# COLLEGE POLICY ON CREDIT/DEBIT CARD PAYMENT PROCESSING

Supersedes: None
Date: March 17, 2014

## I. PURPOSE

To establish business processes and procedures for the processing of credit/debit card payments as defined herein on behalf of New York Medical College, its departments, units, faculty, staff, students or any affiliates using the College's systems to minimize risk, protect the security of data, comply with the rules and regulations established by the Payment Card Industry and ensure that debit/credit card acceptance procedures are appropriately integrated with the College's financial system.

## II. POLICY

It is the policy of New York Medical College to require a valid business purpose is established in advance of the processing of credit/debit card transactions and that proper authorization is obtained for acceptance of debit/credit payments in accordance with the procedures set forth in this Policy.

## III. SCOPE

This policy applies to all forms of credit/debit card processing on behalf of the College by its departments, units, faculty, staff and students, or by affiliates using the College's systems. Credit card processing includes any payment card transaction (whether credit card, debit card, or other instrument linked to such a card) or other transmission, processing or storage of credit card data regardless of the means by which that transaction is actuated. This includes transactions initiated in-person, via the telephone or other telephonic means, in paper form, by US mail or other courier, through a terminal, kiosk, computer system, website, mobile device or any other means. This policy applies to whether the processing is performed by the College or by an outside party acting as a service provider to the College. This policy applies to all College departments, units, faculty, staff, students who, in the course of doing business on behalf of the College, accept process, transmit or otherwise handle the cardholder information in physical or electronic format. This Policy applies to existing, new and changed services and applies regardless of whether revenue/expense is deposited/withdrawn in a College or departmental account.

## IV. DEFINITIONS

Credit Card - A card issued by a financial institution giving the holder an option to borrow funds, usually at point of sale.

Debit Card - A card which allows vendors to access holder funds immediately, electronically.

Payment Card Industry Data Security Standard (PCI-DSS) – A multi-faceted security standard that includes requirements for security management, policies and procedures, network architecture, software design and other critical protective measures.

## V. EFFECTIVE DATE

This policy is effective as of the date signed below.

## VI. PROCEDURES

### A. Department

1. Before initiating any transactions or arrangements within the scope of this Policy, obtain a completed "Application To Become A Merchant Department" form that has been approved in writing by the Associate Vice President and Controller. The form is attached and incorporated hereto as Exhibit A.
2. Designated an individual within that department who shall have primary authority and responsibility for debit/credit card transaction processing, protection, storage and disposal of personal information and reporting of any security breach.
3. Obtain equipment and/or software application (e-Commerce) that is PCI-DSS compliant.
4. Create, maintain and update menu of services for which the department can accept payment including minimum amount per transaction.
5. Verify monthly all revenues and processing fees on the Payment Card Merchant Statement indicating department's approval and signature prior to submission to the Office of General Accounting for further processing.
6. Ensure all processing fees, including those on the monthly Payment Card Merchant Statement, will be charged against the expense account of each department.
7. Retain a copy of the fully executed vendor Agreement(s) and subsequent official documents related to terms and pricing.
8. Ensure that all payment card data collected in the course of performing College business, regardless of how the payment data is stored, is secured. Data may be physical or electronic, and includes, but is not limited to, card imprints and account numbers.
9. Annually submit to the Office of the Controller a completed PCI-DSS Self-Assessment Questionnaire A or B, as applicable. Such form is available at https://www.pcisecuritystandards.org/security_standards/documents.php?category=saq_standard

10. Ensure that no debit/credit information is obtained or transmitted via e-mail. If it should be necessary to transmit debit/credit card information via e-mail only last four digits of the debit/credit card number can be displayed.
11. Ensure that no debit/credit card information shall be stored on individual PCs or servers that have not been deemed PCI compliant. All hard-copy debit/credit card information must be stored in a manner that would protect the individual cardholder information from misuse.
12. Hard copy debit/credit card information must not be stored for more than 24 months.
13. Ensure that access to cardholder data is restricted to authorized College personnel with a business "need to know".
14. Ensure that fax transmissions (both sending and receiving) of electronic debit/credit information occurs using only fax machines which are attended by those individuals who must have contact with payment card data to do their job.
15. Prohibit the use of vendor-supplied defaults for system passwords and other security parameters.
16. Promptly report any security breach (even perceived) first to the Payment Card Processor then to Office of the Controller, Information Technology, Office of General Counsel and Security.
17. Notify the Office of the Controller when changes occur to the most recently submitted "Application To Become A Merchant Department" form and complete a new form.

## B. Information Technology

1. Build and maintain a secure system and application through installation and maintenance of a firewall configuration.
2. Maintain a program of continuous use and regular update of anti-virus software or programs.
3. Implement strong access control measure by assigning a unique ID to each person with computer access.
4. Regularly monitor and test networks by testing security systems and processes, documenting the efforts.

