PCI Compliance and Payment Card Processing Policy

Policy Number:

Effective Date:

Approval:

Office:

PURPOSE:

The University of Indianapolis accepts payment cards on payment for goods and services under controlled conditions to protect against the exposure and possible theft of account and personal cardholder information that has been provided to the University, and to comply with Payment Card Industry (PCI) requirements which became effective June 30, 2005. The University must adhere to these standards in order to limit its liability and to continue to process payments using payment cards.

SCOPE:

This policy applies to all University of Indianapolis departments and affiliated units, employees, contractors, consultants, temporaries, and other workers. This policy is applicable to any unit that processes, transmits, or handles cardholder information in a physical or electronic format. All computers and electronic devices involved in processing payment card data, as well as manually obtained payment card information, are governed by the PCI Data Security Standard. This includes servers which store payment card numbers, workstations which are used to enter payment card information into a central system, any computers or credit/debit card devices through which the payment card information is transmitted, phone calls, fax, e-mail, instant message, chat, brochures and any documents which have Payment Card information listed.

REFERENCE DOCUMENTS/ RELATED INFORMATION:

The Employee Credit Card Security Agreement and the Credit Card Processing Request forms can be found at the end of this document.

POLICY HISTORY:

Policy Statement

All transactions that involve payment card information must be performed on systems approved by the Accounting Office and Information Technology (IT), and obtaining approval will require a compliance and security review. Any specialized servers that have been approved for this activity must be housed behind a University Data Center firewall and be administered in accordance with the requirements of this policy, and the PCI-DSS. Departments involved with the acceptance of and processing of payment cards for payment of goods and services must design adequate processes to ensure the following are maintained:

- Approval from the Accounting Office and Information Technology (IT) before entering into any contracts or purchases of software and/or equipment related to payment card processing. This requirement applies regardless of the transaction method or technology used (e-commerce or point-of-sale devices).
- Accounting verifies annually that the maintained list of service providers are still PCI compliant.
- Contractually require all third parties with access to cardholder data to adhere to PCI security requirements and provide evidence of PCI certification to Accounting.
- Departments must comply with the PCI Data Security Standards and this University Policy.
- Sensitive cardholder data (full account number, card type, expiration date, PIN, and card-validation code) should not be stored in any University system, personal computer, paper form, email account, instant message or chat.
- All documentation containing card account numbers must be stored in a secure environment until processed. Secure environments include locked drawers and safes, with limited access to only individuals who are processing the credit card transaction. Processing should be done as soon as possible and the credit card number should immediately be shredded.
- Credit card numbers must not be transmitted in an insecure manner, such as by e-mail, instant message, chat, unsecured or unmonitored fax, or through campus mail.
- Do not print the entire credit card number on either the department copy or customer copy of any receipt. Do not print the full credit card number under any circumstances.
- Old receipts, brochures, forms, etc., with the entire credit card number should be disposed of in a secure container, not a trash can.
- Credit Card Terminals must remain attached to a phone line (not Ethernet) or a cellular network (not on WiFi). To re-locate the device, IT must administer this change due to PCI server requirements.
- Credit card cashiering functions, meaning UIndy employees are entering the credit card and not a third-party organization, can only be processed on-campus with an IT and Accounting approved segregated network. This method is very limited.
- Credit Card terminal processors must accurately complete a monthly reconciliation worksheet, provided by Accounting, and submit it to Accounting via email by the third business day of each month.
- Background checks must be performed by Human Resources prior to the hiring of any positions with access to stored cardholder information.
- Credit card handlers and processors must not disclose or acquire any information concerning a cardholder’s account without the card holder's consent and follow all PCI standards. This includes not using vendor supplied default passwords.
- Require all personnel involved in credit card handling to attend card security training every year in conjunction with required PCI audits.
- All payment card handlers must complete the Payment Card Security Agreement and return to the Accounting Office.

- The Accounting Office will delete software access for terminated employees for third party vendors.
- Information Technology must contract with a third-party approved PCI vulnerability scanning vendor to perform quarterly network scans.

