GEORGETOWN UNIVERSITY
DIVISION OF FINANCIAL AFFAIRS

Policy 192: **Payment Card Industry Data Security Standard (PCI DSS)**

Responsible Department	Financial Affairs	**Effective Date**	6/2016
Responsible Person	Rosalyn Furukawa	**Prior Revision Date**	N/A

Contents

192.01 Purpose

The purpose of this Payment Card Industry Data Security Standard ("PCI DSS") Policy is to secure payment card transaction data in order to protect account and personally identifiable information provided by cardholders using payment cards (e.g. credit cards or debit cards) for business with Georgetown University (the "University"). This policy defines and describes the responsibilities and required practices with respect to the receipt, use, storage, processing, and retention of payment card data to conduct University business.

All collection, use, and processing of payment card data must be conducted under the auspices of Georgetown University Treasury Operations ("Treasury Operations") and the Georgetown University Information Security Office ("UISO"), and must comply with the current PCI DSS, as well as with legal, regulatory, and Georgetown University policy requirements, to protect cardholder data and protect the University from risk.

No University campus, school, department, or organization is authorized to process payment card transactions without prior approval from Treasury Operations and UISO.

192.02 Applicability

This Policy applies to all Georgetown University Payment Card Service Centers (as defined in Section 192.07) and University employees who have been authorized by Treasury Operations and UISO to process payment card transactions ("Authorized Users"). Contracts with third parties that accept payment cards on behalf of the University must contain terms that are consistent with this Policy. Treasury Operations and UISO must approve all contractual terms related to credit card processing or acceptance of payment cards on behalf of the University by third parties.

Georgetown University Payment Card Service Centers and Authorized Users that process, maintain, or accept payment cards must demonstrate compliance with this Policy or achieve satisfactory compliance. Payment Card Service Centers that fail to maintain compliance may be subject to suspension or cancellation of their Merchant IDs.

192.03 Guiding Principles

The University is committed to protecting and preserving the privacy and security of payment card data collected and processed to conduct University business. The PCI DSS supports this goal by establishing requirements for the secure handling and processing of payment card data.

Members of the University community share responsibility for protecting the information and data with which they are entrusted. The University is committed to ensuring that all payment card transactions are properly secured. All cardholder data is classified as Restricted under the University's Information Classification Policy, and must be protected accordingly. Appropriate practices and procedures for the use, processing, and destruction of payment cards and associated data must be followed without exception.

This Policy complements and supports other University policies that protect the University's financial and information technology operations including, but not limited to, the Information Security Policy and the University Record Retention and Disposal Policy.

192.04 Administration and Implementation

A Merchant ID is required to process payment card transactions. Treasury Operations controls the assignment of Merchant IDs to Payment Card Service Centers, pursuant to a formal application and approval process. Any University campus, school, department, or organization that wishes to accept payment cards must first apply for and receive authorization from the relevant Payment Card Service Center.

UISO, Treasury Operations, and Payment Card Service Centers share responsibility to ensure PCI DSS, legal, regulatory, and University policy compliance. Treasury Operations shall manage the distribution, revocation and reinstatement of Merchant IDs to Payment Card Service Centers. Payment Card Service Centers and authorized card processors shall adhere to practices and procedures that safeguard the collection, retention, disposal, and destruction of payment card data consistent with the University's Record Retention and Disposal Policy and current process requirements. Payment Card Service Centers must comply at all times with the terms of the Georgetown University PCI DSS Handbook ("PCI DSS Handbook"), including but not limited to its provisions regarding applicable: procedures; training; data collection (including acceptable submission methods); card transaction processing; data retention and destruction; and audits.

192.05 Responsibilities

Specific areas and responsibilities governed by this Policy are listed below.

Each Georgetown University Payment Card Service Center must:

- Adhere to all applicable University policies, in addition to this Policy.
- Ensure full PCI DSS compliance at all times. Failure to comply fully may result in suspension or termination of the privilege of processing payment cards.
- Supervise all departments, schools, organizations, and individuals within the scope of the Payment Card Service Center whose roles and responsibilities require the handling of payment card data, and require that all such individuals fulfill training obligations.
- Carry out appropriate reconciliations and accounting journals on behalf of the departments within the scope of the Payment Card Service Center.
- Advise applicants for card processing authorization as to the application process.
- Inform prospective and approved card processors as to the University's expectations and requirements for compliance with this Policy and with all applicable laws, regulations, and University policies.
- Comply fully with this Policy and the PCI DSS Handbook.
- Exercise segregation of duties among those employees who process payment card transactions, reconcile daily batches, and post to the general ledger.
- Ensure appropriate storage and handling of all payment card related data, as set forth in the PCI DSS Handbook.
- Create and maintain PCI DSS compliant data retention and disposal policies and procedures.
- Ensure destruction of all payment card related transactional and restricted information using UISO-approved methods pursuant to the University's Policy on the Retention and Disposal of Records.
- Comply with the provisions of the UISO PCI DSS Security Policy and ensure that card processors within the scope of the Payment Card Service Center do so.
- Accept responsibility for any financial loss incurred by the University resulting from inadequate controls or insufficient adherence to this Policy, the PCI DSS Handbook, or other relevant University policies or requirements.
- Clear accounts and transfer revenues to appropriate cost centers that generated the revenue.

