Medgar Evers College PCI DSS Compliance Procedural Manual

Goldene Lewis
MEDGAR EVERS COLLEGE | REV FEBRURY 2021

TABLE OF CONTENT

Medgar Evers College of the City University of New York Payment Card Industry Data Security Standards (PCI DSS) Procedural Manual applies to the entire campus community.

It directs payment card transaction practices applicable to all departments, mainly, the College Related Entities and their Merchant Services Accounts through the **College the Virtual Terminals (VT) and Point of Sale (POS)** venues (Bursar's and Student Life Services).

The standards outlined in this manual are congruent with those of the University and the Payment Card Industry. The College Administration and Finance, IT, Security, and Compliance teams are committed to performing periodic audits or assessments on computer hardware and software to ensure the campus environment operates to meet PCI DSS standards and best business practices.

Practices are updated synchronously with those of the PCI DSS Council to combat the on-going threats by cybercriminals. Therefore, the entire community must ensure that the College network is secured and audit ready. Non-adherence to PCI-DSS subjects the University and College to significant reputational and financial risks.

College Departments and Related Entities

- Medgar Evers College Bursar Office, Office of Student Life Services, Office of Development
- Medgar Evers College Auxiliary Enterprises Corp
- Medgar Evers College Educational Foundation Inc.
- Medgar Evers College Student Faculty Association Inc.

Medgar Evers College PCI DSS Committee Members

Jacqueline Clark	Senior Vice President, Administration & Finance
Rebecca Fraley-Corrado	Assistant Vice President, Administration & Finance
Xavier Barreto	Chief Information Officer
Kin Lam	Deputy Chief Information Officer
Goldene Lewis	Director, Risk Management & Internal Control
Thais Pilieri	Bursar/Director
Sharon Bartell	Director, Development Office
Amani Reece	Director, Student Services
Lisa Arnold	Executive Assistant to the Senior Vice President Administration & Finance

About Payment Card Industry Data Security Standards (PCI DSS)

The Payment Card Industry Data Security Standard (PCI DSS) is one of the most wide-reaching standards today that drives the need to safeguard customers' data. As higher education institutions reliance on the use of credit cards increases, so does the need for the security of customers' data. Securing customers' data does not suggest we ourselves compromise the information received but by leaving such data to the purview of others can very well comprise such data.

Payment Card Industry (PCI) compliance, therefore, refers to the technical and operational standards that organizations must adhere to; and relate to securing and protecting cardholder data. PCI compliance applies to any organization that accepts, transmits, or stores cardholder data.

The goal of the PCI DSS is to enhance payment data security and facilitate the broad adoption of consistent data security measures globally. Additionally, by providing a baseline of technical and operational requirements to protect payment data and their systems, PCI DSS can ultimately reduce fraud and security threats

Across industries, PCI DSS assigns fines and penalties to those who failed to comply. Particularly, since malicious users have access to free and widely available tools to eavesdrop on wireless communications, therefore, such industries are encouraged the use of strong cryptography can help limit disclosure of sensitive information across wireless networks.

What is a Virtual Terminal?

The Virtual Terminal (VT) is a web-based system of operation that allows customers access to a central, secured location where they can manage all credit card transactions efficiently. Users can only access the VT by way of an individual assigned User Login Identification and Password.

Using a VT allows users:

- To run secured transactions
- Individual set up web site that runs his/her transactions
- To prevent fraud
- Accessibility to view transaction reports

Additionally, the VT allows users the flexibility to process payment transactions via the Internet by turning any Personal Computer (PC) into a Point of Sale (POS) terminal. This conversion of the PC to a POS makes the functionality like that of a cashier's terminal commonly used at retail stores. The user enters data for individual and recurring transactions.

VT usability in generating transaction reports, charts and graphs, helpful for business visualization and presentations are added features the College can maximize to its advantage. Users can view consolidated statements for multiple sub-accounts by setting up a multi-sub

reporting structure. VT offers users the functions they need to set up and customize the integration of a web page.

