Office of Information Technology

IT Standard
CREDIT CARD PROCESSING/E-COMMERCE STANDARD

Standard:	IT20001
Original Effective Date:	01/19/2012
Last Revised:	05/20/2020
Last Reviewed:	04/01/2022
Next Scheduled Review Date:	04/01/2023
Version No.:	5.1
Administrative Owner:	Chief Business Officer /Director of Information Security Services

PURPOSE

Montgomery College ("College") accepts credit cards in payments for products and services provided to its community. As noted in College Policy 61001 Fiscal Control, the Office of Business Services (OBS) is charged with ensuring that "Credit card processing procedures or standards shall be implemented to protect the fiscal integrity of the College that comply with relevant laws and regulations, adhere to best business practices, as well as meeting requirements set for in the Payment Card Industry Data Security Standards (PCI DSS)."

This standard establishes OBS and Office of Information Technology (OIT) credit card processing and E-commerce direction and identifies the role of each College Merchant Unit in the secure processing and compliant handling of Cardholder Data. This Standard also fulfills the role of collegewide credit card security policy as required by the PCI DSS requirement 12.1.

SCOPE

This standard applies to all College administrative offices and academic departments that accept or support credit card payments for products and services provided and to all vendors or third parties that support College credit card processing.

DEFINITIONS

Term	Definition
Cardholder Data	According to the PCI DSS, Cardholder Data is the primary account number ("PAN" or credit card number) and other data obtained as part of a payment transaction, including the following data elements, Cardholder Name, Expiration Data, and Service Code.
CDE	Cardholder Data Environment (CDE) is the networked collection of IT systems that process, store and/or transmit cardholder data or sensitive payment authentication data for the College. This includes any peripheral components that directly connect to or support the IT systems.
College Credit Card Companies	Montgomery College accepts MasterCard, Visa, and Discover credit cards. Montgomery College Foundations accepts American Express cards.
College Merchant Unit	Administrative offices and academic departments approved by OBS to process credit cards in payment for products or services.
E-commerce	The purchasing of products and services using computer and Internet technologies.
PCI DSS	Payment Card Industry Data Security Standard (PCI DSS) is an industry based regulation developed by major credit card companies

	and serves as a set of technological and procedural requirements for better securing credit card processing and cardholder information.
E2EE POI Device	End-to-End Encryption (E2EE) Point of Interaction (POI) device is a credit card processing device that receives cardholder data either by card swipe, card tap (contactless) or EMV chip and encrypts the data at the point of entry. The data is then unencrypted at the final point of processing maintained by a third party.
Redact	Remove sensitive information from the viewing or publishing of a document.
Sensitive Authentication Data	According to the PCI DSS, Sensitive Authentication Data is (1) full magnetic stripe data, (2) CAV2/CVC2/CVV2/CID also referred to security or verification code, and (3) PINs/PIN blocks.
Third Party Vendor	A vendor contracted by a College Merchant Unit to take credit card payments for products and services on behalf of the College Merchant Unit.

STANDARD

A. E-commerce PCI DSS Version 3.0 (et. Seq.) Requirements:

College Policy prohibits storing any credit card information in an electronic format on any College technology resource. It further prohibits the transmission of credit card information other than encrypted format. The College will comply with the PCI DSS. The following list communicates the full PCI DSS scope of compliance requirements. Based upon College infrastructure and business process, some listed requirements might not be relevant. In other cases, further detail of compliance requirements is provided in this document and the PCI DSS.

PCI Goals	PCI DSS Requirements
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 for system passwords and other security parameters
Protect Cardholder Data	**3.** Protect stored cardholder data **4.** Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	**5.** Protect all systems against malware and regularly update anti-virus software or programs **6.** Develop and maintain secure systems and applications
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

Regularly Monitor and Test Networks	**10.** Track and monitor all access to network resources and cardholder data **11.** Regularly test security systems and processes
Maintain an Information Security Policy	**12.** Maintain a policy that addresses information security for all personnel

