by the cardholder. Compliance is enforced by the Council's founding members. In addition to PCI DSS, each payment card brand has defined its own specific requirements for compliance, validation and enforcement.

The University is required by contract to safeguard cardholder data, whether printed, stored or transmitted. Therefore, every NYU school/unit that accepts payment cards must be PCI DSS compliant. In addition, any affiliated or unaffiliated party involved with accepting or processing credit/debit card payments for goods or services on the University's behalf must be PCI DSS compliant and provide validation of its compliance to NYU. NYU is obligated to identify such parties' responsibilities for securing cardholder data and monitor such parties' PCI DSS compliance.

This policy defines the framework to allow NYU to ensure that all cardholder data it receives is processed in compliance with the current PCI DSS and related security standards. All NYU schools/units accepting payment cards must comply with the security requirements involved with being a payment card merchant.

All NYU schools/units that process payment card transactions also must comply with NYU's defined methodologies and acceptable technology. Complete cardholder data may not be transmitted, processed, or stored on any University-owned or University-controlled devices.

The Office of the Bursar oversees NYU's method for accepting and processing payment card transactions as well as distribution of policies, procedures, and other guidance required under PCI DSS and ongoing maintenance of a the PCI DSS compliance program. All schools/units wishing to process payment card transactions are advised to visit the ePayment website at http://www.nyu.edu/epayments for instructions to complete the Merchant Onboarding Form which is required to be submitted for approval.

The University Bursar will review a school/unit's completed Merchant Onboarding Form and, upon approval, will establish a specialized Merchant Account Number/ID for the school/unit. The school/unit then becomes responsible for achieving and maintaining compliance with PCI DSS and this policy.

The Policy Specifications set out below are mandated to help meet PCI DSS. A glossary of certain terms used in this policy is provided in Appendix A.

Any questions on the NYU PCI Policy should be directed to the PCI Team at pci.compliance@nyu.edu

Policy Specifications

I. General Requirements – Schools/Units Accepting Payment Cards

A. A school/unit desiring to accept payment cards must obtain advance approval from the University Bursar, who will issue a specialized Merchant Account Number/ID.

B. Using the procedural templates available at the ePayment web site (http://www.nyu.edu/epayments), a school/unit must prepare and maintain documented security procedures that clearly define information security responsibilities for all individuals within the school/unit who handle or will have access to cardholder data. These individuals are required to complete Security Awareness Education training annually (see Section II: General Requirements – Individuals with Access to Cardholder Data).

C. All schools/units approved to accept payment cards are responsible for reviewing and maintaining their respective **Dept PCI Management File** on the Google Drive. This file contains the following information:

1. Merchant Procedures - eCommerce
2. Merchant Procedures – POS (Point of Sale)
3. Security Awareness Education List
4. Device Inventory
5. Device Sign-out Log
6. NYU PCI Policy
7. Related Policies

Contact the PCI Team at pci.compliance@nyu.edu if access is needed to this folder.

D. Cardholder data is considered "Restricted" data under NYU's *Data and Computer Security Policy* (http://www.nyu.edu/its/policies) and the *Data Classification at NYU* table (http://www.nyu.edu/its/policies/data-classification.html) with high institutional risk from disclosure.

E. University Bursar approval is required before implementing software and installing equipment that processes, transmits, or stores cardholder data.

F. When processing payment card transactions, a school/unit must use only vendors and technologies that have been reviewed by the PCI Team. See **Appendix B** for list of compliant technologies and current PCI vendors.

G. Schools/unit with a Merchant Account Number/ID must maintain and secure an inventory of payment card processing devices and implement a system to track removal or substitution of these devices. All devices and serial #s for devices must be recorded on "Device Inventory" tab of **Dept PCI Management** file on Google Drive.

H. Appropriate facility entry controls must be used to limit and monitor physical access to systems in the cardholder data environment.

1. Appropriately identify restricted areas with visible signage (e.g., Authorized Personnel Only).
2. All keys allowing access to restricted areas must be unique to the site.

I. A school/unit processing payment card transactions must annually complete a Self-Assessment Questionnaire (SAQ). The SAQ is a PCI-mandated attestation intended to allow each school/unit to demonstrate their compliance with the PCI DSS.

II. General Requirements – Individuals with Access to Cardholder Data

A. Access to system components and cardholder data must be limited to only those individuals whose job requires such access. Schools/units must ensure that:

1. Individuals are given access to as little cardholder data as necessary to perform his/her job.
2. Individuals are instructed not to share cardholder information with others unless deemed necessary by a supervisor.
3. All individuals who are involved with the acceptance of payment cards must be trained on this policy and the applicable school/unit's procedures relevant to payment card processing.

