B-IP	3.2.1
SAQ B-IP Template for Verifone Vx520 Ethernet	2022

Self-Assessment Questionnaire B-IP 3.2.1 and Attestation of Compliance

Instructions for Submission

This document must be completed as a declaration of the results of the merchant's self-assessment with the Payment Card Industry Data Security Standard Requirements and Security Assessment Procedures (PCI DSS). Complete all sections: The merchant is responsible for ensuring that each section is completed by the relevant parties, as applicable. Contact acquirer (merchant bank) or the payment brands to determine reporting and submission procedures.

Part 1. Merchant and Qualified Security Assessor Information

Part 1a. Merchant Organization Information

Company Name: University of Oregon

DBA (doing business as): #### SAQ B-IP Template Vx 520 Ethernet

Contact Name: Mark McCulloch

Title: Director Info Systems Business Affairs

Telephone:

E-mail: * mmccullo@uoregon.edu

Business Address:

City

State/Province

Country

Zip

URL:

Part 1b. Qualified Security Assessor Company Information (if applicable)

Company Name: CampusGuard LLC

Lead QSA Contact Name: Jarvis Gilmore

Title: Security Advisor

Telephone:

(832) 598-1475

E-mail:

jgilmore@campusguard.com

Business Address:

4740 North Cumberland Avenue, Suite 365

City

Chicago

State/Province

IL

Country

USA

Zip

60656

QSA URL:

Part 2. Executive Summary

Part 2a. Type of Merchant Business (check all that apply)

- [ ] Retailer
- [ ] Telecommunication
- [ ] Grocery and Supermarkets
- [ ] Petroleum
- [ ] E-Commerce
- [ ] Mail order/telephone order (MOTO)
- [x] Others

(please specify):

Higher Education

What types of payment channels does your business serve?	Which payment channels are covered by this SAQ?
[x] Mail order/telephone order (MOTO)	[x] Mail order/telephone order (MOTO)
[ ] E-Commerce	[ ] E-Commerce
[x] Card-present (face-to-face)	[x] Card-present (face-to-face)

Note: *If your organization has a payment channel or process that is not covered by this SAQ, consult your acquirer or payment brand about validation for the other channels.*

Part 2b. Description of Payment Card Business

How and in what capacity does your business store, process and/or transmit cardholder data?

No storage, process over phone or in person using Verifone Vx 520 and transmit via UO Ethernet.

Part 2c. Locations

List types of facilities (for example, retail outlets, corporate offices, data centers, call centers, etc.) and a summary of locations included in the PCI DSS review.

Type of facility	Number of facilities of this type	Location(s) of facility (city, country)

Office	1	Building and Room #

Part 2d. Payment Application(s)

Does the organization use one or more Payment Applications?

○ Yes ◉ No ○ Don't Know

Provide the following information regarding the Payment Applications your organization uses:

Payment Application Name	Version Number

Application Vendor	Is application PA-DSS Listed?	PA-DSS Listing Expiry date (if applicable)
	○ Yes ○ No ○ Don't Know	
	○ Yes ○ No ○ Don't Know	
	○ Yes ○ No ○ Don't Know	

Part 2e. Description of Environment

Provide a high-level description of the environment covered by this assessment.
For example:

- ***Connections into and out of the cardholder data environment (CDE).***
- ***Critical system components within the CDE, such as POS devices, databases, web servers, etc., and any other necessary payment components, as applicable.***

Terminal connected to PCI VLAN via Ethernet port.

Does your business use network segmentation to affect the scope of your PCI DSS environment?
(Refer to "Network Segmentation" section of PCI DSS for guidance on network segmentation)

(●) Yes ( ) No ( ) Don't Know

Part 2f. Third-Party Service Providers

Does your company have a relationship with a Qualified Integrator Reseller (QIR) for the purpose of the services being validated? If Yes:

( ) Yes (●) No ( ) Don't Know

Name of QIR Company:

QIR Individual Name:

Description of services provided by QIR:

Does your company share cardholder data with any third-party service providers (for example, Qualified Integrator & Resellers (QIR), gateways, payment processors, payment service providers (PSP), web-hosting companies, airline booking agents, loyalty program agents, etc.)?

(●) Yes ( ) No ( ) Don't Know

If Yes:

Name of service provider:	Description of services provided:
Elavon	Merchant services

Note: *Requirement 12.8 applies to all entities in this list.*

Part 2g. Eligibility to Complete SAQ B-IP

Merchant certifies eligibility to complete this shortened version of the Self-Assessment Questionnaire because, for this payment channel:

- [x] Merchant uses only standalone, PTS-approved point-of-interaction (POI) devices (excludes SCRs) connected via IP to merchant's payment processor to take customers' payment card information;
- [ ] The standalone IP-connected POI devices are validated to the PTS POI program as listed on the PCI SSC website (excludes SCRs);
- [x] The standalone IP-connected POI devices are not connected to any other systems within the merchant environment (this can be achieved via network segmentation to isolate POI devices from other systems);
- [x] The only transmission of cardholder data is from the PTS-approved POI devices to the payment processor;
- [x] The POI device does not rely on any other device (e.g., computer, mobile phone, tablet, etc.) to connect to the payment processor;
- [x] Merchant does not store cardholder data in electronic format; and
- [x] If Merchant does store cardholder data, such data is only paper reports or copies of paper receipts and is not received electronically.

