Merchant Checklist

Payment Card Industry
Data Security Standard (PCI DSS)
PCI DSS Version 3.2
Campus Merchant Requirements

Campus merchants have responsibilities to the UGA Credit Card committee in order for the University to maintain PCI compliance.

Below references a list of items that are to be completed and provided by the designated point of contact for each merchant to the PCI Committee on an annual basis.

- Self-Assessment Question (SAQ)- CampusGuard Portal
- Maintain inventory of all devices, workstations, laptops used for inputting cardholder data.
  - Make/Model
  - Serial Number
  - Description of Use/Purpose
- Maintain daily Inspection Logs of all Payment Card Processing Equipment
- Maintain list of all software/websites/applications used for payment card acceptance in your department.
- Payment Card Handling/Authorization Data Flow Diagram
- Departmental Payment Card Procedures (to include incident response procedures, procedures for physical security of POS devices, etc.)
- Listing of all staff involved with accepting or handling payment cards.
- Documented training of all staff members upon hire, and annually thereafter- see PEP UGA PCI Training Course
- Documented staff acknowledgements of Payment Card Security Policy- see also PEP UGA PCI Training Course
- Annual Service Provider compliance review- work with Bursar’s office

CampusGuard provides templates to assist in document creation. You can find these templates and other useful information in the CampusGuard Portal in the Library section.