Andrews University

Payment Card Acceptance

Policies & Procedures

Prepared by Financial Administration

July 12, 2011

Part I: Introduction of Policy and Purpose

Formatted: Font: 12 pt

In order to protect payment cardholders' data the Payment Card Industry has established Data Security Standards (PCI-DSS) for merchants processing credit card transactions. Compliance with PCI-DSS is required of all merchants that process, store, or transmit cardholder data.

This document outlines the policies and procedures adopted by Andrews University which govern all aspects of payment card processing.

This policy shall be reviewed at least annually and updated as needed to reflect changes to business objectives or the risk environment.

All Departments of the University which accept payment (credit) cards for payment of goods or services must comply with the policies and procedures outlined in this document. Failure to comply with this policy could result in the loss of the University ability accept credit card transactions for payment.

The most current version of this policy is available at the Financial Records web page or in the Office of the Controller.

Part II: Adherence to Standards

See ITS PCI Policy/Procedures for policies related to configuration standards for software applications, network components, critical servers, and wireless access points.

Part III: Handling of Cardholder Data

Definition of Credit Card Information or Cardholder data:

For the Purpose of the policy, Credit Card Information is defined as Cardholder number, expiration date, PIN, and the 3 or 4 digit number on the back of the card.

Policy Statement:

- All transactions that involve the transfer of credit card data must be performed on systems provided or approved by University Financial Administration and the CIO's office for that purpose.
- No credit card numbers or documentation containing credit card numbers or cardholder data shall be stored in any electronic form including personal computer, mobile device, network storage drive-on or off campus, email or any other end user messaging service.

Credit card data shall only be transmitted electronically in encrypted forms using ITS approved computer systems.

- Sites storing credit card information on paper must be approved by Financial Administration and must comply with all PCI-DSS standards for data card information storage. A list of approved sites is included in this document.
- No paper documents, including, but not limited to paper receipts and hand written notes, containing credit card numbers or cardholder data shall be stored by unapproved departments. Approved departments would be Financial Records, Student Financial Services, Childcare and the Airpark. They will store the data in a safe, secure and locked place (i.e. a safe).

Credit Card Information Security Procedures

Collection

- Collection of credit card information over the phone or through the mail is permitted, if all other procedures as set forth below are followed.
- Collection of credit card information through email or other end user messaging is not permitted. Should unsolicited credit card information be received via email, the email should be deleted immediately and the trash folder immediately emptied as well.
- Collection of credit card information using an electronic fax machine is discouraged, but permitted. The fax machine should be a non-networked machine hooked up only via a phone line and accessible only to department staff. No credit card information should be received through multi-purpose machine such as copier/scanner/printer/fax machines.

Storage

- **Electronic storage of credit card information is not permitted under any circumstances.**
- Temporary physical storage- Any document containing credit card information must be stored in a locked cabinet or file until no longer needed at which time it should be cross-cut shredded or transported to Financial Records.
- Permanent physical storage of credit card information in campus departments is not permitted except as approved by Financial Administration. Documents or forms used to collect credit card information for payment processing may be maintained in approved secured locations or in the Financial Records office for a maximum of 3 months. Then

these documents must be destroyed in their entirety via cross-cut shredding or incineration.

- Credit card information contained on documents or forms that are to be maintained must be physically removed (i.e. cut out or off) from the document within two business days.
- Any department wishing to store documents containing credit card information must maintain procedures for secure data retention and disposal, and be approved by Financial Administration.
- No scanning of documents containing cardholder information is permitted. Should a document need to be scanned which contains credit card information the cardholder information must be removed first.

Campus Departments Using Credit Card Terminals

- All Credit Card terminals shall be programmed so the credit card number is masked.
- Credit card terminal transactions shall be settled at the end of each business day.
- All credit card terminal receipts from the terminal's daily settlement along with any undestroyed credit card information shall be stored in a secured area until it can be transported to the Head Cashier in the Financial Records Department.
- The physical location of the credit card terminal must be accessible to authorized departmental staff only.

Campus Departments Not Using Credit Card Terminals

- All credit card information collected by a campus department for manual processing must be transported to the Head Cashier in the Financial Records Department within two business days for processing and storage.

Part IV: Access and Transportation of Cardholder data

- Access to credit card information should be limited to department employees on a "need-to-know" basis.
- Transportation of credit card information should be limited to employees who have regular access to the information, who have been properly trained and have a signed Employee Payment Card Security Statement on file.
- Fax-machines used in the receipt of credit card information must be located in a secure office and only be accessible to departmental staff authorized to access this information. (See previous statement about fax machines.)

Part V: Roles and Responsibilities

It is the responsibility of every employee of the University handling credit card information to be aware of the potential of fraud and theft of cardholder information and to do their part in protecting our customers from experiencing a loss due to the mishandling or misuse of their credit card information.

Each department that processes this type of data is required to designate a staff person who is responsible for the collection and proper handling of cardholder data. This individual will:

- Be required to attend University provided training on the appropriate handling of cardholder data. The employee will be required to sign a form indicating the time and date of training and the understanding of their responsibility.
- Be responsible for limiting access to this data by other employees and ensuring that employees who handle this data are trustworthy and know the proper policies and procedures for handling cardholder information.

In addition, Departments with credit card terminals are responsible for:

- Limiting access to the terminal to authorized personnel only.
- Monitoring the activity on the machine and reporting any suspicious activity immediately. See Incident Process Part VII.

The office of Financial Administration in conjunction with the office of the CIO is responsible for overseeing all aspects of information security, including but not limited to:

- Creating, maintaining and distributing security policy and procedures.
- Incident planning and response for incidents involving merchant terminals and non-electronic handling of credit card information.
- Training and awareness programs.

The CIO shall maintain daily administrative and technical operational security procedures that are consistent with the PCI-DSS including:

- Incident planning and response for incidents involving electronic handling of credit card information.
- Ensuring service providers comply with PCI-DSS requirements.

The Human Resource Office is responsible for tracking employee participation in the security awareness program including

- Facilitating participation upon hire and at least annually
- Ensuring that employees acknowledge in writing at least annually that they have read and understand the company's Payment Card Acceptance Policies and Procedures
- Screen potential employees prior to hire to minimize the risk of attacks from internal sources

Internal Audit is responsible for executing an annual risk assessment process that identifies threats, vulnerabilities, and results in a formal risk assessment as well as periodic audits of credit card processing areas

Part VI: New Electronic Credit Card Transaction Sites

Any department wishing to begin accepting credit card transactions electronically must either use the ATX interface provided by ITS or obtain approval by Financial Administration and ITS for use of other software system or third party hosting solution.

Part VII: Incident Process

Should a departmental employee obtain knowledge of or suspect theft or illegal use of credit card data, they should report the incident immediately to Ildiko Gyeresi or Esther Lonto in the Financial Records Department.

The Financial Records Department will then contact the University Merchant Bank and appropriate law enforcement and will work with them to notify the cardholder and limit losses.

See ITS Incident Process for reporting of suspected or confirmed security breaches at the ITS system level.