Payment Card Industry (PCI)
Data Security Standard

Self-Assessment Questionnaire P2PE-HW

and Attestation of Compliance

Hardware Payment Terminals in a Validated P2PE Solution only, No Electronic Cardholder Data Storage

Version 2.0

June 2012

Document Changes

Date	Version	Description
June 2012	2.0	To create SAQ P2PE-HW for merchants using only hardware terminals as part of a validated P2PE solution listed by PCI SSC. This SAQ is for use with PCI DSS v2.0.

Table of Contents

PCI Data Security Standard: Related Documents and Publications

The following documents were created to assist merchants and service providers in understanding the *PCI Data Security Standard Requirements and Security Assessment Procedures* and the PCI DSS SAQs.

Document	Audience
PCI Data Security Standard: *Requirements and Security Assessment Procedures*	All merchants and service providers
Navigating PCI DSS: *Understanding the Intent of the Requirements*	All merchants and service providers
PCI Data Security Standard: *Self-Assessment Questionnaire Guidelines and Instructions*	All merchants and service providers
PCI Data Security Standard: *Self-Assessment Questionnaire A and Attestation*	Eligible merchants[1]
PCI Data Security Standard: *Self-Assessment Questionnaire B and Attestation*	Eligible merchants[1]
PCI Data Security Standard: *Self-Assessment Questionnaire C-VT and Attestation*	Eligible merchants[1]
PCI Data Security Standard: *Self-Assessment Questionnaire C and Attestation*	Eligible merchants[1]
PCI Data Security Standard: *Self-Assessment Questionnaire D and Attestation*	Eligible merchants and service providers[1]
PCI Data Security Standard: *Self-Assessment Questionnaire P2PE-HW and Attestation*	Eligible merchants[1]
PCI Data Security Standard, Payment Application Data Security Standard: Glossary of Terms, Abbreviations, and Acronyms	All merchants and service providers

[1] To determine the appropriate Self-Assessment Questionnaire, see *PCI Data Security Standard: Self-Assessment Guidelines and Instructions*, "Selecting the SAQ and Attestation That Best Apply to Your Organization."

Before you Begin

Merchant Eligibility Criteria for this Questionnaire

SAQ P2PE-HW has been developed to address requirements applicable to merchants who process cardholder data only via hardware payment terminals included in a validated and PCI SSC-listed PCI Point-to-Point Encryption (P2PE) solution.

SAQ P2PE-HW merchants are defined here and in the *PCI DSS Self-Assessment Questionnaire Instructions and Guidelines*. SAQ P2PE-HW merchants do not have access to clear-text cardholder data on any computer system and only enter account data via hardware payment terminals from a PCI SSC-approved P2PE solution. SAQ P2PE-HW merchants may be either brick-and-mortar (card-present) or mail/telephone-order (card-not-present) merchants. For example, a mail/telephone-order merchant could be eligible for SAQ P2PE if they receive cardholder data on paper or over a telephone, and key it directly and only into a validated P2PE hardware device.

These merchants validate compliance by completing SAQ P2PE-HW and the associated Attestation of Compliance, confirming that:

- Your company does not store, process, or transmit any cardholder data on any system or electronic media (for example, on computers, portable disks, or audio recordings) outside of the hardware payment terminal used as part of a validated PCI P2PE solution;
- Your company has confirmed that the implemented PCI P2PE solution is listed on the PCI SSC's List of Validated P2PE Solutions;
- Your company does not store any cardholder data in electronic format, including no legacy storage of cardholder data from prior payment devices or systems, **and**
- Your company has implemented all controls in the *P2PE Instruction Manual (PIM)* provided by the P2PE Solution Provider.

Each section of the questionnaire focuses on a specific area of security, based on the requirements in the *PCI DSS Requirements and Security Assessment Procedures*. This shortened version of the SAQ includes questions that apply to a specific type of small-merchant environment, as defined in the above eligibility criteria. If there are PCI DSS requirements applicable to your environment that are not covered in this SAQ, it may be an indication that this SAQ is not suitable for your environment.

Additionally, you must maintain full compliance with the controls described in this SAQ P2PE-HW at all times, and you recognize that if any changes are made to your P2PE environment, or if you accept payment cards in a method not covered by the P2PE solution, you must reassess eligibility for this P2PE SAQ and refer to your acquirer and/or payment brand for requirements for filing a new SAQ.

