Departmental Procedures for Accepting Payment Cards

Departments that have received approval to accept card payments must adopt the below departmental procedures or create and maintain their own. All departmental procedures must be submitted to the Finance Office prior to accepting card payments and then annually.

Name: _____ **Date:** _____

Department: _____

☐ The department indicated above will create and maintain separate departmental procedures for accepting card payments and submit those procedures to the Finance Office annually.

☐ The department indicated above will adopt the below procedures and submit the procedures to the Finance Office annually.

The _____ department will use the following methods to accept payment cards.

☐ Online through a Market Place Store
☐ Online through an affiliated Market Place platform (T2)
☐ Another online platform as described below

_____

☐ In-Person Point of Sale machine issued by College
☐ Another In-Person method as described below

_____

The amount of payment card devices (i.e. point-of-sale machines) the _____ department has is _____.

Farmingdale State College
State University of New York
Farmingdale State College
2350 Broadhollow Road
Farmingdale, New York 11735
934-420-2000
farmingdale.edu

The Payment Card Processing Environment Access

The processing environment includes; processing a payment card transaction by means of a payment card device, referring customers to make online payments, virtual access to online platforms utilized for processing transactions, and the physical access to payment card devices and other related documentation. Only those authorized by the department head are permitted to process card payments.

The _____ department will limit access to accepting card payments, the processing environment, and cardholder data to only those employees with a business need. The processing environment includes physical and virtual access to workstations, storage areas, and online platforms where card payments are processed, and devices and related documents are stored.

The department head will immediately notify the Finance Office if an employee's access to the processing environment needs to be changed or removed (i.e. due to separation from the College or transfer on campus).

The following student employees have access to the payment card processing environment as part of their job function.

The following professional employees have access to the payment card processing environment as part of their job function.

Related Entities

Related entities may utilize PCI-DSS compliant third-parties for payment card services. The third-party platforms and its connection to the College's network will be reviewed and approved by Information Technology prior to use to ensure compliance with PCI-DSS. Agreement and/or contract language will include language to ensure the service provider is PCI compliant and a copy of the agreement/contract will be submitted to the Finance Office. The department head will obtain the Annual Attestation of Compliance (AOC) from the third-party and submit it to the Finance Office annually.

PCI-DSS Training

The department head, _____ will ensure all employees with access to the processing environment will be given the College's Payment Card Policy, will have a business need, and will complete PCI-DSS training provided by the PCI Committee upon hire and annually.

Processing Online Transactions
Only online platforms approved by the Finance Office will be utilized to accept and process card payments. All authorized employees will receive access to the online platform from the Finance Office or third-party.

The ☐ department will be given a link which will redirect customers to make a payment. This link will be used in the following manners:

☐ Department's web page ☐ In email communications from the department

☐ Other means as described below

☐

Departmental employees will direct customers to pay online on a device of their choosing. Employees will not direct customers to a specific computer. Employees must not make a payment on behalf of a customer, that is, not enter a customer's credit card number on a website for a payment or donation.

Processing In-Person Transactions
Only College issued point of sale devices will be used to accept payment cards to ensure PCI-DSS compliance.

The department head will maintain a list of all devices, their corresponding serial numbers, and employees authorized to use them.

The payment card device(s) in this department will be used:

☐ daily ☐ weekly ☐ monthly ☐ only during events/activities

☐ other, as described below

☐

Below is a description of where the payment card device is located when in use and measures taken to safeguard it while in use.

☐

Devices should be kept in a secure location when not in use. Below is a description of where the payment card device(s) is stored when not in use and measures taken to safeguard it while not in use.

Payment cards with a Chip must be processed using the Chip Reader. If the Chip does not work, the card number may not be entered directly in the device. The customer must use a different card or another method of payment.

Someone other than the cardholder may not authorize payment and picture ID is required if the card is not signed.

Employees must provide the customer with a receipt of the payment card transaction.

Transaction documentation and merchant receipt should be stored in a secure (locked) area. This department will store such documentation in:

Credit card terminal passwords must be kept in a secure location and should never be displayed.

Below is a description of how and where payment card transaction documentation (physical paper documents), including merchant receipts, will be processed and stored.

Closing Out the Credit Card Batch

At the end of each day/shift, the department will reconcile and close out the credit card batch for payment card devices. The department will complete the Student Accounts *Off-Site Revenue Report* or third-party procedures. Receipts must be stapled to the Off-Site Revenue Report and brought to Student Accounts daily.

For business continuity purposes, departments are encouraged to document any additional procedures related to card payments (i.e. accounting processes) that may not be included in this document.

Prohibited Transaction Methods
Insecure transmission of cardholder data is prohibited. Under no circumstances will payment card data be accepted or transmitted through the following insecure methods; email, fax, electronic messaging, over the phone, or through the mail. If payment card information is sent in these manners identify steps to delete or dispose of the cardholder data as soon as possible.

If payment card data is received via email, the department will respond with the below template response or similar message.

"Thank you for your recent communication regarding payment for *item or event*. For your protection, we cannot accept credit card information via email. Email is an insecure means of transmitting information and you should never use it to send your credit card number or other sensitive personal information (passwords, Social Security Number, etc.). Please visit *website if available* to complete the transaction. Thank you."

Security Incident Reporting
The department head is responsible for reviewing the FSC Credit Card Incident Response Plan and contacting an Incident Response Team member in the event of suspected tampering or substitution of a Point-of-Sale device or computer belonging to the payment card processing environment, or suspected loss or theft documents or files containing cardholder data.

Farmingdale State College Credit Card Security Incident Response Team

Justina Geremia	934-420-5365	justina.geremia@farmingdale.edu
Jeff Borah	934-420-2661	jeff.borah@farmingdale.edu
Margaret Steinhauer	934-420-5246	margarget.steinhauer@farmingdale.edu
Keri Franklin	934-420-2424	keri.franklin@farmingdale.edu
Dorothy Hughes	934-420-2166	dorothy.hughes@farmingdale.edu

PCI Compliance Form
On an annual basis the department head will submit a PCI compliance form including the following information

- A listing of staff who process payment card transactions, have access to cardholder data, and those with access to the processing environment
- Acknowledgement that all appropriate staff have completed PCI-DSS training
- Indicate methods of collecting card payments
- Submit department specific procedures for collecting and processing card payments and cardholder data
- Submit PCI Device Inspection Logs, if applicable
- Attest that cardholder data is not being stored in any manner
- Attestation of Compliance for Third Parties, if applicable
- Other information necessary to assist the PCI Committee in completing the Self-Assessment Questionnaire (SAQ)