Georgetown University PCI DSS Handbook

Procedures for Payment Card Processing: Guidance for Departments and Card Processors

March 2017

Table of Contents

Section 1: Mission Statement....4
Section 2: PCI DSS Overview 4
Section 3. University Policies and Procedures 4
Section 4. Card Payment Service Centers 4
Section 5. General Requirements & Procedures....5
Section 6. Financial Procedures....9
Section 7. Annual PCI Security Audit 9
Section 8. Applying to Take Card Payments 11
Section 9. Enforcement....11
Section 10. Glossary....12
Section 11. Policies 13

Revision History

Date	***Version***	***Author***	***Description***
2/23/15	1.0	Judith House	Initial Draft
3/16/15	2.0	Judith House	Revision, with Treasury Operations
5/18/15	3.0	Jessica Pierce	Revision, with Treasury Operations
9/18/15	4.0	Judith House	Revision, with PCI Working Group, to reflect final decisions about GU acceptable practices
11/4/15	4.1	Judith House	Revision to reflect Service Center structure
1/12/16	4.2	Judith House	Separation of Coordinator and Department procedures
5/3/16	4.3	Jessica Pierce	Post QSA Modifications
11/11/16	4.4	Jessica Pierce	Annual Review/Update of Documentation
3/2/17	4.5	Jessica Pierce	Clarification Process and Retention Requirements in Section 7.

Section 1: Mission Statement

The purpose of Georgetown's PCI procedures is to process credit card transactions in a manner that protects confidential customer data using industry best practices, by well-trained University personnel, and ensure that GU partners also protect customer data appropriately.

Section 2: PCI DSS Overview

PCI DSS stands for Payment Card Industry Data Security Standard. It is not a governmental regulation, but a contractual obligation imposed by the payment card companies in return for allowing Georgetown to accept credit and debit card payments. The requirements of PCI are aimed at protection of Cardholder Data (CHD), in particular the Personal Account Number (PAN). The requirements are quite stringent, and are not subject to negotiation.

The office of Treasury Operations within Financial Affairs oversees the PCI process. The University Information Security Office provides support to Financial Affairs by establishing standards for securely handling Cardholder Data, by conducting reviews and risk assessments, and by assisting with remediation efforts as needed.

Section 3. University Policies and Procedures

In compliance with the requirements of PCI, Georgetown University has created the *Payment Card Industry Data Security Standard (PCI DSS) Policy (FA 192)*. The purpose of this policy is to secure payment card transaction data in order to protect account and personally identifiable information provided by customers using credit or debit cards for business with Georgetown University. It defines and describes the responsibilities and required practices for all members of the University community with respect to the use, storage, processing and retention of payment card data (e.g. credit cards, debit cards) to conduct University business.

The University Information Security Office publishes the PCI DSS Security Policy, which describes the security measures required for PCI compliance. The policy is published on the UISO web site, security.georgetown.edu.

Section 4. Card Payment Service Centers

In order to effectively manage, control, and support PCI compliance, the University has established campus based Service Centers, through which all card processing and PCI compliance is administered. Each Campus is responsible for managing credit card processing and PCI compliance through central Service Centers.

Service Centers are required to assess, monitor, and where necessary reassess the procedures of all departments that accept card payments on behalf of the Center. The procedures for Center Coordinators and staff are found in the PCI DSS Handbook for Service Center Coordinators.

Responsibilities of Service Centers Include:

- Card Processor and Department Support and Oversight
- Equipment Oversight and Control

- Compliance Monitoring and Oversight
- Transaction Review, Journal Management, and Reconciliation
- Annual PCI Audit
- Annual Review of Center departments
- Management of Applications for Acceptance of Payment Cards

Service Centers

Main Campus
- Central Service Center
- Student Affairs
- School of Continuing Studies
- SFS-Q

Medical Center
- Central Service Center

Law Center
- Central Service Center
- CLE

University Services
- Central Service Center
- Advancement
- Office of Billing & Payment Services

Section 5. General Requirements & Procedures

All individuals who are engaged in payment card processing are required to adhere to the Procedures described here, as well as those documented in the Service Center and department business processes.

