UNIVERSITY OF FLORIDA
TREASURY MANAGEMENT – PAYMENT CARD OPERATIONS
E-COMMERCE APPLICATION FOR CREDIT CARD TRANSACTIONS

Requesting Department Name:	

Contact Information:

Contact Name:	
Street Address:	
City:	
Phone Number:	
Email:	

Planned Business Processes:

The applicable (departmental) web page from where customers are redirected to third party vendor's credit card processing site will be:

Website URL: http://	

Desired Type of Implementation (please mark your solution of choice):

	IPay (preferred University payment gateway)
	CASHNet eMarket Module
	Eventbrite
	Other: ………………………………………………………………………

Provide reasons – if applicable - why any of the University's approved web payment solutions would not be suitable in your particular situation:

Please list the services or types of products you will be selling by means of E-Commerce:

Please describe your potential customers:

Transaction Estimates per Month:			
Number of Transactions:		Revenue $:	

Will anyone in your department have access to cardholder data?

Yes		No	

If applicable, how do you plan to secure the storage, processing, transmission, backup and destruction of collected cardholder data?

All funds must be deposited into a University of Florida account. The following chart field string for revenue as well as processing and other fees applies:

Dept ID	Fund	Program	Account	Source	Flex	Project

Certifications (please initial): I understand that……

I am responsible for the security and safeguarding of cardholder information as required by the Payment Card Industry Data Security Standard (PCI-DSS) and all applicable UF policies.	
Any E-Commerce implementation may only go live once all pertinent approvals have been obtained by the Controller's Office.	
As an E-Commerce merchant, there are fees associated with the acceptance of credit and debit card processed transactions. All incurred fees, including fees regarding PCI compliance efforts, will be charged to my department's account.	
All staff involved in the E-Commerce process described herein are completing the annual training requirements at hire and annually thereafter.	
Any third party vendor must provide proof of PCI-DSS compliance.	
We are not permitted to sell advertisements on our departmental webpage. (Requirements can be found at https://marcom.ufl.edu)	
Payment Card Operations as well as the Privacy Office need to be notified immediately upon a suspected data breach.	
Cardholder information is not permitted to be entered into any UF-owned device, and therefore customers cannot be directed to any such device for payment processing.	

I confirm that I have read and familiarized myself with (please initial):

University of Florida Credit Card Standards: http://www.fa.ufl.edu/directive-categories/credit-card-operations/	

Signatures:

_____   _____

Signature of Department Head or Director   Date

_____

Printed name of Department Head or Director

Please complete this form and submit to:

Treasury Management, Payment Card Operations
PO Box 112008, S113 Criser Hall

Email: Treasury-CreditCards@ad.ufl.edu
Phone: (352) 392-9057

For Internal Use Only:

Who is Merchant of Record? (Attach blank Merchant Agreement)				
Does Merchant Agreement include language to satisfy PCI DSS 12.8.2. (see explanation below**)		Yes		No
Is Service Provider/Third Party Vendor PCI compliant? (Please attach current Attestation of Compliance)		Yes		No
Is implementation PA-DSS listed?		Yes		No
Is a completed risk assessment on File with UFIT Security?		Yes		No

_____   _____   ☐   Approved
Finance & Accounting E-Commerce Committee   Date   ☐   Not Approved