



Georgetown University
Information Services

POLICY: Payment Card Industry Data Security Standards (PCI DSS) Security Policy

STATEMENT:

The Payment Card Industry Data Security Standards (PCI) constitutes a set of procedures contractually required by the payment card industry. The primary intent of PCI is to ensure the protection of payment card transactions and cardholder data.

SCOPE:

This policy sets forth the framework for Georgetown University's compliance with PCI security and technical requirements.

APPLICABILITY:

The PCI Security Policy applies to every University Payment Card Service Center ("Center"), and all individuals who accept, process, store, manage or otherwise interact with payment card data ("Card processor".)

DEFINITIONS:

Acquirer: Also referred to as "Center bank," "acquiring bank," or "acquiring financial institution." Entity that initiates and maintains relationships with Centers 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 to Treasury Operations as a card processor, has successfully completed the mandatory training, and has been notified by Treasury Operations of their authorization.

Card processor: Any member of the University community who accepts, processes, stores, reviews, or in any way handles cardholder data on behalf of a Center.

Cardholder data: The full Primary Account Number (PAN) or the full PAN along with any of the following elements: Cardholder name, Expiration date, Service code.

Center ID: Number used to identify the University unit processing each transaction.

Clover GO: Card Swipe Device from FirstData, provided through PNC. CURRENTLY UNDER REVIEW

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

PAN: Full Primary Account Number

Payment Application: In the context of PA-DSS, 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 Center: Any University unit with responsibility for processing and managing payment card transactions and financial procedures, and which is assigned one or more Merchant IDs by Treasury Operations for the purpose of accepting and processing payment card transactions.

Service Provider: Any company that stores, processes, or transmits cardholder data on behalf of another entity

Terminal: See POS Device

GUIDING PRINCIPLES/PURPOSE:

The PCI DSS Security Policy defines the security standards that Service Centers and card processors must follow in implementing basic safeguards to protect the confidentiality, integrity, and availability of payment transaction and cardholder data.

ADMINISTRATION AND IMPLEMENTATION:

Georgetown University will maintain the security of payment card data in the manner set forth in the Georgetown PCI Security policy and the associated procedures. Georgetown University will adhere to all applicable general requirements, approaches, standards, specifications, and maintenance requirements of PCI DSS in developing and maintaining policies and procedures for security standards for the protection of PCI data. Whenever there is a change in the standards that necessitates a change to Georgetown University Security policies and procedures, Georgetown University will promptly document and implement the revised policies and procedures.

RESPONSIBILITIES:

PCI requires the University to put into place appropriate safeguards to protect the integrity, confidentiality and availability of payment card data that is received or managed by the University's Service Centers.

1. ADMINISTRATIVE SAFEGUARDS

- 1.1. Risk Assessment:** Georgetown will perform a risk assessment of University Service Centers at least annually, and upon significant changes to the environment (for example, relocation, etc.) This assessment will identify critical assets, threats, and vulnerabilities and produce a formal, documented analysis of risk.

[Addresses PCI DSS Section 12.2.]

- 1.2. Information Security Policy:** Georgetown will implement a general Information Security Policy, applicable to all members of the University Community. The University will establish, publish, maintain, and disseminate a University information security policy, and will review the security policy at least annually and update the policy when the environment changes. [Addresses PCI DSS Section 12.8.]

- 1.3. Administrative Security – E-Commerce & Third Party Services Only:** The University will define policies and procedures to ensure proper user identification management for non-consumer users and administrators on all e-commerce and third-party solution system components [Addresses PCI DSS Section 8.] Service Centers shall:

- 1.3.1.** Establish a procedure that requires authorization before any person is granted access to systems managing PCI data.
- 1.3.2.** Immediately revoke access for any terminated users.
- 1.3.3.** Remove/disable inactive user accounts within 90 days.
- 1.3.4.** Limit repeated access attempts by locking out the user ID after not more than six attempts.
- 1.3.5.** Set the lockout duration to a minimum of 30 minutes or until an administrator re-enables the user ID.
- 1.3.6.** Incorporate two-factor authentication for users

- 1.3.7. Require password change at least every 90 days
- 1.3.8. Periodically review the accounts on systems managing PCI to ensure that only currently authorized persons have access to these systems.

