PCI Compliance Program
Overview
All University of the Pacific departments that accept credit card payments must process those payments in a manner compliant with the Payment Card Industry Data Security Standards (PCI-DSS) as per the University of the Pacific’s card processing contracts. It is the responsibility of each department to maintain compliance with the PCI-DSS.

Pacific’s eCommerce group, under the auspices of the Controller’s Office, directs a compliance program as an extension of managing Merchant Identification Numbers (MIDs) or Terminal Identification numbers (TIDs). Participation in, and adherence to, PCI data security program(s) run by eCommerce is mandatory for all Pacific merchants. Failure to fully participate in and comply with the program guidelines may result in the department’s MID or TID being revoked and the department’s ability to accept payment cards suspended indefinitely.

There are several components to Pacific’s Compliance Program:
- Annual Self-Assessment Questionnaires (SAQs)
- Annual Security Training
- System Vulnerability Scans (as appropriate and applicable)
- System Penetration Testing (as appropriate and applicable)
- Periodic Reviews and Audits of Departments

Each component is described below.

Annual Self-Assessment Questionnaires (SAQs)
Pacific is required to complete a self-assessment questionnaire on an annual basis. One SAQ is completed for each MID. A new SAQ must be filled out whenever any of the following have occurred:
- The payment processing system or environment has been changed;
- A year has passed since the last SAQ, or;
- Pacific has been directed to by our acquiring bank to do so.

Pacific’s eCommerce Group prepares and submits these SAQs electronically through our acquirers SAQ website (http://www.pcirapidcomply.com/). All SAQs shall be completed through this interface prior to the expiration of our existing SAQ or when otherwise directed.

The PCI Security Council has issued 5 versions of the SAQ. The eCommerce Group will determine which SAQ applies to each MID that is active. General definitions are below.

<table>
<thead>
<tr>
<th>SAQ Version</th>
<th>Type of Payment System</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>Card-not-present merchants. All cardholder data functions outsourced.</td>
</tr>
<tr>
<td>B</td>
<td>Imprint-only merchants. No electronic data storage/terminals.</td>
</tr>
<tr>
<td>C-VT</td>
<td>Merchants using only web-based virtual terminals. No electronic storage.</td>
</tr>
<tr>
<td>C</td>
<td>Merchants with payment application systems connected to the internet.</td>
</tr>
<tr>
<td>D</td>
<td>All other merchants not qualified to use the above (A, B, C-VT, C)</td>
</tr>
</tbody>
</table>

Source: PCI DSS Quick Reference Guide, Data Security Standard version 2.0 (Page 30)

The eCommerce Group will monitor and maintain the University’s overall PCI compliance effort.
Annual Security Training
Pursuant to PCI DSS requirement 12.6, eCommerce will provide PCI-DSS security training at least annually. At least one representative from each merchant must attend the centralized training. It is at the department’s discretion whether to send additional employees to the central training or to disseminate the information through a “train-the-trainer” awareness program.

System Vulnerability Scans
Merchants with on-campus payment systems connected to the internet are required to run vulnerability scans against their systems at least quarterly. Our contract with FirstData, and via the rapid comply service, includes these external scans.

System Penetration Testing
Merchants with on-campus payment systems connected to the internet are required to have penetration testing performed at least once a year. This testing is not executed as part of Pacific’s contract with FirstData but rather is run in conjunction with wider penetration testing efforts coordinated by Pacific’s Office of Information Security.

Periodic Reviews and Audits
Compliance is not a destination but rather a milestone that shall be celebrated and scrutinized. As fraud methodology adapts and changes, so shall the efforts we engage in to maintain our compliance posture. The eCommerce group may perform periodic interviews or unannounced visits to monitor the adherence of each department to the Data Security Standards. The intention of these activities is to reduce Pacific’s overall risk associated with payment card fraud.