Requirement 1: Install and maintain a firewall configuration to protect data

1.1.2 (a) Is there a current network diagram that documents all connections between the cardholder data environment and other networks, including any wireless networks?

◉ Yes ○ No ○ Don't Know ○ Not Applicable (N/A) ○ Compensating Control Used

1.1.2 (b) Is there a process to ensure the diagram is kept current?

◉ Yes ○ No ○ Don't Know ○ Not Applicable (N/A) ○ Compensating Control Used

1.1.4 (a) Is a firewall required and implemented at each Internet connection and between any demilitarized zone (DMZ) and the internal network zone?

◉ Yes ○ No ○ Don't Know ○ Not Applicable (N/A) ○ Compensating Control Used

1.1.4 (b) Is the current network diagram consistent with the firewall configuration standards?

◉ Yes ○ No ○ Don't Know ○ Not Applicable (N/A) ○ Compensating Control Used

1.1.6 (a) Do firewall and router configuration standards include a documented list of services, protocols, and ports, including business justification and approval for each?

◉ Yes ○ No ○ Don't Know ○ Not Applicable (N/A) ○ Compensating Control Used

1.1.6 (b) Are all insecure services, protocols, and ports identified, and are security features documented and implemented for each identified service?

◉ Yes ○ No ○ Don't Know ○ Not Applicable (N/A) ○ Compensating Control Used

1.2 Do firewall and router configurations restrict connections between untrusted networks and any system in the cardholder data environment as follows:

Note: *An "untrusted network" is any network that is external to the networks belonging to the entity under review, and/or which is out of the entity's ability to control or manage.*

1.2.1 (a) Is inbound and outbound traffic restricted to that which is necessary for the cardholder data environment?

◉ Yes ○ No ○ Don't Know ○ Not Applicable (N/A) ○ Compensating Control Used

1.2.1 (b) Is all other inbound and outbound traffic specifically denied (for example by using an explicit "deny all" or an implicit deny after allow statement)?

◉ Yes ○ No ○ Don't Know ○ Not Applicable (N/A) ○ Compensating Control Used

1.2.3 Are perimeter firewalls installed between all wireless networks and the cardholder data environment, and are these firewalls configured to deny or, if traffic is necessary for business purposes, permit only authorized traffic between the wireless environment and the cardholder data environment?

◉ Yes ○ No ○ Don't Know ○ Not Applicable (N/A) ○ Compensating Control Used

1.3 Is direct public access prohibited between the Internet and any system component in the cardholder data environment, as follows:

1.3.3 Are anti-spoofing measures implemented to detect and block forged sourced IP addresses from entering the network?

(For example, block traffic originating from the internet with an internal address.)

◉ Yes ○ No ○ Don't Know ○ Not Applicable (N/A) ○ Compensating Control Used

1.3.4 Is outbound traffic from the cardholder data environment to the Internet explicitly authorized?

◉ Yes ○ No ○ Don't Know ○ Not Applicable (N/A) ○ Compensating Control Used

1.3.5 Are only established connections permitted into the network?

◉ Yes ○ No ○ Don't Know ○ Not Applicable (N/A) ○ Compensating Control Used

Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters

2.1 (a) Are vendor-supplied defaults always changed before installing a system on the network? *This applies to ALL default passwords, including but not limited to those used by operating systems, software that provides security services, application and system accounts, point-of-sale (POS) terminals, Simple Network Management Protocol (SNMP) community strings, etc.).*

(●) Yes ( ) No ( ) Don't Know ( ) Not Applicable (N/A) ( ) Compensating Control Used

2.1 (b) Are unnecessary default accounts removed or disabled before installing a system on the network?

(●) Yes ( ) No ( ) Don't Know ( ) Not Applicable (N/A) ( ) Compensating Control Used

2.1.1 For wireless environments connected to the cardholder data environment or transmitting cardholder data, are ALL wireless vendor defaults changed at installations, as follows:

2.1.1 (a) Are encryption keys changed from default at installation, and changed anytime anyone with knowledge of the keys leaves the company or changes positions?

( ) Yes ( ) No ( ) Don't Know (●) Not Applicable (N/A) ( ) Compensating Control Used

2.1.1 (b) Are default SNMP community strings on wireless devices changed at installation?

( ) Yes ( ) No ( ) Don't Know (●) Not Applicable (N/A) ( ) Compensating Control Used

2.1.1 (c) Are default passwords/passphrases on access points changed at installation?

( ) Yes ( ) No ( ) Don't Know (●) Not Applicable (N/A) ( ) Compensating Control Used

2.1.1 (d) Is firmware on wireless devices updated to support strong encryption for authentication and transmission over wireless networks?

( ) Yes ( ) No ( ) Don't Know (●) Not Applicable (N/A) ( ) Compensating Control Used

2.1.1 (e) Are other security-related wireless vendor defaults changed, if applicable?

