Emory University & Emory Healthcare

Payment Card Processing and Compliance Policy and Procedures Manual

Office of Cash and Debt Management
Mailstop 1599-001-1AE
1599 Clifton Road, 3rd Floor
Atlanta, GA 30322
paymentcardservices@emory.edu

Last Revised: 12/14/2012

Contents

Policy

I. Overview

Emory University and Emory Healthcare, hereinafter referred to as "Emory", have a fiduciary responsibility to their customers and payment card processors to comply with the Payment Card Industry Data Security Standard (PCI DSS) when handling payment card transactions. Non-compliance can result in serious consequences for Emory, including reputational damage, loss of customers, litigation, and financial costs. The objective of this policy is to:

- ensure compliance with PCI DSS and other applicable policies and standards,
- establish the governance structure for payment card processing and compliance activities at Emory,
- define responsibilities for payment card services to various Emory constituents, and
- provide general guidelines regarding the handling of cardholder data.

II. Applicability

This policy applies to all University and Healthcare departments & employees as well as non-employees acting as agents of Emory who handle or support the handling of cardholder data.

III. Definitions

Cardholder data is any personally-identifiable data associated with a cardholder. Examples include but are not limited to: account number, expiration date, card type, name, address, social security number, and Card Validation Code – a three-digit or four-digit value printed on the front or back of a payment card referred to as CAV, CVC, CVV, or CSC depending on the payment card brand. The term cardholder data is interchangeable with payment card data throughout this policy.

Merchant refers to an Emory department or operating unit that has applied for and been approved to accept credit/debit card payments for goods and/or services. A merchant is assigned a specific merchant account, which is used to process all credit/debit card transactions via an Emory-approved payment card processer.

Payment card refers to both credit and debit cards. Payment card processing is defined as using any application or device to process a credit/debit card transaction as payment for goods or services from an Emory merchant. This policy does not apply to the EmoryCard, P-card, and Corporate card programs.

IV. Policy Details

a. Background Information

In an effort to enhance the security of payment card data, the credit card industry has formed a council called the Payment Card Industry Security Standards Council comprised of the five founding global payment brands: Visa Inc., MasterCard Worldwide, American Express, Discover Financial Services, and JCB International. The Council has developed the PCI Data Security Standard (PCI DSS), an actionable framework for developing a robust payment card data security process which includes prevention, detection and appropriate reaction to security incidents. This standard is mandated by the industry in order for a merchant to accept credit/debit card payments, and failure to abide by it may result in reputation risk as well as financial penalties.

Emory accepts credit/debit card payments as a convenience to its customers. To protect our customers' payment card information, Emory's reputation, and to reduce the financial risk or impact associated with a breach of payment card information, this policy addresses Emory's responsibilities to abide by PCI DSS and other applicable policies and standards.

In order for a department, or any other entity at Emory, to process credit/debit card transactions, it must be established as a merchant. Departments may accept VISA, MasterCard, Discover, American Express, and debit cards with a VISA or MasterCard logo. All merchants at Emory are required to use First Data Merchant Services to process credit/debit card transactions, with an exception for The Emory Clinic which uses Sage Payment Solutions.

b. Authority and Delegation

The University Vice President for Finance has overall authority to ensure PCI DSS compliance for Emory University and Emory Healthcare. The University Vice President for Finance has delegated authority to the Assistant Vice President for Cash and Debt Management to define responsibilities for payment card services and modify this policy as necessary, provided that all modifications are consistent with PCI DSS then in effect.

c. Applicable Policies and Standards

In addition to the directives and procedures set forth in this policy, any employee, contractor, or agent who, in the course of doing business on behalf of Emory, is involved in the handling of credit card payments must adhere to the following applicable policies and standards:

- **Emory Policy 5.1 – Information Technology Conditions of Use**

"Computers, networks, and software applications are powerful tools that can facilitate Emory's core missions in teaching, learning, research, and service. Access and utilization of these tools is a privilege to which all University faculty, staff, students, and authorized guests are entitled. This policy documents the responsibilities that accompany this privilege. Campuses, schools, colleges, departments, and other administrative units have considerable latitude in developing complementary information technology conditions of use policies, as long as they are consistent with this Emory policy and any other applicable policies of the University. Such policies may be more restrictive than the Emory policy, but must not be more permissive."