B. College E-commerce

1. TouchNet Information Systems E-commerce applications and E2EE POI Device technology are the official College standards for E-commerce solutions. Any exception to this standard must be approved by OBS and OIT.
2. College administrative offices and academic departments must be approved by OBS in order to obtain a merchant account to become a College Merchant Unit, and process credit cards payment for products or services.
3. College Merchant Units must notify OBS prior to initiating any new or enhanced E-commerce activities in an effort to promote collegewide consistency and Federal, State, and industry (PCI) based regulation compliance. Proper due diligence must be performed prior to engagement with any vendor in order to maintain College compliance status and insure the security of card holder data and the College's CDE.
4. All E-commerce technology connected to the College network must be verified for network compatibility with OIT prior to purchase.
5. College technology used to process credit card transactions must be configured to reasonably prohibit access to Internet sites that are not directly involved in the credit card processing function.
6. College Merchant Units are required to document unit credit card processing procedures in order to ensure that the standards noted in this document are followed by all unit personnel, business process is consistent collegewide, and that unit checks and balances are in place in order to properly secure Cardholder Data.
7. Background checks, as applicable and directed by the Office of Human Resources, should be conducted for all personnel who routinely access credit card numbers and/or Cardholder Data.
8. Access and termination of access to all TouchNet Information Systems E-commerce applications is governed by OBS.
9. Annual PCI training is mandatory for all College personnel involved in the processing of credit cards or Cardholder Data. Participants must acknowledge that they have participated in the annual training and have read and understood the standard.

C. Information Security and Standard Compliance

1. Cardholder Data must be kept secure and confidential at all times. Physical access to Cardholder Data and systems in the College's CDE is restricted to authorized College representatives and in accordance with approved least privileges necessary to perform defined job responsibilities.
2. Shared and generic user IDs and passwords must not be used to access credit card processing technology or applications.
3. As the College must comply with PCI DSS, a self-assessment initiative will be conducted annually to evaluate and report compliance status. Network scanning will be conducted quarterly.
4. College computer technology resources used for processing E-commerce transactions must comply with the PCI DSS, College policy, and OIT standards and guidelines. Certain specific requirements are detailed in this standard.
5. College computer technology resources used for processing E-commerce transactions must operate current anti-virus software.

6. College units equipped with E2EE POI Devices must only process Cardholder Data using the E2EE POI Device. Cardholder data must never be entered or processed using the associated College desktop keyboard.

7. College workstations other than merchant unit workstations specifically designated for processing credit cards transactions must not be used to process credit card payments.

D. Electronic Storage and Transmittal of Credit Card Data

1. Credit Card transaction processing involving the transmittal of Cardholder and Sensitive Authentication Data outside of the College's TouchNet application must use analog, cellular or other non-College network solutions.
2. Cardholder and Sensitive Authentication Data must be deleted or rendered unrecoverable upon completion of the transaction authorization process and never stored on College owned or provisioned technology resources.
3. Cardholder and Sensitive Authentication Data must not be moved, copied or stored to local hard drives and removable electronic media via remote-access technologies.
4. Cardholder and Sensitive Authentication Data must not be stored on personal computers, mobile devices, or removable electronic media.
5. Cardholder and Sensitive Authentication Data must not be stored in hardcopy format after transaction authorization and completion.
6. College servers within the CDE, which are not part of a third party application, must be stored in the College Information Technology Network Operating Center (NOC), unless an exemption is granted.
7. Electronic files containing full credit card numbers must not be created on College computers.
8. Cardholder Data transmitted over the College hard wired network must be encrypted.
9. Cardholder Data must never be transmitted via the College wireless or Voice Over IP (VOIP) networks.
10. Full credit card numbers must not be transmitted using the College E-mail system.
11. Credit card numbers must not be transmitted using end user messaging technologies (i.e. SMS, text messaging, IM, etc.).
12. FAX transmittal of Cardholder Data is permissible only if transmitted on an analog line and the receiving FAX is located in a secured location (i.e. locked office).
13. Cardholder Data must not be placed on voicemails.
14. Telephone transmittal of Cardholder Data is permissible only if transmitted on a College owned cellular phone with no Internet connectivity.
15. Manual swipe or imprint machines are not authorized for use without the approval of OBS.
16. Credit card devices and point of sale (POS) terminal displays must mask or truncate credit card number so that only the last four digits of the credit card number are exposed or printed on receipts.
17. Technology with storage capability used within the CDE must be reviewed by IT Security before being disposed of in order to confirm that all Cardholder Data has been removed or that a secure technology disposal process will be followed.