B. Individuals, including full or part time employees, temporary employees, contractors or consultants, who may be exposed to cardholder data, webmasters developing eCommerce sites, and merchant managers responsible for merchant ID and location, must complete NYU Security Awareness Education (SAE) training annually.

C. To comply with NYU SAE training, all schools/units must:

1. Create and maintain a list of individual whose jobs expose them to cardholder data.
2. Send requests to the PCI Team at pci.compliance@nyu.edu to onboard personnel who need to take SAE training; or to remove personnel who no longer require SAE training
3. Ensure personnel comply with NYU's SAE training upon hire or engagement and at least annually hereafter.

D. This policy must be disseminated to all relevant persons and entities who must acknowledge at least annually that they have read this policy and the applicable school/unit's procedures.

E. Individuals who do not complete SAE training within the established timeline may compromise a school/unit's ability to process credit card payments.

III. <u>STORAGE of Sensitive Authentication Data and Cardholder Data</u>

A. Payment systems that involve receiving sensitive authentication data must have processes in place to delete such data after authentication and verify that it is unrecoverable.

B. All systems that store sensitive authentication data after authorization must adhere to the following requirements:

1. The complete payment card number is not to be stored under any circumstances.
2. The card-validation code or value (three-digit or four-digit number printed on the front or back of a payment card) used to verify card-not-present transactions, and the personal identification number (PIN), or the encrypted PIN block is not to be stored under any circumstances.

C. The Primary Account Number (PAN) must be masked when displayed (the first six and last four digits are the maximum number of digits permitted to be displayed). This must be done through the following means:

1. Truncation by the POS system.
2. If using a paper imprinter slip for card-present transactions and retention of the slip is necessary, the imprint slip should be photocopied after all digits of the PAN except the last four are masked. **Merchant then can retain the photocopied version, but must cross shred the original copy**.
3. If paper forms are used for card-not-present transactions (e.g., telephone and mail order) and retention of a section of the form is necessary, then the cardholder data section of the payment form must be removed and cross shredded. The form can be photocopied and retained after all digits of the PAN except the last four are masked. Merchants must cross shred the original copy.

D. All paper and electronic media that contain cardholder data must be physically secured. Cardholder data that must be stored for business or legal reasons must be stored according to the *NYU Policy on Retention and Destruction of Records* (http://www.nyu.edu/about/policies-guidelines-compliance/policies-and-guidelines/retention-and-destruction-of-records.html) and the

Retention Periods for General Categories of Retainable Records
(http://www.nyu.edu/content/dam/nyu/compliance/documents/Retention_Schedule.pdf).

Cardholder data storage should be kept to a minimum and retention time should be limited to that which is required for a business, legal, and/or regulatory purpose.

E. All cardholder data must be kept in a locked filing cabinet in a secure area or a safe that is accessible only by employees whose jobs require that they have access to cardholder data. The filing cabinet or safe containing the cardholder data must be locked both during and after business hours.

IV. Protection of Devices Against Tampering

A. Any schools/units with access to credit card processing equipment including point-of-sale swipe devices or terminals must record device and serial # on the "Device Inventory" tab of department's **Dept PCI Management** file maintained on the Google Drive**.** Contact the PCI team at pcicompliance@nyu.edu if access is needed to this folder.

B. Schools/units must take protective action against tampering to prevent against the unauthorized capture and use of payment data for fraudulent purposes.

C. Protective action against tampering includes:

1. Periodic inspection of devices – See Appendix C for a "Device Inspection Checklist"
2. Ensuring only authorized staff have access to credit card processing devices.

D. Any devices that are signed out by staff for an event must comply with the following procedures:

1. Record employee and device being signed out in department's device log.
2. Have employee complete device sign-out sheet and provide employee with copy of NYU PCI Compliance Policy.
3. Upon return of device, Merchant Manager should inspect device per the "Device Inspection Checklist" provided in Appendix C.

E. The identity of any third party persons claiming to be repair or maintenance personnel must be verified prior to granting them access to modify or troubleshoot devices. Do not install, replace or return devices without verification.

F. Be aware of suspicious behavior around devices (for example, attempts by persons to unplug or open devices).

G. Report suspicious behavior and indications of device tampering or substitution to the PCI team at pci.compliance@nyu.edu.