Treasury Operations must:

- Advise Payment Card Service Center Merchant ID applicants as to the application process.
- Inform prospective and approved Payment Card Service Center Merchant ID holders as to the University's expectations and requirements for compliance with this Policy and with all applicable laws, regulations, and University policies.
- Assign Merchant IDs only when the formal application and approval process has been completed.
- Maintain a registry of all Payment Card Service Center Merchant ID holders and authorized users.
- Develop training on the appropriate University, financial, and security procedures for all individuals whose roles and responsibilities include handling of payment card data.
- Maintain a current knowledge and awareness of policies, laws, regulations, and industry standards relevant to the handling and processing of payment card data.
- Provide guidance to potential and current Payment Card Service Centers of any changes to applicable policies, laws, regulations, and industry standards.
- Promote PCI DSS policy compliance by Payment Card Service Centers.
- Review and approve third-party contracts for processing of payment cards on behalf of the University.

UISO must:

- Advise Treasury Operations on any changes in policies, laws, regulations, and industry standards affecting PCI DSS compliance requirements.
- Maintain a PCI DSS compliance and audit program, including annual audits pursuant to PCI DSS, or other standards, as necessary.
- Review and approve third-party contracts for processing of payment cards on behalf of the University.
- Monitor all third-party suppliers who process payment cards on behalf of the University for PCI DSS certification and compliance.

192.06 Enforcement

Payment Card Service Centers and Authorized Users who fail to comply fully with the provisions of this Policy, or with the provisions of the PCI DSS Handbook, may be subject to suspension or termination of payment card processing privileges. Payment Card Service Centers and Authorized Users found to be non-compliant are required to complete remediation as specified in a remediation plan. Failure to complete required remediation within the time period specified in the PCI DSS Handbook may result in suspension or termination of payment card processing privileges. Payment Card Service Centers and Card Processors are responsible for any financial loss incurred by the University resulting from inadequate controls or insufficient adherence to this Policy, the PCI DSS Handbook, or other relevant University policies or requirements. Employees who violate the University's PCI DSS Policy or fail to adhere to the PCI DSS Handbook may be subject to disciplinary action, up to and including dismissal. The University may routinely monitor network traffic to assure the continued integrity and security of University resources in accordance with applicable laws and University policies. The University may refer suspected violations of applicable laws to appropriate law enforcement agencies.

192.07 Definitions

For clarification on the terms used in this document, please refer to the University Information Services Policy Definitions, Roles, and Responsibilities. Terms used in this Policy include:

Authorized User - A member of the University community who has been identified as a Card Processor, has successfully completed the mandatory training, and has been notified by the Payment Card Service Center of their authorization.

Card Processor - Any campus, school, department, organization, or individual who accepts, processes, stores, reviews, or in any way handles cardholder data on behalf of a Center.

Merchant ID - Number assigned by Treasury Operations to a Payment Card Service Center, which identifies transactions associated with that Center (also called Center ID)

Payment card - Credit or debit card

PCI DSS - Payment Card Industry Data Security Standards (also called PCI)

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

Payment Card Service Center - A Campus based unit created to effectively manage, control, and support PCI compliance in the departments served by the Center. Each Payment Card Service Center performs reconciliation, accounting journaling, and other services for respective departments, which could include multiple departments, and Merchants within the scope of the Center.

Treasury Operations - Division within Financial Affairs responsible for the management of PCI DSS activity.

University Information Security Office ("UISO") - Division within University Information Services charged with providing information security services and education to the GU community.

UISO-approved PCI Compliant Vendor - Third party vendor that has successfully completed the UISO vendor review process and is approved to conduct PCI related activities on behalf of the University.

192.08 Resources

Information and resources relating to this Policy are available on the UISO website. Relevant policies and procedures include but are not limited to:

Payment Card Industry Data Security Standard

UISO PCI DSS Security Policy

University Record Retention & Disposal Policy

University Information Classification Policy

University Human Resources Confidential Information Policy (HR Policy # 403)

University Information Services Policy Definitions, Roles, & Responsibilities

Georgetown University PCI DSS Handbook ("PCI DSS Handbook")

192.09 Review Cycle

This Policy will be reviewed and updated as needed, but no less often than annually, unless changes in institutional policy or relevant law or regulation dictate otherwise.