## C. General Accounting

1. Record monthly recurring journal entry for debit/credit activities.
2. Journalize monthly debit/credit activities using as support Payment Card Merchant Statement as verified and signed by departments.

3. Verify that all activities submitted by the department on a monthly basis are accounted for and accurately credited in the proper general ledger account(s) and on the actual month the activities occurred.
4. Ensure that debit/credit fees per approved Payment Card Merchant Statements agree to the debit/credit fees per the bank statement retaining the documents for three (3) years.

D. **Office of the Controller**

1. Review and approve all submissions of 'Application To Become A Merchant Department' form. Originals to be retained for three (3) years after the Department's merchant number is no longer used.
2. Obtain annual documentation from all College-authorized payment processors to ensure that they are PCI-DSS compliant.
3. Obtain completed PCI-DSS Self-Assessment Questionnaires from departments annually.
4. Overall administration and oversight of the College's PCI-DSS compliance.
5. Provide advice and guidance with respect to the interpretation and administration of this policy.
6. Provide business terms, including pricing, to the Office of the General Counsel.

E. **Office of the General Counsel** - negotiate vendor Agreement(s), to include the business terms and pricing provided by the Office of the Controller, and subsequent official documents related to terms and pricing. Maintain copies of and forward all documents.

## VII. POLICY RESPONSIBILITIES

A. Department – maintain all records and process all transactions in accordance with this policy.

B. Information Technology – provide necessary technical support for processing of debit/credit card transactions in accordance with this policy.

C. Controller's Office – process applications and maintain necessary documentation to ensure compliance with this policy.

D. Office of General Counsel - review and retain copies of fully executed vendor Agreement(s) and subsequent official documents related to terms and pricing.

E. Vendor(s) / Payment Processor(s)

1. Provide a secure gateway and hosted solution in which all debit/credit card transactions and personal payment information is transmitted to and stored on off-site computers which the payment processor maintains.
2. Ensure PCI-DSS compliance.
3. Assign a unique merchant identification number to each College department that has been approved by the Controller to accept payments by debit/credit cards.
4. Provide monthly Payment Card Merchant Statements for each department accepting debit/credit cards including the Office of General Accounting.

## VIII. POLICY MANAGEMENT

Responsible Executive: Senior Vice President and Chief Financial Officer

Responsible Officer: Associate Vice President and Controller

Responsible Office: Office of the Controller

**Approved:**

E Hal

Edward C. Halperin, M.D., M.A.
Chancellor for Health Affairs and
Chief Executive Officer

3/10/14

Date

Exhibit A


## APPLICATION TO BECOME A MERCHANT DEPARTMENT

---

**Application Date:**
**Name:**
**Title:**
**School/Division:**
**Department:**
**Email:**
**Extension:**
**Fax:**

---

**Describe the goods, services and/or gifts for which you will receive payments. Please be specific:**

**Is this an existing or new source of revenue?**

**Provide the Account Number where funds will be deposited:**

| | | - | | | | | - | | | | . | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|

**Provide the Account Number where processing fees will be charged:**

| | | - | | | | | - | | | | . | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|

**What benefits do you expect to gain by accepting debit/credit cards? Please quantify and/or provide additional documentation to support this application.**

**Describe the frequency of payments. Is this a one-time event? Are payments for seasonal or year-round activity? Provide detailed timeframes.**

**Will debit/credit be the sole method of payment? If not, what other methods of payment do you anticipate accepting for this specific purpose?**
**How do you plan to process these payments? (Check all that apply)**

☐ In-person (card present) ☐ Mail/phone/fax order* ☐ Internet

**Note: Payment card data should never be transmitted via email correspondence. Faxes must be secured.*

**If you are planning to accept payments via the Internet, do you have a College webpage for this purpose?**

**If so, please provide the URL:**

**Please indicate the estimated annual dollar volume and number of transactions for each applicable debit/credit card acceptance process:**

In-person $ # transactions

Mail/phone/fax order $ # transactions

Internet $ # transactions

**Who will be the Department Responsible Person? The Department Responsible Person is responsible for managing debit/credit card and/or eCommerce transaction processing including protection, storage and disposal of personal information and reporting of any security breach. Include name, job title and phone extension and describe duties.**

**Please identify any additional staff who will be involved in processing payments. Include name, job title and phone extension and describe duties.**

**Will any other departments, software packages or outside vendors be involved in the processing of payments? If so, please identify all parties and describe their roles and responsibilities.**

Signatures: _____

Name
Department Responsible Person

_____

Name
Department Head

_____

Name
Associate Vice President and Controller

***By signing this form, the Department Responsible Person acknowledges that he/she understands his/her role and accepts the responsibility of that role.***

***By signing this form, the Associate Vice President and Controller approves of the business case presented for the department to become a Merchant Department, the account numbers provided and designated Department Responsible Person.***