H. The NYU PCI Compliance Team reserves the right to conduct periodic announced and unannounced device inspections as part of the University's compliance requirements.

V. TRANSMISSION of Sensitive Authentication Data and Cardholder Data

A. Transactions processed using a standalone dial-out POS terminal must be settled daily.

B. Unencrypted PANs must never be sent by end-user messaging technologies (e.g., e-mail or instant messaging).

C. Each school/unit must maintain strict control over the internal or external distribution of any kind of media that contain cardholder data. All material moved from a designated secure area must be marked confidential, documented on a media removal tracking log, and transported by a document service such as Fed Ex or the U.S. Post Office with a tracking number.

D. No material containing cardholder data may leave the premises of the school/unit that accepted it for processing.

VI. DESTRUCTION of Sensitive Authentication Data and Cardholder Data

A. All physical cardholder data (e.g., paper documents) that is deemed not essential must be properly destroyed. All electronic storage data also must be properly destroyed if there is no business or legal reason for which it should be kept. Proper means of destroying hard-copy material include physical destruction, such as shredding, incineration, or pulping hard copy materials, so that cardholder data cannot be reconstructed. Electronic cardholder data must be rendered unrecoverable via a secure wipe program in accordance with industry-accepted standards for secure deletion.

B. If storage of cardholder data is necessary for business or legal purposes, portable media used to store cardholder data, including hard-copy material, must be stored in a locked cabinet. All electronic cardholder data must be encrypted and password protected.

VII. Disposition of Devices

A. Disposal of credit card processing devices must comply with the following procedures:

1. Contact the PCI Team at pci.compliance@nyu.edu to inform team of need to dispose of device.
2. A PCI Team member will arrange for pick-up of device in order to comply with proper disposal procedures.
3. Once PCI Team member picks up device, update the department's device inventory list.
4. Devices should not be placed in the trash or disposed of without notification to the PCI Team.

B. Any credit card processing devices that are inactive or not utilized for more than two years may be requested by the NYU PCI Team for return and disposal.

VIII. Processing Using External Service Providers

A. When cardholder data is shared with external service providers, procedures to manage these providers must be developed and maintained by the applicable school/unit utilizing their services. These procedures must include:

1. Creating and maintaining a complete list of service providers who can access any POS system or any cardholder data, including companies or individuals who are not employees of NYU.
2. Coordinating with the University's Office of Purchasing Services & Contract Administration to obtain and maintain a written agreement with the service provider that includes the service provider's acknowledgement that it is responsible for the security of

cardholder data that it stores, processes, or transmits.

3. Obtaining and monitoring each service provider's PCI DSS compliance status by requesting a copy of its annual Self-Assessment Questionnaire (SAQ) or Report on Compliance (RoC)/ Attestation of Compliance (AoC).

B. The process for engaging service providers must include proper due diligence prior to engagement. Merchants should liaise with the University's Office of Purchasing Services & Contract Administration to contract work only with PCI DSS compliant service providers and check the references of such providers. Contracts with external service providers must incorporate NYU's third party service requirements language.

IX. Incident Management

A. Anyone who learns of an actual or potential cardholder data security breach must immediately inform the school/unit Merchant Manager, the NYU PCI Team at pci.compliance@nyu.edu and IT Security at security@nyu.edu.

B. NYU will respond to and investigate any incident in which there is a risk that cardholder data has been accessed without authorization. Indications that such an investigation may be necessary include, but are not limited to, the following:

1. A computer or device involved in credit card processing is compromised. You may observe a virus or other malware installed on the system or that unauthorized configuration changes have been made that cannot be adequately explained.
2. Vulnerability is discovered that could be used to gain unauthorized access to cardholder data.
3. An external report is received that indicates that NYU may be a source of fraudulent transactions, or that cardholder data from NYU has been accessed without authorization.
4. Paper, tapes, usb-keys, laptops, or other media containing cardholder data have been lost or cannot be accounted for.
5. Cardholder data has been discussed in public or overheard without authorization.
6. Any of the above occurs with a service provider or other third party involved in payment card processing for NYU.

C. If a cardholder data security breach involving electronic resources is suspected, the *NYU IT Security Information Breach Notification Procedure* (http://www.nyu.edu/its/policies), as well as the procedure of the affected credit card company/companies, must be followed. You must notify the relevant school/unit Merchant Manager immediately to report the suspected breach. The school/unit Merchant Manager is required to report the suspected breach to IT Technology Security Services (security@nyu.edu) and the PCI Team at pci.compliance@nyu.edu

D. In the event a cardholder data breach involving non-electronic resources (for example, paper documents) is suspected, you must notify the relevant school/unit Merchant Manager immediately to report the suspected breach. The school/unit Merchant Manager is required to notify the University Bursar.

