PAYMENT CARD INDUSTRY DATA SECURITY STANDARD (PCI-DSS)

GUIDELINES FOR COLLEGES AND RELATED ENTITIES OF CUNY

OFFICE OF BUDGET AND FINANCE

May 2019

OBJECTIVE

The City University of New York (CUNY) is committed to safeguarding personal and account information transmitted or stored during the processing of payment card payments.

SCOPE

Unless otherwise specified, these guidelines apply to Colleges and Related Entities, as defined below. These guidelines do not apply to college foundations or separately-incorporated alumni associations, unless these entities are using a College network to process payment cards. However, those entities are strongly encouraged to implement best practices of similar scope to protect personal and account information transmitted or stored during the processing of payment cards.

DEFINITIONS

"College" means a constituent unit of the University, including without limitation senior and community colleges, graduate and professional schools, Macaulay Honors College and the Central Office, as well as fund groups and organizations that are not legally separate from the University (e.g., the Queens College Athletic and Recreational Fund, the college associations of Hunter College, the School of Professional Studies and the Graduate School of Public Health and Health Policy). "CUNY" and "University" mean The City University of New York.

"Payment card" means a debit or credit card.

"Related Entities" means the following types of entities and their subsidiaries, if legally separate from the University: auxiliary enterprise corporations, college associations, student services corporations, childcare centers, performing arts centers, and art galleries that accept payment cards using technology owned, operated or made available by a College and/or University, such as servers, networks, hardware and software, and/or using the name or a trademark of CUNY or a constituent unit of CUNY, in connection with its operations.

For list of PCI-DSS related definitions, see Appendix A.

OVERVIEW

As payment card use has become more widespread both online and offline, and as concern about payment card security has grown, the Payment Card Industry (PCI) established standards to help ensure that organizations follow best practices for protecting their customers' payment card information.

In 2006, the major credit card companies (American Express, Discover Financial Services, JCB, Visa International, and MasterCard Worldwide) formed the PCI Security Standard Council and established the PCI Data Security Standard (PCI-DSS), a set of operating and technical compliance requirements. Merchants, such as CUNY and its related entities must follow these requirements regardless of the size of the institution and/or the number of payment card transactions handled. The compliance with the requirements, if done properly, will help protect consumer data.

While PCI-DSS compliance is not mandated by law, non-adherence to PCI-DSS can subject the University to significant financial and reputational risks. Failure to comply can result in: a) fines and penalties imposed by payment card institutions and banks; b) monetary costs associated with legal proceedings, settlements and judgements; and c) suspension of the merchant account and the inability to accept payment cards for payment.

At a high level, PCI-DSS comprises 6 Categories and 12 Requirements[1] (See below):

I	Build and Maintain a Secure Network and Systems	1.	Install and maintain a firewall configuration to protect cardholder data
		2.	Do not use vendor-supplied defaults to system passwords and other security parameters
II	Protect Cardholder Data	3.	Protect stored cardholder data
		4.	Encrypt transmission of cardholder data across open, public networks
III	Maintain a Vulnerability Management Program	5.	Protect all systems against malware and regularly update anti-virus software or programs
		6.	Develop and maintin secure systems and applications
IV	Implement Strong Access Control Measures	7.	Restrict access to cardholder data by business need to know
		8.	Identify and authenticate access to system components
		9.	Restrict physical access to cardholder data
V	Regularly Monitor and Test	10.	Track and monitor all access to network resources and cardholder data
		11.	Regularly test security systems and processes
VI	Maintain an Information Secruity Policy	12.	Maintain a policy that addresses information security for all personnel

The merchant environment and complexity of compliance depends on the merchant level (see Appendix B) and corresponding merchant level requirements (see Appendix C) by the major payment card companies. In most cases, a Self-Assessment Questionnaire (SAQ) is required.

The SAQ includes a series of yes-or-no questions for each applicable PCI Data Security Standard requirement. If any answer is no, the College may be required to state the future remediation date and associated actions. There are different questionnaires available to meet different merchant environments. The SAQ that best describes how to accept payment cards is located in Appendix D.

Every College and Related Entity shall be PCI-DSS compliant. The Central Office is responsible for ensuring that University-wide vendors and systems are PCI-DSS compliant. Colleges and Related Entities are responsible for ensuring that their local vendors and systems are compliant. Related Entities must provide validation of their compliance to their supported College and/or the University.