This SAQ P2PE-HW would never apply to e-commerce merchants.

SAQ Completion Steps

1. Determine eligibility to complete this SAQ P2PE-HW.
    - Merchant meets all eligibility criteria as defined in Part 2c of the Attestation of Compliance
    - Merchant has implemented all elements of PIM as defined in Part 5 of the Attestation of Compliance.
2. If merchant meets all eligibility requirements:
    - Assess your environment for compliance with the applicable PCI DSS requirements
    - Complete the following Self-Assessment Questionnaire (SAQ P2PE-HW) according to the instructions in this document and in the *Self-Assessment Questionnaire Instructions and Guidelines.*
    - Complete all parts of the Attestation of Compliance in its entirety.
3. Submit the SAQ and the Attestation of Compliance, along with any other requested documentation, to your acquirer or payment card brand as appropriate.

Guidance for Non-Applicable Requirements

Non-Applicable Requirements: If you determine that a requirement is not applicable to your environment, and if "N/A" is an available choice for that requirement, you must use the "N/A" column of the SAQ for that requirement. In addition, complete the "Explanation of Non-Applicability" worksheet in Appendix D for each "N/A" entry.

Self-Assessment Questionnaire P2PE-HW

Note: *The following questions are numbered according to the actual PCI DSS requirement, as defined in the* PCI DSS Requirements and Security Assessment Procedures *document. As only a subset of PCI DSS requirements are provided in this SAQ P2PE-HW, the numbering of these questions may not be consecutive.*

Date of Completion:

Protect Cardholder Data

Requirement 3: Protect stored cardholder data

Note: Requirement 3 applies only to SAQ P2PE-HW merchants that store paper (for example, receipts, printed reports, etc.) with full Primary Account Numbers (PANs).

PCI DSS Question	Response:	Yes	No	N/A[*]	Guidance for SAQ P2PE-HW
3.1	Are data retention and disposal policies and procedures implemented as follows:				*"Yes" answers for requirements at 3.1 mean that if a merchant stores any paper (for example, receipts or paper reports) that contain full PANs, the merchant only stores the paper as long as it is needed for business, legal, and/or regulatory reasons and destroys the paper once it is no longer needed.* *If a merchant never prints or stores any paper containing full PAN, the merchant should mark the N/A column and complete the "Explanation of Non-applicability" worksheet in Appendix D.*
3.1.1	(a) Are data retention and disposal policies and procedures implemented and do they include specific requirements for retention of cardholder data as required for business, legal, and/or regulatory purposes? *For example, cardholder data needs to be held for X period for Y business reasons.*	□	□	□	
	(b) Do policies and procedures include provisions for the secure disposal of data when no longer needed for legal, regulatory, or business reasons, including disposal of cardholder data?	□	□	□	
	(c) Do policies and procedures include coverage for all storage of cardholder data?	□	□	□	

[*] "Not applicable" (N/A) - If this requirement is not applicable to you, you must mark this column and complete the "Explanation of Non-applicability" worksheet in Appendix D.

PCI DSS Question		Response:	Yes	No	N/A*	Guidance for SAQ P2PE-HW
		(d) Do processes and procedures include at least one of the following? • A programmatic process (automatic or manual) to remove, at least quarterly, stored cardholder data that exceeds requirements defined in the data retention policy • Requirements for a review, conducted at least quarterly, to verify that stored cardholder data does not exceed requirements defined in the data retention policy.	□	□	□	
		(e) Does all stored cardholder data meet the requirements defined in the data retention policy?	□	□	□	
3.2	(c)	Does all paper storage adhere to the following requirement regarding non-storage of sensitive authentication data after authorization:				
	3.2.2	If the card verification code or value (three-digit or four-digit number printed on the front or back of a payment card, or "card security code"), is written down during a transaction, it is not stored under any circumstance after the transaction is completed?	□	□	□	*A "Yes" answer for requirement 3.2.2 means that if the merchant writes down the card security code while a transaction is being conducted, the merchant either securely destroys the paper (for example, with a shredder) immediately after the transaction is complete, or obscures the code (for example, by "blacking it out" with a marker) before the paper is stored.* *If the merchant never requests the three-digit or four-digit number printed on the front or back of a payment card ("card security code"), the merchant should mark the N/A column and complete the "Explanation of Non-applicability" worksheet in Appendix D.*

