Payment Card Acceptance

Category: Financial Affairs
Responsible Department: Treasurer
Responsible Officer: Treasurer
Effective Date: 1/10/2017

Policy Summary

This policy explains the requirements for obtaining and maintaining the ability to process payment card transactions for the benefit of a university department, and it assists with the compliance of mandated payment card standards, university contractual obligations and university policies and procedures.

Scope

This policy affects the following groups of the University:

- Budget Mangers

This policy applies to all university business and budget managers, their supervisors, or designees that currently process or seek to process payment cards.

Policy

Overview:

DePaul University processes hundreds of millions of dollars from payments cards each fiscal year. The university's Access to and Responsible Use of Data policy categorizes payment card data as "Highly Sensitive," meaning that users of this data must have proper access authorization and the data must be secured with the highest possible levels of protection. The Information Security Policy requires that a payment card data security breach must be reported immediately to DePaul's Director of Information Security using the e-mail security@depaul.edu.

The Payment Card Industry Security Standards Council and the university's payment card processor require the university to comply with the Payment Card Industry Data Security Standard (PCI-DSS). PCI-DSS is an information security standard for organizations that process cardholder information for major debit, credit, prepaid, automated teller machine (ATM), and Point of Sale (POS) cards.

The Treasurer's Office and Information Security are responsible for coordinating the annual PCI-DSS attestation and for determining if technologies a department employs are PCI-DSS compliant.

The Treasurer's Office also provides guidance to departments on the creation of business procedures to minimize the risk of payment card theft and fraud.

Purpose:
This policy and the accompanying procedures have been designed to achieve the appropriate level of security of the university's payment card data and to achieve annual PCI-DSS compliance. This will be accomplished by requiring university departments processing payment cards to:

1. Create and utilize departmental procedures for safeguarding, monitoring and reporting on payment card transactions.
2. Provide the Treasurer's Office contact information of person(s) within the department responsible for payment card processing.
3. Annually complete a PCI-DSS questionnaire and attest in writing to their department's PCI-DSS compliance if the department's method of payment card processing is applicable to PCI-DSS.
4. Proactively inform the Treasurer's Office if the department wants to accept payment cards or modify the method payment card data is processed in their department.
5. Comply with other relevant university policies.

Procedures

All university departments must comply with the following:

1. Written payment card processing procedures, reporting and contact information requirements:

    a. University departments processing payment card data must have in place written procedures which document the processing and reconciliation of payment card receipts in their area as well as outlining how payment card data is protected. The Treasurer's Office will provide guidance in the creation of the departmental procedures and may request a copy of the procedures, if needed, for PCI-DSS compliance.

    b. Appropriate chartfield(s) must be provided to the Treasurer's Office upon request twice each month in order for Financial Accounting to correctly and timely book all payment card transactions. Chartfields must be provided to the Treasurer's Office no later than the second business day at the beginning of each month and the second business day after the middle of the month.

    c. Departments must comply with all requests for information by the Treasurer's Office or Information Security in a timely manner and must immediately report any suspicious or unusual payment card activity to the Treasurer's Office at paymentcard@depaul.edu and data security breaches to Information Security at security@depaul.edu. Members of the DePaul community can also report fraud by following the procedures detailed in the university's Reporting Misconduct policy.

    d. Departments must also supply the Treasurer's Office with appropriate and up-to-date contact information of individuals responsible for monitoring payment card information. This person is typically the business manager and/or budget manager. This contact information will be utilized by The Treasurer's Office for:

- The timely reporting of service outages experienced by DePaul's primary payment card processor,
- Investigating the occurrence of fraud and security breaches, and
- Informing departments about new industry standards, data security tips and other relevant payment card processing information.

e. Departments processing payment cards as a special deposit receipt at the Loop or Lincoln Park Payment Centers must follow the guidelines attached as an appendix to this policy.

2. Annually attesting to PCI-DSS compliance

a. On or around August 1 the Treasurer's Office and Information Security will notify qualifying departments that must complete the PCI-DSS compliance process.

b. On or before December 1 qualifying departments must complete the annual PCI-DSS questionnaire and attest to their PCI-DSS compliance.

3. Implementation or modification of payment card processes

A department desiring to implement or modify the method of payment card acceptance must:

a. Contact the Treasurer's Office to describe the purpose and supporting business processes for initiating or changing the payment card payment method to determine if a university-wide solution is available to meet the business need.

b. Use vendor software solutions, technologies and devices that are pre-approved by the Treasurer's Office and Information Security. If a department identifies vendor software, a technology or a device that does not fall within current university approved offerings, that department must meet with the Treasurer's Office and the Information Security team to review the new solution for approval. Vendor software, technologies and devices not approved by the Treasurer's Office and Information Security are prohibited from being implemented. Additional departmental reporting and monitoring responsibilities may result if a new solution is implemented.

