



Medical College of Georgia

Administrative
Policy Library

Credit Card Processing Policy

CITATION REFERENCE

Official Title: Credit Card Processing Policy

Abbreviated Title: Credit Card Processing Policy

Volume: Finance & Administration

Responsible Office: Controller

Originally issued: March 2009

Revised: Not applicable

Policy Statement

This policy applies to any department or individual accepting credit card funds on behalf of or in the name of MCG. This policy applies continuously. No major conditions or restrictions apply

Reason for Policy

This policy provides for centralized control of all credit card processing activities associated with MCG in order to facilitate compliance with the Payment Cardholder Industry Data Security Standard (PCI-DSS). Compliance with the Standard ensures that our customers are not unnecessarily exposed to the risk of identify theft in connection with their credit card transactions with MCG, and that MCG is not unnecessarily exposed to the risk of adverse publicity associated with failure to protect customer bank and credit card information or fines associated with non-compliance.

Entities Affected By This Policy

Any department or individual accepting credit card funds in the name of or in association with any MCG activity or grant/contract on or off this campus must comply with this policy.

Who Should Read This Policy

Any department or individual on campus who accepts funds in the name of MCG for any reason should read this policy.

Any and all personnel who have access to information resources (payment card applications and associated infrastructure, as defined below) that transmit, process, or store payment card data from students or any other MCG customers are responsible for the application of this and related policies.

Information Technology personnel responsible for security and for PCI compliance should also be familiar with this policy.

Contacts

Contact	Phone	e-mail/URL
Cashier's Office	706-721-2926	CASHIERS_OFFICE@mcg.edu

Website Address for This Policy

www.mcg.edu/policies

Related Documents

MCG Information Security Standards for Payment Card Applications, describing Information Technology standards and practices for managing a secure platform for Institution hosted payment card applications, specifically payment card transactions, and the data related to card holders.

Definitions

PCI Data Security Standard: The Payment Card Industry (PCI) Data Security Standard details security requirements for merchants and service providers that store, process or transmit cardholder data.

Payment Card Application: Anything that stores, processes, or transmits card data electronically. In most cases, this does not include the hardware running the application unless the hardware and software are intertwined similar to a credit card swipe terminal. Anything from a Point of Sale System to a Website e-commerce shopping are all classified as payment applications. Therefore, any software that has been designed to touch credit card data is considered a payment application.

Payment card application infrastructure: Computing resources (i.e. servers, storage, network and storage switches, firewalls, physical racks containing these, and related software) which process, transmit, or store payment card data or can directly access such resources.

Credit Card Swipe Machine: Any device through which a credit card is manually swiped to read the credit card data embedded in the data strip on back of the card. Such device may or may not internally store credit card data. Devices internally storing credit card data are strictly prohibited by this policy and by the related Information Technology Standard referenced above.

Credit Card Scanner: A device similar to a Credit Card Swipe Machine in which there is no data storage capability. Such device serves only to electronically transmit data off of a credit card magnetic strip to the software application processing such data.

Overview

Credit Card Swipe Machines, especially older models, internally store consumer credit card data. Theft of such a device can result in theft of a cardholder's credit card data and possible fines from the payment card industry. Additionally,

software, computers or networks used to transmit or store credit card data should be adequately secured to prevent unauthorized access to card holder data.

The University System of Georgia Board of Regents holds contracts with both First Data Merchant Services, the credit card processor MCG currently utilizes to process the great majority of its credit card business, as well as with TouchNet Payment Gateway, a software vendor that offers a secured, PCI certified payment gateway over which to accept and transmit credit card data electronically to First Data Merchant Services. To facilitate compliance with PCI Data Security Standards for all credit card activities associated with MCG, the Institution strongly encourages all departments and operating units to utilize TouchNet and First Data Merchant Services to the greatest extent possible.

Specifications:

- Any individual or department accepting credit cards in the name of MCG or in association with MCG activities, services or contracts must contact the Accounts Receivable Manager to register. Registration information required to be provided includes:
 - The name and description of any credit card payment application currently used to transmit or store credit card data
 - Contact information for the software vendor
 - A brief description of the business process surrounding use of the software
 - The make and model of any credit card swipe machines, scanners or smart terminals being used to store or transmit credit card data
 - Identification of all MCG work stations used to store or transmit credit card data
 - Name and contact information for any associated credit card processor, and the MCG merchant id used by such processor
 - Justification for retaining the current credit card processor, should the department wish to seek a waiver for use of TouchNet Payment Gateway and First Data processing.

- Departments not currently using TouchNet and First Data Merchant Services processing must convert unless a waiver is secured from the Controller's Division. In response to any request for waiver, the Accounts Receivable Manager and Assistant Controller for Financial Operations, in conjunction with an IT security administrator, will exercise all diligence to assess the adequacy of the current payment software and credit card data collection and processing mechanisms with respect to security concerns and PCI compliance. Departments and or individuals involved are expected to cooperate fully during this investigational process. A wavier will not be unreasonably withheld if the inquiring Department can document adequate levels of security and PCI compliance. The Controller's Office, in conjunction with IT

personnel responsible for PCI compliance, will issue a written determination letter.

- Requirements relating to the payment card application infrastructure are listed in the *MCG Information Security Standards for Payment Card Applications* and incorporated by reference herein. Considerations related to these requirements will contribute to whether waiver is or is not granted for Touchnet/First Data exemption requests. These requirements include, but are not limited to the following:
 - Servers that are part of the payment card application infrastructure and any workstations or systems that can otherwise directly access computing resources that contain payment cardholder data must be registered with IT Security as regulated computers
 - All workstations must meet PCI Data Security Standards. MCG IT Security reserves the right to determine the suitability of such workstations to support applications operating with the MCG payment card infrastructure.
 - Workstations and software must be strictly controlled for access on a “need to know” basis, and access rights continually monitored for any changes in roles or employment status of individuals.
 - Storage of credit card authentication data on workstations or other peripheral devices is strictly prohibited.
- New Payment Card Applications and associated Infrastructure, to include but not limited to Touchnet/First Data conversions, must be coordinated through MCG IT Applications Support. Applications Support is responsible for coordinating communication and interaction between MCG, any application vendor(s), credit card processors, and other MCG groups in order to ensure secure implementation and operation. Applications Support will not implement systems other than Touchnet/First Data without first ensuring a waiver has been appropriately secured and documented.

Process/Procedures

No procedures beyond the specifications described above apply to this policy.

Responsibilities

The responsibilities each party has in connection with the *Credit Card Processing Policy* are:

Controller’s Division	Reasonably and fairly determine any exemptions granted based on departmental needs and PCI / data security requirements.
-----------------------	--

Departmental Directors/Managers	Provide full and timely cooperation on any system modifications required under this policy, and to bear the associated costs, if any.
Information Technology Support & Services	Ensure that any known credit card activities are disclosed to the Controller's Division.

Forms

None

Appendices

None