REQUIREMENTS:

- PCI DSS Training:
  - Every employee who meets the criteria for card processor, as defined by Georgetown University, is required to complete annual PCI training, and to present evidence of successful completion to the Service Center Coordinator.
  - Every authorized user must annually accept notification of the PCI-related policies by completing the form: https://sites.google.com/a/georgetown.edu/pci-training/
  - Only persons who have completed all required training will be permitted to handle card data.
  - Fulfillment of the training requirement is logged in employee's GMS record.
- Business process and business cycle:
  - Every department is required to maintain with their Service Center documentation of the business process and business cycle for handling payment card data.
    - This process is to be reviewed annually as part of the PCI audit requirement
  - Adherence to these procedures is mandatory
    - Changes of procedure must be documented immediately and provided to the appropriate Service Center Coordinator
- Segregation of Duties
  - Each department engaged in payment card processing must establish segregation of duties with regard to payment card processing, the processing of refunds, and reconciliation of revenue.
- General Procedures:
  - Acceptable methods for receiving payment card data:

        - Postal mail and in-person are permitted
        - E-Mail is not permissible
            - When cardholder data is received by e-mail the processor should:
                - Notify the sender that it cannot be accepted;
                - Direct the sender to the appropriate method, and
                - Destroy the data.
        - Phone and Fax are permitted only with a documented exception from Financial Affairs/UISO. Receipt of cardholder data via these methods requires a Plain Old Telephone Service (POTS) line provisioned by Verizon and installed and maintained at the expense of the department. The standard phone/fax lines at the university are Voice Over Internet Protocol (VOIP) and are not permitted for transmission of such data.

    - Storage
        - Card data may not be stored, in whole or in part, on electronic media.
        - Where approved, masked card data on paper may be stored in locked storage for the minimum required by the business process, or for the duration of the retention period, whichever is shorter.
        - Stored card data on paper must effectively mask the PAN except for the last 4 digits
            - Black marker is insufficient masking
            - Physical removal (cutting it off the form) is required prior to storage
    - Compliance with University financial procedures is mandatory.

- Staff Changes
    - Changes in staff engaged in processing payment cards must be reported to the Service Center Coordinator immediately
        - All designated card processors must successfully complete the mandatory PCI DSS training before beginning to handle cards or card data.
        - New employees have 30 days to complete training.

- Secure Environment
    - Departments must maintain an appropriately secured environment at all times
        - Secured Devices
            - All card processing devices within a department's cardholder data environment must be appropriately secured.
                - Machines that are left unattended must be locked or logged-off.
                - Non-computer devices must never be left unattended in an area where unauthorized individuals may have access to the device.
        - Patching and Security Updates
            - Each department engaged in payment card processing must complete all security enhancements to processing systems as required by Treasury Operations/Internal Audit/UIS.
            - All vendor supplied security patches to systems must be applied as soon as possible, based on risk factors, but no later than 30 days from issue date.
        - Changes to the Processing Environment

    - The Service Center, in conjunction with UISO, must approve any changes to the departmental processing environment, including any software/hardware additions, prior to purchase.
    - Noncompliance will result in sanctions, as described elsewhere in this document.

- Audit
    - Treasury Operations, UISO, and/or internal/external audit staff will perform regular internal assessment of departments' systems, security policies and controls related to University payment card processing.
    - Compliance
        - Each department engaged in payment card processing must cooperate with all required reporting and audits, including full compliance with PCI DSS, University policy, and all other industry security requirements
        - Noncompliance will result in sanctions, as described elsewhere in this document.
- Contracts & Agreements
    - Contracts with PCI components must be submitted to the Service Center Coordinator for review. The Coordinator will work with Treasury Operations and UISO on the approval process.
    - Treasury Operations and UISO must approve all new contracts and contract renewals related to payment card processing prior to execution.
    - All such contracts must contain contract language appropriate to PCI DSS, as determined by Office of General Counsel.
- Dedicated PCI Facility
    - The facility must be secured at all times, with locked doors and controlled access (keycard, key, etc.)
    - Only authorized facility staff may remain in the facility unescorted.
    - Devices must be locked down
    - Devices must be scanned on a regular schedule, but at least quarterly.
    - Visitor access must be strictly limited, and appropriately controlled:
        - Visitors must be signed in, present photo ID, and record purpose and person being visited.
        - Visitors must receive badges or other devices that visually identify them as such
        - Visitors must be escorted at all times within the facility
    - Visitor logs must be retained for a minimum of 3 months

