Information Technology Standard for PCI environment

Syracuse University – Information Technology and Services

Information Security Standard – S0101

1.0 Scope

- Any technology based equipment used to store, process, or transmit credit card data for Syracuse University.
- All information systems that can electronically communicate with any of the devices described above.
- This includes (but is not limited to) computers, laptops, PDA's, card readers, point of sale systems, and network equipment (both wired and wireless)

2.0 Purpose

In order for Syracuse University to accept Credit Cards as a form of payment for any of its services, it must comply with the Payment Card Industry's Data Security Standard (PCI DSS). The purpose of this standard is to define the appropriate PCI DSS requirements for systems considered to be in scope as defined in Section 1.0 of this document.

3.0 Introduction

Syracuse University allows use of e-commerce to conduct business and thus must adhere to the mandatory security standards and control requirements for protecting cardholders' information.
A University Department accepting credit cards is a credit card merchant.

Campus credit card vendors must comply with **Payment Card Industry Data Security Standards**, must complete annual self-assessment questionnaires, and must attest to their PCI DSS compliance.

All Syracuse University vendors shall be responsible for costs associated with PCI DSS compliance as well as any fines or other fees associated with their non-compliance. Overall as a Level 3 Merchant, SU must attest PCI compliance to the processing bank. All vendors are responsible for complying with the standard assigned to their group (detailed below).

The PCI Steering Committee (the Committee) serves as Syracuse University's (SU) primary oversight body to ensure customer's card holder data is processed securely according to the PCI Data Security Standards (PCI DSS).

Based on the information provided to SU PCI Committee, it has allocated following PCI DSS Groups to the merchants and associated standard which are essential for their compliance :-

Group Number	Merchant Group	Related SAQ	Required Standard(s)
1	Group A	A	4.4.3
2	Group B	B	4.2 (ALL), 4.4.1, 4.4.3

3	Group E	C-VT	4.1-4.4.1 (ALL), 4.4.3
4	Group C	C	4.1-4.5 (ALL)
5	Group D	D	4.1-4.5 (ALL) , Appendix 1-5

4.0 Standard

The standard below sets forth requirements covering a broad range Information Technology and Security procedures for scoped systems. The requirements have been derived from the *Payment Card Industry Data Security Standard Self-Assessment Questionnaires and* by the SU PCI Committee.

The PCI DSS SAQ has been segregated into major adherence areas with each area pertaining to specific groups.

- 4.1 Build and Maintain a Secure Network
  - 4.1.1 Establish firewall and router configuration standards
  - 4.1.2 Change/remove vendor-supplied defaults for system passwords and security parameters
- 4.2 Protect Cardholder Data
  - 4.2.1 Protect stored cardholder data
  - 4.2.2 Encrypt transmission of cardholder data across open, public networks
- 4.3 Maintain a Vulnerability Management Program
  - 4.3.1 Use and regularly update anti-virus software or programs
  - 4.3.2 Develop and maintain secure systems and applications
- 4.4 Implement Strong Access Control Measures
  - 4.4.1 Restrict access to cardholder data by business need to know
  - 4.4.2 Assign a unique ID to each person with computer access
  - 4.4.3 Restrict physical access to cardholder data
- 4.5 Regularly Monitor and Test Networks
  - 4.5.1 Track and monitor all access to network resources and cardholder data
  - 4.5.2 Regularly test security systems and processes

5.0 Exception

Currently no exceptions have been identified in the environment. Please note any exception will necessitate need to re comply with PCI DSS standard for entire Syracuse University. In case of any questions and clarifications, please involve the contacts listed below.

6.0 Referred Documents, Web Pages and Contact Information

Item	Location/Info
Standard: Payment Card Industry Data Security Standard V3.2	https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2.pdf?agreement=true&time=1481746845214

Guideline: PCI DSS Self-Assessment Questionnaire D v3.2	https://www.pcisecuritystandards.org/documents/PCI-DSS-v3_2-SAQ-D_Merchant.pdf?agreement=true&time=1481747436821
Guideline: PCI DSS Self-Assessment Questionnaire C-VT v3.2	https://www.pcisecuritystandards.org/documents/PCI-DSS-v3_2-SAQ-C_VT.pdf?agreement=true&time=1481747436766
Guideline: PCI DSS Self-Assessment Questionnaire C v3.2	https://www.pcisecuritystandards.org/documents/PCI-DSS-v3_2-SAQ-C.pdf?agreement=true&time=1481747436786
Guideline: PCI DSS Self-Assessment Questionnaire B v3.2	https://www.pcisecuritystandards.org/documents/PCI-DSS-v3_2-SAQ-B.pdf?agreement=true&time=1481747436738
Guideline: PCI DSS Self-Assessment Questionnaire A v3.2	https://www.pcisecuritystandards.org/documents/PCI-DSS-v3_2-SAQ-A.pdf?agreement=true&time=1481747436698
Appendix 1	PCI Network Security Standard
Appendix 2	PCI Credit Card Handling Standard
Appendix 3	PCI Vulnerability Management Standard
Appendix 4	PCI Access Control Standard
Appendix 5	PCI Network Monitor Standard
Contact: Director of Information Security	Christopher Croad ccroad@syr.edu

Document Info

Version:	3.0
Effective Date:	October, 1, 2016
Date of Last Review	October 25, 2016
Date of Next Mandatory Review	October 31st, 2017