Florida State University
Office of the University Controller

Student Financial Services
1500 University Center A
Tallahassee, FL 32306-2394
Ph: (850) 644-9452 Fax: (850) 644-5142

Merchant Questionnaire

Purpose: To comply with PCI DSS, https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml regulations and FSU policies toward payment cardholder information security and to centralize information for FSU compliance requirements.

Instructions: Fill out the questionnaire as best as possible (**one form for each Merchant Account**). If you need more space for comments use the additional sheet(s) at the end of this form. Be sure to sign the questionnaire and return to the contact person listed below at Student Financial Services.

Contact: For assistance or questions, please contact Curt Caito, FSU Credit Card Manager at 850/644-9475 (ccaito@fsu.edu) or Jill St. Angelo at 850/644-1551.

Merchant:		Supervisor:	
Location:		Phone:	
Mail Code:		E-mail:	

Enter the corresponding merchant numbers in the boxes below. Is the merchant agreement on hand? (Yes/No)		
Visa/MC:		No
AMEX:		No
Discover:		No

Give a brief description of your payment card business. Describe how and in what capacity do you process, transmit and/or store cardholder data:

(use additional sheet at the end of questionnaire if you need more space to answer)

Equipment	Terminal	Pin Pad	Other	Other
Model #				
Serial #				

Terminal Connection:		Phone #:	
IP Address:		Firewall:	

Florida State University
Office of the University Controller

Student Financial Services
1500 University Center A
Tallahassee, FL 32306-2394
Ph: (850) 644-9452 Fax: (850) 644-5142

1. Do you know what is in the Merchant Agreement?

2. Do you have the instructions on how to operate the card terminal?

3. Do you educate employees on practices for accepting and processing credit cards, closing out daily credit card batches, the totals with the point-of-sale, as well as on common types of credit card fraud, how to counteract them, on common merchant mistakes and how to avoid them?

4. Do you perform background checks for employees who process payment cards prior to hire or re-assignment of duties?

5. Do you require employees to acknowledge at least annually that they have read and understood policies and procedures on processing payment cards, confidentiality agreement, security, passwords, etc?

6. Did you know that the following five card types are the only ones accepted for FSU on campus merchants: Visa, MasterCard, American Express, Discover, and the FSU Card?

7. Do you use the Address Verification Service (AVS) or the Card Verfication Value (CV2) for identity verification? (3 digit number on back of card next to signature).

8. Do you audit transactions and settle batches daily?

9. Are you aggressively avoiding chargebacks? How?

(use additional sheet at the end of questionnaire if you need more space to answer)

10. Are there other campus entities that use this Merchant Account?

11. Do you have the ability to process payment cards if normal modes of processing are down?

12. Are employees who process payment cards aware of the Emergency Contact Plan (and trained) in case the system has been breached/compromised?

Florida State University
Office of the University Controller

Student Financial Services
1500 University Center A
Tallahassee, FL 32306-2394
Ph: (850) 644-9452 Fax: (850) 644-5142

13. Do you test the Emergency Contact Plan at least annually?	
14. Do you limit the number of employees who process payment cards to appropriate people based on their job duties?	
15. Are there departmental written policies and procedures for processing payment cards and training employees?	
16. Are account numbers truncated on the receipt (e.g. last four digits only)?	
17. Do you take every measure possible to prevent duplicate transactions?	
18. Do you keep the Controller's Office aware of any changes in your credit card program?	
19. Are default security settings, accounts, and passwords changed on production systems before taking the system into production?	
20. Is it prohibited to store the full contents of any track from the magnetic stripe (on the back of the card, in a chip, etc.) in the database, log files, or POS products?	
21. Is it prohibited to store the card-validation code (3 digit value printed on the signature panel of a card) in the database, log files, or POS products?	
22. Is transmission of cardholder data and other sensitive information across public networks encrypted using SSL or other industry acceptable methods?	
23. Do you store cardholder info (hard copy/electronic)? Explain how and why.	

(use additional sheet at the end of questionnaire if you need more space to answer)

24. If yes to #23, is hard-copy cardholder data stored in a locked cabinet in a locked room and protected against unauthorized access?	
25. Do you cross-cut shred documents that are to be destroyed?	

Florida State University
Office of the University Controller

Student Financial Services
1500 University Center A
Tallahassee, FL 32306-2394
Ph: (850) 644-9452 Fax: (850) 644-5142

26. Do you mark "confidential" when archiving records?	
27. Is there an anti-virus scanner installed on all servers and all workstations and is the virus scanner regularly updated?	
28. Is access to payment cardholder information restricted for users on a need to know basis?	
29. Are all payment processing equipment (terminals, jacks, etc.), secured and restricted from public access?	
30. Is a unique user ID assigned to each person with access to credit card processing?	
31. Are passwords for credit card terminals being changed every 90 days?	
32. When an employee leaves your department, is his/her access to payment card processing immediately revoked?	
33. Are user accounts reviewed on a regular basis to determine their appropriateness?	

34. Complete this section only if you process payment cards over the web and/or use 3rd party processors or gateways (e.g. PayPal, Paciolan, Authorize.Net)	Company:	Contact:	Phone:

35. Do you have a written agreement that includes an acknowledgement that any service providers you may use are responsible for the security of cardholder data?	
36. Has the service provider supplied you with a certificate of PCI DSS Compliance and do you annually monitor their compliance?	
37. Are development, testing, and production systems updated with the latest security-related patches released by the vendors?	
38. Are controls implemented on the server side to prevent SQL injection and other bypassing of client side-input controls?	
39. Are unused services/applications on servers completely disabled/removed from all production environments, for security, increased system performance, and to improve system stability -- e.g., for carrying out database, FTP, email, or web-hosting related tasks?	

Florida State University
Office of the University Controller

Student Financial Services
1500 University Center A
Tallahassee, FL 32306-2394
Ph: (850) 644-9452 Fax: (850) 644-5142

Statement

Florida State University is committed to meeting or exceeding the Payment Card Industry Data Security Standards (PCI DSS). The need for stronger policies and procedures on data security has never been greater. The threat from hackers and people who willingly engage in credit card fraud is real and growing. The PCI has set stricter standards and has imposed heavy fines for security breaches of cardholder information.

FSU is rising to the challenge of ensuring security for people who use payment cards for tuition, purchases, etc. However, this challenge depends on the entire community here at FSU. The effort cannot be successful unless we have the cooperation from all the merchants.

The information we are requesting is an important part of our effort. Each year we are required to review the status of all of our merchants. The purpose of this questionnaire is to be able to centralize information for our compliance requirements. It is essential that this form be completed to the best of your ability. Please do not hesitate to seek assistance if you are unsure what is asked of you.

Note: Notification for any changes in your payment card program (including closing your account) must be submitted 30 days prior to the change. Requests to add an online merchant account must be submitted at least 90 days in advance with the appropriate completed paperwork.

Attestation Statement

I attest that the information in this questionnaire has been completed truthfully and as accurately as possible. I have read the above statement. I understand the intent of this questionnaire and that the information I have provided is vital to the successful implementation of Florida State University's Payment Card Policies and Procedures as well as the Payment Card Industry Data Security Standards (PCI DSS). If I had any questions as to the content and meaning of the requested information, I made every effort to contact the appropriate personnel to seek clarification.

Authorized FSU Merchant Representative

_____ _____
Signature ***Date***

_____ _____
Print Name ***Title***

Florida State University
Office of the University Controller

Student Financial Services
1500 University Center A
Tallahassee, FL 32306-2394
Ph: (850) 644-9452 Fax: (850) 644-5142

Question #	Additional Comments