NORTHWESTERN
UNIVERSITY

PCI Compliance Program

Revised December, 2014

Overview

All Northwestern University departments (Merchant locations) 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 and the Payment Card Industry Security Standards Council (PCI-SSC). It is the responsibility of each Merchant location to maintain compliance with PCI DSS.

e-Commerce Operations, under the auspices of Treasury Operations, directs a compliance program as an extension of managing NU Merchant accounts. 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 account being revoked.

Below is a list of the main components of the NU PCI Compliance Program based on the requirements set forth by the PCI-SSC, followed by details regarding each component:

1. NU Security Awareness Education (PCI DSS Required Security Training)
2. System Vulnerability Scans
3. System Penetration Testing
4. Periodic Reviews and Audits
5. Trustwave-TrustKeeper and Annual SAQ (Self-Assessment Questionnaires)

NU Security Awareness Education

Pursuant to PCI DSS requirement 12.6, NU e-Commerce Operations will hold centralized PCI DSS Security Training annually. At least one representative from each Merchant location must attend the centralized training. Though 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, Treasury Operations and/or e-Commerce Operations may require individual or group participation in this and/or other forms of PCI security awareness education training offerings whenever they see fit.

ALL NU Merchant Personnel who interact with the CDE (cardholder Data Environment) in any manner, from the initial entry to the final reconciliation, are required to complete NU's PCI Security Awareness Training and Attestation annually. This mandatory requirement includes student employees and contractors.

- Individuals who have not completed this training are not allowed to process CHD (Cardholder Data) on behalf of NU interests, and Merchant locations using untrained, un-attested individuals to process CHD may have their merchant account revoked.

Before completing this Training and Attestation, each Merchant employee, student employee or contractor must first read and understand the NU PCI Compliance Program and the NU PCI Security Policy.

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 that are scheduled on the TrustKeeper Portal; scan reports are posted on the TrustKeeper Portal as well. It is the responsibility of the Merchant to review the scans and address any vulnerabilities that have been identified. Failure to address identified vulnerabilities can result in the Merchant location, as well as the entire University, falling out of compliance.

System Penetration Testing

Northwestern University is now a PCI Level 3 Merchant based upon recent card processing metrics, and NU Merchants with on-campus payment systems connected to the Internet are now required to have internally conducted penetration testing performed at least quarterly. Since this service is not currently a part of our Trustwave contract, arrangements need to be made by e-Commerce Operations and NU IT Security and Compliance, coordinated with Merchant onsite Administrators and IT staff. Failure to cooperate with this mandatory requirement may result in your Merchant account being revoked. Please contact e-Commerce Operations at 1-5382 for more information.

Periodic Reviews and Audits

e-Commerce Operations will regularly review the completed SAQs and vulnerability scans on the Merchant's TrustKeeper Portal, along with internal Penetration Tests, all personnel, attestations, training, procedures, controls and documentation within the CDE (Cardholder Data Environment). Periodically, additional information and follow-up interviews may be requested and visits to NU Merchant locations may take place with or without notice.

At the discretion of e-Commerce Operations, audits by an external PCI-Certified QSA (Qualified Security Assessor) or internally by NU Office for Audit and Advisory Services may occasionally be requested in order to comprehensively review a Merchant card location's credit card operations. 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 account being revoked.

Trustwave-TrustKeeper 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.

As of v.3.0 (January, 2015) PCI has issued 8 versions of the SAQ. e-Commerce Operations will help determine which SAQ applies to your situation. General definitions are below.

SAQ Type	Type of Payment System
SAQ A v.3.0	Card-not-present merchants (e-commerce or mail/telephone-order) that have fully outsourced all cardholder data functions to PCI DSS compliant third-party service providers, with no electronic storage, processing, or transmission of any cardholder data on the merchant's systems or premises. ***Not applicable to face-to-face channels.***
SAQ A-EP v3.0 (new 2015)	Card Not Present, E-commerce merchants who outsource all payment processing to PCI DSS validated third parties, and who have a website(s) that doesn't directly receive cardholder data but that can impact the security of the payment transaction. No electronic storage, processing, or transmission of any cardholder data on the merchant's systems or premises. ***Applicable only to e-Commerce channels***
SAQ B v.3.0	Merchants using only Imprint machines with no electronic cardholder data storage and/or Standalone, dial-out terminals with no electronic cardholder data storage. ***Not applicable to e-Commerce channels.***
SAQ B-IP v.3.0 (new 2015)	Merchants using only standalone, PTS-approved payment terminals with an IP connection to the payment processor, with no electronic cardholder data storage. ***Not applicable to e-commerce channels.***
SAQ C v.3.0	Merchants with payment application systems connected to the Internet, no electronic cardholder data storage. ***Not applicable to e-Commerce channels.***
SAQ C-VT v.3.0	Merchants who manually enter a single transaction at a time via a keyboard into an Internet-based Virtual Terminal solution that is provided and hosted by a PCI DSS validated third-party service provider. No electronic cardholder data storage. ***Not applicable to e-Commerce channels.***
SAQ D v.3.0	All other SAQ-Eligible Merchants
SAQ P2PE-HW v.3.0	Merchants using only hardware payment terminals that are included in and managed via a validated, PCI SSC-listed P2PE solution, with no electronic cardholder data storage. ***Not applicable to e-Commerce channels.***

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.

Related Documents

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