PCI DSS Question	Response:	Yes	No	N/A[*]	Guidance for SAQ P2PE-HW
3.3	Is the PAN masked when displayed on paper (the first six and last four digits are the maximum number of digits to be displayed)? ***Notes:*** • *This requirement does not apply to employees and other parties with a specific need to see the full PAN;* • *This requirement does not supersede stricter requirements in place for displays of cardholder data—for example, for point-of-sale (POS) receipts.*	□	□	□	*A "Yes" answer to requirement 3.3 means that any PANs displayed on paper only show at most the first six and last four digits.* *If the merchant never displays or prints PAN on paper, the merchant should mark the N/A column and complete the "Explanation of Non-applicability" worksheet in Appendix D.*

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

PCI DSS Question	Response:	Yes	No	N/A[*]	Guidance for SAQ P2PE-HW
4.2	(a) Are policies in place that state that full PANs are not to be sent via end-user messaging technologies (for example, e-mail, instant messaging, or chat)?	□	□		*A "Yes" answer to requirement 4.2 means that the merchant has a written document or policy for employees, so they know they cannot use email, instant messaging or chat (or other end-user messaging technologies) to send full PANs, for example, to other employees or to customers.*

[*] "Not applicable" (N/A) - If this requirement is not applicable to you, you must mark this column and complete the "Explanation of Non-applicability" worksheet in Appendix D.

Implement Strong Access Control Measures

Requirement 9: Restrict physical access to cardholder data

Note: Requirement 9.6 only applies to SAQ P2PE-HW merchants that store paper (for example, receipts, printed reports, etc.) with full Primary Account Numbers (PANs).

	PCI DSS Question Response:	Yes	No	N/A[*]	Guidance for SAQ P2PE-HW
9.6	Are all paper media physically secured (including but not limited to paper receipts, paper reports, and faxes)?	□	□	□	*A "Yes" answer for requirement 9.6 means that the merchant securely stores any paper with PANs, for example by storing them in a locked safe.* *If the merchant never stores any paper with full PANs, the merchant should mark the N/A column and complete the "Explanation of Non-applicability" worksheet in Appendix D.*

[*] "Not applicable" (N/A) - If this requirement is not applicable to you, you must mark this column and complete the "Explanation of Non-applicability" worksheet in Appendix D.

Maintain an Information Security Policy

Requirement 12: Maintain a policy that addresses information security for all personnel

Note: Requirement 12 specifies that merchants must have information security policies for their personnel, but these policies can be as simple or complex as needed for the size and complexity of the merchant's operations. The policy document must be provided to all personnel so they are aware of their responsibilities for protecting the, payment terminals, any paper documents with cardholder data, etc. If a merchant has no employees, then it is expected that the merchant understands and acknowledges their responsibility for security within their store(s).

PCI DSS Question	Response:	Yes	No	N/A[*]	Guidance for SAQ P2PE-HW
12.1	Is a security policy established, published, maintained, and disseminated to all relevant personnel? *For the purposes of Requirement 12, "personnel" refers to full-time part-time employees, temporary employees and personnel, and contractors and consultants who are "resident" on the entity's site or otherwise have access to the company's site cardholder data environment.*	□	□		*"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 POS devices in accordance with the P2PE Instruction Manual (PIM), and who to call in an emergency.*
12.1.3	Is the information security policy reviewed at least once a year and updated as needed to reflect changes to business objectives or the risk environment?	□	□		
12.4	Do the security policy and procedures clearly define information security responsibilities for all personnel?	□	□		*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.*

[*] "Not applicable" (N/A) - If this requirement is not applicable to you, you must mark this column and complete the "Explanation of Non-applicability" worksheet in Appendix D.