4. Complying with other relevant university polices when accepting payment cards.

All university employees involved in the processing of payment cards must be knowledgeable of and responsive to the following university policies:

- Information Security Policy- This policy (i) encourages the security, availability, privacy, and integrity of DePaul's information systems, networks and data; (ii) outlines procedures for reporting breaches of information security; and (iii) encourages compliance with various federal and state laws as well as other DePaul information security-related policies and procedures.
- Access to and Responsible Use of Data - This policy explains the approval process and requirements for system data (i) access (*e.g.*, appropriate management level approval, request for data access forms); (ii) use (*e.g.*, need-to-know type requirements); and (iii) security (*e.g.*, user

IDs/passwords; users required to protect against unauthorized access) and a link to the Security Classifications and Control Matrix.

- Cash Receipts and Departmental Deposits - This policy explains the responsibilities of all departments involved in the collection of funds, including payment cards, on behalf of the university.
- Gift Acceptance and Processing - This policy explains that all private donations (gifts) received by any area of the university must be sent to the Office of Advancement for processing to encourage that the donor receives proper acknowledgement of the gift. This policy includes payment card receipts.
- Fundraising Events and Activities - This policy explains that all DePaul University faculty and staff members must obtain approval from the Office of Advancement prior to planning, publicly announcing and/or conducting fundraising events aimed at generating charitable contributions for DePaul University, its schools, colleges, programs, and/or student groups. This policy also requires that if an event is approved, the event organizers must schedule a meeting with the Director of Gift Processing to implement standards for conducting a fundraising event. These standards include implementing a plan for payment card processing before and at the event.
- Records Management - This policy provides a framework for managing, retaining, and disposing of Official Records, including payment card data.

5. Failure of the department to follow the above procedures may result in the Treasurer terminating the department-s ability to process payment cards.

Treasurer's Office Responsibilities

1. The Treasurer's Office will work with university departments to make available secure and PCI-DSS compliant payment card payment resources. Questions and requests about payment card acceptance for university departments can be sent to the Treasurer's Office via e-mail to paymentcard@depaul.edu or by calling (312) 362-8945.

2. The Treasurer's Office will provide guidelines for departmental procedures for their payment card processes by utilizing industry best practices.

3. The Treasurer's Office will also serve as liaison to the university's recognized payment card processing vendors, Information Security and the Office of the General Counsel if the initiation of a new solution, technology, device or contract for payment card processing requires their involvement.

4. The Treasurer's Office serves as an immediate point of contact (paymentcard@depaul.edu) if a department suspects payment card fraud.

5. The Treasurer's Office will maintain an e-mail list of staff responsible for processing departmental payment card payments to notify these individuals of service outages experienced by DePaul's primary payment card processor. Continuing education and PCI-DSS compliance materials will also be made available to these individuals through e-mail and the Financial Affairs website located at: http://financialaffairs.depaul.edu/treasurer/index.htm.

6. The Treasurer's Office, with the assistance of Information Security, will work with departments to complete their PCI-DSS questionnaires and attestations, to report non-compliance and to establish solutions and timelines for achieving full compliance.

7. In the event a department is unable to achieve PCI-DSS compliance or violates other sections of this policy, the Treasurer will make the determination if the department may continue to process payment cards.

Information Security Responsibilities

1. Information Security will assist departments in the completion of their PCI-DSS questionnaires and attestations.

2. Information Security will assist the department in establishing solutions and timelines for achieving full PCI-DSS compliance.

3. Information Security will assess vendor solutions, technologies and devices to minimize security risk and assure ongoing PCI-DSS compliance.

4. Information Security will serve as the immediate point of contact (security@depaul.edu) in the event of a suspected payment card data security breach.

Divisional Collaborations

Academic Affairs
Controller's Office
Information Services
Records Management
Office of Development
Office of the General Counsel
Student Financial Accounts

Contact Information

Treasurer's Office
Phone: (312) 362-8945
Website: http://financialaffairs.depaul.edu/treasurer/index.htm

Appendices

a. Departmental Guidelines for Special Receipting of Credit Cards
b. Special Receipting - Payment Card Processing Form

History/Revisions

Origination Date: 10/13/2013
Last Amended Date: 01/10/2017
Next Review Date: N/A