E. If you suspect credit card fraud, please follow the procedures outlined in the NYU *Identity Theft Prevention Program* (http://www.nyu.edu/about/policies-guidelines-compliance/policies-and-guidelines/identity-theft-prevention-program.html).

X. Enforcement of On-Going Compliance

A. Periodic reviews of safeguarding and storing of payment card information are conducted by the University Bursar, and payment card handling procedures are subject to audit by NYU Internal Audit, the Office of Compliance and Risk Management, and external auditors. In addition, NYU IT Technology Security Services periodically conducts assessments of security controls put in place to safeguard technology implementations, including but not limited to periodic network-based vulnerability scans.

B. NYU schools/units with Merchant Account Numbers that do not comply with this policy and approved protection, storage, and processing procedures may lose the privilege to serve as a payment card merchant and to accept payment card payments.

C. Individuals in violation of this policy are subject to the full range of sanctions.

X. Related Policies and Legal Considerations

The following University policies address topics that are related to this policy:

- *Policy on Responsible Use of NYU Computers and Data* (http://www.nyu.edu/its/policies/responsibleuse.html)
- *University Data Management Policy* (http://www.nyu.edu/its/policies)
- *Data and Computer Security Policy* (http://www.nyu.edu/its/policies)
- *Reference for Data and System Classification* (http://www.nyu.edu/its/policies)
- *Data and System Security Measures* (http://www.nyu.edu/its/policies)

Many states and countries have laws that apply to payment card transactions with which schools/units accepting payment cards for goods or services must comply. Current applicable New York State law is summarized in Appendix E. For further information regarding applicable law, schools/units accepting payment cards should contact the Office of General Counsel.

XI. Appendices

- Appendix A: PCI DSS Definitions
- Appendix B: NYU PCI Vendors & Payment Card Processing Technologies
- Appendix C: Device Inspection Checklist
- Appendix D: NYU PCI Team: Roles and Responsibilities
- Appendix E: Other Applicable Law

Appendix A: PCI DSS Definitions

1. **Cardholder Data:** At a minimum, cardholder data consists of the full PAN. Cardholder data also may appear in the form of the full PAN plus any of the following: cardholder name, expiration date and/or service code. See the definition of "Sensitive Authentication Data" for additional data elements that constitute account data and may be transmitted or processed (but not stored) as part of a payment transaction. As generally used in this policy, cardholder data refers to all of the information specified above.

2. **Cardholder Data Environment:** The people, processes and technology that store, process or transmit cardholder data or sensitive authentication data, including any connected system components.

3. **Payment Card:** Any payment card, including debit cards, which is issued by one of the leading payment card brands or associations.

4. **Merchant:** Any person or entity (such as a school/unit) that accepts payment cards bearing the logos of any of the five founding members of PCI SSC (American Express, Discover, JCB, MasterCard or Visa) as payment for goods and/or services.

6. **Payment Application Data Security Standard (PA DSS):** Requirements and security assessment procedures that apply to software vendors and others who develop payment applications that store, process, or transmit cardholder data as part of authorization or settlement where these payment applications are sold, distributed, or licensed to third parties. This standard includes what a payment application must support to facilitate an entity's PCI DSS compliance.

7. **Payment Card Industry Data Security Standard (PCI DSS):** A comprehensive set of requirements established by the PCI SSC for enhancing payment account data security. It is a multifaceted standard that includes requirements for security management, policies, procedures, network architecture, software design, and other critical safeguard measures.

8. **PCI Security Standards Council (PCI SSC):** The organization founded by American Express, Discover, MasterCard, JCB and Visa that defines credentials and qualifications for assessors and vendors, as well as maintaining the PCI DSS.

9. **Point of Sale (POS):** Hardware and/or software used to process payment card transactions at merchant locations.

10. **Primary Account Number (PAN):** The composite number code of 14 or 16 digits embossed on a bank or payment card and encoded in the card's magnetic strip. The PAN identifies the issuer of the card and the account including part of the account number, and contains a check digit that verifies the authenticity of the embossed account number.

11. **Report on Compliance (ROC):** Report containing details documenting an entity's compliance status with the PCI DSS.

