Georgetown University PCI DSS Handbook
Service Centers

March 2017

Table of Contents

Revision History

Date	***Version***	***Author***	***Description***
1/11/16	1.0	Judith House	Initial Draft
1/27/16	1.1	Judith House	Committee agrees to forward for final approvals
3/28/16	2.0	Judith House	Post-training modifications and revisions
5/2/16	3.0	Jessica Pierce	Post QSA modifications
11/9/16	4.0	Jessica Pierce	Annual Review/Update of documentation
3/2/17	4.1	Jessica Pierce	Clarification Process and Retention Requirements in Section 6.
3/28/17	4.2	Jessica Pierce	Addition to Section 3: Equipment Oversight and Control to clarify terminal transaction threshold requirements. Addition to Section 4: List of pre-approved third party functions.

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. 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 except where one of the following conditions applies:

- A school or department anticipates having over 200 transactions AND over $100,000 in sales per year
- A school or department requires a separate bank account in order to conduct its activity
- A school or department is in a foreign location (SFS-Q)
- A school or department has special needs or requirements that warrant a separate service center
    - Subject to approval of the Treasurer and the Campus CFO/CBO

Service Center eligibility will be reviewed annually, with the possibility that Centers will be consolidated if conditions are not met.

Section 3. Service Center Responsibilities

Compliance Oversight

The requirements for compliance with PCI DSS (Payment Card Industry Data Security Standards) are stringent and complex. In order for the University to become and remain compliant, Service Centers have been established to oversee and manage all card processing transactions for the University. Personnel in each Center will be fully trained and well versed in the requirements and in how they are applied at Georgetown, and will provide both oversight and education to the departments within their scope. The Service Center Coordinator is responsible for ensuring that established procedures are being properly followed and that each department's data retention, storage, and destruction is adequate and is being implemented appropriately. Center Coordinators exercise the first line controls over the PCI DSS process.

Card Processor Oversight

PCI DSS requires that GU ensure that all individuals who are, or are likely to be, engaged in some part of the card handling and transaction process, are properly trained on an annual basis, and has indicated that GU policies have been read and accepted. In order to ensure that this requirement is met, each Service Center is responsible for maintaining a current, complete, accurate roster of all individual card processors and their training compliance. This roster must be kept current within a month. Authorized card processors are required to have a bona fide business need to engage in card processing.

Equipment Oversight and Control

PCI DSS requires that GU ensure that all equipment used for card processing is properly managed and secured. In order to ensure that this requirement is met, each Service Center is responsible for maintaining a current, complete, accurate list of all POS devices in use by the departments supported by the Center, including identifiers and use and storage locations. In addition, each Center must maintain a current list of all their e-commerce websites with URLs. Centers are also responsible for verifying the completion of tampering audits.

Any requests for new equipment will be routed to the Center Coordinator, who will ensure that there is a bona fide business requirement for the equipment, manage the acquisition of new equipment, and oversee the decommissioning of existing equipment. All equipment will be centrally managed through the Office of Financial Affairs before it is deployed to the Service Centers. The Office of Financial Affairs will maintain the official University inventory of POS equipment and oversee distribution and proper decomissioning of the equipment.

Financial Affairs reserves the right to recall equipment if transactions on terminals do not meet the minimum annual threshold for merchant IDs of $25,000. Additionally, terminals may be recalled to Financial Affairs if they have not been used in 6 months.

Transaction Review and Reconciliation

Service Center Coordinators are responsible for management of the financial processes related to card processing, including journal processing, reconciliation of transactions, and chargeback processing. The Center is accountable for ensuring that transactions are properly recorded in GMS.

Annual PCI Audit

Under PCI DSS, the University is required to conduct audits, at a minimum annually, to ensure compliance by all merchants. The University Information Security Office will conduct annual audits. Each Center Coordinator is responsible for the maintenance of the PCI DSS Audit Workbook, the required documentation, and participation in the actual audit itself.