PCI-DSS compliance is a continuous process. Colleges and Related Entities will need to assess their compliance, remediate, report and assess again. It represents common sense steps that mirror

[1] There are over 200 sub requirements to the 12 primary requirements. Please refer to the respective PCI-DSS requirements for the specific details, which can be located at https://www.pcisecuritystandards.org/document_library.

information security best practices. There is no official certificate of PCI-DSS compliance, as compliance is not judged by a "moment in time". Ultimately, compliance is judged by whether cardholder data is kept secure by meeting all of the requirements, all of the time.

GUIDELINES

Adequate Oversight

In order to ensure compliance with the various PCI-DSS requirements, it is essential that the right individuals be involved in the process. Having one individual coordinate the efforts of a PCI committee at a College for both the College and its Related Entities is the recommended approach. The designated individual should be someone who reports (at least in this capacity) directly to a member of the College senior cabinet (e.g., VP for Administration) to ensure executive leadership is appropriately engaged. Committee membership shall include members from information technology, the college business office and other pertinent stakeholders. Ideally, a representative from every College unit and Related Entity that oversees the acceptance of payment cards should participate, as well as those who maintain the network and/or systems that are involved in payment card information transmission, processing and storage.

It is important to note that while PCI-DSS requirements heavily involve information technology and security controls, the responsibility for maintaining PCI-DSS compliance is considered a business function. The underlying determining factors for the required controls are dependent on the number of payment card transactions processed and the methods by which payment cards are accepted, stored and processed, both of which are business activities.

Self-Assessment Questionnaires

Each College and Related Entity is required to complete a Self-Assessment Questionnaire (SAQ, see Appendix D) for each merchant account and each method of processing and transmitting payment card payments. In some cases, a College or Related Entity may need to complete several SAQs, which may further increase PCI compliance requirements as the applicable requirements are determined by the types of SAQs an entity is required to complete.

Qualified Security Assessor (QSA)[2]

CUNY recommends that each College and Related Entity engage a certified Qualified Security Assessor (QSA) to assess compliance with PCI-DSS requirements. The QSA should be initially engaged to identify PCI compliance weaknesses the College and/or its Related Entities may have and to recommend corrective actions to achieve compliance. A QSA can also assist Colleges and Related Entities in completing the appropriate Self-Assessments Questionnaires (SAQ), as well as assist in developing a plan to effectively implement required corrective actions. Whether a QSA needs to be reengaged after an initial engagement is dependent on a number of factors, such as a College's ongoing ability to assess compliance, magnitude of deficiencies noted, complexity of the transaction environment, new or changed handling of payment information, etc.

[2] See list of PCI Certified Qualified Security Assessors: https://www.pcisecuritystandards.org/assessors_and_solutions/qualified_security_assessors

Cardholder Data

Cardholder data shall not be stored unless absolutely necessary. Storing cardholder data poses significant risks and increases the number of requirements that must be satisfied in order to be PCI-DSS compliant. Cardholder data captured as part of a transaction where a College or Related Entity is the Merchant shall be purged, deleted or destroyed, in an irretrievable manner, immediately after the transaction is successfully completed, except for the following data: payment cardholder name, transaction authorization number, transaction date, and transaction dollar amount. This data should be retained, in accordance with CUNY's retention schedule, in order to facilitate transaction inquiries, corrections and refunds. Colleges are strongly encouraged to periodically run internal data scans to identify any cardholder data that may be stored on their systems, to review merchant accounts and eliminate those that are not needed, and to only process payment cards when absolutely necessary using secure methods to effectively serve the students and the broader College community.

Credit Card Information provided via Email or Text Message

Colleges and Related Entities shall avoid the receipt of cardholder data via email or text message which are not secure means of transmission. Forms and other documents that collect cardholder data shall not include an email address or cell phone number as a method of submission. Cardholder data may be accepted by fax only if the fax messages are not handled by devices that convert the fax into an email, that store the faxed document in memory, or that are connected to a local data network and not a landline phone jack.

External Vulnerability Scans

Each College that stores, processes or transmits payment cards through a CUNY network must conduct an external vulnerability scan on at least a quarterly basis, as required by PCI-DSS. These scans must be conducted by a PCI-certified Approved Scanning Vendor[3].