- **Payment Card Industry Data Security Standard**

PCI DSS is the global data security standard adopted by the payment card brands for all entities that process, store, or transmit cardholder data. It consists of common sense steps that mirror security best practices. Below is a high-level overview of PCI DSS. The complete standard is accessible at the web address listed in section V – Related Links.

<u>Build and Maintain a Secure Network</u>
Requirement 1: Install and maintain a firewall configuration to protect cardholder data.
Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters.

<u>Protect Cardholder Data</u>
Requirement 3: Protect stored cardholder data.
Requirement 4: Encrypt transmission of cardholder data across open, public networks.

<u>Maintain a Vulnerability Management Program</u>
Requirement 5: Use and regularly update anti-virus software or programs.
Requirement 6: Develop and maintain secure systems and applications.

<u>Implement Strong Access Control Measures</u>
Requirement 7: Restrict access to cardholder data by business need to know.
Requirement 8: Assign a unique ID to each person with computer access.
Requirement 9: Restrict physical access to cardholder data.

Regularly Monitor and Test Networks
Requirement 10: Track and monitor all access to network resources and cardholder data.
Requirement 11: Regularly test security systems and processes.

Maintain an Information Security Policy
Requirement 12: Maintain a policy that addresses information security for all personnel.

- **Credit Card Brand Standards**

Each card brand has its own program for compliance validation levels and enforcement. Departmental merchants should be familiar with all of the individual credit card brand standards (American Express, Discover Financial Services, MasterCard Worldwide, and Visa Inc.) and refer to them periodically. More information about compliance with specific credit card brands can be found at the web addresses listed in section V – Related Links.

d. Core Responsibilities

The University Vice President for Finance has overall authority to ensure PCI DSS compliance for Emory University and Emory Healthcare. The University Vice President for Finance has delegated authority to the Assistant Vice President for Cash and Debt Management to define responsibilities for payment card services to various Emory constituents. Core responsibilities for each constituent are listed below.

- The Office of Cash and Debt Management is responsible for initiating and overseeing an annual PCI DSS self-assessment, making appropriate revisions to this policy as needed and coordinating any remediation activities as required by PCI DSS or other applicable policies and standards. The annual self-assessment will include oversight by the Way and Means Committee and the Enterprise Risk Management Program, in coordination with Emory Healthcare and the Office of Information Technology (OIT). Other responsibilities include providing annual security awareness & training programs and contracting with third-party credit card processing vendors and service providers.

- The Office of Information Technology Information Security is responsible for maintaining and disseminating security policies and procedures that address PCI DSS requirements, testing Emory's infrastructure and network environment, and assisting the Office of Cash and Debt Management in completing the technical sections of the annual PCI DSS self-assessment.

- The University Cash Operations Office is responsible for initial setup and ongoing administration of all University and Emory Hospital merchant accounts. Key responsibilities include approval of merchant applications, procurement of credit card terminals and other equipment, and operations liaison to Emory's third-party credit card processing vendor, First Data.

- The Emory Clinic Finance Office is responsible for initial setup and ongoing administration of all Emory Clinic merchant accounts. Key responsibilities include approval of merchant applications, procurement of credit card terminals and other equipment, and operations liaison to The Emory Clinic's third-party credit card processing vendors, First Data and Sage Payment Solutions.

- Local IT Services Departments, including University Technology Services (UTS), are responsible for configuring and managing all computer systems and other IT resources in compliance with PCI DSS and Emory security requirements, limiting access to IT resources and cardholder data, and assisting the Office of Cash and Debt Management in completing the technical sections of the annual PCI DSS self-assessment.

- Departmental Merchants are responsible for ensuring that all business processes for accepting, processing, retaining, and disposing of cardholder data comply with PCI DSS and all other applicable policies and standards. Departmental merchants are also responsible for performing an annual PCI DSS self-assessment in partnership with the Office of Cash and Debt Management. Departmental employees who

handle cardholder data must attend a security awareness & training program and sign the Payment Card Merchant Compliance Statement.

e. Consequences of Non-Compliance

Non-compliance can result in serious consequences for Emory, including reputational damage, loss of customers, litigation, and financial costs. Failure to comply with this policy and/or applicable policies, standards, and procedures carries severe consequences which may include:

- loss of the ability to process payment card transactions,
- departmental repayment of financial costs imposed on Emory, and
- employee disciplinary action, which can include termination of employment.