12. **Self-Assessment Questionnaire (SAQ):** Tool used by any entity to validate its own compliance with the PCI DSS.

13. **Sensitive Authentication Data:** Security-related information including, but not limited to, card validation codes/values (e.g., three-digit or four-digit value printed on the front or back of a payment card, such as CVV2 and CVC2 data), full magnetic-stripe data, PINs, and PIN blocks) used to authenticate cardholders and/or authorize payment card transactions. Sensitive authentication data must not be stored after authorization.

Appendix B: NYU Approved Payment Card Processing Technologies & Current Vendors

I. Payment Gateway /Middleware

The NYU Payment Gateway/Middleware is the preferred service for accepting online electronic payments at NYU.

The NYU Payment Gateway/Middleware is NYU's Electronic Payment processing system that leverages Cybersource PSP, which is NYU's preferred eCommerce solution. It is a transaction-based system that accepts ePayment transactions for both one-time and recurring payments. This service may be implemented to receive payment for items such as online gift donations, conference registration, and specific fees related to a university event, or other products and services.

Specific instructions to establish this service for your school/unit are available at www.nyu.edu/epayments.

Note: The Payment Gateway/Middleware service provides only electronic payment processing. Additional functionality, such as event enrollment or inventory sales, is not specifically provided by this service.

Alternative technologies for accepting online electronic payments must be approved by the University Bursar.

II. Standalone Point of Sale (POS) terminals

Standalone POS terminals will be used to process card-present, phone order, mail order, and faxed credit card payments. These terminals, which have a built in key pad and magnetic card reader, encrypt cardholder data at the point of swipe or entry and can be configured to communicate via an IP network, a plain old telephone service (POTS) line, or a cellular wireless connection.

The following are approved standalone terminals at NYU:

1. FD410 (cellular POS terminal/device)
2. FD130 (Analog phone line connection POS terminal/device)

Any exceptions to approved standalone terminals must be evaluated and approved by the Bursar's Office based on need, solution and processing standards of the University.

III. List of Current Vendors

Below is a list of current NYU vendors who may possess, process, store, transmit cardholder data, or have the ability to impact the security of cardholder data.

Merchants looking to contract with a vendor that is ***not*** listed below must contact the PCI Team at pci.compliance@nyu.edu to request a PCI vendor review ***prior*** to contract or purchase order issuance.

1. Cybersource
2. Touchnet
3. Verifone
4. Merkle
5. iModules
6. Ruffalo Noel Levitz
7. Apply Yourself/Hobsons
8. Symplicity
9. Tessitura
10. Element Payment
11. JSA Tech
12. Technolutions
13. Sequoia
14. Cvent
15. 2U
16. Paypal
17. Dupli

Appendix C: Device Inspection Checklist

When first receiving a credit card processing device, record the device model, date of receipt, serial #, and device location on your department's **Device Inventory** log which can be found within your **Dept PCI Management** file on the Google Drive. Contact pci.compliance@nyu.edu if you need access or have questions on maintaining this file.

Once device is connected and active, conduct periodic device inspections. At the minimum, inspections should occur monthly, or for devices that are signed out by a staff for an event, device inspection should be performed upon return of the device.

When inspecting a device, check for the following:

1. Check the serial # on sticker and ensure it matches the serial # recorded in your device inventory log. If your device has a method of displaying the serial number for the device, check that the serial # on the back of device matches the serial # electronically displayed for the device.

2. Run your finger along the serial # label to confirm there is nothing under it or that it is hiding a compromise.

3. Terminals often have security stickers placed over screw holes to indicate potential tampering of a device. Check the stickers and labels to confirm nothing may have been tampered with.

4. Inspect the device for any additions you may not recognize, looking for small skimming devices or key loggers could be attached to a device.

5. Inspect the wires and connections to the device for anything unfamiliar.

6. Check for any unfamiliar devices around the work area. Smartphones should not be utilized near any credit card devices to prevent from potential capturing of credit card data.

7. Inspect the surrounding area for the device, looking for possible cameras that may have been added (these can often be very small and easy to hide).

The NYU PCI Team reserves the right to conduct periodic, announced and unannounced inspection of devices as part of the University's compliance requirements.

Any devices inactive for over two years may be requested by the NYU PCI Team for return and disposal.

Appendix D: Roles and Responsibilities

The following tables contain recommended roles and responsibilities for compliance activities within NYU PCI Compliance Program. The tasks, which have been broken down by their frequency, are standard activities that would be required of any merchant who processes payment cards.