Processing Sale Transactions

To do a **Sale Transaction**, users must enter all the necessary data as appropriate for each transaction.

All applicable offices should assign at least two staff who are knowledgeable about the process. No one person should be the sole user; therefore, this practice is discouraged. Offices must ensure business continuity if one user is absent.

Bursar's staff have one credit card device that housed all the College Related Entities accounts. Staff can manually select the associated credit card account and complete the transaction.

Simple Navigation of The Process is as follows:

Select Related Entity → Enter order information (product code)→ Select Credit Card as the Payment Method → Enter Credit Card Information → Select Transaction Type (Sale) →Click on the Continue button → Note If there are data entry errors or any required fields are missing, the same page will reappear with an error message at the top, and all incorrect/missing fields flagged with a warning graphic. Make any necessary corrections, then click the Continue button again →Review the data, make corrections if needed by clicking on the Back button, then click the Submit button→A Transaction Result page will appear→ Review the Results.

Generate a Payment URL (Payment Page)

The College IT staff can create a Payment URL link for customers to process their transactions. The code or web-address will give customers access to a webpage where they can securely make the payment with their preferred payment method, at their convenience.

To enable a Payment URL functionality on the merchant account, First Data provides customized direction IT staff can follow to set up a Payment Page.

CUNY PCI DSS Responsibilities

The City University of New York (CUNY) PCI Compliance Office is responsible for monitoring and coordinating University-wide PCI compliance by providing guidance and expertise on PCI compliance standards and requirements. CUNY also would develop strategies to enhance compliance with PCI DSS and improve monitoring of PCI compliance at all CUNY colleges.

These responsibilities include but not limited to--

- Providing monthly updates at various University councils meetings on PCI efforts.
- Conducting routine training throughout the year for all pertinent staff University-wide that gears toward the completion of the PCI Self-Assessment Questionnaire (SAQ)
- Deploying a portal page to manage and provide oversight of SAQs University-wide. Contracts with an Approved Scanning Vendor to conduct vulnerability scanning.
- Launches an eLearning solution for PCI Awareness Training, which aims to ensure 24/7 and year-round training to new and existing hires about PCI-DSS requirements.
- Creates a PCI sub-page on the Office Risk Management and Internal Control web page to house guidance memos and documents, including PCI-DSS FAQs colleges, can use to drive compliances.

College Responsibilities

Medgar Evers College senior administration upholds, articulates, and sets the tone for campus-wide adherence to PCI DSS standards regulations. The administration recognizes the need for safeguarding customers' data and allocates the resources to the Office of Information Technology to ensure the IT infrastructure can support all PCI DSS requirements.

The College responsibilities are and not limited to—

- Facilitate monthly meetings among senior administrator and stakeholders to keep abreast of all new developments
- Identify and remediates policy violations in real-time by designating alert mechanisms differently than other automated alerts.
- Readily addresses PCI DSS violations to maintain continuous compliance.
- Direct a clear separation with proper network segmentation of cardholders' data environment and cardholder data from the rest of the network.

The College would incorporate the ten best practices for complying with PCI DSS network security mandates for the industry:

1. Establish consistent, auditable exception designation and management that ensures violations that have been approved exceptions unto our network do not prompt a failure of the PCI DSS audit.

2. Enforce documentation of reasons for any exceptions, the owner along with a date for expiration and a method for consistently reviewing exceptions prior to expiration.

3. Allocate resources to improve the automation of workflow process to meet PCI DSS requirements. The College would automate change processes and execute them through automation to ensure consistency in steps and completion.

4. Promote a controlled environment conducive to safeguarding cardholders' data within the confines of the required guidelines: Rule of operation to always include regular recertification or expiration.

5. Implement requirements for every network change to be completed with an audit trail with the who, what, when, and why.