The Assistant Vice President for Cash and Debt Management has the authority to restrict and/or terminate merchant account status for non-compliance.

V. Related Links

- Emory Policy 5.1 – Information Technology Conditions of Use: http://policies.emory.edu/5.1
- Payment Card Industry Data Security Standard (PCI DSS): http://www.pcisecuritystandards.org
- American Express: www.americanexpress.com/datasecurity
- Discover Financial Services: http://www.discovernetwork.com/fraudsecurity/disc.html
- MasterCard Worldwide: http://www.mastercard.com/sdp
- Visa Inc.: http://usa.visa.com/merchants/operations/op_regulations.html
- Emory Payment Card Processing and Compliance Procedures Manual: TBD

VI. Contact Information

For questions or comments regarding this policy, contact:
Office of Cash and Debt Management
Mailstop 1599-001-1AE
1599 Clifton Road, 3rd Floor
Atlanta, GA 30322
paymentcardservices@emory.edu

Procedures Manual

1. Detailed Responsibilities

While Policy section VI.d lists core responsibilities for each Emory constituent, this section provides an exhaustive list of detailed responsibilities for the Office of Cash and Debt Management, the Office of Information Technology Information Security, IT Services Departments, University Technology Services, the Cash Operations Office, the Emory Clinic Finance Office, and Departmental Merchants.

a. The Office of Cash and Debt Management will:

- Comply with all relevant PCI DSS requirements.
- Establish, document, and distribute payment card processing and compliance policies and procedures.
- Provide a security awareness & training program to ensure that all employees handling cardholder data are knowledgeable of Emory's policies and procedures on the acceptance, processing, retention, disposal and security of cardholder data.
- Obtain and retain on file a signed Payment Card Merchant Compliance Statement from all employees handling cardholder data. This statement includes acknowledgement by the employee that he/or she has read and understood the Payment Card Processing and Compliance Policy and Procedures Manual.
- Perform an annual self-assessment of Emory's card processing activities across the enterprise in partnership with an independent compliance partner that is certified by the cardholder industry.
- Assist merchants with the completion and submission of all PCI DSS self-assessment questionnaires.
- Work with non-compliant merchants to implement appropriate remediation activities. Provide regular status updates to the University Vice President for Finance.
- Negotiate fee structures and agreements with third-party credit card processing vendors.
- Regularly monitor the payment card data environment and update policies and procedures to address changes, such as technological improvements.
- Verify that the information security policy includes an annual risk assessment process that identifies threats, vulnerabilities, and results in a formal risk assessment. This risk assessment will be reviewed, at a minimum, annually.
- Maintain a repository of merchant information, assessment, and remediation artifacts including completed self-assessment questionnaires, remediation plans, accurate depictions of the cardholder data environments, data flow diagrams, and a list of current merchants and key business and technical contacts.
- Maintain a list of authorized third-party credit card processing vendors and service providers with key business and technical contacts. For all service providers, a written agreement must be on file. This agreement must include: 1) acknowledgement by the service provider that it is responsible for the security of cardholder data processed through its system, and 2) documentation indicating that the service provider is PCI DSS compliant.
- Maintain and coordinate a unified PCI DSS change management process for all merchants that includes a cross functional review of all new payment card processing activities or significant changes to these activities including (but not limited to) any changes to cardholder data flows, vendors used for payment card processing, system or application upgrades/migrations, or any change that results or could result in a change in PCI DSS compliance status (from non-compliant to compliant or vice versa).

b. The Office of Information Technology (OIT) Information Security will:

- Comply with all relevant PCI DSS requirements.
- Maintain and disseminate IT security policies and procedures that address PCI DSS requirements.
- Assist the Office of Cash and Debt Management in completing the technical sections of the annual self-assessment questionnaire.