PCI DSS Question	Response:	Yes	No	N/A*	Guidance for SAQ P2PE-HW
12.5	Are the following information security management responsibilities formally assigned to an individual or team:				
12.5.3	Establishing, documenting, and distributing security incident response and escalation procedures to ensure timely and effective handling of all situations?	□	□		*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	Is a formal security awareness program in place to make all personnel aware of the importance of cardholder data security?	□	□		*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 email 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 if a payment terminal has been tampered with, and how to identify legitimate personnel who may come to service hardware payment terminals.*
12.8	If cardholder data is shared with service providers, are policies and procedures maintained and implemented to manage service providers, 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 full PAN.* *If the merchant never shares cardholder data with any third party, the merchant should mark the N/A column and complete the "Explanation of Non-applicability" worksheet in Appendix D.*
12.8.1	Is a list of service providers maintained?	□	□	□	
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?	□	□	□	

PCI DSS Question		Response:	Yes	No	N/A*	Guidance for SAQ P2PE-HW
12.9	Has an incident response plan been implemented in preparation to respond immediately to a system breach or other emergency, as follows:					*"Yes" answers for requirements at 12.9 means 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.*
12.9.1	(a) Has an incident response plan been created to be implemented in the event of system breach or other emergency?		□	□		
12.9.2	(b) Is the plan tested at least annually?		□	□		

Appendix A (not used)

Appendix B (not used)

Appendix C (not used)

Appendix D: Explanation of Non-Applicability

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

Requirement	Reason Requirement is Not Applicable
Example: *12.8*	*Cardholder data is never shared with service providers.*

Attestation of Compliance, SAQ P2PE-HW

Instructions for Submission

The merchant must complete this Attestation of Compliance as a declaration of the merchant's compliance status with the *Payment Card Industry Data Security Standard (PCI DSS) Requirements and Security Assessment Procedures*. Complete all applicable sections and refer to the submission instructions outlined under "SAQ Completion Steps" in this document.

Part 1. Merchant and Qualified Security Assessor Information

Part 1a. Merchant Organization Information

Company Name:		DBA(S):			
Contact Name:		Title:			
Telephone:		E-mail:			
Business Address		City:			
State/Province:		Country:		ZIP:	
URL:					

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

Company Name:					
Lead QSA Contact Name:		Title:			
Telephone:		E-mail:			
Business Address		City:			
State/Province:		Country:		ZIP:	
URL:					

Part 2. Type of merchant business (check all that apply):

□ Retailer	□ Telecommunication	□ Grocery and Supermarkets
□ Petroleum	□ Mail/Telephone-Order	□ Others (please specify):

List facilities and locations included in this Self-Assessment:

Part 2a. Relationships

Does your company have a relationship with one or more third-party agents (for example, gateways, airline booking agents, loyalty program agents, etc.)?	□ Yes	□ No
Does your company have a relationship with more than one acquirer?	□ Yes	□ No

Part 2b. Transaction Processing	
Please provide the following information regarding the validated P2PE solution your organization uses:	
Name of P2PE Solution Provider:	
Name of P2PE Solution:	
PCI SSC Reference Number	
Listed P2PE Devices used by Merchant:	

Part 2c. Eligibility to Complete SAQ P2PE-HW	
Merchant certifies eligibility to complete this shortened version of the Self-Assessment Questionnaire because:	
□	All payment processing is via the validated P2PE solution approved by the PCI SSC (per above).
□	The only systems in the merchant environment that store, process or transmit account data are the Point of Interaction (POI) devices which are approved for use with the validated P2PE solution.
□	Merchant does not otherwise receive or transmit cardholder data electronically through any channel.
□	Merchant does not store cardholder data in electronic format, even if encrypted.
□	Merchant verifies there is no legacy storage of electronic cardholder data in the environment.
□	Merchant has implemented all controls in the *P2PE Instruction Manual (PIM)* provided by the P2PE Solution Provider, as documented in part 5 of this Attestation of Compliance. ***Note****: Part 5 must be completed.*

Part 3. PCI DSS Validation

Based on the results noted in the SAQ P2PE-HW dated *(completion date)*, *(Merchant Company Name)* asserts the following compliance status (check one):

□	**Compliant:** All sections of the PCI SAQ P2PE-HW are complete, and all questions answered "yes," or are documented and verified as being N/A, resulting in an overall **COMPLIANT** rating.
□	**Non-Compliant:** Not all sections of the PCI SAQ P2PE-HW are complete, or some questions are answered "no," resulting in an overall **NON-COMPLIANT** rating. **Target Date** for Compliance: An entity submitting this form with a status of Non-Compliant may be required to complete the Action Plan in Part 4 of this document. *Check with your acquirer or the payment brand(s) before completing Part 4, since not all payment brands require this section.*

Part 3a. Confirmation of Compliant Status

Merchant confirms:

□	PCI DSS Self-Assessment Questionnaire P2PE-HW, Version *(version of SAQ)*, 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.
□	I have read this SAQ and understand maintaining full compliance with the controls described in this SAQ is required at all times. I recognize that if any changes are made to my P2PE environment, or if I accept payment cards in a method not covered by the P2PE solution, I must reassess eligibility for this SAQ P2PE-HW and refer to my acquirer and/or payment brand for requirements for filing a new SAQ.
□	No sensitive authentication data (for example, magnetic stripe (i.e., track) data[2], CAV2, CVC2, CID, or CVV2 data[3], or PIN data[4]) was found in the environment during this assessment.

