



Payment Card Merchant Application Form

Date of Request: _____

Department/Organization Name: (Merchant Name) _____

Faculty/Admin Unit: _____

Location of Terminal(s): _____

Contact name for merchant: _____

Contact telephone number: _____

Business Manager of Faculty/Admin Unit: _____

Type of revenue: (eg. Conference fee, T-shirts sales) _____

Is revenue type subject to GST: [radio] Yes [radio] No

Is revenue type subject to PST: [radio] Yes [radio] No

Payment types requested: [checkbox] Visa [checkbox] MasterCard [checkbox] Interac

Annual Volume: \$ _____ \$ _____ \$ _____

Average Transaction Amount: \$ _____ \$ _____ \$ _____

FOAP for Deposits: (Must be Revenue Account)

FOP for merchant fees: (RCGA to use appropriate account code) XXXXXX

Is a third party system being used to collect payment data [radio] Yes [radio] No

If yes: 1. what is the name of the vendor/software: _____

2. A certificate from the vendor confirming that the software is Payment Application Data Security Standard (PA-DSS) compliant is required prior to go-live.

Is the link to Beanstream from a website? [radio] Yes [radio] No [radio] N/A

If yes, what is the URL?

The merchant contact and unit business manager, as employees of the University of Manitoba, acknowledge the following statements:

I have reviewed the following documents, available from the Financial Services website as indicated:

Payment Card Industry Data Security Standards (PCI DSS) FAQ:

[http://umanitoba.ca/admin/financial_services/media/PCI_DSS_FAQ\(4\).pdf](http://umanitoba.ca/admin/financial_services/media/PCI_DSS_FAQ(4).pdf)

Recommended Best Practices for Credit Card processing:

[http://umanitoba.ca/admin/financial_services/media/recommended_best_practice\(2\).pdf](http://umanitoba.ca/admin/financial_services/media/recommended_best_practice(2).pdf)

University of Manitoba Cash Control Policy and Procedures:

http://www.umanitoba.ca/admin/governance/governing_documents/financial/389.html

I understand how this information relates to payment card merchants and will comply with the guidelines and regulations as set out.

I also understand that any breach of security must be reported immediately in accordance with the Recommended Best Practices document and may result in the suspension of my merchant account(s).

Merchant Contact Signature _____
Date

Business Manager Signature _____
Date

Reset Form

Mail completed form to:

Revenue, Capital and General Accounting office room 315 Administration Building

ORIGINAL SIGNATURES ARE REQUIRED.

FOR OFFICE USE ONLY

Date request was received from Unit:	_____			
Date request sent to TD:	_____			
Date of response from TD:	_____			
New 3rd party payment application?	<input type="checkbox"/> Yes	<input type="checkbox"/> No		
If yes, has a PA-DSS Certification been supplied? (copy must be on file)	<input type="checkbox"/> Yes	<input type="checkbox"/> No		
Merchant type:	<input type="checkbox"/> POS	<input type="checkbox"/> Beanstream	<input type="checkbox"/> MR	
Merchant account number(s)	_____			
	TD Visa:	_____		
	Beanstream:	_____		
Term of use:	<input type="checkbox"/> Conference	<input type="checkbox"/> Continual		
Info to merchant:	CC Fraud, Card Security Features, TD Merchant Guide, PCI FAQ, New Merchant FAQ			
Go Live Date:	_____			