Annual Review of Center departments

Each Service Center is required to conduct an annual review of all departments and other units supported by the Center. The purpose of this review is to assess eligibility to continue transaction processing, and well as to identify candidates who meet the conditions for a separate Center.

Accept and Review Applications for Acceptance of Payment Cards

Each Center will distribute, assist with, review, and determine disposition of applications to accept payment cards. To do so they must ensure that the requestor submits a completed application with the requisite signatures, providing assistance with the process where necessary.

When an application has been submitted, the Center Coordinator will review the request and determine whether it should be approved for use under the existing Campus Center, referred to Treasury Operations for consideration as a new Service Center, or denied.

Service Centers	***Coordinator***	***E-Mail/Box***
	LAW CENTER	
Central Service Center	Cora Osborne	PCI-LawCtr
CLE	Simona Rosu	PCI-LawCtr-CLE
	MAIN CAMPUS	
Central Service Center	Christopher Mehrholz	PCI-Main
Student Affairs	Patrick Durbin	PCI-Main-SA
School of Continuing Studies	Heather Malneritch	PCI-Main-SCS
SFS-Q	Shaida Sonde	PCI-Main-SFSQ
	MEDICAL CENTER	
Central Service Center	Victoria Kromer-Crooke	PCI-MedCtr
	UNIVERSITY SERVICES	
Central Service Center	Jon Hendrix	PCI-UnivSvcs
Advancement	Katya White	PCI-UnivSvcs-Adv
Office of Billing and Payments	Rico Headly-Soto	PCI-UnivSvcs-BPS

Section 4. General Requirements & Procedures

- PCI DSS Service Center staff training:
  - Every individual who performs tasks on behalf of the Service Center is required to complete annual Service Center Training. The Center Coordinator will maintain the record of this training.
    - 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/

- Service Center –Level documentation and Data Flow
  - Every Service Center is required to maintain documentation of the purpose of the credit card processing for its Service Center. This includes a detailed diagram and explanation of how the credit card data is processed and transmitted.

- Business process and business cycle:
  - Every Service Center is required to maintain documentation of the business process and business cycle for each department handling payment card data. This process is to be reviewed annually as part of the PCI audit requirement. 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
    - *Batching:*
      - Terminal users are required to batch out at the end of every session, but minimally once daily.
    - *ClientLine/AmexOMS Oversight:*
      - Terminal users must login to ClientLine/AmexOMS at least once every 30 days.
      - The Center Coordinator must send a written request to Treasury Operations to add or remove users.

- Secure Environment
    - Each Center will periodically review the departments served by the Center, to ensure that they continue to maintain a secure environment. Center Coordinators may coordinate with UISO as needed.
- Audit
    - Treasury Operations, UISO, and/or internal/external audit staff will perform regular internal assessment of Centers' and departments' systems, security policies and controls related to University payment card processing. Each Center Coordinator is responsible for maintaining the Center's Audit Workbook, keeping it current, and maintaining supporting documents. At least annually, each Center will be audited for compliance. The workbook will form the basis of the audit.
    - Center Coordinators are responsible for participation in the audit.
    - Audit findings will be documented and provided to the Coordinator, the relevant CFO or CBO, and the Treasurer. Findings must be remedied within the agreed-upon timeframe; failure to do so may cause a reassessment of the Center's scope and staffing, and may result in consolidation and/or staffing changes in some cases. Centers with significant findings will be subject to more frequent audits for a period of not less than one year.
- Contracts & Agreements
    - In addition to the standard contract procedures, Treasury Operations and UISO must review and approve all new contracts and contract renewals related to payment card processing prior to execution.
        - There are several pre-approved third parties that provide specific services or functions for the University. The pre-approved third party contracts must still undergo a review by Treasury Operations and UISO, but review is expedited. The following usages are pre-approved and should be considered for usage before seeking another vendor:
            - Shopify- Shopping Cart Function
            - Cvent- Event Registration
            - Eventbrite- Event Registration
            - BidPal- Auctions
    - All such contracts must be identified by the Service Center Coordinator in the Audit Workbook
    - All such contracts must contain contract language appropriate to PCI DSS, as determined by Office of General Counsel.
    - All such contracts must have an accompanying data flow diagram demonstrating how credit card data is stored, transmitted, and processed.