( ) Yes ( ) No ( ) Don't Know (●) Not Applicable (N/A) ( ) Compensating Control Used

2.3 Is non-console administrative access encrypted as follows:

Note: Where SSL/early TLS is used, the requirements in Appendix A2 must be completed.

2.3 (a) Is all non-console administrative access encrypted with strong cryptography, and is a strong encryption method invoked before the administrator's password is requested?

(●) Yes ( ) No ( ) Don't Know ( ) Not Applicable (N/A) ( ) Compensating Control Used

2.3 (b) Are system services and parameter files configured to prevent the use of Telnet and other insecure remote login commands?

( ) Yes ( ) No ( ) Don't Know (●) Not Applicable (N/A) ( ) Compensating Control Used

2.3 (c) Is administrator access to web-based management interfaces encrypted with strong cryptography?

(●) Yes ( ) No ( ) Don't Know ( ) Not Applicable (N/A) ( ) Compensating Control Used

2.3 (d) For the technology in use, is strong cryptography implemented according to industry best practice and/or vendor recommendations?

(●) Yes ( ) No ( ) Don't Know ( ) Not Applicable (N/A) ( ) Compensating Control Used

Requirement 3: Protect stored cardholder data

3.2 (c) Is sensitive authentication data deleted or rendered unrecoverable upon completion of the authorization process?

(•) Yes ( ) No ( ) Don't Know ( ) Not Applicable (N/A) ( ) Compensating Control Used

3.2 (d) Do all systems adhere to the following requirements regarding non-storage of sensitive authentication data after authorization (even if encrypted):

3.2.1 The full contents of any track (from the magnetic stripe located on the back of a card, equivalent data contained on a chip, or elsewhere) are not stored after authorization?
This data is alternatively called full track, track, track 1, track 2, and magnetic-stripe data.

Note: In the normal course of business, the following data elements from the magnetic stripe may need to be retained:

- ***The cardholder's name,***
- ***Primary account number (PAN),***
- ***Expiration date, and***
- ***Service code***

To minimize risk, store only these data elements as needed for business.

(•) Yes ( ) No ( ) Don't Know ( ) Not Applicable (N/A) ( ) Compensating Control Used

3.2.2 The card verification code or value (three-digit or four-digit number printed on the front or back of a payment card) is not stored after authorization?

(•) Yes ( ) No ( ) Don't Know ( ) Not Applicable (N/A) ( ) Compensating Control Used

3.2.3 The personal identification number (PIN) or the encrypted PIN block is not stored after authorization?

(•) Yes ( ) No ( ) Don't Know ( ) Not Applicable (N/A) ( ) Compensating Control Used

3.3 Is the PAN masked when displayed (the first six and last four digits are the maximum number of digits to be displayed) such that only personnel with a legitimate business need can see more than the first six/last four digits of the PAN?
Note: This requirement does not supersede stricter requirements in place for displays of cardholder data—for example, legal or payment card brand requirements for point-of-sale (POS) receipts.

(•) Yes ( ) No ( ) Don't Know ( ) Not Applicable (N/A) ( ) Compensating Control Used

Requirement 4: Encrypt transmission of cardholder data across open, public networks

4.1 (a) Are strong cryptography and security protocols used to safeguard sensitive cardholder data during transmission over open, public networks?
Examples of open, public networks include but are not limited to the Internet; wireless technologies, including 802.11 and Bluetooth; cellular technologies, for example, Global System for Mobile communications (GSM), Code division multiple access (CDMA); and General Packet Radio Service (GPRS).

(●) Yes ( ) No ( ) Don't Know ( ) Not Applicable (N/A) ( ) Compensating Control Used

4.1 (b) Are only trusted keys and/or certificates accepted?

(●) Yes ( ) No ( ) Don't Know ( ) Not Applicable (N/A) ( ) Compensating Control Used

4.1 (c) Are security protocols implemented to use only secure configurations, and to not support insecure versions or configurations?

(●) Yes ( ) No ( ) Don't Know ( ) Not Applicable (N/A) ( ) Compensating Control Used

4.1 (d) Is the proper encryption strength implemented for the encryption methodology in use (check vendor recommendations/best practices)?

(●) Yes ( ) No ( ) Don't Know ( ) Not Applicable (N/A) ( ) Compensating Control Used

4.1 (e) For TLS implementations, is TLS enabled whenever cardholder data is transmitted or received?
For example, for browser-based implementations:

- ***"HTTPS" appears as the browser Universal Record Locator (URL) protocol, and***
- ***Cardholder data is only requested if "HTTPS" appears as part of the URL.***

( ) Yes ( ) No ( ) Don't Know (●) Not Applicable (N/A) ( ) Compensating Control Used

4.1.1 Are industry best practices used to implement strong encryption for authentication and transmission for wireless networks transmitting cardholder data or connected to the cardholder data environment?

( ) Yes ( ) No ( ) Don't Know (●) Not Applicable (N/A) ( ) Compensating Control Used

4.2 (b) Are policies in place that state that unprotected PANs are not to be sent via end-user messaging technologies?

