Department PCI Self-Assessment Questionnaire

Version 1.1

2009

Attestation of Compliance

Instructions for Submission

This *Department PCI Self-Assessment Questionnaire* has been developed as an assessment tool intended to assist departments in self-evaluating their compliance with Payment Card Industry Data Security Standard (PCI DSS). PCI DSS is a worldwide security standard that was developed by credit card companies (Visa, Master Card, etc) to help organizations that process card payments prevent credit card fraud, hacking and various other security vulnerabilities and threats. The standards apply to all organizations that store, process or transmit cardholder data. Since credit cards are used for payments in the University, Hofstra must be in compliance with these industry standards.

University departments that process credit card payments must complete this self assessment questionnaire and return to Mr. Sean Cover (ext: 3-6348), Assistant Treasurer, by July 6, 2009.

Departments that are in compliance with PCI standards should complete this questionnaire and include local management signoff. If a department is not in compliance, please return the completed form unsigned and the Hofstra University PCI Compliance Committee will assist the department in complying with PCI standards.

Department Information

Dept Name:			
Contact Name:		Title:	
Telephone:		Date:	

Vendor

Does your department use a third-party vendor for processing credit card payments?

TouchNet ☐ Yes ☐ No

Other vendor: ☐ Yes ☐ No Please provide vendor name:

Part 1. Processing Information

Please indicate how your department accepts / processes cardholder information (**select all that apply**).

Payment Process Type	(Select One) YES	(Select One) NO	If yes, please indicate number of units (e.g., 4 card swipe terminals, 2 fax machines, etc)
1.1 Using a credit card swipe terminal	☐	☐	
1.2 Via telephone (with information written on paper)	☐	☐	
1.3 Via fax	☐	☐	
1.4 On paper (Via mail or in person)	☐	☐	
1.5 Via email	☐	☐	

Payment Process Type	(Select One) YES	NO	If yes, please indicate number of units (e.g., 4 card swipe terminals, 2 fax machines, etc)
1.6 Using software on a PC	☐	☐	
1.7 Via a web site	☐	☐	
1.8 Paper forms are brought from another office	☐	☐	

Part 2. Protecting Cardholder Data

Please confirm that your department is appropriately protecting cardholder data in compliance with PCI standards.

		Confirm Compliance		
	Statement	**YES**	**NO**	**Please provide details if not in compliance**
2.1	The department does not store the full contents from the magnetic stripe taken from the back of a credit card or anywhere elsewhere. *<u>Note:</u> In the normal course of business, the following data elements from the magnetic stripe may need to be retained:* • *Accountholder's name* • *Primary account number (PAN)* • *Expiration date* • *Service code.* *To minimize risk, store only those data elements needed for business.*	**Yes – the department is in compliance** and does not store this information ☐	No – the department is not in compliance ☐	
2.2	The department does not store the card-validation code or value (three-digit or four-digit number printed on the front or back of a payment card) used to verify card-not-present transactions.	**Yes – the department is in compliance** and does not store this information ☐	No – the department is not in compliance ☐	
2.3	The department does not store the personal identification number (PIN) or the encrypted PIN block. ***<u>Note:</u>*** *Hofstra University does not allow payments in the form of Debit Cards with an associated PIN block.*	**Yes – the department is in compliance** and does not store this information ☐	No – the department is not in compliance ☐	

		Confirm Compliance		
	Statement	**YES**	**NO**	**Please provide details if not in compliance**
2.4	The primary account number (PAN) is masked when displayed. Specifically, only the first six and last four digits are the maximum number of digits that are displayed. *Note: This requirement does not apply to employees and other parties with a specific need to see the full PAN; nor does the requirement supersede stricter requirements in place for displays of cardholder data (for example, for point-of-sale [POS] receipts).*	**Yes – the department is in Compliance** ☐	No – the department is not in compliance ☐	

Part 3. Restricting Access to Cardholder Data

Please confirm that your department is appropriately restricting access to cardholder data in compliance with PCI standards.

		Confirm Compliance		
	Question	**YES**	**NO**	**Please provide details if not in compliance (e.g., "N/A" - not applicable)**
3.1	Is access to computing resources and cardholder information limited to only those individuals whose **jobs require such access?**	☐	☐	
3.2	Are all paper and electronic media that contain cardholder data physically secure? *(Such media includes computers, electronic media, networking and communications hardware, telecommunication lines, paper receipts, paper reports, and faxes.)*	☐	☐	
3.3	Is strict control maintained over the internal or external distribution of any kind of media that contains cardholder data?	☐	☐	
3.4	Is media managed and controlled by University staff classified so it can be identified as confidential? For example, ensure folders/envelopes that contain cardholder data are marked "confidential" before they are sent to other departments to facilitate appropriately handling by staff members.	☐	☐	
3.5	If media is sent outside an area (e.g., off campus), is the media sent by secured courier or other delivery method that can be accurately tracked?	☐	☐	
3.6	Are processes and procedures in place to ensure management approval is obtained prior to moving any and all media from a secured area (especially when media is distributed to individuals)?	☐	☐	
3.7	Is strict control maintained over the storage and accessibility of media that contains cardholder data?	☐	☐	

		Confirm Compliance		
	Question	**YES**	**NO**	**Please provide details if not in compliance (e.g., "N/A" - not applicable)**
3.8	Is media containing cardholder data destroyed when it is no longer needed for business or legal reasons?	☐	☐	
3.9	Are hardcopy materials **cross-cut shredded**, incinerated, or pulped?	☐	☐	

Part 4. Security Policy

Please confirm that your department is aware of the security policies related to credit card security.