Part 3b. Merchant Acknowledgement

Signature of Merchant Executive Officer ↑	*Date* ↑
Merchant Executive Officer Name ↑	*Title* ↑
Merchant Company Represented ↑	

Part 3c. Qualified Security Assessor (QSA) Acknowledgement (Optional, if applicable, per acquirer or payment brand requirements)

Signature of QSA↑	*Date* ↑
QSA Individual Name ↑	*Title* ↑
QSA Company Represented ↑	

[2] Data encoded in the magnetic stripe or equivalent data on a chip used for authorization during a card-present transaction. Entities may not retain full magnetic-stripe data after transaction authorization. The only elements of track data that may be retained are account number, expiration date, and name.

[3] The three- or four-digit value printed on or to the right of the signature panel or on the face of a payment card used to verify card-not-present transactions.

[4] Personal Identification Number entered by cardholder during a card-present transaction, and/or encrypted PIN block present within the transaction message.

Part 4. Action Plan for Non-Compliant Status

Please select the appropriate “Compliance Status” for each requirement. If you answer “NO” to any of the requirements, you are required to provide the date Company will 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, since not all payment brands require this section.*

PCI DSS Requirement	**Description of Requirement**	**Compliance Status (Select One)**		**Remediation Date and Actions (if Compliance Status is “NO”)**
		YES	**NO**	
3	Protect stored cardholder data	□	□	
4	Encrypt transmission of cardholder data across open, public networks	□	□	
9	Restrict physical access to cardholder data	□	□	
12	Maintain a policy that addresses information security for all personnel	□	□	

Part 5: Attestation of PIM Implementation	
Date of PIM document:	
Date PIM received from solution provider:	

Merchant has implemented the following in accordance with the instructions documented in the P2PE Instruction Manual (PIM):

P2PE Reference	PIM Requirement	Description	YES	NO
3A-1	• A device-tracking system is in place to identify and locate all point-of-interaction (POI) devices	Merchant has a way to track where each of their POI devices are located, including, for example, which store they are at, whether they are in service or in storage, whether they have been sent away for repair, etc.	□	□
	• POI device inventories are performed at least annually to detect removal or substitution of devices	Merchant inspects all their POI devices at least annually to check that devices have not been removed and that they have not been substituted with counterfeit devices.	□	□
	• A detailed inventory of all POI devices is maintained and secured to prevent unauthorized access	An up-to-date list (inventory) of all POI devices is kept, and is only available to staff who need to access the list in order to perform their job. The following details are documented for each device • Make and model of device • Location of device (e.g. shop or office where device is in use) • Serial number of device • General description of device (e.g. counter-top pin-entry device) • Information about any security seals, labels, hidden markings, etc. which can help identify if device has been tampered with • Number and type of physical connections to device • Date last inventory performed for the device • Firmware version of device • Hardware version of device	□	□

Merchant has implemented the following in accordance with the instructions documented in the P2PE Instruction Manual (PIM):				
P2PE Reference	**PIM Requirement**	**Description**	**YES**	**NO**
	• Procedures are in place to detect and report variances in the annual inventory, including missing or substituted devices	Merchant has written procedures for staff to follow (including details of whom to contact and how to contact them) if a POI device is found to be missing or has been substituted with a counterfeit device.	□	□
3A-2	• POI devices not in use (including devices awaiting deployment or transport, or undergoing repair) are stored in a physically secure location	POI devices that are not in service are stored in a secure area (for example, a securely locked room or a safe) which is only available to staff who need to access the device in order to perform their job. This includes devices waiting to be deployed, waiting to be transported to another location, or undergoing repair.	□	□
	Procedures for transporting POI devices are in place and include: • Procedures for packing the device using tamper-evident packaging prior to transit • Procedures for inspecting device packaging to determine if it has been tampered with, including specific details on how tamper-evidence may appear on the packaging used • Defined secure transport method, such as bonded carrier or secure courier	Procedures are followed for sending or receiving POI devices, including: • Devices to be sent are packed in specific packaging as defined in the PIM • When devices are received the packaging is inspected (before being opened) to see if it has been opened previously, damaged or tampered with • Devices are only sent using a transport method (e.g. secure courier or bonded carrier) defined in the PIM	□	□
	Procedures are in place to be followed in the event that device packaging has been tampered with, including: • Devices must not be deployed or used • Procedures for returning device to authorized party for investigation • Contact details for reporting tamper-detection	If any POI device is received in packaging that appears to have been already opened, damaged or otherwise tampered with: • The device is not be deployed or used • The situation is reported to the authorized party defined in the PIM • The device is returned to the authorized party defined in the PIM	□	□