E. Hardcopy Document Handling

1. Hardcopy documents containing Cardholder or Sensitive Authentication Data must be kept in a secure environment (i.e. safe, locked file cabinet, etc.) and must not be retained after the credit card transaction has been completed unless all Cardholder and Sensitive Authentication Data is removed or completely redacted and unreadable.
2. Before hardcopy documents containing Cardholder or Sensitive Authentication Data are submitted for document imaging, the credit card number, expiration date and any Sensitive Authentication Data must be removed or completely redacted so as not to appear in the document image. Retention of the imaged documents should comply with the retention/destruction information contained in the College Records Retention Schedule.

3. The transmittal of hardcopy documents containing credit card numbers and/or Cardholder Data through the College mail system is not permitted.
4. The physical transfer of hardcopy documents containing credit card numbers and/or Cardholder Data by a College employee is permitted only when using a secured delivery method that can be accurately tracked.
5. Hardcopy documents containing Cardholder or Sensitive Authentication Data must be destroyed using a cross-cut shredder or a College sanctioned document destruction service. Storage containers used for documents that are to be destroyed must be secured.

F. System Configuration Standard

1. System configuration standards will be developed for all CDE system components and will be consistent with CIS standard and PCI DSS requirements.
2. System configuration standards will be updated as new vulnerability issues are identified based on operational risk.

G. Records Retention of Credit Card Related Documents

1. College unit credit card records should be retained and subsequently securely destroyed only as directed by the College's Record Retention Schedule.
2. Any document requiring offsite storage must have all Card Holder and Sensitive Authentication Data redacted before the document can be sent to the Records Management Office.

H. College Merchant Third Party Vendor Management

1. A vendor Request for Purchase (RFP) issued for any form of E-commerce must contain PCI requirements and responsibility language as provided by OIT and OBS,
2. Vendor contracts for any form of E-commerce must contain appropriate PCI DSS 12.8.2 compliance language acknowledging responsibility for the security of College card holder data it processes, stores or transmits.
3. Before the Office of Procurement and a College Merchant Unit select a Third Party Vendor, a copy of the vendor's most current PCI attestation of compliance for the services being provided must be reviewed and accepted by the IT Compliance and Security teams.
4. College Third Party Vendors will not transmit Cardholder data on the College network.
5. The College as well as the College Merchant Unit will monitor the unit's Third Party Vendor's PCI DSS compliance status at least annually.

I. College Unit Responsibilities

College unit credit card processing responsibilities are identified as follows:

1. OBS personnel are responsible for:
    a. Abiding by the rules of this standard.
    b. Reviewing and initiating requests from College units/departments to establish a merchant account and accept credit cards as a form of payment for services performed or for merchandise sold by such units/departments.
    c. Reviewing requests from College units/departments to change credit card procedures or technology. This includes any College Merchant Unit E-commerce initiative or major enhancement.
    d. Providing information and assistance to College units that are analyzing the responsibilities and costs of accepting credit cards as a form of payment.
    e. Coordinating all fiscal compliance activities for College Merchant Units.
    f. Reconciling the depository bank account to the general ledger cash account monthly.
    g. Reviewing monthly merchant statements for accuracy.
    h. Maintaining procedures to ensure the appropriate and timely recording of deposits onto the general ledger.

i. Responding to chargeback notifications and acquiring bank or Card Company inquiries within chargeback notification letter deadlines.
j. Administrating and coordinating of chargeback notification to the Merchant Units.
k. Fiscal administration of the College's centralized third party credit card application (TouchNet).
l. Following the workflow documented in the Third Party Review Standard to ensure that secure and compliant vendors are selected for College E-Commerce.

3. OIT personnel are responsible for:
   a. Abiding by the rules of this standard.
   b. Managing the procurement, installation, and maintenance of E-commerce technology products and services and maintaining an inventory of such products and services.
   c. Coordinating all College and Merchant Unit compliance activities that are required or directed by College Policies and Procedures, payment card industry standards, OIT, and acquiring bank standards.
   d. Implementing third party application gateways and technology for Merchant Units approved for accepting credit cards.
   e. Coordinating technical administration of the College's centralized third party credit card application (TouchNet).
   f. Conducting periodic network, POS desktop, and POI device security activities in compliance with the PCI DSS.
   g. Incorporating PCI DSS compliance language into third party credit card vendor RFPs and contracts.
   h. Monitoring PCI DSS compliance status of contracted third party credit card vendors.
   i. Conducting PCI training on secure and compliant credit card processing and handling of Cardholder Data. The training will be provided annually to College merchant and technical support employees and as required for any new hire employees.
   j. Managing E-Commerce security incident response activities.