Quarterly Tasks

Process	Task	Responsible Office		
		Bursar	FSM	Treasury
Vendor Management	Review vendor Attestations of Compliance (AoC) and ensure current AoCs on file	X		
Reporting, Documentation & Merchant Support	Compile quarterly PCI Scorecard	X		

Semi-Annual Tasks

Process	Task	Responsible Office		
		Bursar	FSM	Treasury
Equipment Inspection	Run Bank of America front-end Device Support	X	X	X
	Conduct on-site physical device inspections for selected merchants	X	X	X

Annual Tasks

Process	Task	Responsible Office		
		Bursar	FSM	Treasury
Merchant ID Reconciliation	Run extracts for merchant ID reconciliation	X		
	Conduct merchant ID reconciliation b/w bank, middleware & Trustwave	X		
Merchant ID Deactivation	Run revenue reports to identify merchant IDs with no revenue in last 2 fiscal years	X		
	Correspond with merchants to confirm deactivation of merchant IDs	X		
	Provide IT with list of merchant IDs to deactivate	X		
Webform Deactivation	Run webform revenue reports to identify webforms with no activity in 3 years	X		
	Correspond with merchants to confirm deactivation of inactive webforms	X		
	Provide IT with list of webforms to deactivate	X		

Annual Tasks (cont.)

Process	Task	Responsible Office		
		Bursar	FSM	Treasury
Self-Assessment Questionnaire (SAQ)	Compile annual corporate SAQ submission for PCI Manager sign-off	X		

Ongoing Tasks

Process	Task	Responsible Office		
		Bursar	FSM	Treasury
Equipment Requests	Coordinate with IT to ensure computers used to initiate credit card transactions are regularly updated for anti-virus and malware definitions		X	
Self-Assessment Questionnaire (SAQ)	Monitor and ensure merchants submit SAQs	X		
	Assist merchants as needed to complete SAQ	X		
Security Awareness Education (SAE)	Correspond with merchants to maintain current SAE enrollments	X		
	Enroll/de-enroll in Trustwave as needed	X		
	Send periodic email reminders on SAE completion	X		
	Distribute reports (quarterly, at minimum) to Merchant Managers on SAE completion status	X		
Reporting, Documentation & Merchant Support	Maintain Master Merchant Detail File and documentation	X		
	Respond to ServiceLink PCI inquiries	X		

As Needed Tasks

Process	Task	Responsible Office		
		Bursar	FSM	Treasury
Merchant Onboarding	Register merchant for SAQ	X		
	Register merchant for SAE	X		
	Set-up merchant in middleware		X	
Equipment Requests	Support PCI Manager to review requests for equipment *not* on NYU approved device list		X	
	Support PCI Manager in migrating merchants to more secure devices (ie. EMV pin-chip)		X	
	Address questions related to middleware		X	
Vendor Management	Support PCI Manager in evaluating PCI compliance implications for new vendor requests		X	
Reporting, Documentation & Merchant Support	Compile Merchant Card Processing Snapshots (summary reports)		X	
	Participate as needed in PCI-Related meetings	X	X	X

Appendix E: Other Applicable Law

New York State Law

Schools/units accepting payment cards for goods and services in New York must apply with New York state law. In summary, current New York State law mandates that:

A. A merchant in a sales transaction is prohibited from imposing a surcharge on a purchaser who elects to use a credit card in lieu of payment by cash, check, or similar means.
B. A merchant who accepts credit cards and who imposes minimum purchase amounts for use of a credit card or excludes card payments for discounted items must conspicuously post such limitations or conditions and include them in all advertisements that otherwise mention that credit cards are accepted.
C. A merchant must use paper forms for payment card transactions which do not produce carbon copies or render a separate piece of paper that readily identifies the cardholder by name or number, except as necessary to allow the merchant to complete the transaction. A merchant is prohibited (i) from writing or requiring a cardholder to write any personal identification information (such as an address or phone number) on such form or any attachment to it that is not required to complete the sales transaction (such as a shipping address) and (ii) from printing the expiration date of the card or more than the last five digits of the card number on any receipt provide to the cardholder.

See the following sections of New York General Business Law for further information.

- New York General Business Law §518. Credit card surcharge prohibited.
- New York General Business Law §519. Disclosure by commercial establishments honoring credit.
- New York General Business Law §520-a. Certain credit and debit card transaction forms required.

Schools/units accepting payment cards in or from other jurisdictions should contact the Office of General Counsel regarding applicable law.