Instruction Manual for PCI P2PE v3.1

1. P2PE Solution Information and Solution Provider Contact Details

1.1. P2PE Solution Information

Solution name:	Shift4 P2PE
Solution reference number per PCI SSC website:	2023-00127.006

1.2. Solution Provider Contact Information

Company name:	Shift4 Payments, LLC.
Company address:	3501 Corporate Parkway, Center Valley, PA 18034
Company URL:	https://www.shift4.com
Contact name:	Compliance
Contact phone number:	
Contact e-mail address:	pci@shift4.com

P2PE and PCI DSS

Merchants using this P2PE solution may be required to validate PCI DSS compliance and should be aware of their applicable PCI DSS requirements. Merchants should contact their acquirer or payment brands to determine their PCI DSS validation requirements.

2. Confirm Devices were not tampered with and confirm the identity of any third-party personnel

2.1. Instructions for ensuring POI devices originate from trusted sites/locations only

Shift4 and its partners take all necessary precautions to ensure devices are not tampered with or compromised prior to being shipped to you. However, there are steps that you must undertake to ensure that devices have not been tampered with during transit. P SEP

First you must confirm that shipment of devices originated from one of the following True P2PE Key Injection Facilities:

- ScanSource, Inc. – SSC Listing # 2023-01087.003
- POS Portal, Inc. – SSC Listing # 2022-01084.003
- First Data TASQ Technology – SSC Listing # 2023-01085.005
- Verifone, Inc. – SSC Listing # 2021-00154.083
- Ingenico US KIF – SSC Listing # 2021-00470.037
- ID TECH US KIF – SSC Listing # 2021-01106.005
- POSDATA KIF – SSC Listing # 2021-01142.002
- The Phoenix Group Key Injection Services – USA – SSC Listing # 2023-01098.004
- JR's POS Depot Key Injection Services – SSC Listing # 2021-01164.002
- Spencer Technologies Inc., Spencer Secure Services KIF – SSC Listing # 2021-01196.002
- Shift4 Payments Key Injection Services – SSC Listing # 2022-00127.005
- UCP Key Injection Facility – SSC Listing # 2022-01269.002
- PAX Technology Inc. – SSC Listing # 2023-00841.004

In order to remain compliant, you may only deploy POI devices that are shipped from one of the aforementioned PCI P2PE Component Solution Providers. Confirmation that devices were shipped from an authorized source may be performed by comparing the providers shipping information with the information listed above. P SEP

If you receive POI devices from another provider, you must contact us at PCI@Shift4.com for confirmation. We will take necessary steps to communicate with you if our list of providers of POI devices has changed.

2.2. Instructions for confirming POI device and packaging were not tampered with, and for establishing secure, confirmed communications with the solution provider.

In addition to confirmation of shipping origination, you must confirm that neither the packaging nor the device has been tampered with. All POI devices will be shipped using tamper-evident packaging. This packing will be evident on the shipping package itself and internally. Examples of said packaging include:

- Sealed Tamper Evident Bags: like Tamper Evident Deposit Bags

- Tamper Evident Tape used on all seams of the box

You must also inspect the device. You should look for broken security seals and cracks around device's seals to determine if the POI device itself has been compromised. If you believe the packaging or the device has been tampered with, **DO NOT** deploy the device.

Physically secure POI devices in your possession, including devices:

- Awaiting deployment
- Undergoing repair or otherwise not in use
- Waiting transport between sites/locations

2.3. Instructions to confirm the business need for, and identities of, any third-party personnel claiming to be support or repair personnel, prior to granting those personnel access to POI devices

Access to POI devices by third-party personnel for repair/maintenance must be monitored. This monitoring is required to ensure there is no unauthorized access to device that could result in tampering, theft, or substitution of the device. To ensure proper third-party access monitoring, you should have a policy in place that requires the following steps:

1) Maintenance/repair of the device must be pre-arranged with date and timeframe of third-party personnel defined. Unexpected visits for repair/maintenance must be verified. If they cannot be verified, access to the device must be denied;
2) Prior to granting access to a device, personnel must be identified and authorized to access the device;
3) Third-party personnel access must be recorded and include personnel name, company, time of access, and purpose of access. Log must be maintained for no less than one year;
4) Personnel must be escorted and observed at all times; and
5) Personnel may not remove or replace a device without prior authorization. If authorized, new devices must be properly inspected and inventoried.

3. Approved POI Devices, Applications/Software, and the Merchant Inventory

3.1. POI device details

The following information lists the details of the PCI-approved POI devices approved for use in this P2PE solution.

All POI device information can be verified by visiting:
https://www.pcisecuritystandards.org/approved_companies_providers/approved_pin_transaction_security.php
See also Section 9.2, "Instructions for how to confirm hardware, firmware, and application versions on POI devices."