Outside Vendor Compliance

Third-party vendors that store, process or transmit cardholder data on behalf of a College or Related Entity can impact the security of the environment, and must also be PCI-DSS compliant. Because the PCI standards change from time to time, Colleges and Related Entities shall verify the PCI compliance of those vendors that are Merchants on an annual basis by requiring the vendor to annually provide an attestation stating it is PCI compliant to the current standard or by confirming the vendor's status in an appropriate database--such as the PCI Vendor Database and the VISA Global Registry--that contains an up-to-date listing of PCI-certified vendors.

Vending Machines and Other Points of Sale

Some third-party vendor Point of Sale (POS) devices on College premises, such as vending machines, cash management stations and parking ticket kiosks that accept payment cards, may be within the College's PCI-DSS compliance scope. This depends on how the payment card transaction is processed and

[3] PCI Certified Approved Scanning Vendors: https://www.pcisecuritystandards.org/assessors_and_solutions/approved_scanning_vendors

transmitted (e.g., via the College's data network, traditional phone line, cellular network, etc.) as well as the Merchant vendor account associated with the transaction.

Prioritizing Your Approach

The prioritized approach developed by PCI-DSS (link included below) provides six security milestones to address the highest PCI risk factors and threats associated with storing, processing, and/or transmitting cardholder data while progressing toward full PCI-DSS compliance. The prioritized approach roadmap focuses efforts on those that can reduce risk and achieve substantial compliance quickly to lower the risk of cardholder data breaches earlier in the compliance process. It is not intended as a substitute, short cut or stop gap approach to PCI-DSS compliance. To achieve PCI-DSS compliance, CUNY Colleges and the Related Entities must meet all PCI-DSS requirements, regardless of the order in which they are satisfied.

HELPFUL RESOURCES

External Links:

PCI Data Security Standards
https://www.pcisecuritystandards.org/

PCI-DSS Document Library
https://www.pcisecuritystandards.org/document_library

PCI-DSS v3.2.1
https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2-1.pdf

PCI-DSS Prioritized Approach
https://www.pcisecuritystandards.org/documents/Prioritized-Approach-for-PCI-DSS-v3_2_1.pdf

PCI-DSS Requirements and Self-Assessment Questionnaires:
https://www.pcisecuritystandards.org/document_library?category=saqs#

PCI Certified Approved Scanning Vendors:
https://www.pcisecuritystandards.org/assessors_and_solutions/approved_scanning_vendors

PCI Certified Qualified Security Assessors:
https://www.pcisecuritystandards.org/assessors_and_solutions/qualified_security_assessors

PCI Compliance 101:
http://www.compliance101.com/

PCI FAQ's:
https://www.pcicomplianceguide.org/pci-faqs-2/

List of third party service providers per Visa that are PCI Compliant:
https://www.visa.com/splisting/searchGrsp.do

PCI-DSS DEFINITIONS **Appendix A**

Payment card(s) mean credit and debit cards bearing the logo of Visa, MasterCard, American Express, Discover and JCB used to make a payment.

Payment Card Industry (PCI) refers to the council made of the major credit card brands including Visa, MasterCard, American Express, Discover and JCB.

Data Security Standards (DSS) established by the card brands and the PCI Security Standards Council for payment card security.

Card verification value (CVV2 or CVV) is a three digit number on the back or four digit number on the front of a payment card. PCI does not permit the CVV2/CVV to be stored on paper, electronically, or by any other means.

Cardholder data (CD) is any personally identifiable information (PII) associated with a person who has a credit or debit card. Cardholder data includes the primary account number (PAN), which consists of customer's 16 digit payment card number along with any of the following data types: cardholder name, expiration date, and card verification value.

Merchant means 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).

Personal Identification Number (PIN) is the personal number used in debit card transactions.

*Smart cards (*also called chip) that store their data on integrated circuits in addition to magnetic stripes.

Sensitive Authentication Data – this is the full magnetic strip data (Track Data) including chip and PIN. The data encoded in the magnetic stripe used for authorization during transactions when the card is presented as well as the chip and PIN data. This data must be purged and never kept subsequent to transaction authorization including the service code, card validation value, code and proprietary reserved value.

Payment Application is approved software sold, distributed, or licensed which stores, processes, or transmits cardholder data as part of authorization or settlement. This includes customized, pre-installed, and "off-the-shelf" software.

Qualified Security Assessor (QSA) is a PCI assessor certified and listed on the PCI Security Standards Council's list of QSAs: pcisecuritystandards.org/approved_companies_providers/qsa_companies.php

Third party vendor (also called "third party service provider") are business entities directly involved in transmitting, processing, or storing of cardholder data or which provides services that control or could impact the security of cardholder data.

