E-Business Resource Group Guidelines

Introduction

Payment Card Industry (PCI) Data Security Standards (DSS) compliance is required of all merchants and service providers that store, process, or transmit cardholder data. The University is responsible to make certain that its merchant locations and any third party vendors associated with those locations adhere to PCI DSS. The E-Business Resources Group (EBRG) will assist departments to comply with the requirements of the Payment Card Handling and Acceptance Policy 05-11-02, and the guidelines listed below.

Process

Any University department or group that desires to accept payment cards must follow the steps provided below. Additional details about PCI compliance and this process can be found on the EBRG website (ebusiness.pitt.edu).

1. Submit a project proposal and merchant account application approved by the appropriate Responsibility Center head. An outline for a brief proposal is on the EBRG website located at http://www.cfo.pitt.edu/ebusiness/ . The proposal and the merchant account application form must be signed by your Responsibility Center Head.
2. Any third-party payment solutions, software or equipment that will be used to process payments must be explicitly approved by the EBRG.
3. If a University website is to be built or an existing one modified to permit acceptance of payment cards, it must be located on the University's Enterprise Web Infrastructure (EWI) servers. Please have your IT person review that aspect with Computing Services and Systems Development (CSSD) and confirm that will be the case.
4. If no website is to be built or if your process will collect payment card information while at various events, we recommend use of any approved terminals that can be easily supplied by the University's merchant bank. Contact the EBRG for information about those products.
5. Any proposed vendor(s) will be required to complete a security questionnaire [add hyperlink] provided by the EBRG to ensure appropriate security is in place.
6. Any contracts or purchased services that are involved for this project must be vetted by Purchasing Services and the Office of General Counsel and must contain language requiring vendor's compliance with PCI DSS.
7. Final approval from the EBRG must be received before the Office of Finance will establish a merchant account. The Office of Finance will contact our merchant bank to establish the merchant account only when all of the above noted items are completed or confirmed. The process of opening a merchant account can take as long as 10 business days to complete.

8. Allow 8 to 12 weeks to complete this entire process. The process time can be shortened by using payment solutions, software or equipment that has been pre-approved.
9. Note: the EBRG must also conduct a formal review when you are changing technology, renewing or modifying a contract.

Control and Reporting

All departments or units are required to:

1. Restrict access to payment cardholder data to those employees who have completed internal training or PCI training as provided by the University. Those employees must demonstrate a comprehensive understanding of the security requirements for processing payment card holder information and the department will maintain formal documentation of this compliance.
2. Demonstrate employees handling payment cardholder data have been sufficiently screened, which must include background checks.
3. Review (and update as needed) existing departmental operational procedures and policies to ensure that they demonstrate compliance with the University's Customer Information Security Plan (CISP), these EBRG Guidelines and PCI DSS. Departmental procedures and policies to review should include those addressing employee training and selection, transaction processing methods, refund policies, reconciling procedures, notification of potential breaches, and compliance with other related University policies (such as, University policies and procedures related to computing, information and data security as well as, General Accounting Guidelines for Transacting Credit Card Payments.
4. Segregate employee duties among payment processing, refund processing, and reconciliation of revenue to the extent possible. Each Department or Unit must notify the Office of Finance immediately of any changes to staff handling payment card data.
5. Secure any computer or handheld device processing payment cardholder information (see University of Pittsburgh Payment Card Industry Technology Guidelines). Machines left unattended must be locked or logged-off. Payment card processing devices should never be left unattended in an area where customers or visitors may have access to the device.
6. When notified, ensure that all security enhancements to payment card processing systems are completed as required by the PCI DSS. All merchant vendor supplied security updates must be applied to systems as soon as possible but in any event no later than within 30 business days of issue date.
7. Provide all information requested for reporting and audits.
8. All proposed merchant account applications will be approved by the Department or Unit responsibility center head before being submitted to the Office of Finance.
9. Prepare annually the Self-Assessment Questionnaire (SAQ) as required by the PCI DSS using account or technical information as may be provided by the EBRG and CSSD.

ANY EMPLOYEE SUSPECTING LOSS OR THEFT OF ANY MATERIALS CONTAINING PAYMENT CARDHOLDER INFORMATON MUST IMMEDIATELY NOTIFY THEIR SUPERVISOR AND DEPARTMENT HEAD, WHO MUST THEN IMMEDIATELY NOTIFY CSSD, IF THE PROBLEM INVOLVES COMPUTER SECURITY, THE DESIGNATED CUSTOMER SECURITY INFORMATION OFFICER, AND THE UNIVERSITY POLICE.

Related Information and References

The following documents are incorporated by reference into this guideline:

1. PCI Data Security Standards
   https://www.pcisecuritystandards.org/security_standards/index.php
2. Payment Card Handling and Acceptance Policy 05-11-02
   add link when available
3. University of Pittsburgh Policies and Procedures related to Support Services – Computing, Information, and Data such as the following examples:
   a. 10-02-04 – Computer Data Administration
      http://www.cfo.pitt.edu/policies/policy/10/10-02-04.html
   b. 10-02-05 – Computer Access and Use
      http://www.cfo.pitt.edu/policies/policy/10/10-02-05.html
   c. 10-02-06 – University Administrative Computer Data Security and Privacy
      http://www.cfo.pitt.edu/policies/policy/10/10-02-06.html
4. University of Pittsburgh Payment Card Industry Technology Guidelines
   http://ebusiness.pitt.edu/documents/Payment_Card_Industry_Technology_Guidelines.pdf
5. University of Pittsburgh Customer Information Security Plan (CISP)
   http://www.provost.pitt.edu/documents/Information_Security_Plan.pdf
6. University of Pittsburgh Record Retention Requirements
   http://www.cfo.pitt.edu/frs/FinancialRecordRetentionSchedule.html
7. University of Pittsburgh General Accounting Guidelines for Transacting Credit Card Payments
   http://www.cfo.pitt.edu/ga/credcard.html