    - **Who** does what? Aligning requirements for segregation of duties and documentation of actions are important and can satisfy audit
    - **What** is important for understanding modified policies, especially those connecting to PCI-regulated network zones
    - **When** it is important to understand adherence to a change window, identify emergency changes, or flag unscheduled and undocumented changes as anomalous behavior for investigation
    - **Why** it is critical for ensuring effective reporting for auditors, particularly in consideration of retaining necessary violations as exceptions.

6. Empower the IT staff to evaluate every network change with the given criteria:
    - Risk analysis based on security policy to determine whether access control configurations violate PCI DSS
    - Approval by the business owner to close the change request ticket as complete and close the process
    - Best Practices for PCI DSS v3.2.1 Network Security Compliance © 2019 Tufin 6/11
    - Implementation according to the PCI-compatible network change workflow to ensure consistent adherence to PCI DSS process requirements.

7. Ensure that access controls protecting cardholder data adhere to the following guidelines:
    - Every rule has a comment that includes a date for regular recertification or expiration
    - Every rule has a log
    - No rules with "Any" in the source, destination, and service
    - No rules with risky services (un-encrypted)
    - Delete unused and redundant rules
    - Adopt a process for recertifying aging access rules

8. Enforce proper documentation of every access rule to ensure your audit preparedness with the following information:

    - Business justification
    - Business owner
    - Application name
    - Expiration or recertification date

9. Mandate that firewall and cloud security group logs are kept for at least 12 months for retrieval during your PCI DSS audit and align to data retention best practices.

10. Automate the rule cleanup and recertification processes to ensure all rules comply with PCI DSS standards.

Information Technology Responsibilities

The Information Technology staff provides a secured protocol for transport and proper encryption strength for cardholder data using trusted keys/certificates. Implements connection measures from systems that do not support the required encryption strength.

Ensures sensitive information is encrypted during transmission over public networks to block malicious individuals from intercepting and/or diverting data while in transit.

Monitors the use of strong cryptography that can help limit disclosure of sensitive information across wireless networks to safeguard against malicious users' free and widely available tools to eavesdrop on wireless communications

Facilitates strong cryptography for authentication, and transmission of cardholder data is required to prevent malicious users from gaining access to the wireless network or utilizing wireless networks to access other internal systems or data.

Always follows the masking approach to ensure that only the minimum number of digits is displayed as necessary to perform a specific business function.

Examines documented standards and compare to system configuration settings to verify the following for all wireless networks identified:

- Industry best practices (for example, IEEE 802.11i) are used to implement secure encryption for authentication and transmission.
- Weak encryption (for example, WEP, SSL) is not used as a security control for authentication or communication.

Verifies certificates are trusted (for example, have not expired and are issued from a trusted source) helps ensure the integrity of the secure connection.

Stays abreast of all protocol implementations (such as SSL, SSH v1.0, and early TLS) known vulnerabilities that an attacker can use to gain control of the affected system. Whichever security

protocol is used, ensure it is configured to use only secure versions and configurations to prevent the use of an insecure connection—for example, by using only trusted certificates and supporting only secure encryption (not supporting weaker, insecure protocols or methods).

- Completes all College vulnerability scans for all virtual terminals and POS devices quarterly
- Provides maintenance of Network: Firewall installation and network configuration
- Restrict inbound and outbound traffic to that which is necessary to the Cardholder Data Environment (CDE).
- Implements thorough packet inspection and reviews rule sets every six months.
- Ensures provisions are in place that protects cardholders' data
- Collaborates with the Administration and Finance Office to develop and maintain an Information Security Policy that overall safeguards customers' data.

IT Security Incident Response

The information security incident response and handling sequence of action are as follows:

- Preparation – writing of incident response policies, training, preparation of appropriate tools and anything that may be required to handle an information security incident.
- Identification – when events are analyzed in order to determine whether those events might compromise an information security incident.
- Containment – the attempt to keep further damage from occurring as a result of the incident.
- Eradication – the process of understanding the cause of the incident so that the system can be reliably cleaned and ultimately restored to operational status in the following step.
- Recovery – cautiously restoring the system or systems to operational status.
- Lessons Learned – provide a final report on the incident, which will be delivered to management.