- Device Tampering Review

  POS Devices (such as terminals) used in card-present transactions must be protected from tampering or substitution. Each department that is assigned such devices is required to conduct and document a review of all such devices. The official inventory of POS devices assigned to the department forms the basis for this review.
    - The Tampering Review consists of:
        - Formal review on a regular schedule as established by the Center Coordinator, but at least annually.
        - Inspection of device exterior for additions such as extra cables or attachments
        - Inspection of device exterior for alternations such as altered or missing security labels, broken or differently colored casing, serial number not found in inventory, or changes to external markings

        - Record of the review in the department's Tampering Review Audit Log
        - Submission of signed log provided to the Center Coordinator

- Dedicated PCI Facilities

Centers whose departments include a Dedicated PCI Facility must meet additional auditing and procedural requirements. The Center Coordinator will exercise oversight, and will ensure that required documentation for audit is available.

- The facility must be secured at all times, with locked doors and controlled access (keycard, key, etc.)
- A roster of authorized facility staff must be maintained as current within a month.
- Only authorized facility staff may remain in the facility unescorted.
- Devices must be locked down:
    - Secured in a locked closet or storage space when not in use
    - Properly protected from tampering or misuse.
- 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.
- The annual audit of Dedicated PCI Facilities will review:
    - The Device Tampering Audit Log
    - The authorized staff roster
    - Visitor logs
    - Facility security measures
    - Key Logs

All Service Center Coordinators and staff are required to conform to these requirements.

Section 5. Financial Procedures

Card Processing

Service Centers are required to assess, monitor, and where necessary revise the procedures of all departments that accept card payments on behalf of the Center, based on the procedures for departmental card processors found elsewhere in this handbook. These procedures provide a basis for departmental business process documentation as well as describing the processes each Center is required to enact.

Center Coordinators review and exercise oversight over the procedures in place in each of the departments they support, including:

- *ClientLine & AmexOMS:* 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. The Center Coordinator must send a written request to Treasury Operations to add or remove users.

Procedure for Credit Card Terminals and e-commerce

- Each Service center 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 Treasury Operations 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.

Reconciliation:
Service Centers are responsible for appropriately recording credit card sales and returns in a timely and accurate fashion, and to recognize revenues to the appropriate department. On a daily, or at most weekly, basis at a minimum, create a journal (see below) to record the credit card proceeds to each department. Proceeds for Card Present and Card Not Present can be included on the same Journal. This reconciliation must be completed at a minimum on a monthly basis.

Each service provider offers some reporting capabilities, although the content and format vary. Under the Service Center model, each department will run a report from the service provider (Cvent, etc.) on a monthly basis, and provide that report, suitably annotated, to the Center Coordinator to be used in completing reconciliation. Coordinators will retain the reports as documentation for reconciliations. Sample reports and instructions on how to run them will be available for departments on request.

Center staff will sign into ClientLine to view credit card proceeds for the Center's accounts. ClientLine stores information for 45 days. Match the ClientLine report to the masked receipts. If there are missing transactions or amount differences please immediately contact pci-support@georgetown.edu.

Chargebacks:
When a credit cardholder disputes a charge they contact the card-issuing bank. The issuing bank then sends via fax a Chargeback notice to the service center. At this time the funds are deducted from the service center's bank account. Centers must respond to Chargebacks (disputes filed by credit cardholders) within 72 hours of receipt. Failure to respond will cause the Center to forfeit the funds processed. If the Center provides sufficient documentation supporting the charge the funds will be returned. If the Service Center does not respond to the chargeback or cannot substantiate the charge the funds will not be returned.

.

Voucher Preparation:

Transactions are to be recorded on a daily, or at most weekly, basis. Frequency of submission is based on volume of transactions.

Centers must send copies of statements to the General Accounting office service desk at gaojvf@georgetown.edu (for electronic statements) or mail them to 2121 Wisconsin Ave, #400, Washington, DC 20007 (for hard copies).