4. College Merchant Unit personnel are responsible for:
   a. Abiding by the rules of this standard and using College CDE technology only for the purposes of performing acceptable College merchant business.
   b. Not directing individuals to a College workstation to make credit card payments but instead directing the individual to their own computer technology to make the payment if they are unable to do so while using a College cashiering device.
   c. Completing Registration/Inventory documents regarding credit card processing and returning it to OBS or OIT as applicable.
   d. Recording all card transactional activity on the general ledger within three (3) business days of settlement.
   e. Notifying OBS immediately when accounts are no longer needed and should be deactivated.
   f. Insuring that no Cardholder or Sensitive Authentication Data is stored electronically on College technology resources.
   g. Securing all hardcopy documents that contain Cardholder or Sensitive Authentication Data and destroying the documents or redacting the data once the credit card transaction is authorized and completed.
   h. Verifying cardholder identity during all credit card processing transactions.
   i. Following security measures established by PCI, OIT and OBS standards and procedures.
   j. Performing all periodic compliance activities in a timely manner that is requested by OIT in coordination with OBS.
   k. Inspecting as required and documented by OIT all unit credit card processing technology for the purposes of detecting possible tampering and fraud.
   l. Maintaining secure chain of custody of CHD so that only personnel with need for access to the CHD have that access.
   m. Assuring that staff that are responsible for credit card activity in the unit/department have read this standard and attended appropriate awareness training.

n. Managing their Third Party Vendors according to this standard.
o. Participating in the annual PCI DSS self-assessment conducted by OIT in coordination with OBS.

5. College E-commerce Vendors or Third Party Agents are responsible for:
   a. Abiding by the rules of this standard as is applicable.
   b. Providing evidence of their PCI DSS compliance status at RFP, vendor contract initiation or renewal, and during an annual College PCI DSS self-assessment if requested.
   c. Taking responsibility for protecting College sensitive and confidential information as stated in PCI DSS Requirement 12.8.2.

EXCEPTIONS

This standard is applicable as of its Effective Date. Exceptions to this standard will be considered on a case-by-case basis in accordance with the IT Standard Exception Request Form.

COMPLIANCE AND RECOURSE FOR NON-COMPLIANCE

Montgomery College has established College Policies/Procedures and the OIT has established IT Standards and Processes and associated guiding documents to provide appropriate protection of technology resources, to assure protection of personally identifiable and sensitive information and to promote privacy. Any faculty, staff, contractor, or vendor found to have violated any part of College Policies, Procedures or IT Standards or Processes may be subject to disciplinary action and/or legal action.

RELATED DOCUMENTS

- 66001 Acceptable Use Policy and the accompanying Procedure/Guidelines Statement
- 66002 Confidential Data Management and Security
- 61001 Fiscal Control
- 62003 Public Information, Communications, and Marketing
- Montgomery College IT Standard Exception Request Form
- Montgomery College Records Retention Schedule
- Montgomery College Procedures for Records Management
- Montgomery College E2EE Device Security Management Standard
- Montgomery College Credit Card Account Security Incident Response Process
- Montgomery College device inspection reference guides
- Montgomery College Verifone Device Security Management Standard
- Montgomery College Analog POI inspection reference guide

WEB SITE ADDRESS FOR THIS STANDARD

https://info.montgomerycollege.edu/offices/information-technology/it-security/it_standards.html

APPROVALS / REVISION HISTORY

DATE	VERSION / REVISION / NOTES	APPROVER
January 19, 2012	Original roll-out of this Credit Card Processing/E-Commerce Standard document.	Patrick Feehan, Information Security and Privacy Director/ITPA
May 20, 2020	Revised.	Patrick Feehan, Information Security and Privacy Director/ITPA
April 1, 2021	Reviewed.	Tim Neill, IT Security Analyst
April 2021	Decided upon and added review cycle dates.	Nell Feldman / Keith Wilson
March 2022	Reviewed (Minor grammatical clean-ups, removed sign a form to acknowledge training, updated College cards. Website address added to standard).	Nell Feldman, Interim Director of Information Security Services/CISO/ITPA

Nell Feldman

Digitally signed by Nell Feldman
Date: 2022.03.29 14:15:40 -04'00'