Date of Las Revision: September 2024
Responsible Department: Information Technology

Policy Statement

Annual Merchant Checklist

Payment Card Industry
Data Security Standard (PCI DSS)
PCI DSS Version 4.0

Campus Merchant Requirements

Campus merchants have responsibilities to ensure that the institution maintains PCI DSS compliance.

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

- □ Merchant Survey*
- □ Self-Assessment Questionnaire(s) (SAQs)
- □ Maintain inventory of all devices/terminals, workstations, and software used to interact with payment card data*
  a. Make/Model
  b. Serial Number (for payment terminals)
  c. Location
  d. Description of Use/Purpose
- □ Maintain Inspection Logs of all Payment Card Processing Equipment* (best practice recommendation)
- □ Payment Card Handling/Authorization Data Flow Diagram (best practice recommendation for most merchants)
- □ Departmental Payment Card Procedures (to include incident response procedures, procedures for physical security of POS devices, etc.)
- □ Listing of all staff who interact with payment cards (best practice recommendation)
- □ Documented training of all staff members upon hire, and annually thereafter
- □ Documented staff acknowledgements of Payment Card Security Policy (best practice recommendation for most merchants)
- □ Annual Third-Party Service Provider (TPSP) compliance review (coordinate with your PCI Team), to include:
  a. Current Attestation of Compliance (AOC) for all TPSPs
  b. Responsibility Matrix for all TPSPs