Procedures

All credit and debit card processing contracts and renewals, including web based payments, must be initiated and approved through the Accounting Office to assess the business purpose of the revenue, any related accounting issues and to oversee University credit card activity. Forms for initiating services are on the My UIndy-Accounting webpage. Upon reviewing the Credit Card Processing Request Form, Accounting will determine if a Credit Card terminal or a web entry program will be used.

University of Indianapolis' preferred credit card system is Touchnet, a web-based solution to execute credit card sales. If it is determined a department should use Touchnet, a specialized Store will be established and Touchnet will provide the secure payment gateway. The department will assign a store manager to create products that will link to the department's location on the UIndy website. Accounting will attach the proper General Ledger codes and provide instructions for store set-up. Each time a payment is made and fulfilled, the transaction will automatically post to our General Ledger system.

Some departments may need to accept credit or debit cards through a payment terminal. Accounting will obtain a Merchant Number, deliver the payment card and deliver any necessary training. Any fees associated with procurement or ongoing maintenance of the payment card system may be assessed to the department. If necessary and instructed by the Accounting Office, the department will reconcile monthly activity and send an Excel file to the Accounting Office by the third day of the month. If this is not completed in a timely and accurate manner, Accounting reserves the right to revoke this method of card processing.

The University has established the PCI Compliance Team to review all proposed business plans involving credit card sales over the Internet. The committee includes representatives for the Accounting Office, Information Technology and the Student Business Office.

- The PCI Compliance Team will review each proposal to accept payment cards for intended business purpose, consistency with the University's policies, and the departments' ability to support an E-commerce activity.
- Following review and approval, the Accounting Office will notify the requesting department of approval status.
- The development of Touchnet Marketplace products will be vested by departments.

Failure to comply with this policy may result in the loss of payment card privileges. Additionally, fines may be imposed by the affected credit card company, typically in excess of $50,000 for the first violation. Some violations may constitute criminal offenses under local, state, and federal laws. The University will carry out its responsibility to report such violations to the appropriate authorities.

Employee Credit Card Security Agreement

Questions about this form – Contact the Accounting Office at (317) 788-3399

I confirm that acting as an employee or agent of the University of Indianapolis, I will keep in strictest confidence all the credit card information to which I have access in a manner in accordance with the PCI Data Security Standards and the University of Indianapolis Credit Card Processing Policy.

I understand that access to credit card information requires the highest degree of public trust to protect the University and the cardholders.

I understand that it shall be a breach of security standards for any employee of the University or third party with access to credit cardholder's personal information to divulge either directly or indirectly, any cardholder information except on a need-to-know basis. Accordingly, I agree not to release any personal or privileged information of any type without proper authorization from an appropriate supervisor.

I will strive to protect the University and cardholders at all times when making decisions concerning credit cards and cardholder information.

I understand that all credit card information received verbally, in paper format or via phone, will be destroyed after processing.

I certify that I have read the University of Indianapolis Credit Card Processing Policy and will abide by its guidelines.

I understand that failure to comply with this agreement may result in criminal and/or disciplinary action, up to and including termination.

Full Name: ____

Employee ID: ____

Department Name: ____

Daytime Phone #: ____

____

Signature   Date

____

Supervisor's Signature   Date

Please print this form. Once completed return the form to Accounting, Esch Hall, Room 151

Credit Card Processing Request Form

This form must be completed and returned to the Accounting Office in order to be processed. For every store requested, a separate form must be completed. All credit card fees associated with this store will be booked to the same index as the revenue.

Step 1 – General Set-up	
Date:	Name:
Contact Phone Number:	Department:
E-mail Address:	
New Store Name:	
Store Manager(s):	
Index & Acct. Revenue will be deposited (if more than one account is used, proceed to Step 2; otherwise go to Step 3):	

Step 2 – Additional Accounting Codes. Complete Columns 2 & 3 (additional space on Page 2)		
Detail Code (for Accounting use only)	Index & Acct. Revenue will be deposited:	Description

Step 3 – General Description of New Store

Store Manager Signature: ____

Department Head Signature: ____

Accounting Office Signature: ____

Step 2 – Additional Accounting Codes. Complete Columns 2 & 3 (additional space on Page 2)		
Detail Code (for Accounting use only)	Index & Acct. Revenue will be deposited:	Description