- Review logs, at least daily, for those servers that perform security functions like intrusion-detection system (IDS) and authentication, authorization, and accounting protocol servers.
- Establish, document, and distribute security incident response and escalation procedures to ensure timely and effective handling of all situations.
- Test, at least quarterly, for the presence of wireless access points by using a wireless analyzer or deploying a wireless IDS/IPS to identify all wireless devices in use.
- For public-facing web applications, address new threats and vulnerabilities on an ongoing basis and ensure these applications are protected against known attacks by reviewing public-facing web applications via manual or automated application vulnerability security assessment tools or methods, at least annually and after any changes.
- Perform external and internal penetration testing, at least annually and after any significant infrastructure or application upgrade or modification (such as an operating system upgrade, a sub network added to the environment, or a web server added to the environment).
- Run internal and external network vulnerability scans, at least quarterly and after any significant change in the network (such as new system component installations, changes in network topology, firewall rule modifications, or product upgrades).
- Test, at least annually, the security incident response plan.
- Coordinate standing quarterly meetings with IT Services Departments, University Technology Services, and Emory Healthcare Information Security.
- Have the authority to make final interpretations of technical PCI DSS requirements for Emory.
- Maintain and coordinate all relationships and engagements with Emory's Qualified Security Assessor(s) and Authorized Scanning Vendor(s).

c. IT Services Departments and University Technology Services (UTS)

There are specific responsibilities for securing and protecting cardholder data and the IT resources that process or transmit such information. These responsibilities are as follows:

IT Services Departments will:

- Comply with all relevant PCI DSS requirements.
- Manage all computer systems and other IT resources in a manner that complies with PCI DSS and Emory security requirements.
- Limit access to computing resources (e.g., computers, mobile devices) only to those individuals whose jobs require such access.
- Assist the Office of Cash and Debt Management in completing the technical sections of the annual self-assessment questionnaire.
- Remove and destroy electronically stored cardholder data. Notify the Office of Cash and Debt Management of the incident.
- Review logs, at least daily, for all system components. Log reviews must include those servers that perform security functions like intrusion-detection system and authentication, authorization, and accounting protocol servers.
- Retain audit trail history of payment card transactions for at least one year, with a minimum of three months immediately available for analysis (e.g., online, archived, or restorable from back-up).
- Deploy anti-virus software on all systems and ensure that anti-virus programs are capable of detecting, removing, and protecting against all known types of malicious software.
- Assign all employees a unique network ID before allowing them to access system components or cardholder data. User names and passwords may not be shared.
- Store media back-ups in a secure location and review the location's security at least annually. Classify the media so it can be identified as confidential. (Note: As a good business practice, back-ups should not be retained any longer than required.)
- For encryption of cardholder data, verify that key management procedures are implemented, at least annually, to require periodic cryptographic key changes.
- Test, at least annually, the security incident response plan.

- Disable and remove inactive user accounts at least every 90 days.
- Migrate all systems that process and/or transmit cardholder data to the PCI Core network, a dedicated and secure network created and maintained by UTS.
- Provide resources who can describe current technical processes and configurations to a sufficient degree to validate the compliance state of devices, systems, applications, and processes utilized in the storage, processing or transmission of cardholder data.

University Technology Services will:

- Comply with all relevant PCI DSS requirements.
- Establish firewall and router configuration standards to ensure that all systems are protected from unauthorized access. Configuration standards are to be reviewed in accordance with Emory's security policies.
- Limit access to network resources (e.g., network jacks, wireless access points, gateways) only to those individuals whose jobs require such access.
- Create and maintain the PCI Core network, a secure network dedicated for systems that process and/or transmit cardholder data.

d. The Cash Operations Office will:

- Comply with all relevant PCI DSS requirements.
- Assist University departments and Emory Hospitals with the submission of merchant account applications.
- Review and approve/deny merchant account applications.
- Administer merchant accounts, including additions, deletions and modifications.
- Maintain a list of authorized University and Emory Hospitals merchants and key operational and technical contact information for each merchant.
- Procure, log, and disseminate credit card terminals and other equipment to merchants.
- Maintain a registry of all card processing devices (e.g., swipe terminals, point-of-sale devices, vending systems) and all computer systems (e.g., workstations, kiosks, web servers, database servers) involved in the storage, processing, and/or transmission of cardholder data.
- Provide a registry of card processing devices and computer systems to the Office of Cash and Debt Management and OIT Information Security.
- Act as operations liaison to Emory's third-party payment card processor, First Data. Monitor and analyze security alerts and information from First Data and distribute these notifications to appropriate personnel.