Merchant has implemented the following in accordance with the instructions documented in the P2PE Instruction Manual (PIM):				
P2PE Reference	**PIM Requirement**	**Description**	**YES**	**NO**
	• POI devices are only sent to and accepted for use from trusted locations. • In the event that a device is received from an untrusted or unknown location: ○ Procedures (including contact details for authorized parties) are followed to verify location from which device was sent ○ Procedures are followed to ensure devices are not used unless and until the source location is verified as trusted.	POI devices are only sent to and accepted for use from trusted locations, as defined in the PIM. If a device is received from an untrusted or unknown location: • The location from which device was sent is confirmed • Devices are not used unless and until the source location is confirmed as being trusted	□	□
3A-3	Procedures for purchasing, receipt and deployment of devices are implemented including: • Matching device serial numbers • Maintaining records of serial-number verifications • Transporting documents used for validating device serial numbers via a separate communication channel and not with the device shipment • Performing pre-installation inspection procedures, including physical and functional tests and visual inspection, to verify devices have not been tampered with or compromised • Maintaining devices in original, tamper-evident packaging or in physically secure storage until ready for use • Recording device serial numbers in merchant inventory-control system as soon as possible	When sending/receiving POI devices: • Serial numbers of received devices are matched to the serial numbers documented by the sender (for example, in a purchase order, waybill, or invoice), and a record of the matching numbers is kept • The documented serial numbers are sent/received separately from the devices themselves, and not by the same method of delivery • Devices are inspected and tested per PIM instructions, before they are installed • Devices are kept in their original packaging or in physically secure storage area until ready for use • Device serial numbers are added to the list of all devices (inventory) as soon as possible	□	□

Merchant has implemented the following in accordance with the instructions documented in the P2PE Instruction Manual (PIM):				
P2PE Reference	**PIM Requirement**	**Description**	**YES**	**NO**
	Procedures are implemented to control and document all access to devices prior to deployment including: - Identifying personnel authorized to access devices - Restricting access to authorized personnel - Maintaining a log of all access including personnel name, company, reason for access, time in and out	POI devices that are not in service are available only to staff who need access to the device in order to perform their job. Every time someone needs to access the device, details of the person's name, company, reason for access, time in, and time out is recorded and kept.	□	□
	- A documented audit trail is in place to demonstrate that devices are controlled and not left unprotected from receipt through to installation	A documented record of device movements, locations, and activities performed on devices is kept for all devices, from the time they are first received.	□	□
3A-4	- POI devices are deployed in appropriate locations	POI devices that are in service are placed in suitable locations in order to prevent them from being tampered with.	□	□
	- Deployed POI devices are physically secured to prevent unauthorized removal or substitution	POI devices that are in service are fixed into place to prevent them from being stolen, removed or swapped out by anyone who is not approved to do so by the merchant.	□	□
	- Where POI devices cannot be physically secured – for example, wireless or handheld devices – procedures are implemented to prevent unauthorized removal or substitution of devices.	POI devices which are in use that cannot be fixed into place (for example, portable or handheld terminals) are kept secure so they can't be stolen, removed or swapped out.	□	□
3A-5	- Procedures are implemented for identification and authorization of repair /maintenance personnel and other third parties prior to granting access	Before any unknown persons are allowed to access POI devices (e.g. for maintenance or repair purposes), their identification and reason for being there is checked and confirmed, and a record is kept of all such persons. All persons who are allowed access to the devices are escorted at all times.	□	□