		Confirm Compliance		
	Statement	**YES**	**NO**	**Please provide details if not in compliance (e.g., "N/A" - not applicable)**
4.1	Please confirm that your department is aware that the University has a security policy that is established, published, maintained and disseminated.	☐	☐	
4.2	Please confirm that your department is aware of the policies, procedures, and practices in place to preclude the sending of unencrypted cardholder data by electronic mail (e.g., instant messaging, chat, email, etc).	☐	☐	
4.3	Please confirm that your department is aware that security policy is reviewed on an annual basis and updates are made when environments change.	☐	☐	
4.4	Please confirm that your department is aware of usage policies that are developed to define proper use of computers for all employees and contractors.	☐	☐	
4.5	Please confirm that your department is aware of security incident response and escalation procedures to ensure timely and effective handling of all situations.	☐	☐	
4.6	Please confirm that your department is aware that all employees must understand the importance of properly protecting cardholder data (i.e., security awareness).	☐	☐	

Part 5. Business Operations

Please answer the following questions regarding your department's credit card operations.

	Questions	(Select One)		Additional Comments
		YES	NO	Please provide details (e.g., "N/A" - not applicable)
5.1	Are internal records well organized, and can past transactions be readily identified and source documents effectively retrieved?	☐	☐	
5.2	Does the unit have a training program for new staff, or staff accepting new payment processing responsibilities?	☐	☐	
5.3	Does the unit have a **secure** fax machine available to which transmissions with cardholder information can be directed? (Not a fax server)	☐	☐	
5.4	Does the unit understand that it is prohibited to store cardholder data in any electronic form whatsoever without first obtaining the approval of the Office of Financial Affairs?	☐	☐	
5.5	Does the department understand that they must respond to and report any and all incidents to the Office of Financial Affairs that might entail cardholder data, whether that data is on paper or in electronic form?	☐	☐	
5.6	Are refund transactions properly controlled and approved by senior management before funds are returned to the payee (dual controls on disbursements)?	☐	☐	
5.7	Are refund transactions properly documented and accounted for?	☐	☐	
5.8	Are refunds on credit cards credited only to the original card which was used for the purchase of goods or services?	☐	☐	
5.9	Does the unit respond timely to chargeback / disputed items? Are faxed chargeback notices promptly processed or forwarded to the unit?	☐	☐	

Important Note

All individuals that process credit card information should read the PCI Data Security Standard (DSS), which are industry requirements for the safe handling of sensitive information. The standard provides a framework for developing an effective data security process - including preventing, detecting and reacting to security incidents. The updated version of the standard (DSS v1.2 replaced v1.1 on October 1, 2008) is available on the PCI Security Standards Council web site (www.pcisecuritystandards.org).

Confirmation of Compliant Status

	After the questionnaire has been completed, please confirm compliance status (select all that apply).
Yes ☐	The Department PCI DSS Self-Assessment was completed according to the instructions therein.
Yes ☐	All information within the above-referenced questionnaire and in this attestation fairly represents the results of my assessment.
Yes ☐	I recognize that the department must maintain full PCI DSS compliance at all times
Yes ☐	No evidence of magnetic stripe (i.e., track) data[1], CAV2, CVC2, CID, or CVV2 data[2], or PIN data[3] storage after transaction authorization was found on ANY systems reviewed during this assessment.
NO – Department is not in compliance ☐	The Department is not in compliance with PCI Standards. We will require assistance from the Hofstra PCI Compliance Committee.

[1] Data encoded in the magnetic stripe used for authorization during a card-present transaction. Entities may not retain full magnetic-stripe data after transaction authorization. The only elements of track data that may be retained are account number, expiration date, and name.

[2] The three- or four-digit value printed on or to the right of the signature panel or on the face of a payment card used to verify card-not-present transactions.

[3] Personal Identification Number entered by cardholder during a card-present transaction, and/or encrypted PIN block present within the transaction message.

Confirmation Signatures

After all parts of this questionnaire are completed - please **save and print** this document.

Once printed – If the department is in compliance with all parts, please sign below

If the department is <u>not in compliance</u>, please return the completed form unsigned and the Hofstra PCI Compliance Committee will help your department comply with PCI standards.

Signature of Area Supervisor: _____

Print Name: _____

Date: _____

Signature of Vice President: _____

Print Name: _____

Date: _____