PCI Compliance Program
Overview

All Northwestern University departments that accept credit card payments must process those payments in a manner compliant with the Payment Card Industry Data Security Standard (PCI DSS) per the NU Merchant Card Processing Policy. It is the responsibility of each department to maintain compliance with PCI DSS.

e-Commerce Operations, under the auspices of Treasury Operations, directs a compliance program as an extension of managing merchant identification numbers. Participation in the PCI compliance program run by e-Commerce Operations is mandatory for all NU Merchants. Failure to fully participate in the program may result in your Merchant ID being revoked.

There are four main components to the NU PCI Compliance Program:
1. Annual self-assessment questionnaires
2. Annual security training
3. System vulnerability scans (as applicable)
4. System penetration testing (as applicable)
5. Periodic reviews and audits

Each of these components is described below.

Annual Self-Assessment Questionnaires (SAQ)

All merchants are required to complete a self-assessment questionnaire at least annually. A separate questionnaire must be completed for each merchant ID. A new questionnaire must be filled out whenever any of the following have occurred:
   a) the payment processing system has changed;
   b) a year has elapsed since your last SAQ;
   c) you have been prompted to do so by e-Commerce Operations.

Treasury Operations maintains a contract with Trustwave to administrate SAQs through their Trustkeeper web site (https://www.trustkeeper.net/). All SAQs should be completed through that interface.

PCI has issued 4 versions of the SAQ. e-Commerce Operations will help determine which SAQ applies to your situation. General definitions are below.

<table>
<thead>
<tr>
<th>SAQ Version</th>
<th>Type of Payment System</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAQ A</td>
<td>Card-not-present, All Cardholder Data Functions Outsourced</td>
</tr>
<tr>
<td>SAQ B</td>
<td>Imprint Merchant Only, No Electronic Cardholder Data Storage Or Standalone, Dial-out Terminal Merchant, No Electronic Data Storage</td>
</tr>
<tr>
<td>SAQ C</td>
<td>Merchants with Payment Application Systems Connected to the Internet</td>
</tr>
<tr>
<td>SAQ D</td>
<td>All Other Merchants Eligible to Complete an SAQ but not qualified for A, B, or C</td>
</tr>
</tbody>
</table>

Source: PCI DSS Self-Assessment Questionnaire Instructions and Guidelines, Version 2.0, October 2010

e-Commerce Operations will monitor the university’s overall PCI Compliance on the Trustkeeper portal; however, departments are responsible for responding to Trustwave notifications regarding expired SAQs and/or vulnerability scan notifications. Failure to
complete your SAQ or vulnerability scan remediation in a timely and accurate manner may result in your Merchant ID being revoked.

**Annual Security Training**
Pursuant to PCI DSS requirement 12.6, e-Commerce Operations will hold PCI DSS Security Training annually. At least one representative from each merchant must attend the centralized training. It is at the discretion of the department whether to send additional employees to the central training or to disseminate the information through its own security awareness program.

**System Vulnerability Scans**
Merchants with on-campus payment systems connected to the Internet are required to run vulnerability scans against their systems. Our contract with Trustwave includes external vulnerability scans. The reports are posted on the Trustkeeper web site. It is the responsibility of the merchant to review the scans and address any vulnerabilities that have been identified.

**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 service is not currently a part of our Trustwave contract. NUIT ISSC can perform penetration testing on request or an outside entity can be hired to perform this service.

**Periodic Reviews and Audits**
e-Commerce Operations will review the completed SAQs and vulnerability scans on the Trustkeeper web site. Periodically, additional information and follow-up interviews may be requested. At the discretion of e-Commerce Operations, internal audits may occasionally be requested. The intention of these activities is to reduce the University’s risk by ensuring that merchants comply with PCI DSS. Failure to cooperate with such activities may result in your merchant ID being revoked.

**Related Documents**
- NU Merchant Card Processing Policy
- Payment Card Industry Data Security Standard (PCI DSS)