TERMINAL (POS) processing:
Terminal Management:

The Point of Sale (POS) device must be an approved PNC issued terminal. Treasury Operations manages the acquisition, tracking, and return of all POS devices. Service Center Coordinators shall make requests for additional devices, report damaged or inoperative devices, and return unneeded devices to Treasury Operations for disposition. Only Treasury Operations may lease or purchase POS devices through PNC.

Each POS device must be stored in a locked, secure location except when actively used. When in use the device must be connected to a non-GU POTS line provisioned by Verizon and installed and maintained at the expense of the department. Approved devices include FD130 or FD130Duo with FD-35, FD400 or CloverMobile (see appendices for product information on each approved device)

Payment Processing (Card Present):
Payment is "Card Present" (the cardholder is physically present and presents or swipes the card him or herself.)

Terminal Card Present

1. Press **ENTER** (green key on terminal) or touch screen to light up Main Screen display.
2. Press **CREDIT/DEBIT**
3. Press **SALE**
4. Key **$ amount** and press **ENTER**
5. At the prompt, swipe the credit/debit card then press **ENTER**
6. Terminal then communicates with host (PNC) for approval
7. When transaction is approved a merchant receipt with masked cardholder data automatically prints out for the patron to sign. Remove this receipt from the terminal. This receipt will be stapled to the cash register transaction receipt.
8. Press **YES** to print a customer receipt to give to the patron.
9. Press **CLEAR or ENTER** to return to the Main Screen.

Payment Processing (Card Not Present)
Payment is "Card Not Present" (phone or USPS mail only). Credit Card Payment Authorization (CCPA) forms may be used to collect and process both mail and phone transactions.

Payment Processing:
The paper form and phone method uses the department Credit Card Payment Authorization (CCPA) form. Either the cardholder will complete a paper form including cardholder data (CHD), or a staff member will use the same form to record information from the caller, including the cardholder data (CHD). The CHD is recorded on the bottom section of the form. CCPA forms must be formatted so that the cardholder data is at the end of the form, and can be removed once the transaction is completed.

Terminal Processing

After the form is completed the card transaction payment is processed using the terminal, following the steps below:

1. Press "1" button (Credit)
2. Press "1" button (Sale)
3. Key $ amount, i.e. if five dollars, then key-in: 500 (decimal automatically inserted)
4. Press, "enter" (green button)
5. Key customer's credit card number and press "enter" (green button)
6. Key Expiration Date (for instance 0415) and "enter" (green button)
7. Choose "6" button for NO
8. Base amount and tax amount screen, skip by pressing "enter" (green button)
9. Tax Exempt? – Press "4", for Yes
10. Customer Code? – Press "enter" (green button)
11. Address – skip by pressing "enter" (green button)
12. Zip Code - skip by pressing "enter" (green button)
13. Processing "Dialing/Transmitting/Receiving" (Terminal communicates with the host for approval)
14. Once the merchant masked receipt is printed, remove receipt from terminal
15. Print customer receipt copy? – Press "4" for Yes
16. Press "enter" (green button) once customer receipt has printed

17. Press red button for CLEAR or get the start screen
18. Separate the CHD section from the CCPA form and immediately destroy by shredding.

E-Commerce

E-commerce refers to the process of conducting transactions over a web site designed for payment processing. Georgetown requires that all e-commerce activities be conducted using approved hosted sites. No in-house e-commerce development is permitted. Both Treasury Operations and the Service Center must approve e-commerce vendors prior to initiating a contract.

E-commerce transactions are conducted by the customer directly, with no intermediation between the customer and University employees**. University employees may not, under any circumstances, enter cardholder data into an e-commerce site on a customer's behalf.**

In some cases, selected staff will access customer information from the site, acting as a 'non-consumer user' (administrator). Each such non-consumer user must:

- Use only an account specific to the individual (no shared IDs)
- Change the password on that account at least every 90 days

Printing, downloading, or otherwise capturing and storing cardholder data on University devices or networks is not permitted under any circumstance.