Virtual payment terminals are web-browser-based access to a third party service provider website to authorize payment card transactions, when the merchant manually enters payment card data via a securely connected web browser. Unlike physical terminals, virtual payment terminals do not read data directly from a payment

Attestation of Compliance (AOC) - A report to attest to the results of a PCI-DSS assessment and can be requested from a third party vendor.

Report of Compliance (ROC) is prepared by a Qualified Security Assessor to verify a merchant's compliance with the PCI-DSS.

Internet Protocol (IP) Address is a unique number used to represent every computer in a network. The format of an IP address is four sets of numbers separated by dots (e.g. 10.10.10.123)

Level 1 Service Provider is a vendor that provides access to the internet and to applications to facilitate the transfer and/or storage of payment card information. The following link provides a complete list of PCI Compliant Level 1 Service Providers: http://www.visa.com/splisting/searchGrsp.do

PIN Entry Device (PED) is a terminal that allows entry of a customer's PIN.

Approved Scanning Vendor (ASV) refers to a company qualified by the PCI Security Standard Council to conduct external vulnerability scanning services in accordance with PCI-DSS.

Self-Assessment Questionnaires (SAQ) are eight questionnaires listing the PCI Data Security Standards that apply to each method of processing payment cards.

MERCHANT LEVEL: **Appendix B**

Level	Amex	Discover	JCB	MasterCard	Visa
1	Merchants processing over 2.5 million AMEX transactions annually or any merchant that American Express deems a level 1	Merchants are currently not categorized into levels based on transaction volume. Discover takes a risk based approach for validating compliance.	Merchants processing over 1 million JCB transactions annually or compromised merchants	Merchants processing over 6 million MasterCard transactions annually or identified by another payment card brand as level 1, or merchants that have experienced an account data compromise	Merchant processing over 6 million Visa transactions per year. Any merchant that Visa, at its sole discretion, determines should meet the Level 1 merchant requirements to minimize risk to the Visa system
2	Merchants providing 50,000 to 2.5 million AMEX transactions annually or any merchant that American Express otherwise deems level 2	N/A	Merchants processing less than 1 million JCB transactions annually.	Merchants processing 1 million to 6 million MasterCard transactions annually	Any merchant processing 1 million to 6 million Visa transactions per year
3	Merchants processing less than 50,000 AMEX transactions annually	N/A	N/A	Merchants processing 20,000 to 1 million MasterCard e-commerce transactions annually	Any merchant processing 20,000 to 1 million Visa e-commerce transactions per year
4	N/A	N/A	N/A	All other MasterCard Merchants	Any merchant processing fewer than 20,000 Visa e-commerce transactions per year, and all other merchants - regardless of acceptance channel - processing up to 1 million Visa transactions per year

MERCHANT LEVEL REQUIREMENTS: **Appendix C**

Level	Amex	Discover	JCB	MasterCard	Visa
1	Annual onsite review by QSA (PCI DSS Assessment) and Quarterly Network Scan by ASV	Quarterly Network Scan by ASV AND one of the following: Annual onsite review by QSA-PCI DSS assessment Annual Self Assessment Questionaire	Annual onsite review by QSA (PCI DSS Assessment) and Quarterly Network Scan by ASV		
2	Quarterly Network Scan by ASV	Annual Self Assessment Questionaire and Quarterly Network Scan by ASV			
3	Quarterly Network Scan by ASV	Quarterly Network Scan by ASV AND one of the following: Annual onsite review by QSA-PCI DSS Assessment Annual Self Assessment	N/A	Annual Self Assessment Questionaire and Quarterly Network Scan by ASV	
4	Quarterly Network Scan by ASV	N/A	Annual Self Assessment Questionaire and Quarterly Network Scan by ASV		