NOTE: Section 1.3 does not apply to Service Centers using only POS terminal devices.

- 1.4. **Information Access Management:** All Service Centers will establish procedures in compliance with the University Information Security Policy and its associated procedures, to ensure that only authorized users have access to Cardholder data and to the devices and systems that manage such data. [Addresses PCI DSS Section 8.]
- 1.5. **Security Awareness and Training:** All Service Centers will ensure that everyone who receives, handles, stores, or otherwise interacts with PCI (Cardholder) data receives PCI security training and periodic security updates at least annually [Addresses PCI DSS Sections 9, 12.]
- 1.6. **Password Management:** All Service Centers will adhere to the University's Information Security Policy as well as the Standards for Password and Passphrase Management.
 - 1.6.1. Passwords must be changed immediately if compromised. [Addresses PCI Section 8.4.]
- 1.7. **Device and Media Controls:** Georgetown University does not permit storage of Cardholder data except in temporary form as a paper document. All Service Centers will establish procedures to govern the receipt and destruction of paper media that contain PCI data, and to appropriately secure and manage PCI related devices. The movement of these items within the department must be documented. [Addresses PCI DSS Section 9.5.]
- 1.8. **Visitor Identification:** Georgetown must document procedures to identify and authorize visitors to any Dedicated PCI Facility operated by the University. Such procedures shall include:
 - 1.8.1. Identifying onsite visitors (for example, assigning badges, using a visitor log that is maintained for at least 3 months) so as to distinguish them from authorized personnel
 - 1.8.2. Documenting changes to access requirements
 - 1.8.3. Revoking or terminating onsite personnel and expired visitor identification (such as ID badges). [Addresses PCI DSS Section 9.2.]
- 1.9. **Service Providers:** The University will maintain and implement policies and procedures to manage service providers with whom cardholder data is shared, or that could affect the security of cardholder data, as follows:
 - 1.9.1. Maintain a list of service providers.

- 1.9.2. Maintain a written agreement that includes an acknowledgement that the service providers are responsible for the security of cardholder data the service providers possess or otherwise store, process or transmit on behalf of the customer, or to the extent that they could impact the security of the customer's cardholder data environment.
 - 1.9.3. Ensure there is an established process for engaging service providers including proper due diligence prior to engagement.
 - 1.9.4. Maintain a program to monitor service providers' PCI DSS compliance status at least annually.
 - 1.9.5. Maintain information about which PCI DSS requirements are managed by each service provider, and which are managed by Georgetown. [Addresses PCI DSS Section 12.8-9.]
- 1.10. **Incident Reporting:** All Service Centers must have procedures in place so that the University Information Security Office is notified when PCI data is involved in a security incident (examples include virus or worm infection, accounts being compromised, and unintended disclosure of data to unauthorized individuals). [Addresses PCI Section 12.10.]