(●) Yes ( ) No ( ) Don't Know ( ) Not Applicable (N/A) ( ) Compensating Control Used

Requirement 6: Develop and maintain secure systems and applications

6.1 Is there a process to identify security vulnerabilities, including the following:

- **Using reputable outside sources for vulnerability information?**
- **Assigning a risk ranking to vulnerabilities that includes identification of all "high" risk and "critical" vulnerabilities?**

Note: Risk rankings should be based on industry best practices as well as consideration of potential impact. For example, criteria for ranking vulnerabilities may include consideration of the CVSS base score and/or the classification by the vendor, and/or type of systems affected.

Methods for evaluating vulnerabilities and assigning risk ratings will vary based on an organization's environment and risk assessment strategy. Risk rankings should, at a minimum, identify all vulnerabilities considered to be a "high risk" to the environment. In addition to the risk ranking, vulnerabilities may be considered "critical" if they pose an imminent threat to the environment, impact critical systems, and/or would result in a potential compromise if not addressed. Examples of critical systems may include security systems, public-facing devices and systems, databases, and other systems that store, process or transmit cardholder data.

◉ Yes ○ No ○ Don't Know ○ Not Applicable (N/A) ○ Compensating Control Used

6.2 (a) Are all system components and software protected from known vulnerabilities by installing applicable vendor-supplied security patches?

◉ Yes ○ No ○ Don't Know ○ Not Applicable (N/A) ○ Compensating Control Used

6.2 (b) Are critical security patches installed within one month of release?
Note: Critical security patches should be identified according to the risk ranking process defined in Requirement 6.1.

◉ Yes ○ No ○ Don't Know ○ Not Applicable (N/A) ○ Compensating Control Used

Requirement 7: Restrict access to cardholder data by business need-to-know

7.1.2 Is access to privileged user IDs restricted as follows:

- **To least privileges necessary to perform job responsibilities?**
- **Assigned only to roles that specifically require that privileged access?**

(●) Yes ( ) No ( ) Don't Know ( ) Not Applicable (N/A) ( ) Compensating Control Used

7.1.3 Are access assigned based on individual personnel's job classification and function?

(●) Yes ( ) No ( ) Don't Know ( ) Not Applicable (N/A) ( ) Compensating Control Used

Requirement 8: Assign a unique ID to each person with computer access

8.1 Are policies and procedures for user identification management controls defined and in place for non-consumer users and administrators on all system components, as follows:

8.1.5 (a) Are accounts used by third parties to access, support, or maintain system components via remote access enabled only during the time period needed and disabled when not in use?

○ Yes ○ No ○ Don't Know ◉ Not Applicable (N/A) ○ Compensating Control Used

8.1.5 (b) Are third party remote access accounts monitored when in use?

○ Yes ○ No ○ Don't Know ◉ Not Applicable (N/A) ○ Compensating Control Used

8.3 Is all individual non-console administrative access and all remote access to the CDE secured using multi-factor authentication, as follows:
Note: Multi-factor authentication requires that a minimum of two of the three authentication methods (see PCI DSS Requirement 8.2 for descriptions of authentication methods) be used for authentication. Using one factor twice (for example, using two separate passwords) is not considered multi-factor authentication.

8.3.1 Is multi-factor authentication incorporated for all non-console access into the CDE for personnel with administrative access?

○ Yes ○ No ○ Don't Know ○ Not Applicable (N/A) ○ Compensating Control Used

8.3.2 Is multi-factor authentication incorporated for all remote network access (both user and administrator, and including third party access for support or maintenance) originating from outside the entity's network?

○ Yes ○ No ○ Don't Know ◉ Not Applicable (N/A) ○ Compensating Control Used

8.5 Are group, shared, or generic accounts, passwords, or other authentication methods prohibited as follows:

- **Generic user IDs and accounts are disabled or removed;**
- **Shared user IDs for system administration activities and other critical functions do not exist; and**
- **Shared and generic user IDs are not used to administer any system components?**

○ Yes ○ No ○ Don't Know ◉ Not Applicable (N/A) ○ Compensating Control Used

Requirement 9: Restrict physical access to cardholder data

9.1.2 Are physical and/or logical controls in place to restrict access to publicly accessible network jacks?
For example, network jacks located in public areas and areas accessible to visitors could be disabled and only enabled when network access is explicitly authorized. Alternatively, processes could be implemented to ensure that visitors are escorted at all times in areas with active network jacks.

◉ Yes ○ No ○ Don't Know ○ Not Applicable (N/A) ○ Compensating Control Used

9.5 Are all media physically secured (including but not limited to computers, removable electronic media, paper receipts, paper reports, and faxes)?
For purposes of Requirement 9, "media" refers to all paper and electronic media containing cardholder data.

◉ Yes ○ No ○ Don't Know ○ Not Applicable (N/A) ○ Compensating Control Used

9.6 (a) Is strict control maintained over the internal or external distribution of any kind of media?

