Austin Peay State University
PCI Compliance Standard

Overview and Purpose

This standard has been created to assist employees in understanding the importance of protecting card holder data and informing employees about rules surrounding safeguarding information. The Payment Card Industry (PCI) was formed by the five major card brands (Visa, MasterCard, American Express, Discover and JBC International). This group established a standard set of guidelines around the handling of card holder data by merchants. These guidelines make up the Payment Card Industry Data Security Standard (PCI DSS) and provide merchants with rules for physical, application and network security, as well as security policy management, which merchants are required to implement and follow. Penalties are enforced for violators.

Merchant Accounts

Austin Peay State University is considered a merchant because it accepts payment by credit card for specific services or products. As such, the University is required to follow the standards established by the Payment Card Industry. A Merchant Account is a relationship between the University and the University's bank account. The University has two Merchant Accounts – one dedicated to TouchNet and online payments; the other dedicated to individual machines that are on POTS lines. The Controller must approve all new merchant accounts and Student Account Services should be contacted when problems or questions occur. Additionally, Student Account Services staff will provide training to employees and others who have access to credit card information and card terminals.

Who is Impacted by this Standard

All employees or other designated individuals that collect, maintain or have access to credit card information or University terminals must comply with the PCI Compliance Standard. Others who do not have access but accidently gain access must immediately report that information to his or her supervisor, to the Information Technology Security Director and to the Bursar.

Third party vendors

The University uses a third party vendor to collect payments who may accept credit cards. This third party vendor is TouchNet Information Systems.

Employees do not have access to credit card information from the third party vendor and the third party vendor approved to collect payments on behalf of the University must provide PCI DSS Certificate of Compliance yearly. Please notify the Bursar if your office plans to use a vendor other than TouchNet to collect payments for Austin Peay State University which is directly or indirectly recorded into the University's general ledger.

Access to POS (point of sale) or Card Swipe Terminals and Credit Card Information

Only employees authorized and who have a business purpose may have access to process credit card payments. Those individuals with access must read and sign the PCI Compliance Statement Form. An

original (or copy) of the signed form must be sent to the Bursar in the Student Account Services. All card terminals must be kept in a secured area during business hours. After business hours, terminals need to be settled and transmitted to the bank, unplugged and stored in a secured locked area.

Credit Card Processing

Cards may be accepted by phone, fax, in person or by mail. Any payments by credit card related to a student's account can be processed by the student or their designee through Onestop.apsu.edu. These payments are processed through the third party vendor and Austin Peay State University employees do not have access to any credit card information from this vendor.

If cards are accepted in person, the card must be swiped through the machine and not manually keyed in. If the card is received by phone, fax or mail, once the authorization for the charge is received any paper copies of card holder information must be shredded immediately. Cardholder information must be kept in a secured locked location and only employees with a business need to know may have access to the stored receipts. If a debit card is presented the individual should key in his or her security PIN number instead of running debit cards through as a credit. Under no circumstances should the payer provide the PIN number to the person processing the card information.

NO card information may be received via email. Email is not a secured transmission method. If an email is received, do not process the payment. Immediately respond to the sender that the payment cannot be processed with an email request. Be sure that you do not include the card number in your reply and once you have responded, delete the original email that contained the card information.

Only card terminals are allowed for processing credit cards. Manual credit card machines that make an imprint of the credit card are not allowed. The full card number must not print on the receipt that is given to the card holder or kept by the University. Only the last 4 digits may appear.

Employees are not allowed to log card holder information into a computer or keep the information in a paper log. Again, receiving or recording of PIN numbers is forbidden.

Training

New employees that have access to card holder information must receive training from the Bursar or their designee before being allowed to have access. Annual training will be done for all individuals having access to card holder information and terminals. All individuals who will or have access must read and sign the PCI Compliance Statement Form.

PCI Network Infrastructure

The university maintains three environments for the acceptance of credit card information by university staff. The first environment is in Student Account Services at the university cashier's computers. The computers used to accept credit cards are segmented into a secure VLAN with the only access available to computers being the third party payment vendor (Touchnet), as well as access to the university's DNS, monitoring, vulnerability scanning, and end point protection services. No other access is allowed.

The second environment is in the University Advancement phone-a-thon room in the Clement building. The computers used to accept credit cards are segmented into a secure VLAN with the only access available to computers being the third party payment vendor (Touchnet), the phone-a-thon software

service (Wilson-Bennet), as well as access to the university's DNS, monitoring, vulnerability scanning, and end point protection services. No other access is allowed.

The second environment consists of various locations across the university utilizing card terminals that are on dedicated POTS lines, and as such, are not on the university's VoIP network.

Incident Response Plan

All employees are responsible to report any incident of theft, damage, fraud, etc. The following University policies provide information regarding protection of information, fraud, theft, misuse, etc:

4:031 Identify Theft Prevention

4:040 Personally Identifiable Information

4:041 Safeguarding Nonpublic Financial Information

1:016 Preventing and Reporting Fraud, Waste, or Abuse

All policies can be found at the following link: http://www.apsu.edu/policy/

Employees should be familiar with these policies. If you believe that an incident has occurred, please notify your immediate supervisor, security and the Bursar in Student Account Services. If you are unable to contact the Bursar, you may notify the University Controller or the Office of Legal Affairs or Vice President for Finance and Administration. Any questions to this policy may be addressed to the Controller or the Bursar.