ACCEPTING PAYMENT CARD ASSESSMENT

Pre-Selection Questionnaire

Overview

This pre-implementation questionnaire is designed to provide the Boston College Internal Audit Department with a general understanding of a potential vendor's control environment when accepting and processing payment cards as a form of payment. This document applies to any University process that accepts payment cards as a form of payment, and must be completed prior to implementation. Please work with your vendor, ITS resources, and Internal Audit to complete all listed questions as thoroughly as possible.

To accept payment card payments and have a new system be implemented, the university department is required to follow specific security rules/standards (Payment Card Industry Data Security Standards –PCI DSS) instituted by Mastercard and Visa. These rules are designed to prevent abuse of the data and protect the consumer from some forms of identify theft. Failure to follow these requirements can involve severe penalties, including fines to the University. All payment card merchants must be compliant with Payment Card Industry Data Security Standards – PCI DSS.

(Note: There are several university approved methods to accept payment cards, please check with Cash Services and FMS prior to completing this questionnaire to discuss which approach would be best for you.)

Please complete the following general information and send it back to the Internal Audit department, audit@bc.edu for review.

Document	Responsible Party	Comments/Notes
Questionnaire Section A	Requesting Department & Potential Vendor	
Questionnaire Section B	Potential Vendor	

ACCEPTING PAYMENT CARD PAYMENT ASSESSMENT

Questionnaire Section A – General Information

Party to complete this section: Requesting Department & Potential Vendor

General Vendor Information – Part a	
Vendor Name & Contact Name/Title:	
Telephone:	
Email Address:	
Business Address:	
General BC Contact Information – Part b	
BC Business Owner Contact Name, Email, Phone #:	
BC ITS Contact Name, if it is applicable:	
Payment application name/version number	
Estimated Projected Implementation Date:	
Business Background Information – Part c	
Please provide a financial justification for implementing the new payment application to accept payment cards.	
Please provide a description of the new system.	
Please provide desired implementation schedule. This should include deliverable, schedules for the potential system.	
Please list all sensitive data that resides on the system. For example: ☐ Social Security numbers ☐ Credit Card numbers ☐ Bank Information ☐ Personal Info -Name, Address, DOB, Telephone # ☐ Personal Financial Info ☐ Health Information ☐ Student Information (FERPA) ☐ Salary ☐ Other, please describe	

Please provide a copy of the Written Comprehensive Information Security Program (WISP) documentation that illustrates MASS 201 CRM 17.00 is in compliance. For more information, refer to: http://www.mass.gov/ocabr/docs/idtheft/201cmr1700reg.pdf and http://www.mass.gov/ocabr/docs/idtheft/compliance-checklist.pdf	
Please provide a copy of formally documented privacy policy.	
Please provide certification of PCI-DSS confirmation of compliant status.	
Do you conduct regular SAS70 Type II/SSAE 16 SOC2/SOC3 or similar third party audits?	
If the system will be hosted by BC, please list all web, database, and application servers.	
Will the vendor sign the Privacy & Security Addendum? If the system is remotely hosted, or the vendor maintains remote access, then the addendum must be signed.	
Has the vendor been aware of any security incidents that affect their system? If so, please provide detail.	
Has the application architecture been documented to illustrate all process flow? Please provide data flow diagram between web servers, application servers, database servers, and network systems.	
Does a Business Continuity Plan and Disaster Recovery Plan exist to protect payment card holder data?	
Who is responsible for security administration (adding & deleting users) to the server?	
Will the vendor provide operating guidance to BC in order to continue PCI compliance effort due to certain parameters of the PCI compliance are sole responsibility of BC?	

Questionnaire Section B – Information System Review

Party to complete this section: Potential Vendor

Network General Information – Part a	System Under Review
Please provide in detail whether a formal firewall and router configuration standards are in place to protect cardholder data environment. Are firewall rules being reviewed regularly? Are firewall logs being monitored?	
Please describe the wireless environment at the company and how cardholder data is being protected.	
Do you have documented information security baselines for every component of your infrastructure (ex. Hypervisors, operating systems, routers, DNS servers, etc.)?	
Has the Intrusion Detection been installed on the host network? If so, please describe in detail.	
Please describe controls in place to prevent unauthorized access to the server over public network	
If the payment application is accessed via web browser, please describe in detail the security of these web browsers.	
Explain how the data is protected in transit over the Internet.	
Do you conduct network penetration tests of your cloud service infrastructure regularly as prescribed by industry best	

practices and guidance?	
Is there a process for incident management? If so, please describe in detail.	
If the system is hosted at BC, does the vendor require remote access to it? If so, please describe it.	
Privacy General Information – Part b	**System Under Review**
Please describe in detail of data retention and disposal policy and procedures.	
Please describe controls in place to prevent from unauthorized downloading of payment card information.	
Please describe the process of protecting removable media.	
Please describe in detail the process of encryption transmission of cardholder data. For example, 1) is HTTPS being used? 2) Is a strong encryption method being used to protect sensitive cardholder data? If so, please describe the encryption schemes that are being used?	
IT General Control Information – Part c **(Note: this section should be completed if the system is not hosted within BC environment)**	**System Under Review**
Please provide a copy of the formal Information Security Policy.	
Please describe the System Development Life Cycle Process.	
Please describe the change management process and procedures that are followed.	
Please describe controls in place to enforce proper segregation of duties.	

Is a code review process in place prior to release to production? Please describe it.	
Is production data, such as live Primary Account Number, being used in the testing environment? If so, please describe the process of data cleaning. Do developers have access to sensitive and confidential data in a test environment?	
Please describe the methods used to protect hacking activities, such as SQL Injection, cross-site scripting, packet sniffing, denial of services, etc.?	
Please describe the user provisioning process (i.e. adding/deleting/modifying user access).	
Please describe the process of managing privileged administrator access (application, network, operating system, and database levels).	
Are periodic user access reviews being performed?	
Please describe physical and environmental controls of the data center where the servers are hosted.	
Please describe the process governing contractors or third party vendor access.	
Please describe the password configuration settings.	
Please describe controls in place to manage shared, generic, or group accounts and passwords.	
Is there an automated audit trail process to monitor	

cardholder data? Is it being periodically reviewed? Who has access to the audit log?	
Please describe the backup process and offsite rotation.	

Questionnaire is completed by: _____ **Department/Vendor**:_____**Date of Completion**: _____