J. Sargeant Reynolds Community College Standard Operating Procedure: PCI Management

18 – Compliance

18.2.4 PCI Management

Version: 1.1
Status: Revised – 05/21/2018
Contact: Primary Information Security Officer; Information Security Shared Services

Control

Payment Card Industry Data Security Standard (PCI DSS) is a security framework created by the PCI Standards Security Council that details requirements necessary to protect the storage, processing, or transmission of cardholder data. The PCI DSS is a mandated set of requirements agreed upon by the five major credit card companies: VISA, MasterCard, Discover, American Express, and JCB. The VCCS and Colleges that handle any cardholder data are required to continually comply with PCI DSS, complete the appropriate Self-Assessment Questionnaire (SAQ) annually, and submit the SAQ to the acquiring bank.

Implement Strong Access Control Measures

Assign a unique ID to each person with computer access. Restrict physical access to cardholder data. Secured environments include locked drawers and safes, with limited access to only authorized individuals.

Security Awareness Training

Security awareness training should include Red Flag training and general information on understanding credit card security requirements. Training should be provided to any employee who handles or has access to credit card information. This information may be placed in the current security awareness training system (Global Learning Systems) for annual recertification. Colleges may contact Shared Services to obtain PDF documents that can assist in this training.

Physical Inspection of PCI Devices

PCI devices should be periodically inspected to verify they are in a secure location and that there has been no tampering of the device.

- Maintain an inventory of all devices.
- PCI devices should not be accessible by the public.
- Physically inspect devices for tampering. The *Skimming Prevention: Best Practices for Merchants* guide can assist colleges in the physical inspection process.

Vulnerability Scans and Penetration Testing

Merchants/ Service providers	Quarterly* external vulnerability scan (ASV)	Quarterly* internal vulnerability scan	Annual** penetration test (Level 2)	Quarterly wireless network analysis	Annual Web application vulnerability scan[1]
	Req. 11.2.2	Req. 11.2.1	Req. 11.3	Req. 11.1	Req. 6.6
ROC	✓	✓	✓	✓	✓
SAQ D for Merchants	✓	✓	✓	✓	✓
SAQ D for Service Providers	✓	✓	✓	✓	✓
SAQ C	✓	✓	✓*	✓	✓
SAQ C-VT					
SAQ P2PE-HW					
SAQ B					
SAQ B-IP	✓				
SAQ A-EP	✓	✓	✓+		✓
SAQ A					

If noted in the previous table, the College shall perform internal and external vulnerability scans at least quarterly or after any significant changes in the network. Address vulnerabilities and perform rescans as needed, until a passing scan is achieved. Quarterly external scans must be performed by an Approved Scanning Vendor (ASV). Scans conducted after network changes and internal scans may be performed by internal staff.

https://www.pcisecuritystandards.org/approved_companies_providers/approved_scanning_vendors.php

The College shall perform internal and external penetration testing at least once a year and after any significant infrastructure or application upgrade or modification. The penetration tests must include network-layer and application-layer penetration testing. The PCI requirement also notes

the penetration tests may be done by a qualified internal resource or qualified external third party.

If segmentation is used to reduce PCI DSS scope, perform penetration tests at least annually to verify the segmentation methods are operational and effective. Service providers using segmentation must confirm PCI DSS scope by performing penetration testing on segmentation controls at least every six months and after making changes to these controls. *(Note: The additional requirement for service providers is a best practice until 31 January 2018, after which it becomes a requirement.)*

Annual Verification of PCI Compliance – On-Site Vendors

Colleges should verify that any vendors who accept credit cards on the campus are in compliance with PCI Data Security Standards (DSS). An example email may include:

<College Name> Community College is required to be in compliance with the PCI Data Security Standards (DSS). Part of the requirement is that we verify on an annual basis that our third-party contractors are also in compliance with this standard. Please verify that your company has completed the requirements to be in compliance with PCI-DSS. Thank you for your assistance.

The college should receive some type of verification from the vendor that the vendor has received their PCI certification for the year. The college should retain all email communication for audit purposes.

Annual PCI SAQ

The PCI DSS SAQ is a validation tool for merchants and service providers that are not required to undergo an on-site data security assessment per the PCI DSS Security Assessment Procedures. The purpose of the SAQ is to assist colleges in self-evaluating compliance with the PCI DSS.

SAQ	Description
A	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.*

A-EP	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.*
B	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.*
B-IP	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.*
C-VT	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.*
C	Merchants with payment application systems connected to the Internet, no electronic cardholder data storage. *Not applicable to e-commerce channels.*
P2PE	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.*
D	SAQ D for Merchants: All merchants not included in descriptions for the above SAQ types. SAQ D for Service Providers: All service providers defined by a payment card brand as eligible to complete a SAQ.

Colleges may download the appropriate SAQ at:

https://www.pcisecuritystandards.org/security_standards/documents.php?category=saqs

Compensating Controls

Compensating controls may be considered for most PCI DSS requirements when a college cannot meet the technical specification of a requirement, but has sufficiently mitigated the associated risk through alternative controls. If the college does not have the exact control specified in PCI DSS but has other controls in place that satisfy the PCI DSS definition of compensating controls, the college should do the following:

a. Respond to the appropriate SAQ question then note the use of each compensating control used to satisfy a requirement.

b. Document the use of compensating controls by completing the Compensating Controls Worksheet in the appropriate appendix of the SAQ.

c. Submit all completed Compensating Controls Worksheets, along with the completed SAQ and/or Attestation, according to instructions from the acquirer or payment brand.

Validated Payment Applications

Part of each SAQ includes verifying the payment application in use by the college is validated. Colleges may use the link below to determine the payment application in use, version number and the date last validated according to PABP/PA-DSS. Colleges may need to use the manufacturer, model number or other information to look up the current payment application in use at the college using the link below:

https://www.pcisecuritystandards.org/approved_companies_providers/validated_payment_applications.php

---

Attestation of Compliance

The Attestation is your self-certification that you are eligible to perform and have actually performed a PCI DSS self-assessment. For those colleges using Aperia to enter the SAQ, the SAQ and Attestation will be transmitted to Nelnet.

For colleges not using Aperia, the SAQ and Attestation shall be emailed to:

pci@paymentspring.com

or

Cindy Cunningham
Customer Relationship Manager – Mid Atlantic Region
Nelnet Business Solutions
(757) 871-9100
Cindy.Cunningham@nelnet.net

Colleges should retain a copy of the email for audit purposes.

PCI Links

PCI Security Standards Council Website:
https://www.pcisecuritystandards.org/

PCI documents Library:

https://www.pcisecuritystandards.org/document_library?category=pcidss&document=pci_dss

REVISION HISTORY

Date	Version	Reviewer	List of Changes
March 2017	1.0	Vicky Carwile	
May 2018	1.1	Mark Webster	Revisions to adapt the SOP to Reynolds, including college branding, and updating contact information and security awareness training.