○ Yes ○ No ○ Don't Know ○ Not Applicable (N/A) ○ Compensating Control Used

9.6 (b) Do controls include the following:

9.6.1 Is media classified so the sensitivity of the data can be determined?

○ Yes ○ No ○ Don't Know ○ Not Applicable (N/A) ○ Compensating Control Used

9.6.2 Is media sent by secured courier or other delivery method that can be accurately tracked?

○ Yes ○ No ○ Don't Know ○ Not Applicable (N/A) ○ Compensating Control Used

9.6.3 Is management approval obtained prior to moving the media (especially when media is distributed to individuals)?

○ Yes ○ No ○ Don't Know ○ Not Applicable (N/A) ○ Compensating Control Used

9.7 Is strict control maintained over the storage and accessibility of media?

○ Yes ○ No ○ Don't Know ○ Not Applicable (N/A) ○ Compensating Control Used

9.8 (a) Is all media destroyed when it is no longer needed for business or legal reasons?

○ Yes ○ No ○ Don't Know ○ Not Applicable (N/A) ○ Compensating Control Used

9.8 (c) Is media destruction performed as follows:

9.8.1 (a) Are hardcopy materials cross-cut shredded, incinerated, or pulped so that cardholder data cannot be reconstructed?

○ Yes ○ No ○ Don't Know ○ Not Applicable (N/A) ○ Compensating Control Used

9.8.1 (b) Are storage containers used for materials that contain information to be destroyed secured to prevent access to the contents?

○ Yes ○ No ○ Don't Know ○ Not Applicable (N/A) ○ Compensating Control Used

9.9 Are devices that capture payment card data via direct physical interaction with the card protected against tampering and substitution as follows?
Note: This requirement applies to card-reading devices used in card-present transactions (that is, card swipe or dip) at the point of sale. This requirement is not intended to apply to manual key-entry components such as computer keyboards and POS keypads.

"Yes" answers to requirements at 9.9 mean the merchant has policies and procedures in place for Requirements 9.9.1 - 9.9.3, and that they maintain a current list of devices, conduct periodic device inspections, and train employees about what to look for to detect tampered or replaced devices.

9.9 (a) Do policies and procedures require that a list of such devices be maintained?

◉ Yes ○ No ○ Don't Know ○ Not Applicable (N/A) ○ Compensating Control Used

9.9 (b) Do policies and procedures require that devices are periodically inspected to look for tampering or substitution?

◉ Yes ○ No ○ Don't Know ○ Not Applicable (N/A) ○ Compensating Control Used

9.9 (c) Do policies and procedures require that personnel are trained to be aware of suspicious behavior and to report tampering or substitution of devices?

○ Yes ○ No ○ Don't Know ○ Not Applicable (N/A) ○ Compensating Control Used

9.9.1 (a) Does the list of devices include the following?

- **Make, model of device**
- **Location of device (for example, the address of the site or facility where the device is located)**
- **Device serial number or other method of unique identification**

○ Yes ○ No ○ Don't Know ○ Not Applicable (N/A) ○ Compensating Control Used

9.9.1 (b) Is the list accurate and up to date?

○ Yes ○ No ○ Don't Know ○ Not Applicable (N/A) ○ Compensating Control Used

9.9.1 (c) Is the list of devices updated when devices are added, relocated, decommissioned, etc.?

○ Yes ○ No ○ Don't Know ○ Not Applicable (N/A) ○ Compensating Control Used

9.9.2 (a) Are device surfaces periodically inspected to detect tampering (for example, addition of card skimmers to devices), or substitution (for example, by checking the serial number or other device characteristics to verify it has not been swapped with a fraudulent device) as follows?
Note: Examples of signs that a device might have been tampered with or substituted include unexpected attachments or cables plugged into the device, missing or changed security labels, broken or differently colored casing, or changes to the serial number or other external markings.

○ Yes ○ No ○ Don't Know ○ Not Applicable (N/A) ○ Compensating Control Used

9.9.2 (b) Are personnel aware of procedures for inspecting devices?

○ Yes ○ No ○ Don't Know ○ Not Applicable (N/A) ○ Compensating Control Used

9.9.3 Are personnel trained to be aware of attempted tampering or replacement of devices, to include the following?

9.9.3 (a) Do training materials for personnel at point-of-sale locations include the following?

- **Verify the identity of any third-party persons claiming to be repair or maintenance personnel, prior to granting them access to modify or troubleshoot devices.**
- **Do not install, replace, or return devices without verification.**
- **Be aware of suspicious behavior around devices (for example, attempts by unknown persons to unplug or open devices).**
- **Report suspicious behavior and indications of device tampering or substitution to appropriate personnel (for example, to a manager or security officer).**

◉ Yes ○ No ○ Don't Know ○ Not Applicable (N/A) ○ Compensating Control Used

9.9.3 (b) Have personnel at point-of-sale locations received training, and are they aware of procedures to detect and report attempted tampering or replacement of devices?

○ Yes ○ No ○ Don't Know ○ Not Applicable (N/A) ○ Compensating Control Used

Requirement 11: Regularly test security systems and processes

11.2 Are internal and external network vulnerability scans run at least quarterly and after any significant change in the network (such as new system component installations, changes in network topology, firewall rule modifications, product upgrades), as follows?
Note: Multiple scan reports can be combined for the quarterly scan process to show that all systems were scanned and all applicable vulnerabilities have been addressed. Additional documentation may be required to verify non-remediated vulnerabilities are in the process of being addressed.