e. The Emory Clinic Finance Office will**:**

- Comply with all relevant PCI DSS requirements.
- Assist Emory Clinic departments with the submission of merchant account applications.
- Review and approve/deny merchant account applications.
- Administer merchant accounts, including additions, deletions and modifications.
- Maintain a list of authorized Emory Clinic merchants and key operational and technical contact information for each merchant.
- Procure, log, and disseminate credit card terminals and other equipment to merchants.
- Maintain a registry of all card processing devices (e.g., swipe terminals, point-of-sale devices, vending systems) and all computer systems (e.g., workstations, kiosks, web servers, database servers) involved in the storage, processing, and/or transmission of cardholder data.
- Provide a registry of card processing devices and computer systems to the Office of Cash and Debt Management and OIT Information Security.
- Act as operations liaison to Emory Clinic's third-party payment card processors, First Data and Sage Payment Solutions. Monitor and analyze security alerts and information from First Data and Sage Payment Solutions and distribute these notifications to appropriate personnel.

f. Departmental Merchants

Within each department, there are specific responsibilities assigned to the departmental business manager, who is ultimately responsible for the merchant account, and the employees handling cardholder data. These responsibilities are as follows:

Departmental Business Manager will:

- Comply with all relevant PCI DSS requirements.
- Ensure that all business processes for accepting, processing, retaining, and disposing of cardholder data complies with this policy.
- Sign the Payment Card Merchant Application/Renewal which outlines merchant duties and responsibilities for which the departmental business manager is ultimately responsible.
- Identify positions that require access to payment card data and system components and limit access to only those employees whose job requires such access.
- Ensure that employees have reviewed and understand their responsibilities outlined in this policy and procedures manual and have been properly trained on departmental business processes for handling cardholder data.
- Ensure that employees have signed the Payment Card Merchant Compliance Statement, send a copy of the Compliance Statement for each employee to the Office of Cash and Debt Management, and retain a copy in the department.
- Notify the Office of Cash and Debt Management of all employee changes in positions that require the handling of and/or access to cardholder data.
- Perform an annual self-assessment in partnership with the Office of Cash and Debt Management.

Departmental Employees will:

- Comply with all relevant PCI DSS requirements.
- Sign the Payment Card Merchant Compliance Statement to document the employee's understanding of and compliance with this policy and procedures manual. A copy of the signed Compliance Statement must be sent to the Office of Cash and Debt Management, and another must be retained in the department.
- Attend a security awareness & training program to ensure that employee is knowledgeable of Emory's policies and procedures on the acceptance, processing, retention, disposal, and security of cardholder data.

2. Merchant Account Approval and Setup

Departments may accept and process credit/debit card payments via face-to-face, mail order, telephone order, and/or via an e-commerce website. In order to do so, a department must first have a merchant account. University departments and Emory Hospitals must request this account through the Cash Operations Office; Emory Clinic departments must request this account through The Emory Clinic Finance Office.

Departments cannot independently contract with third-party credit card processing vendors and services providers; all such contracts are handled by the Office of Cash and Debt Management. Further, centrally managed revenues, such as gifts and grants, are the responsibility of special central administrative units. No department may accept credit/debit card payments for gifts to Emory or grants from sponsors.

a. Merchant Account Application

For University Departments and Emory Hospitals:

The department must complete an online application to establish a merchant account. All applicants are required to complete a PCI DSS Environment Survey. This document identifies the merchant's scope of business applicable to PCI DSS.

The application is available on the Emory University Finance Division website:

- Go to the Emory University Finance Division website at www.finance.emory.edu.
- Under Cash & Debt tab, select Daily Cash Needs, then select Cash Operations.
- Under Cash Operations tab, select Credit Card Merchant Application/Renewal.
- Complete the application in its entirety. Print the application and have all concerned parties sign the application.
- Forward the application to the Cash Operations Office for processing (101 B. Jones Center).

