Policy: Use and Storage of Credit Card Data in the Division of Student Affairs

Purpose:

To provide a Division of Student Affairs policy regulating how credit card information is recorded, processed, transmitted and stored. The policy is written in compliance with the Payment Card Industry Data Security Standard (PCI-DSS) and Penn State information privacy and security policies.

Policy:

In order to meet the requirements of the PCI-DSS, all credit card transactions within the Division of Student Affairs will adhere to the following:

A. Credit Card Processing Equipment
   - All equipment used to process credit card transactions will be approved by Student Affairs Information Technology (SAIT) and adhere to industry standards. Staff in SAIT will maintain regular communications with Penn State’s Security Operations and Services (SOS) Office to ensure that the Division’s processing of credit card purchases remains adherent to evolving Penn State policies.
   - Records of the model, serial number and location of the equipment used for the PCI equipment will be maintained as a part of SAIT’s asset management system.
   - Credit card transactions will only be processed by staff who meet the following requirements and with supervisory review:
     i. Charged with have a job responsibility, which requires access to sensitive credit card information, and must be trained on the PCI-DSS policy.
     ii. Required to change their PSU Access Account password every ninety days.
        a. SAIT and the Finance department will maintain a list of employees who process credit cards at each station. No other employee will be allowed to access these workstations or device.
     iii. Staff having access to the workstation or device must be reviewed every ninety days.
     iv. Supervisors or the Director of the department will notify SAIT when there is a need to change, add or delete staff.
     v. If ePay terminals are being used, SAIT will notify AIS of any staff changes.

B. Receipts and records
   - Unless otherwise required for a business purpose, credit card receipts should only contain the last 4 digits of the credit card number.
   - If it is necessary for the receipts to contain the entire credit card number, the following conditions must be met for storage and disposal.
     i. The processing area must have an adequate storage facility and the numbers must be stored in that area.
ii. Only authorized staff can handle and process the receipts.

iii. The receipts must be stored in one of the following ways:
   a. In a locked safe
   b. A filing cabinet equipped with a supplemental security bar.
      (Storing these records in a standard filing cabinet or a locked desk is not sufficient.)

C. Offsite storage
   • Records Retention has been approved for UHS by PSU IPAS as a compliant storage location and should be used for all storage offsite.
   • If other areas believe that there is a need for office-site storage, they are required to request an exemption from the Privacy Office.

D. Disposal
   • Disposal of receipts should be by cross-cut shredding
   • If a number must be copied for later entry because of machine malfunction, the written document must be stored in a safe lockable location. Once recorded, dispose as above.
   • Electronic storage of credit card number is prohibited in any form.

E. Enforcement:
   • Any employee found to have violated this policy may be subject to serious disciplinary action by the Division of Student Affairs, and or the University

This policy is subject to the approval of the Vice President for Student Affairs.

Approval:

Damon Sims
Vice President for Student Affairs

Date