For initial PCI DSS compliance, it is not required that four quarters of passing scans be completed if the assessor verifies 1) the most recent scan result was a passing scan, 2) the entity has documented policies and procedures requiring quarterly scanning, and 3) vulnerabilities noted in the scan results have been corrected as shown in a re-scan(s). For subsequent years after the initial PCI DSS review, four quarters of passing scans must have occurred.

11.2.2 (a) Are quarterly external vulnerability scans performed?
Note: Quarterly external vulnerability scans must be performed by an Approved Scanning Vendor (ASV), approved by the Payment Card Industry Security Standards Council (PCI SSC).

Refer to the ASV Program Guide published on the PCI SSC website for scan customer responsibilities, scan preparation, etc.

◉ Yes ○ No ○ Don't Know ○ Not Applicable (N/A) ○ Compensating Control Used

11.2.2 (b) Do external quarterly scan and rescan results satisfy the *ASV Program Guide* requirements for a passing scan (for example, no vulnerabilities rated 4.0 or higher by the CVSS, and no automatic failures)?

◉ Yes ○ No ○ Don't Know ○ Not Applicable (N/A) ○ Compensating Control Used

11.2.2 (c) Are quarterly external vulnerability scans performed by a PCI SSC Approved Scanning Vendor (ASV)?

◉ Yes ○ No ○ Don't Know ○ Not Applicable (N/A) ○ Compensating Control Used

11.3.4 (a) Are penetration-testing procedures defined to test all segmentation methods, to confirm they are operational and effective, and isolate all out-of-scope systems from systems in the CDE?

◉ Yes ○ No ○ Don't Know ○ Not Applicable (N/A) ○ Compensating Control Used

11.3.4 (b) Does penetration testing to verify segmentation controls meet the following?

- **Performed at least annually and after any changes to segmentation controls/methods.**
- **Covers all segmentation controls/methods in use.**
- **Verifies that segmentation methods are operational and effective, and isolate all out-of-scope systems from systems in the CDE.**

◉ Yes ○ No ○ Don't Know ○ Not Applicable (N/A) ○ Compensating Control Used

11.3.4 (c) Are tests performed by a qualified internal resource or qualified external third party, and if applicable, does organizational independence of the tester exist (not required to be a QSA or ASV)?

◉ Yes ○ No ○ Don't Know ○ Not Applicable (N/A) ○ Compensating Control Used

Requirement 12: Maintain a policy that addresses information security

12.1 Is a security policy established, published, maintained, and disseminated to all relevant personnel?

◉ Yes ○ No ○ Don't Know ○ Not Applicable (N/A) ○ Compensating Control Used

"Yes" answers for requirements at 12.1 mean that the merchant has a security policy that is reasonable for the size and complexity of the merchant's operations, and that the policy is reviewed annually and updated if needed. For example, such a policy could be a simple document that covers how to protect the store and payment devices in accordance with the P2PE Instruction Manual (PIM), and who to call in an emergency.

12.1.1 Is the security policy reviewed at least annually and updated when the environment changes?

◉ Yes ○ No ○ Don't Know ○ Not Applicable (N/A) ○ Compensating Control Used

12.3 Are usage policies for critical technologies developed to define proper use of these technologies and require the following:

Note: Examples of critical technologies include, but are not limited to, remote access and wireless technologies, laptops, tablets, removable electronic media, e-mail usage and Internet usage.

12.3.1 Explicit approval by authorized parties to use the technologies?

◉ Yes ○ No ○ Don't Know ○ Not Applicable (N/A) ○ Compensating Control Used

12.3.3 A list of all such devices and personnel with access?

◉ Yes ○ No ○ Don't Know ○ Not Applicable (N/A) ○ Compensating Control Used

12.3.5 Acceptable uses of the technologies?

◉ Yes ○ No ○ Don't Know ○ Not Applicable (N/A) ○ Compensating Control Used

12.3.9 Activation of remote-access technologies for vendors and business partners only when needed by vendors and business partners, with immediate deactivation after use?

○ Yes ○ No ○ Don't Know ◉ Not Applicable (N/A) ○ Compensating Control Used

12.4 Do security policy and procedures clearly define information security responsibilities for all personnel?

◉ Yes ○ No ○ Don't Know ○ Not Applicable (N/A) ○ Compensating Control Used

A "Yes" answer for Requirement 12.4 means that the merchant's security policy defines basic security responsibilities for all personnel, consistent with the size and complexity of the merchant's operations. For example, security responsibilities could be defined according to basic responsibilities by employee levels, such as the responsibilities expected of a manager/owner and those expected of clerks.

12.5.3 Establishing, documenting, and distributing security incident response and escalation procedures to ensure timely and effective handling of all situations?

◉ Yes ○ No ○ Don't Know ○ Not Applicable (N/A) ○ Compensating Control Used

A "Yes" answer for Requirement 12.5.3 means that the merchant has a person designated as responsible for the incident-response and escalation plan required at 12.9.

12.6 (a) Is a formal security awareness program in place to make all personnel aware of the cardholder data security policy and procedures?

