Pacific University – PCI Compliance Policy

Overview and Purpose

This policy has been created to assist employees in understanding the importance of protecting card holder data and informing employees about the new 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 Account

Pacific University is considered a merchant because it accepts payment by credit card for specific services or products. As such, the University is required to following the standards established by the Payment Card Industry. A Merchant Account is a relationship between the University and the University's bank account. The Controller must approve all new merchant accounts and the Business Office should be contacted when problems or questions occur. Additionally, Business Office staff will provide training to employees and others who have access to credit card information and card terminals.

Who is Impacted

All employees or other designated individuals that collect, maintain or have access to credit card information or University terminals must comply with the PCI policy. Others who do not have access but accidently gain access must immediately report that information to his or her supervisor, to security and to the Accounts Receivable Manager.

Third party vendors

The University uses third party vendors to collect payments who may accept credit cards. These third party vendors include:

- TouchNet
- CollegeNet
- Common App
- Greater Giving

Employees do not have access to credit card information from third party vendors and all third party vendors approved to collect payments on behalf of the University must provide PCI DSS Certificate of Compliance. Please notify the Controller if your office uses vendors not mentioned above to collect payments for Pacific 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 Accounts Receivable Manager in the Business Office. 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. The Business Office does not accept credit cards for payment on a student account which includes tuition, fees, room and board and other miscellaneous charges. Any payments by credit card related to a student's account must be processed by the student or their designee through Boxer Online. These payments are processed through a third party vendor and Pacific University employees do not have access to any credit card information from this vendor.

For payments other than student account charges, if cards are accepted in person, the card should 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. If there is a reason to retain the information, it can only be retained for a maximum of 120 days, and you must notify the Accounts Receivable Manager if you are doing this. 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 Accounts Receivable Manager 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.

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:

- Red Flag Rules/Identity Theft Policy
- Financial Information Security Plan
- Financial Irregularity Policy

All policies can be found at the following link: www.pacificu.edu/offices/bo/stafffaculty/index.cfm

Employees should be familiar with these policies. If you believe that an incident has occurred, please notify your immediate supervisor, security and the Accounts Receivable Manager in the Business Office. If you are unable to contact the Accounts Receivable Manager, 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 Accounts Receivable Manager.