Montgomery College
Office of
Information
Technology

IT Standard
End-to-End Encryption (E2EE) Device Security Management

Standard:	IT20002
Effective Date:	020615
Revision Date:	032019
Review Date:	043020
Version No.:	2.00
Contact:	Information Security and Privacy Director

Purpose

It is the policy of Montgomery College ("College") to protect and promote secured access to its academic and administrative data. This includes personal Card Holder Data used during credit card transactions with the College. The TouchNet U.Commerce system is the College's primary source for enterprise e-commerce functions.

The purpose of this document is to provide the minimum standard by which End-to-End Encryption point-of-interaction card swipe devices used by merchant business applications to provide encrypted Card Holder Data to TouchNet for processing ("E2EE Devices") are securely stored, deployed, maintained, and monitored.

Scope

This Standard applies to any individual who is responsible for or interacts with E2EE Devices at Montgomery College.

Definitions

Term	Definition
Cardholder Data (CHD)	According to the Payment Card Industry Data Security Standard (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, Service Code, and Sensitive Authentication Data: (1) full magnetic stripe data, (2) CAV2/CVC2/CVV2/CID, and (3) PINs/PIN blocks.
College Credit Card Companies	Montgomery College accepts MasterCard, Visa, and Discover credit cards.
College Merchant Unit	Administrative offices and academic departments approved by OBS to accept credit cards in payment for products or services.
E-commerce	The purchasing of products and services using computer, mobile device, and Internet technologies.
End-to-End Encryption (E2EE) Device	A secure payment technology designed to encrypt the transmission of CHD from transaction inception to completion of a credit or debit card payment transaction.
E2EE Device Deactivation Checklist	A list of tasks to be completed during the deactivation of a E2EE Devices in deployment at the College.

E2EE Device Deployment Checklist	A list of tasks to be completed during the deployment of a E2EE Devices into service at the College
E2EE Device Receipt and Inspection Checklist	A list of tasks to be completed during the initial receipt and inspection of all E2EE Devices received for deployment at the College.
E2EE Device Log	A log developed to document physical description, activity status and College personnel responsible for storage, use and maintenance of E2EE Devices that belong to Montgomery College. Logs are identified by device/system.
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.
Point-of-Interaction (POI) Device	Hardware and/or software component of a point of sales system used to capture credit card data in order to initiate a credit card payment transaction.

STANDARD

A. General

1. E2EE Devices are a standard College POI E-commerce technology used in the processing of College accepted credit cards. The Offices of Business Services, (OBS), Information Technology (OIT) and College Merchant Units are responsible for overseeing the life-cycle of this technology and abiding to this standard.
2. E2EE Devices will be stored, maintained and deployed in accordance with TouchNet guidance and PCI DSS compliance rules and standards.
3. This standard and the E2EE Device Log will be used to track all activity involving E2EE Devices in an effort to protect against device tampering and fraudulent activity.
4. Separation of duty will be maintained between OIT IT Privacy and Security, Applications, and Asset Management groups, and OBS to limit any one person’s ability to modify or tamper with the E2EE Devices.
5. Questions regarding the security of E2EE Devices should be directed to the IT Service Desk.

B. Device Management Logging

1. Physical device characteristics, individuals with custodial responsibilities and all physical activity involving E2EE Devices will be accounted for in the E2EE Device Log.
2. The E2EE Device Log will establish and monitor a chain of custody for all E2EE Device activity.
3. The E2EE Device Log will reside on the College Intranet and will only be accessible to IT Security and Privacy personnel who will be responsible for maintaining it.
4. All E2EE Device Logs and checklists as well as this standard will be reviewed annually as part of the College’s PCI DSS self-assessment.

C. Initial Device Inspection

1. Receipt of E2EE Devices by the College will be the responsibility of designated OIT Asset Management personnel and IT Security and Privacy personnel.

2. E2EE Devices will be inspected and entered in the E2EE Device log and OIT Asset Management inventory within 72 hours of receipt by the College.

3. The *E2EE Device Receipt and Inspection Checklist* will be used to facilitate the initial device inspection process.

D. Daily Device Inspection

1. Merchants are responsible for checking E2EE Devices daily for signs of tampering or substitution, logging this activity, and reporting any issues to the IT Service Desk.

2. The *Daily E2EE Device Inspection Checklist* will be used to facilitate daily device inspections. *Daily Inspection Checklists* must be kept by the merchant for 1 year.

3. The *Credit Card Account Security Incident Response Plan* will facilitate PCI related incident responses.

E. Device Storage Physical Security

1. All E2EE Devices that are in the property of OIT will be secured after initial inspection and inventory in a locked closet within the Central Services Building (CT) and accessible only to Information Security and Privacy personnel.

2. E2EE Devices designated for disposal will be secured in a locked cabinet within Asset Management prior to final disposal and only accessible to Information Security and Privacy and Asset Management personnel.

3. Questions regarding unauthorized access to secured storage of E2EE Devices should be directed to the IT Service Desk.

F. Device Deployment Physical Security

1. E2EE Devices deployed for use at College locations must be physically located so to protect against tampering and unauthorized access. The devices must be located in an area:

   a. designed to visually deter compromise attempts; not in remote locations or areas left unattended for any period of time,

   b. such that there is a straight line view between the device and the cashier,

   c. easily accessible to authorized personnel who may need to physically inspect the device.

2. Deployment of the E2EE Device must be the only objective to be met when the device is transferred to a location for installation. The device must be installed by authorized OIT personnel using the E2EE Device log. The individual responsible for delivering the E2EE Device to the site must oversee the entire deployment effort.

3. The E2EE Device must never be left unattended during the deployment activity.

4. The *E2EE Device Deployment Checklist* must be used to facilitate the deployment of E2EE Devices at the College.

5. E2EE Devices must be fastened or secured and not removable from the deployed location without the use of an authorized unlocking mechanism.

G. Device Deactivation Physical Security

1. The *E2EE Device Deactivation Checklist* must be used to facilitate the deactivation of E2EE Devices at the College including instructions which are included to ship devices to TouchNet or another authorized vendor if necessary.
2. The E2EE Device must be deactivated by authorized OIT personnel using the E2EE Device log. The individual responsible for delivering the E2EE Device to storage must oversee the entire deactivation effort. Deactivation of the device must be the only objective to be met and the device immediately transferred to secured storage and activity logged.
3. The E2EE Device must never be left unattended during the deactivation activity.

H. Device Inventory Audit

1. All E2EE Devices and merchant *Daily Inspection Checklists* will be audited annually by Information Security and Privacy personnel.
2. More than one person should participate in the audit to increase the likelihood of finding a problem and to promote the independence of the auditors.

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 or as approved in writing by the IT Privacy and Cybersecurity Compliance Director.

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

- ♦ Acceptable Use Policy and the accompanying Procedure/Guidelines Statement
- ♦ Montgomery College Policy 66002, Confidential Data Management and Security
- ♦ OIT Standard IT20001, Credit Card Processing / E-Commerce Standard
- ♦ U.Commerce TouchNet Point-to-Point Encryption (P2PE) Instruction Manual

WEB SITE ADDRESS FOR THIS STANDARD

APPROVALS

Approved: 3/20/19	Patrick Feehan, Information Security and Privacy Director/ITPA