Upon initial determination of a possible security incident, the departmental management shall notify MEC IT Security immediately (infosec@mec.cuny.edu)

- The Information Security Response Team is responsible for the execution of security incident plan that are applicable to the specific incident.
- The incident handler shall ensure that resources are assigned to conduct the investigation
- For an electronic incident, Information Security shall conduct the forensic investigation.
- The ISIRT is responsible to ensure that evidence is preserved, and each incident is adequately documented. "Adequate" documentation will stand on its own, without requiring further explanation.
- Additional information on Incident response procedures are found on https://mec.cuny.edu/it/security/

Risk Management and Internal Control Responsibility

Office of Risk Management and Internal Control helps the College to identify and understand the potential vulnerabilities and risks when PCI DSS standards and requirements are not met. By understanding these risks, the College can prioritize risk mitigation efforts to address all critical risks first then resolve those risks that have a less impact on the operation.

The Office works to ensure adequate coverage and coordination of the standards campus-wide that factors risks across all areas of the organization are considered. Additionally, the Office would research strategies for addressing identified risks, and that the risk mitigation efforts are aligned across all business processes.

These responsibilities include but not limited to—

- Confirm that the College operates in full compliance with the PCI DSS requirements and the industry best practices.
- Ensure the College community is aware that the entire network is subject to PCI DSS regulations because all systems will have access to one another in a flat, unsegmented network,
- Ensure that the College creates a clear separation with proper network segmentation of cardholder data environment and cardholder data from the rest of the network

- Review policies and procedures, and examine system configurations to verify the data is not retained after authorization for all other entities, if sensitive authentication data is received

- Work with the offices like the Bursars, Office of Student Life Services, Adult and Continuing Department, and the Related Entities that have credit card devices to inspect such devices for any signs of security breach once per month

- Work with IT Office to ensure all vulnerability scans are performed quarterly and to maintain College PCI DSS Compliance Attestations are current

- Work with IT Office to ensure staff identifies all wireless networks transmitting cardholder data or connected to the cardholder data environment

- Identify all locations where cardholder data is sent or received over open, public networks.

- Examine documented standards and compare to system configurations to verify the use of security

- Educate users to look for a web page URL begin with "HTTPS" and/or the web browser display a padlock icon somewhere in the window of the browser that validates the site as being secured.

Office of the Bursar Responsibility

The Office of the Bursar Office is the custodian of the Credit Card device for the Auxiliary Enterprise Corp.

The credit card terminal is used to collect payments for the "Auxiliary" account. Most of these transactions are payments for parking. In addition to parking fees, the terminal is occasionally used for merchandise payments for Student Government and/or Space Reservations.

Once a payment is collected a copy of the receipt is given to the cardholder. The cashier to be reconciled at the end of the day keeps the “merchant copy”. The Cash Management Coordinator reconciles the cashiers and collects all receipts and supporting documentation.

Under no circumstances the Bursar or its staff have access to collect or save credit card data. All transactions are reconciled and recorded into the secured Bursar shared drive. The merchant receipts and back-up documentation are stored in the safe room located in the Office of the Bursar. Additional procedures are found on MEC CMP Updated (2). Pdf.

Office of Development Responsibilities

The Office of Development uses the First Data Payeezy Virtual Terminal to process online credit card transactions for MEC Educational Foundation.

Staff completes these transactions under the guidance of the Medgar Evers College PCI DSS Procedural Manual, Medgar Evers College Information Security Policy, and CUNY Recommendations for the Office of Development.

The College provides a payment page, MEC Giving, on its website where customers can make their contributions. These contributions are hosted through a donation plugin that accepts donors’ charitable gifts through customizable donation forms integrated into First Data Payeezy.