◉ Yes ○ No ○ Don't Know ○ Not Applicable (N/A) ○ Compensating Control Used

A Yes" answer for Requirement 12.6 means that the merchant has a security awareness program in place, consistent with the size and complexity of the merchant's operations. For example, a simple awareness program could be a flyer posted in the back office, or a periodic e-mail sent to all employees. Examples of awareness program messaging include descriptions of security tips all employees should follow, such as how to lock doors and storage containers, how to determine whether a payment terminal has been tampered with, and how to identify legitimate personnel who may come to service hardware payment terminals.

12.8 Are policies and procedures maintained and implemented to manage service providers with whom cardholder data is shared, or that could affect the security of cardholder data, as follows:

"Yes" answers for requirements at 12.8 mean that the merchant has a list of, and agreements with, service providers they share cardholder data with. For example, such agreements would be applicable if a merchant uses a document-retention company to store paper documents that include account data.

12.8.1 Is a list of service providers maintained, including a description of the service(s) provided?

◉ Yes ○ No ○ Don't Know ○ Not Applicable (N/A) ○ Compensating Control Used

12.8.2 Is a written agreement maintained that includes an acknowledgement that the service providers are responsible for the security of cardholder data the service providers possess or otherwise store, process, or transmit on behalf of the customer, or to the extent that they could impact the security of the customer's cardholder data environment?

Note: The exact wording of an acknowledgement will depend on the agreement between the two parties, the details of the service being provided, and the responsibilities assigned to each party. The acknowledgement does not have to include the exact wording provided in this requirement.

◉ Yes ○ No ○ Don't Know ○ Not Applicable (N/A) ○ Compensating Control Used

12.8.3 Is there an established process for engaging service providers, including proper due diligence prior to engagement?

◉ Yes ○ No ○ Don't Know ○ Not Applicable (N/A) ○ Compensating Control Used

12.8.4 Is a program maintained to monitor service providers' PCI DSS compliance status at least annually?

◉ Yes ○ No ○ Don't Know ○ Not Applicable (N/A) ○ Compensating Control Used

12.8.5 Is information maintained about which PCI DSS requirements are managed by each service provider, and which are managed by the entity?

◉ Yes ○ No ○ Don't Know ○ Not Applicable (N/A) ○ Compensating Control Used

12.10 Has an incident response plan been implemented in preparation to respond immediately to a system breach, as follows:

"Yes" answers for requirements at 12.10 mean that the merchant has documented an incident response and escalation plan to be used for emergencies, consistent with the size and complexity of the merchant's operations. For example, such a plan could be a simple document posted in the back office that lists who to call in the event of various situations with an annual review to confirm it is still accurate, but could extend all the way to a full incident response plan including backup "hotsite" facilities and thorough annual testing. This plan should be readily available to all personnel as a resource in an emergency.

12.10.1 (a) Has an incident response plan been created to be implemented in the event of system breach?

◉ Yes ○ No ○ Don't Know ○ Not Applicable (N/A) ○ Compensating Control Used

Appendix A2 - Additional PCI DSS Requirements for Entities using SSL/early TLS for Card Present POS POI Terminal Connections.

A2.1 *For POS POI terminals* (at the merchant or payment acceptance location) *using SSL and/or early TLS:* Are the devices confirmed to not be susceptible to any known exploits for SSL/early TLS?
Note: This requirement is intended to apply to the entity with the POS POI terminal, such as a merchant. This requirement is not intended for service providers who serve as the termination or connection point to those POS POI terminals. Requirements A2.2 and A2.3 apply to POS POI service providers.

(●) Yes ( ) No ( ) Don't Know ( ) Not Applicable (N/A) ( ) Compensating Control Used

Appendix B: Compensating Controls Worksheet

Use this worksheet to define compensating controls for any requirement where "YES with CCW" was checked.
Note: *Only companies that have undertaken a risk analysis and have legitimate technological or documented business constraints can consider the use of compensating controls to achieve compliance.*
Refer to Appendices B, C, and D of PCI DSS for information about compensating controls and guidance on how to complete this worksheet.

Requirement Number and Definition:

Information Required	Explanation
1. Constraints - List constraints precluding compliance with the original requirement.	
2. Objective - Define the objective of the original control; identify the objective met by the compensating control.	
3. Identified Risk - Identify any additional risk posed by the lack of the original control.	
4. Definition of Compensating Controls - Define the compensating controls and explain how they address the objectives of the original control and the increased risk, if any.	
5. Validation of Compensating Controls - Define how the compensating controls were validated and tested.	
6. Maintenance - Define process and controls in place to maintain compensating controls.	

Appendix C: Explanation of Non-Applicability

If the "N/A" (Not Applicable) column was checked in the questionnaire, use this worksheet to explain why the related requirement is not applicable to your organization.

Requirement #	Reason Requirement is Not Applicable
Req2.1.1a, Req2.1.1b, Req2.1.1c, Req2.1.1d, Req2.1.1e	No wireless is connected to the card data environment (the PCI VLAN).
Req2.3b	There is no remote login to the terminal. All SSL.
Req4.1e	Not a browser based environment.
Req4.1.1	Not using wireless network for transmission of customer card data.
Req8.1.5a, Req8.1.5b	We do not maintain user accounts for these devices. They connect to Elavon for patching only.
Req8.3.2	We do not maintain user accounts for these devices. They connect to Elavon for patching only. We do not have non-console access to these devices. We have no remote network access is maintained by the university.