GAO will access ClientLine to view online statements.

GAO reconciles monthly bank statements to the general ledger, records Center fees reported by the bank, works with Centers to resolve discrepancies, and records unclaimed revenues to a University wide cost center.

Accounting and Recording

- The employee preparing the journal voucher should enter on the journal debit the general ledger account number and cost center combination that coincides with the cash bank account in which the Center account activity is deposited. The account number in GMS will always be 10103 (PNC Bank-Visa/MasterCard/AMEX). Please note; you must use the same departmental cost center on both sides of the entry, in conjunction with all other required Worktags.
- The journal credit contains the general ledger account number and cost center combination that is set up to record credit card revenue to a department. If an item or service is returned or cancelled, a credit to individuals' credit cards (i.e., removing revenue from a cost center) shall be prepared. This Journal records an entry that is the opposite of the entry recorded to recognize revenue Please note; you must use the same departmental cost center on both sides of the entry; in conjunction with all other required Worktags

Section 6. Annual PCI Security Audit

All Service 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 Service Center Annual Audit Workbook* as current. This workbook will form the basis for the annual audit itself. The workbook is divided into multiple worksheets. Each worksheet must be maintained as current, and must encompass the entire scope of the Center. The required documentation is described below

1. **Authorized User List:**
   a. Each Center must maintain a list of all authorized (trained) Cardholder 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. For each department, a 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 and Center Coordinators must conduct a monthly review of all devices to ensure that no tampering has occurred and log each device inspection. Include a copy of the Tampering Audit log in the audit packet.
   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 Site Inventory**
   a. For each department using one or more E-Commerce sites, the Center must maintain 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. Service Center coordinators at any time, but at least annually, comply with the requirement for a desktop audit of the university computer to assure proper configuration, patching, security software, etc. is in place.
11. **Dataflows**
    a. Dataflow diagrams of all credit card channels should be provided
12. **Service Center Overview**
    a. A document summarizing the processes of all merchant numbers should be included with the audit packet. Templates may be found: http://security.georgetown.edu/service-centers-coordinators-materials

Section 7. Review of Applications to Take Card Payments

Departments wishing to accept card payments will contact the Service Center to obtain the necessary documents. The Campus Service Centers will make the application packet available, and will assist in completing the forms as necessary. The Service Center Coordinator 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 2, the Center Coordinator will determine whether to forward the request to Treasury Operations for consideration as a new Center.

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 at https://georgetown.box.com/s/42cte7rb9sadd3ja244hhh89ggwd78lv

Section 8. Enforcement

Card Processors & Departments
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 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.

Service Centers

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

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

Centers found to be non-compliant are required to promptly come into full compliance to retain the use of their Merchant numbers. When a compliance issue is identified, the Center will receive notification of non-compliance from Treasury Operations.

- Treasury Operations and UIS will work with the Center to develop a Remediation Plan designed to bring the Center into full compliance within 15 business days.
- Centers found to be out of compliance are subject to quarterly audits for a minimum of one year.
  - Treasury Operations, at its own discretion, may at any time recommend to the University Treasurer that payment-processing privileges be suspended or revoked pending remediation.
- If the Center fails to come into compliance within 15 business days, Treasury Operations will recommend to the University Treasurer that payment-processing privileges be suspended for a period of no more than 20 business days.
- If at the end of the 20 day suspension, remediation is still incomplete, Treasury Operations may recommend to the University Treasurer that payment processing privileges be revoked
- If, after revocation, the Center becomes fully compliant, the department may petition the University Treasurer for reinstatement of the Center number.
  - If approved, the Center number will be reactivated.
  - The Center will be subject to quarterly review for a period to be determined by the University Treasurer, but no less than 2 years.
  - All individuals who process payment card transactions in the Center's department are required to attend training before the Center number is reactivated.
  - The Center must comply with additional requirements as imposed by Treasury Operations.

Section 9. 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.app.box.com/files/0/f/1390116434/1/f_51977898541