2. Physical Safeguards

- 2.1. **Dedicated PCI Facility Access Controls:** Each Service Center will ensure that Dedicated PCI Facilities are protected by physical security controls that restrict access:
- 2.1.1. Access must be authorized and based on individual job function.
 - 2.1.2. Access is revoked immediately upon termination, and all physical access mechanisms, such as keys, access cards, etc., are returned or disabled [Addresses PCI Section 9.3]
- 2.2. **Identify and authorize visitors:** Implement procedures to identify and authorize visitors to Dedicated PCI Facilities. Procedures should include the following:
- 2.2.1. Visitors are authorized before entering, and escorted at all times within areas where cardholder data is processed or maintained.
 - 2.2.1.1. Visitors are identified and given a badge or other identification that expires and that visibly distinguishes the visitors from onsite personnel.
 - 2.2.1.2. Visitors are asked to surrender the badge or identification before leaving the facility or at the date of expiration.
 - 2.2.2. A visitor log is used to maintain a physical audit trail of visitor activity to the facility.
 - 2.2.2.1. Document the visitor's name, the firm represented, and the onsite personnel authorizing physical access in the log.
 - 2.2.2.2. Retain this log for a minimum of three months, unless otherwise restricted by law. [Addresses PCI Section 9.4.]
- 2.3. **Management of media:** Georgetown University does not permit storage of Cardholder data except in temporary form as a paper document.
- 2.3.1. Physically secure all media including paper in a secure location.

2.3.2. Document notification and approval of any and all movement of media out of a secured area. For example, document the approval for destruction of paper records at the end of processing.

2.3.3. Properly maintain inventory logs of all media and conduct media inventories at least annually. [Addresses PCI Section 9.5-9.]

3. Technical Safeguards

UIS will maintain detailed documentation of standards and procedures in support of these safeguards, and incorporate them into UISO Procedural Requirements.

3.1. **Appropriately implement Risk Management procedures:** The University will implement measures to reduce computer risks and vulnerabilities, including: identifying and documenting potential risks and vulnerabilities that could impact systems managing PCI cardholder data; and performing annual technical security assessments of systems managing PCI data, in order to identify and remedy detected security vulnerabilities. [Addresses PCI DSS Section 12.]

3.2. **Develop usage policies for critical technologies and define proper use of these technologies for PCI processes at Georgetown:** UIS will identify critical technologies, describe the appropriate usage of such technologies, and maintain the required documentation of controls [Addresses PCI Section 12.3.]

3.3. **Information System Activity Review:** UIS will review logs and security events for all system components to identify anomalies or suspicious activity, and will follow up exceptions and anomalies identified during the review process and resolve them. [Addresses PCI Section 10.6]

3.4. **Assign to individual or team appropriate information security management responsibilities.** Georgetown will assign responsibility for security policies, procedures, incident response, and access control. [Addresses PCI Section 12.5]

3.5. **Synchronize all critical system clocks:** Using time-synchronization technology, UIS will ensure the synchronization of critical system clocks. [Addresses PCI Section 10.4.]

3.6. **Review logs and security events for all system components:** UIS will conduct reviews to identify anomalies or suspicious activity, and follow up on exceptions and anomalies. [Addresses PCI 10.6]

3.7. **Penetration Testing:** UIS will Define and Document standards for penetration testing, and perform internal and external Penetration Testing as described in those standards. [Addresses PCI Section 11.3]

3.8. **Incident Response:** The University Information Security Office will create and maintain an incident response plan, so as to be prepared to respond immediately to a system breach. [Addresses PCI Section 12.10.]

COMPLIANCE:

Every employee with access to cardholder data is required to adhere to all PCI mandates. Violation of this policy may result in disciplinary action up to and including termination of employment.

RESOURCES:

University Information Security Policy :: <http://security.georgetown.edu/>

Computer Systems Acceptable Use Policy ::
<http://security.georgetown.edu/technology-policies/acceptable-use>

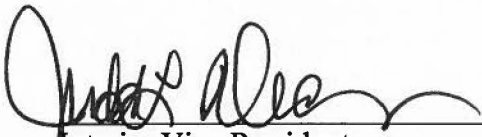
Georgetown University Payment Card Industry Data Security Standard (PCI DSS) Policy
<http://security.georgetown.edu/technology-policies/payment-card-industry-data-security-standard>

REVIEW CYCLE:

This policy will be reviewed and updated as needed, but at least annually, unless changes in institutional policy or relevant law or regulation dictate otherwise.

Reviewed and approved:

Date:



Interim Vice President
and Chief Information Officer

2/3/16