The Cash Operations Office oversees the processing of all applications to create/modify/close merchant accounts with First Data. For more information, the Cash Operations Office can be reached via telephone, 404-727-6095, or email, student.financials@emory.edu.

The Cash Operations Office approves the application and then contacts First Data to set up a merchant account and issue a merchant ID for the department. Copies of all approved applications are forwarded to the Office of Cash and Debt Management. The Office of the Controller then loads the merchant's information in PeopleSoft Financials in order to automatically post payment card transactions to the merchant's chartfield string (Smartkey) and account. All merchants are required to renew their merchant account annually by submitting a renewal application.

For Emory Clinic Departments:
The department must complete an application to establish a merchant account. All applicants are required to complete a PCI DSS Environment. This document identifies the merchant's scope of business applicable to PCI DSS. The application is available through the Emory Clinic Finance Office.

The Emory Clinic Finance Office oversees the processing of all applications to create/modify/close merchant accounts with Sage. For more information, the Emory Clinic Finance Office can be reached via telephone, 404-788-4948, or email kathryn.turner@emoryhealthcare.org.

The Emory Clinic Finance Office approves the application and then contacts Sage to set up a merchant account and issue a merchant ID for the department. Copies of all approved applications are forwarded to the Office of Cash and Debt Management. The Emory Clinic Finance Office then loads the merchant's information in IDX and IRECON (the patient accounting and reconciliation systems).

b. Setting Up a Credit Card Terminal (Swipe) Account
In order to process credit/debit card payments via face-to-face, mail order, and/or telephone order, the merchant will need a credit card terminal (swipe machine).

For University Departments and Emory Hospitals:
Once the merchant application has been approved, the Cash Operations Office will order a credit card terminal to meet the merchant's needs, log the terminal, and then notify the merchant that the terminal is available for pick up. The merchant's Smartkey will be charged for all equipment costs. Only devices approved by the Cash Operations Office are permitted for use.

For Emory Clinic Departments:
Once the merchant application has been approved, the Emory Clinic Finance Office will provide a credit card terminal to meet the merchant's needs and log the terminal. The merchant must have a computer with a USB port in order to connect to the terminal. Also, a printer is needed in order to print related receipts from IDX. Only devices approved by the Emory Clinic Finance Office are permitted for use.

c. Setting Up an E-Commerce (Internet) Account

For University Departments and Emory Hospitals:
In order to process credit/debit card payments via the internet using e-commerce, the merchant must process all transactions through First Data. If a department believes that it has a significant business case or processing requirement that cannot be achieved using the services of First Data and wishes to utilize an alternate vendor, the department must specify this request in the Credit Card Merchant Application/Renewal form. If a department wishes to use an alternate vendor, the department must obtain written documentation from the vendor indicating PCI DSS compliance and that its platform is, at a minimum, a VISA-validated payment application. This documentation must be submitted to the Office of Cash and Debt Management for approval.

For existing e-commerce merchants, any significant changes to currently authorized processes must be approved by the Office of Cash and Debt Management prior to implementation. Such changes include, but are not limited to:

- departmental website,
- products or services for sale,
- intended customer base,
- anticipated transaction volume,
- outside advertising,
- application software, and/or
- departmental contacts responsible for the e-commerce account.

For Emory Clinic Departments:
E-Commerce accounts are not authorized for Emory Clinic Departments.

3. Merchant Account Fees

Merchants are responsible for all costs associated with payment card processing. These costs include, but are not limited to, merchant account setup & administrative fees, equipment purchases, recurring monthly costs, and fees based on a percentage of every transaction from each credit card brand.

4. Third-Party Vendors and Service Providers Operating on Emory's Campus

Third-party vendors and service providers operating on Emory's campus must process payment cards and handle cardholder data according to PCI DSS or use secure standard financial industry practices, if PCI DSS standards are not applicable. Emory reserves the right at any time to request either proof of PCI DSS compliance or a certification (from a recognized third-party IT audit and compliance firm) verifying that the vendor/service provider uses secure standard financial industry practices in its financial transactions.