Under no circumstances, the Office of Development or staff have access to collect or save credit card data.

Office of Student Life Services Responsibilities

The Office of Student Life Services is responsible for the handling of all Credit Card transactions for the Student-Faculty Association. Currently, the Office has one Credit Card device to be used primarily for all activities. Activities are outlined in the Student Services Procedural Manual and conform to CUNY Cash Management Policies. The Office stores this device in an internal locked safe.

Office of Student Life Services will comply with guidelines established in the Medgar Evers College PCI DSS Procedural Manual and Medgar Evers College Information Security Policy.

Procedures for Credit Crad Sales

- The director and two coordinators will conduct all credit card transactions
- Credit card machines would always be stored in the locked safe when not in use. Only the Director and a Coordinator can access the safe to retrieve the credit card machine.
- All sales should be recorded via Pop up Shop Receipt Book and Stamped: Medgar Evers College, CUNY Office of Student Life and Development Pop Up Shop PAID
- The original copy of the receipt must be given to the customer with a visible record of the description of item(s) purchased and the amount registered for the customer's examination
- All sales should be balanced and signed at the end of the day by two staff, one of the staff members signing off must be a full-time employee of the Office.
- All sales must be logged in the sales log sheet with the description of the deal, quantity, amount, and name of the staff that conducted the transaction.

Safeguarding Credit Card Receipts Collected:

Staff will adhere to protocols in place that restrict unattended receipts at the counter, desk, bill counter machine, or safe.

All credit card receipts must be secured in a locked safe. Only the Director and a Coordinator can open the safe while both parties are present.

College PCI DSS Audit Procedures

PCI DSS Audit procedures allow checks and balances, bells and whistles for all PCI DSS practices. Higher governance, the New York State Office of the State Controller, outlines these practices. Because of the skilled and craftiness of cyber hackers, agencies must be vigilant in protecting customers' data.

Auditors would check for the proof that the College is doing the following:

- Monitoring equipment to ensure no external tampering that may compromise cardholders' data.
- Ensuring the operation is compliant with required PCI DSS.
- Routinely reviewing attestations and certificates to validate web domain security.
- Identifying all locations where cardholder data is transmitted or received over open, public networks.

Work with IT staff to examine documented standards and compare to system configurations to verify the use of security protocols and strong cryptography for all locations.

Reassess operation with IT assistance to ensure sensitive information is encrypted during transmission over public networks; it is natural for a malicious individual to intercept and/or divert data while in transit.

Review transmission of cardholder data to ensure data security is achieved by using trusted keys/certificates, a secure protocol for transport, and proper encryption strength to encrypt cardholder data.

Review documented policies and procedures to verify processes are specified for the following:

- Acceptance of only trusted keys and/or certificates
- The protocol in use to only support secure versions and configurations (that insecure versions or configurations are not supported)
- The implementation of proper encryption strength per the encryption methodology in use
- Verifying that certificates are trusted (for example, have not expired and are issued from a trusted source) helps ensure the integrity of the secure connection.
- Evaluate whether users are aware of the general requirement for the web page URL, to begin with, "HTTPS" and/or the web browser display a padlock icon somewhere in the window of the browser.

Many TLS certificate vendors also provide a highly visible verification seal—sometimes referred to as a "security seal," "secure site seal," or "secure trust seal"— which may provide the ability to click on the seal to reveal information about the website.

Refer to industry standards and best practices for information on strong cryptography and secure protocols (e.g. NIST SP 800-52 and SP 800-57, OWASP, etc.)

Because new vulnerabilities could emerge at any time, the College must remain up-to-date with vulnerability trends and determine whether or not they are susceptible to any known exploits.

In closing, all procedures in this manual are subject to change as the industry changes. To keep abreast of all new developments and required trainings, the College will conduct its research and work directly with CUNY to ensure these are achieved.