Merchant has implemented the following in accordance with the instructions documented in the P2PE Instruction Manual (PIM):				
P2PE Reference	**PIM Requirement**	**Description**	**YES**	**NO**
3B-1	Procedures are implemented for securing POI devices being returned, retired, or replaced, including: • Notifying affected entities—including the entity to which the device is being returned—before devices are returned • Transporting devices via a trusted carrier service • Packing and sending devices in serialized, counterfeit-resistant, and tamper-evident packaging • Following procedures for the solution provider can track devices during the return process	When POI devices are being returned for repair or replacement, the merchant notifies the relevant parties, packs the devices properly, and sends the devices using the approved method.	□	□
	Procedures are implemented for secure disposal of POI devices, including: • Returning devices only to authorized parties for destruction (including a list of authorized parties) • Procedures to render sensitive data irrecoverable, prior to device being shipped for disposal	When POI devices have reached the end of their useful life, and are due to be returned for disposal or destruction, the merchant sends devices to the specific parties defined in the PIM, and prepares devices prior to shipping as instructed in the PIM.	□	□
3B-2	Procedures are followed in the event of a POI device encryption failure, including that devices are not re-enabled for use until merchant has confirmed with solution provider that either: • The issue has been resolved and P2PE encryption functionality is restored and re-enabled, or • The merchant has formally opted out from using the P2PE solution according to the solution provider's opt-out procedures, and has accepted responsibility for using alternative controls and/or processing method.	Merchant has read the procedures documented in the PIM and follows these procedures if encryption stops working on a POI device.	□	□

Merchant has implemented the following in accordance with the instructions documented in the P2PE Instruction Manual (PIM):				
P2PE Reference	**PIM Requirement**	**Description**	**YES**	**NO**
	• Procedures are followed in the event that, upon device encryption failure, the merchant chooses to opt out of the P2PE solution and process transactions without P2PE protection.	Merchant has read the opt-out procedures documented in the PIM and follows these procedures if, upon POI encryption failure, they wish to opt out of the solution and stop using P2PE protection.	□	□
3B-6	• Troubleshooting procedures are implemented.	Merchant follows procedures in the PIM for dealing with device problems.		
3B-8	• Periodic physical inspections of devices are performed to detect tampering or modification	Devices are examined at regular intervals to check for suspicious attachments and any signs that they have been altered or interfered with.	□	□
	• Mechanisms are in place to detect tampering of devices deployed in remote or unattended locations and alert appropriate personnel.	For POI devices located in areas away from merchant personnel, methods are in place to ensure that suspicious attachments or alterations would be found and investigated.	□	□
	• Procedures are implemented for responding to detection of tampered devices	The merchant reports suspicious attachments or alterations to POI devices, and follows instructions for removing or securing the device.	□	□
3B-9	• Procedures are implemented to notify the solution provider of suspicious activity	The merchant knows how to report suspicious activity and who to report it to.	□	□
3C-1	• Procedures for installing and connecting POI devices are followed to maintain the integrity of P2PE solution	The merchant follows all procedures in the PIM for connecting and starting up POI devices. Only approved POI devices as documented in the PIM are used.	□	□
	• Procedures for connecting PCI-approved components to other devices and/or components are followed	The merchant follows all procedures in the PIM for connecting the approved POI devices to any other pieces of equipment or computer systems.	□	□
	• If a PCI-approved POI component is connected to another device or data-capture mechanism, the non PCI-approved capture mechanism is not secured by the P2PE solution, and the use of any such mechanisms to collect PCI payment-card data would negate any PCI DSS scope reduction	The merchant understands that if they use any other methods or devices to collect or capture payment card data, that they will not be eligible for PCI DSS scope reduction.	□	□

Merchant has implemented the following in accordance with the instructions documented in the P2PE Instruction Manual (PIM):				
P2PE Reference	**PIM Requirement**	**Description**	**YES**	**NO**
	Changing or attempting to change device configurations or settings negates the solution's ability to provide PCI DSS scope reduction. Examples include but are not limited to: • Attempting to enable any device interfaces or data-capture mechanisms that were disabled on the P2PE POI device • Attempting to alter security configurations or authentication controls • Physically opening the device • Attempting to install applications onto the device	The merchant understands that if they attempt to change POI device configurations or settings (see PIM Requirement column for examples), that they will not be eligible for PCI DSS scope reduction.	□	□