Req8.5	These devices have a generic password for administrative tasks but it is not a user account for which credentials are shared amongst employees.
Req12.3.9	There is no remote access for stand alone payment card terminals. Firewall is not configured to allow inbound traffic. Terminals dial out only.

Part 3. PCI DSS Validation

This AOC is based on results noted in SAQ B - IP (Section 2), dated *(SAQ completion date)*.

Based on the results documented in the SAQ B - IP noted above, the signatories identified in Parts 3b-3d, as applicable, assert(s) the following compliance status for the entity identified in Part 2 of this document: ***(check one):***

☐ **Compliant**

All sections of the PCI DSS SAQ B-IP are complete, all questions answered affirmatively, resulting in an overall **COMPLIANT** rating; thereby {Company Name} has demonstrated full compliance with the PCI DSS.

☑ **Non-Compliant**

Not all sections of the PCI DSS SAQ B-IP are complete, or not all questions are answered affirmatively, resulting in an overall **NON-COMPLIANT** rating, thereby {Company Name} has not demonstrated full compliance with the PCI DSS.

Target Date for Compliance (below):

☐ **Compliant but with Legal exception:** One or more requirements are marked "No" due to a legal restriction that prevents the requirement from being met. *This option requires additional review from acquirer or payment brand.*

If checked, complete the following:

Affected Requirement	Details of how legal constraint prevents requirement being met

Part 3a. Acknowledgement of Status

Signatory(s) confirms:
(Check all that apply)

☐ PCI DSS Self-Assessment Questionnaire SAQ B-IP, Version 3.2.1, was completed according to the instructions therein.

☐ All information within the above-referenced SAQ and in this attestation fairly represents the results of my assessment in all material respects.

☐ I have confirmed with my payment application vendor that my payment system does not store sensitive authentication data after authorization.

☐ I have read the PCI DSS and I recognize that I must maintain PCI DSS compliance, as applicable to my environment, at all times.

☐ If my environment changes, I recognize I must reassess my environment and implement any additional PCI DSS requirements that apply.

☐ No evidence of full track data , CAV2, CVC2, CID, or CVV2 data , or PIN data storage after transaction authorization was found on ANY system reviewed during this assessment.

☐ ASV scans are being completed by the PCI SSC Approved Scanning Vendor

ASV Name:

Part 3b. Service Provider Attestation

Signature of Merchant Executive Officer:

Date:

Merchant Executive Officer Name:

Title:

Part 3c. Qualified Security Assessor (QSA) Acknowledgement (if applicable)

If a QSA was involved or assisted with this assessment, describe the role performed:

CampusGuard LLC provided one or more of these services to the Merchant as part of their overall PCI self-assessment project: assessment services, project coordination, technical guidance, vulnerability scanning and/or penetration testing services. CampusGuard makes no representation, guarantee or warranty as to the security of the Merchant's systems, and accepts no liability whatsoever to Merchant or any other party for any expense, loss or damage of any kind in connection with weaknesses, failures, attacks on, breaches of or other problems related to Merchant's systems or security.

Signature of Duly Authorized Officer of QSA Company:

Date:

Duly Authorized Officer Name:

Edward J. Ko, Director, Information Security Services

QSA Company:

CampusGuard LLC

Part 3d. Internal Security Assessor (ISA) Involvement (if applicable)

If an ISA(s) was involved or assisted with this assessment, identify the ISA personnel and describe the role performed:

Signature of ISA:

Date:

ISA Name:

Title:

Part 4. Action Plan for Non-Compliant Requirements

Select the appropriate response for "Compliant to PCI DSS Requirements" for each requirement. If you answer "No" to any of the requirements, you may be required to provide the date your Company expects to be compliant with the requirement and a brief description of the actions being taken to meet the requirement.

Check with your acquirer or the payment brand(s) before completing Part 4.

Req. 1 - Install and maintain a firewall configuration to protect cardholder data

○ Yes ○ No ○ Don't Know

Req. 2 - Do not use vendor-supplied defaults for system passwords and other security parameters

○ Yes ○ No ○ Don't Know

Req. 3 - Protect stored cardholder data

○ Yes ○ No ○ Don't Know

Req. 4 - Encrypt transmission of cardholder data across open, public networks

○ Yes ○ No ○ Don't Know

Req. 6 - Develop and maintain secure systems and applications

○ Yes ○ No ○ Don't Know

Req. 7 - Restrict access to cardholder data by business need to know

○ Yes ○ No ○ Don't Know

Req. 8 - Identify and authenticate access to system components

○ Yes ○ No ○ Don't Know

Req. 9 - Restrict physical access to cardholder data

○ Yes ○ No ○ Don't Know

Req. 11 - Regularly test security systems and processes

○ Yes ○ No ○ Don't Know

Req. 12 - Maintain a policy that addresses information security for all personnel

○ Yes ○ No ○ Don't Know

Appen. A2 - Additional PCI DSS Requirements for Entities using SSL/early TLS for Card Present POS POI Terminal Connections.

○ Yes ○ No ○ Don't Know