Section 6. Financial Procedures

Card Processing

ClientLine & AmexOMS are online reporting services that provide timely service center payment processing information. ClientLine provides processing information for Visa, MasterCard, and Discover. AmexOMS provides processing information for American Express. Users must login to these services at least once every 30 days or lose access. Contact the Service Center to add or remove users.

Procedure for Credit Card Terminals and e-commerce

- Each Service Center and department is required to regularly review card activity using ClientLine/AmexOMS.
- Each Service center must sign in at least every 30 days
    - Failure to do so may disable the ClientLine/AmexOMS account. Should this occur, contact your Service Center for assistance.
- Terminal Batch Out
    - Card Processors are required to batch out at the end of each session, or minimally daily. Center Coordinators must monitor for compliance.
    - Service Centers are required to report the initial batch for each terminal to Treasury Operations, by email to pci-support@georgetown.edu

Section 7. Annual PCI Security Audit

All Centers will be audited for PCI compliance by UISO and Treasury Operations on at least an annual basis. Each Center Coordinator must maintain the *PCI Merchant Annual Audit Workbook* as current. Departments must provide the relevant documentation to the Center Coordinator in a timely manner. The required documentation is described below

1. **Authorized Card Processor List:**
    a. Provide a list of all authorized (trained) Card Processors, including any ecommerce or terminal access authorization.
    b. This list must be kept current at least on a monthly basis
2. **Process & Retention**
    a. A departmental business process description based on the standard process must be created and maintained. It addresses:
        i. How credit card data is received, processed, stored, and destroyed for each payment channel
        ii. Specifics of storage and destruction procedures
        iii. For E-Commerce, website URL, hosting company, payment gateway, and approved ecommerce provider(s)
        iv. Duration of business cycle
        v. It must contain a quarterly process for audit of cardholder data to identify and securely delete stored cardholder data that exceeds defined retention requirements.
3. **Terminal (POS) Device Inventory**
    a. If the department has one or more terminals maintain the Terminal (POS) Inventory Sheet. Record the identifying information, location information, and ownership.
    b. Departments must conduct a monthly review of all devices to ensure that no tampering has occurred, and log each device inspection. The Tampering Audit log should be provided to the Center
    c. Center Coordinators must track if a POS device is borrowed or moved and for what purpose. **Upon return to its storage place, a Tamper Audit should be performed.**
4. **E-Commerce**
    a. If the department uses one or more E-Commerce sites, the department must complete the E-Commerce Site Inventory Sheet.
5. **Data Management Log**
    a. To be maintained if stored data has been shared with others, moved to a different location, or destroyed
6. **Incident Log**
    a. For any security events or incidents related to payment card data, the Incident Reporting Log sheet must be completed. Include a summary of the event, impact, scope, and resolution. Include copies of the incident reports in the audit packet.
7. **Dedicated PCI Facilities**
    a. GU has few such facilities. For any dedicated PCI Facility, the Dedicated PCI Facility Staff Sheet must be maintained to record everyone who is authorized for access to the facility, with authorization and contact information.
    b. Complete Visitor Logs for the relevant period must be included in the Audit Packet.
    c. A Key Log must be maintained for the control of keys for the facility.
8. **Service Provider List**
    a. All Service Center Coordinators must identify and maintain a list of all third parties who process credit card payments on their behalf. If applicable, this list of third parties must include a document destruction company who handles shredding of all credit card information. A document destruction log must be kept as part of the audit workbook.
9. **Data Destruction Log**
    a. If a third party handles document destruction of cardholder data, it must be logged in the data destruction log.
10. **Desktop Audit**
    a. Card processors may be subject to an annual desktop audit of the university computer to assure proper configuration, patching, security software, etc. is in place.

Section 8. Applying to Take Card Payments

Departments wishing to accept card payments must first obtain the PCI application packet. This contains the *Payment Card Processing Application* and guidance on completing the process. The Campus Service Centers will make the application packet available, and will assist in completing the forms as necessary. The Service Center Coordinators will make the initial determination of eligibility for card processing based on the type, number of transactions, and dollar amount indicated, and the appropriateness of the activity. If the request is deemed appropriate, based on the criteria found in section 4, the Center Coordinator will determine the appropriate resolution.