5. Procedures for Handling Cardholder Data

Credit/debit cards may be accepted by departments for various purposes including patient payments, non-credit course tuitions and fees, and the sale of goods and services. The Office of Cash and Debt Management may revoke a department's ability to accept credit/debit card payments if the department violates any part of this policy and/or places Emory at risk. Contact the Office Cash and Debt Management with any questions regarding permitted transaction types.

Employees whose duties require handling of cardholder data should adhere to the following guidelines for the acceptance, processing, retention, and disposal of this information. Modifications to these guidelines may be appropriate depending on the occurrence and volume of transactions that a merchant processes.

a. Acceptance

- Verify signature of cardholder at the time of the transaction.
- Obtain the signature of the cardholder on the receipt and provide a duplicate copy to the cardholder.

- Match payment card's name and signature to cardholder's driver's license.
- Verify payment card's expiration date is valid.
- Verify that only the last four digits of the payment card number are printed on the receipt.
- If accepting cardholder data via a fax, locate fax machine in a secured, non-public area with limited access.
- Payment card charges should not exceed transaction amount of purchase.
- Do not accept cardholder data via end-user messaging technologies (e.g., e-mail, voicemail, instant messaging, and text messaging).

b. Processing

- Retain and secure merchant copies of receipts until end-of-day batch settlement.
- Compare each day's credit receipts to daily totals and then group them with the daily batch settlement tape for storage/reference.
- Record the daily batch settlement total and batch number for each day in a summary log. Maintain summary log for balancing and reconciliation purposes.
- Paper documents containing cardholder data must be processed within two business days of receipt then immediately disposed (see section 5c).

c. Retention and Disposal

Cardholder data cannot be retained/stored electronically or in paper form. The only exceptions are for solicitations by mail and events in which a credit card terminal or mobile device is unavailable for immediate processing. For both exceptions cardholder data may be received in paper form and must be kept in a secure, locked location. Payment must be processed within two business days of receipt, and then the paper form containing the cardholder data must be immediately disposed. To dispose of paper forms, cross-cut shred them or deposit them in a locked shred bin.

d. Disputes and Chargebacks

A chargeback occurs when a customer has disputed a credit/debit card transaction and the department has either not been able to supply documentation to substantiate the transaction or has not done so on a timely basis. By law the cardholder has two years to file a dispute. Once a cardholder files a dispute, the issuing bank makes an investigation into the complaint. If the transaction proves to be fraudulent, the bank will refund the original value to the cardholder. From the merchant's point of view, if the merchant does not prove the transaction to be legitimate, the bank will charge back to the merchant the entire value of the transaction along with an additional fee.

Procedures for handling disputes:

- When a customer disputes a transaction, the payment card processor sends a sales draft request to the Cash Operations Office.
- The Cash Operations Office forwards each request to the merchant for response. There is a limited amount of time for the merchant to respond, so promptness is critical.
- The merchant must send the required documentation of the transaction to the Cash Operations Office in response to the request and retain a copy of the submitted materials along with the sales draft request. The date when the materials were submitted should be documented.
- Merchants should periodically review their chargebacks to see if there are internal policies that need to be changed in order to minimize the number of chargebacks.
- Merchants experiencing frequent chargebacks or suspect fraud must contact the Cash Operations Office immediately.

For Emory Clinic merchants, the same procedures apply, but Emory Clinic merchants will work with the Emory Clinic Finance Office instead of the Cash Operations Office.

e. Annual PCI DSS Self-Assessment

In the fall the Office of Cash and Debt Management will contact each merchant to schedule a self-assessment. Each merchant must complete an annual self-assessment questionnaire to prove compliance with this policy, PCI DSS, and other applicable standards and policies. Merchants found not in compliance will work with the Office of Cash and Debt Management to implement appropriate remediation activities.

f. Response to a Security Breach

In the event of a breach or suspected breach of security, including the suspicion that payment card data has been exposed, lost, stolen, or misused, the merchant must immediately contact both the Office of Cash and Debt Management at 404-727-4621 or paymentcardservices@emory.edu and OIT Information Security at 404-727-6666 or security@emory.edu.

g. Alteration of Card Processing Environment

Any alteration of the card processing environment must receive prior written approval by the Office of Cash and Debt Management. Changes include but are not limited to:

- the use of existing merchant accounts for a purpose different from the one specified in the merchant application/renewal,
- the alteration of business processes that are not specifically addressed by this policy,
- the addition or alteration of payment card processing systems, technologies, or channels, and
- the addition or alteration of relationships with third-party payment card service providers.

h. Business Continuity Plan

In the event of a security breach or disaster, the payment card processing environment may be halted. Merchants must have in place a business continuity plan that addresses how the department will continue its operations under such adverse conditions. A copy of the plan must be made available to the Office of Cash and Debt Management. For merchants using an alternate third-party service provider, the merchant must be aware of its service provider's business continuity plan and also be able to provide that information to the Office of Cash and Debt Management.