SELF-ASSESSMENT QUESTIONNAIRE: **Appendix D**

SAQ	Description
A	Card-not-present merchants (e-commerce or mail/telephone-order) that have fully outsourced all cardholder data functions to PCI DSS compliant third-party service providers, with no electronic storage, processing, or transmission of any cardholder data on the merchant's systems or premises. Not applicable to face-to-face channels. Shopping Cart - your customers enter their credit card information into a website to make an online purchases, payments, or donations: a) all e-commerce page including all payments acceptance and processing are delivered directly from a 3rd party PCI-validated service provider or b) during the payment process, the consumer browser is redirected to a checkout/payment page (URL or iFrame) that is entirely controlled by a PCI-compliant 3rd party service provider.
A-EP	E-commerce merchants who outsource all payment processing to PCI DSS validated third parties, and who have a website(s) that doesn't directly receive cardholder data but that can impact the security of the payment transaction. No electronic storage, processing, or transmission of any cardholder data on the merchant's systems or premises. Applicable only to e-commerce channels. Shopping Cart - your customers enter their credit card information into a website to make an online purchases, payments, or donations: a) during payment process, the consumer's browser is redirected to a checkout/payment page (URL or iFrame) that is controlled by PCI-compliant third party service provider, but some elements (javascrip, CSS, etc.) are passed from the merchant page to the 3rd party payment page or b) the checkout/payment page directly posts payment information from the merchant website to a 3rd party service provider, but the page resides in the merchant website.
B	Merchants using only: • Imprint machines with no electronic cardholder data storage; and/or • Standalone, dial-out terminals with no electronic cardholder data storage. Not applicable to e-commerce channels.
B-IP	Merchants using only standalone, PTS-approved payment terminals with an IP connection to the payment processor, with no electronic cardholder data storage. Not applicable to e-commerce channels.
C-VT	Merchants who manually enter a single transaction at a time via a keyboard into an Internet-based virtual terminal solution that is provided and hosted by a PCI DSS validated third-party service provider. No electronic cardholder data storage. Not applicable to e-commerce channels. You use a web browser on a computer or mobile device to access a merchant services site for entering and authorizing credit card purchases. You should have a username and password and be able to access the site from any online computer. You never swipe the card, but instead use a keyboard or keypad to manually type in the credit card information
C	Merchants with payment application systems connected to the Internet, no electronic cardholder data storage. Not applicable to e-commerce channels. You are using Point of Sale (POS) software installed on a computer or other device. Computers with POS software are often combined with devices such as cash registers, bar code readers, printers, optical scanners, and card readers or you have a credit card reader connected to your computer that reads the card information and enters it into the virtual terminal.
P2PE-HW	Merchants using only hardware payment terminals that are included in and managed via a validated, PCI SSC-listed P2PE solution, with no electronic cardholder data storage. Not applicable to e-commerce channels.
D	All merchants not included in descriptions for the above types. Your customers enter their credit card information into a website to make an online purchases, payments, or donations. During the payment process, the consumer enters credit card information on a checkout/payment page that is part of the merchant website.

PCI-DSS Program Checklist **Appendix E**

Each College and the Central Office (for Centralized Collections) should do the following:

1. Identify an executive level program sponsor/owner (PCI-DSS is a business requirement; so a non- IT position is recommended)
2. Establish a PCI committee comprised of:
    a. Executive level leader(s) or representative(s)
    b. Functional office representatives from:
        i. Information technology
        ii. Business office
        iii. Related Entities (Foundations, Auxiliary Services Corporation, Alumni Association, and Performing Arts, etc.)
        iv. Staff from locations that accept payment cards (with a focus on the largest volume first)
3. Committee should:
    a. Attend PCI Training
    b. Identify all areas where payment cards are accepted
    c. Identify all Merchant IDs that exist
    d. Define and document the appropriate PCI Compliant Payment Card procedures
        i. For In-Person, Mail, Phone, Special Events, Other
    e. Identify all individuals authorized to process payments of any kind and method
        i. In Person, Via Mail, Swipe or other card entry transactions, securing/destroying card holder information
    f. Specify Closing/Reconciliation transactions at close of business
        i. Daily payment card reconciliation, daily payment card closing / batching, approve daily reconciliation and secure PIN Transaction Security and Point of Sale device daily (e.g. locked safe)
    g. Communicate activities (risks, etc.) to senior management and stakeholders
    h. Coordinate the completion of the Questionnaire/Assessments for each Merchant ID
    i. Coordinate the vulnerability testing as needed
    j. Review payment card procedures annually
4. Require PCI-specific training for:
    a. Anyone processing payment card transactions
    b. Managers with oversight of payment card processing activities
    c. Document all training activities and attendance
5. Understand the suspected breach or fraud reporting procedures:
    a. Incident response and reporting procedures (see CUNY's data breach reporting procedure at security.cuny.edu).
    b. Suspected fraud shall be report to: University's Director of Public Safety, University's Director of Internal Audit, The Office of General Counsel and University Executive Treasurer.