When a Center Coordinator accepts a request, a copy of the application form and accompanying documents is forwarded to Treasury Operations. Treasury Operations reserves the right to audit accepted applications as appropriate.

The *Payment Card Processing Application* and guidance on completing the application process are available separately at https://georgetown.box.com/s/42cte7rb9sadd3ja244hhh89ggwd78lv.

Section 9. Enforcement

Every individual who handles or processes credit cards or cardholder data is required to remain fully compliant with the requirements of PCI DSS at all times.

Departments or individuals that fail to fully comply with the provisions of the Service Center Agreement, or with the provisions of University policy and its associated procedures, are subject to suspension or termination of payment card processing privileges. There are no exceptions.

Departments are responsible for any financial loss incurred by the University resulting from inadequate controls or insufficient adherence to the PCI DSS, University policy and other industry security requirements.

Departments or individuals found to be non-compliant are required to promptly come into full compliance to retain the ability to accept card payments. When a compliance issue is identified, the Center Coordinator will notify the department and relevant card processors. This Warning of Non-Compliance will specify the areas of non-compliance, and establish the date by which the department must demonstrate full compliance. Failure to achieve full compliance within that period will result in a Final Warning of Non-Compliance, with a maximum duration of two weeks. Warnings of Non-Compliance are copied to Treasury Operations.

Failure to comply with the Final Warning will result in referral to Treasury Operations for final disposition. Disposition may include suspension or revocation of payment-processing privileges.

Section 10. Glossary

Acquirer	Also referred to as “Merchant bank,” “acquiring bank,” or “acquiring financial institution.” Entity that initiates and maintains relationships with Merchants for the acceptance of payment cards. The acquiring bank for GU is PNC.
Authorized User	A member of the University community who has been identified as a card processor, and has successfully completed the mandatory training.
Card processor	Any member of the University community who accepts, processes, stores, reviews, or handles cardholder data on behalf of a Center.
Cardholder data (CHD)	The full Primary Account Number (PAN) or the full PAN along with any of the following elements: Cardholder name, Expiration date, and Service code.
Center	Campus based units created to effectively manage, control, and support PCI compliance in the departments under the Center.
Dedicated PCI Facility	Space whose primary purpose, or within which one of the primary activities, is the processing of cardholder data, such as a call center.
E-Commerce	Commercial transactions conducted over the Internet
Masked merchant receipt	Receipt which displays only the last 4 digits of the card number
Merchant ID	Number used to identify the University unit processing each transaction.
PAN	Full Primary Account Number
Payment Application	A software application that stores, processes, or transmits cardholder data as part of authorization or settlement, where the payment application is sold, distributed, or licensed to third parties
Payment card	Credit or debit card
PCI	Payment Card Industry Data Security Standards (also called PCI DSS)
Portable (Removable) Electronic Media	Media that store digitized data and which can be easily removed and/or transported from one computer system to another. Examples of removable electronic media include CD-ROM, DVD-ROM, USB flash drives and removable hard drives.
POS Device	Also called Terminal. Authorized device used to process payment card transaction. Such transactions may be “Card Present” or “Card Not Present”
ROC	Acronym for “Report on Compliance.” Report documenting detailed results from an entity’s PCI DSS assessment.
Security Event	An occurrence considered by an organization to have potential security implications to a system or its environment. In the context of PCI DSS, security events identify suspicious or anomalous activity
Separation of Duties	Practice of dividing steps in a function among different individuals, so as to keep a single individual from being able to subvert the process
Service Provider	Any company that stores, processes, or transmits cardholder data on behalf of another entity
Service Center	See Center
Terminal	See POS Device

Section 11. Policies

PCI DSS POLICY:
http://financialaffairs.georgetown.edu/sites/financialaffairs/files/documents/fa_192_payment_card_industry_data_security_standard_pci_dss_-_june_2016.pdf

PCI SECURITY POLICY :

https://georgetown.box.com/s/68akvfbg2bzhj0uz7x1utqzxgfa4vk6h

Appendix: Approved POS Device Product Information

FD130
FD130 Duo
FD410
CloverMobile