6. Specifications and Procedures for Mobile Devices

Emerging technologies have made it easier to electronically process payment card transactions through the use of mobile online payment (MOP) applications, which can be downloaded and activated on an electronic mobile device (e.g., smart phone, iPad/Tablet, laptop). To ensure that these mobile devices comply with PCI DSS, the subsections below outline mobile device specifications and procedures.

a. Mobile Device Specifications

- The device and its online payment application software must be authorized by Emory's approved third-party credit card processing vendor. Only specific brands of mobile devices are acceptable and must be obtained through the Cash Operations Office.
- The device must be Emory-owned with an Emory-approved data plan.
- The device must be assigned to a specific merchant.
- The departmental business manager must maintain a log of the employees who have used the device. These employees must adhere to this policy in its entirety.
- Mobile devices must adhere to the following specifications:
  - The phone number associated with the device must be "private" or unlisted.
  - Have the ability to be remotely wiped or "killed" in the event of loss or theft.
  - Be password protected at all times.
  - Have encryption capabilities.
  - Utilize a secured internet connection through an Emory-approved data plan. Open (non-secure) wireless internet connections are not permitted.
  - Disable Bluetooth capabilities.
  - Disable automatic search and connect function to wireless networks.

- Online payment application software must adhere to the following specifications:
  - Require authentication and authorization (e.g., login and password).
  - If the online payment application requires an email address, the email address must be an Emory-issued email address, and the owner must be an Emory employee.
- When a mobile device is not being used for online payment processing, it must be powered off and stored in a secure, locked location.
- Prior to its use each time, the device must be checked for software updates in order to reduce vulnerabilities and enhance productivity.
- If it is suspected that a device may be compromised or infected, immediately stop using the device for online payment processing and immediately notify the departmental business manager and OIT Information Security. Be sure to document the reason for suspecting the device to be compromised or infected.

b. Lost or Stolen Mobile Device Procedures

In the event that a mobile device is lost or stolen, the owner of the device must do the following:

- Immediately contact his/her local IT Service department and request that the device be wiped or "killed".
- Notify the departmental business manager. The departmental business manager must notify his/her chief business officer, the Office of Cash and Debt Management, and OIT Information Security (see section 5f).
- The departmental business manager must document the loss/theft, including such details as: date, time, location, type of data on device, and device description (brand, model, and color).

EMORY

APPENDIX A

Payment Card Merchant Compliance Statement

As an Emory employee with responsibilities for handling payment cards and cardholder data, I recognize that I have access to sensitive and confidential information. I will strive to protect Emory and its customers at all times when making decisions concerning payment cards and cardholder data, and I agree with the following statements:

- I have read, understand, and agree to abide by Emory's Payment Card Processing and Compliance Policy and Procedures Manual.
- I will utilize cardholder data for Emory business purposes only.
- I will not use or distribute cardholder data for personal purposes. I understand that such actions are illegal and grounds for prosecution.
- I understand that in cases where I suspect a breach of security, including the suspicion that cardholder data has been exposed, lost, stolen, or misused, I must immediately contact both the Office of Cash and Debt Management and OIT Information Security.
- If I am a department manager, I understand that I must maintain effective business processes for accepting, processing, retaining, and disposing of cardholder data.
- I understand that failure to comply with this policy and/or applicable policies, standards, and procedures carries severe consequences, which may include loss of the ability to process payment card transactions and disciplinary action, which can include termination of employment.

Employee Name:		
Print Name	Signature	Date
Employee ID Number:	Department Number and Name:	
Department Manager Approver:		
Print Name	Signature	Date