PAYMENT CARD ACCEPTANCE AND DATA SECURITY POLICY

Policy Statement

Credit card and debit card (“payment card”) information is regulated information that must be appropriately secured. University units may not collect, process, store, transmit or display payment card information without advance written approval from Treasury Management. This requirement applies to all payment card transactions whether conducted in person, via telephone, facsimile, mail, internet, or through a university-approved third party vendor on behalf of a unit.

University units with a business need to process payment card transactions must contact Treasury Management in advance of accepting any payments to obtain a merchant identification account, training, and the appropriate GW approved secure payment processing method(s).

External entities, such as tenants, caterers, business establishments, volunteer organizations, event organizers, etc., that intend to use the GW Wired or Wireless network to accept payment via payment card must contact the Division of Information Technology to review and approve their processing method prior to conducting any transactions.

Reason for Policy/Purpose

The purpose of this policy is to promote protection of payment card data in accordance with the Payment Card Industry Data Security Standard (PCI-DSS). Failure to comply with the PCI-DSS standards may result in fines, loss of ability to process payment cards, and reputational damage to the university.
Who Needs to Know This Policy

Faculty, staff, students, and external entities that intend to use the GW Wired or Wireless network.

Table of Contents

Policy Statement .................................................................1
Reason for Policy/Purpose..................................................1
Who Needs to Know This Policy...........................................2
Table of Contents ................................................................2
Policy/Procedures ...............................................................2
Website Address ..................................................................3
Contacts ..............................................................................3
Definitions ...........................................................................3
Related Information .............................................................4
Who Approved This Policy .....................................................4
History/Revision Dates .........................................................4

Policy/Procedures

Payment card information is considered regulated data per the Information Security Policy. Members of the university community involved in processing payment card transactions are responsible for protecting such data, and for following the information security practices and policies set forth herein, and in the Related Information section on page 4.

Departments, schools, divisions or other university units (“units”) may not collect, process, store, transmit, or display payment card information without advance written approval from Treasury Management. Treasury Management is responsible for issuing all credit card merchant identification accounts, for arranging GW-approved payment card acceptance services, and for implementing payment card procedures.

In determining the appropriate method for accepting payment via payment card, Treasury Management will consider a number of factors (such as dollar levels, number of transactions involved, whether the need to process such transactions is ongoing or finite in nature, etc.).

In those circumstances when units are authorized by Treasury Management to process payment card transactions, Treasury Management will work with the Division of Information Technology to implement technology to comply with PCI standards.
However, because maintaining the safety of payment card information involves people and processes, it is the responsibility of the unit to become and remain PCI-DSS compliant.

External entities that intend to use the GW Wired or Wireless networks to process a payment card transaction must contact the Division of Information Technology (ithelp@gwu.edu) to review and approve their processing method prior to conducting any transactions.

When payment card information will be accepted on behalf of a unit by a third party vendor, only a university-approved third party vendor may be used. Units should contact Treasury Management for a list of university-approved third party vendors. All third party arrangements require a written agreement that has been reviewed and approved in advance by Treasury Management and in accordance with the Signing of Contracts and Agreements Policy.

All payments, whether accepted directly by units or by university-approved third party vendors, must be deposited per the Deposit of Checks, Cash and Credit Card Receipts Policy. Payments must be deposited only in university-approved bank accounts per the Opening Bank Accounts Policy.

Website Address for This Policy

GW University Policies

Contacts

<table>
<thead>
<tr>
<th>Subject</th>
<th>Contact</th>
<th>Phone</th>
</tr>
</thead>
<tbody>
<tr>
<td>Payment Card Information Sec</td>
<td>Treasury Management</td>
<td>(703) 726-6419</td>
</tr>
<tr>
<td>Security</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Secure Processing Method</td>
<td>Division of Information Technology</td>
<td>(202) 994-4948 / <a href="mailto:ithelp@gwu.edu">ithelp@gwu.edu</a></td>
</tr>
<tr>
<td>Confirmation</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Definitions

| Payment Card Information      | Any information pertaining to a credit or debit card, including but not limited to: card number, cardholder name, card verification (CVC, CVV or CID) number (appearing on the back of most cards), expiration date, personal identification number (PIN), password, etc. Credit and debit cards include, but are not limited to those issued by Visa, MasterCard, Discover, Diners Club, and American Express. The GWorld Card is not a Payment Card. |
Related Information

Deposit of Checks, Cash and Credit Card Receipts Policy
Information Security Policy
Opening Bank Accounts Policy
Records Management Policy
Security Breaches Involving Non-Public Personal Information
Signing of Contracts and Agreements Policy
Payment Card Industry Data Security Standard (PCI-DSS)

Who Approved This Policy

Louis H. Katz, Executive Vice President and Treasurer
Beth Nolan, Senior Vice President and General Counsel

History/Revision Dates

Last Reviewed Date: January 31, 2015
Last Revised Date: January 26, 2015
Origination Date: June 7, 2011