PCI PTS approval #:	POI device vendor:	POI device model name and number	Hardware version #(s):	Firmware version #(s):
4-10144	ID Tech	SecuRED	IDSR-33x1xxxxx	1.08 2.00 SRED: 1.07
4-10184	ID Tech	SecuRED	IDSR-38xxxxxx	V2.00 V2.01
4-10156	ID Tech	SREDKey	IDSK-53XXXXXXX	1.02 1.02.xxx.S SRED:1.01
4-10218	ID Tech	Augusta S	IDEM-8xxxx	V1.03.xxx.s
4-90075	ID Tech	SREDKey 2	80172001(With MSR)	SREDKEY2 FW v2.00.xxx.xxxx.S
4-30501	ID Tech	VP3350	H178-SUR93xxA	VP3350 FW v1.00.xxx.xxxx.S
4-10110	Verifone	Mx925/Mx915	P132-409-02-R (MX 915) P132-509-22-R (MX 925)	App: 10.x.x OP (VFOP): 7.x.x SRED (VFSRED): 7.x.x Vault: 17.x.x
4-20235	Ingenico	iCMP	ICMxxx-31Txxxxx	820528V02.xx (SRED) 820539V01.xx (SRED)
4-20184	Ingenico	iPP310, iPP320, iPP350	IPP3xx-11Txxxxx	SRED (CTLS): 820365 V02.xx
4-30176	Ingenico	iPP320, iPP350, iPP310, iPP315	iPP3xx-51Txxxxx	820180 V01.xx
4-20321	Ingenico	Desk/3200 Desk/3500	DES35DC (CTLS with PIN shield)	820555v01.xx (SRED) 820565v01.xx (SRED)
4-30062	Ingenico	iSC250	iSC2xx-01Txxxxx	SRED (Non CTLS): 820157 V01.xx
4-20183	Ingenico	iSMP	iMP3xx-01Txxxxx	SRED (Non CTLS) : 820528V02.xx
4-30220	Ingenico	iSMP4	iMP6xx-31Txxxxx	820305v11.xx
4-30161	Ingenico	iUC285	iUC28x-01Txxxxx	820177V01.xx
4-30083	Ingenico	iUR250, iUR250P	iUR2xx-11Txxxxx	SRED: 820514V01.xx
4-30250	Ingenico	iUR250, iUR250P	IUR2xx-01Txxxxx standard Ingenico product	820514v12.xx
4-30172	Ingenico	iUC150B	iUC15x-01Txxxxx	820168 v01.xxx
4-20181	Ingenico	iWL220, IWL250	IWL2xx-01Txxxxx	SRED (Non CTLS): 820073v01.xx
4-30075	Ingenico	iUP250	IUP2xx-01Txxxxx	SRED: 820528V02.xx
4-30098	Ingenico	ISC Touch 480	ISC4xx-11Txxxxx (CTLS)	SRED (CTLS): 820528V02.xx
4-30125	Ingenico	iSC Touch 480	ISC4xx-11Txxxxx	820518 V12.xx
4-30310	Ingenico	Lane/3000, Desk/1500	LAN30HA	820561v01.xx (base firmware)

PCI PTS approval #:	POI device vendor:	POI device model name and number	Hardware version #(s):	Firmware version #(s):
4-20286	Ingenico	Lane/5000	LAN50BB (CTLS)	820549V01.xx (SRED) 820555V01.xx (SRED) 820556V01.xx (SRED)
4-20303	Ingenico	Lane/5000	LAN51EA	820556V01.xx (SRED OnGuard SDE) 820559V01.xx (SRED ANL)
4-20324	Ingenico	Lane/5000	LAN51EA (dual MSR head and camera)	820549v01.xx (SRED OnGuard FPE) 820555v01.xx (SRED AWL) 820556v01.xx (SRED OnGuard SDE) 820559v01.xx (SRED ANL) 820565v01.xx (SRED FF1)
4-30226	Ingenico	Lane/7000	LAN70AA	820547v01.xx
4-30237	Ingenico	Lane/7000	LAN70BB	820547v01.xx
4-30257	Ingenico	Lane/8000	LAN80BA	820547v01.xx
4-20282	Ingenico	Move/5000	MOV50JB (CTLS)	820555v01.xx (SRED)
4-20316	Ingenico	Move/5000	MOV50DB	820555v01.xx (SRED)
4-30230	Ingenico	Link/2500	LIN25NA (Touch version with CTLS)	820555v01.xx (SRED AWL) 820556v01.xx (SRED On-Guard SDE)
4-30326	Ingenico	Link/2500	LIN25NC (Touch version with CTLS)	820547v01.xx
4-30287	PAX Computer Technology (Shenzhen) Co Ltd.	Q20, Q20 U	Q20-xxx-Rx5-1xxx (with CTLS)	15.00.xx xxxx
4-40183	PAX Computer Technology (Shenzhen) Co Ltd.	A920	A920-xxx-xx4-0xxx	24.00.xxxx
4-40215	PAX Computer Technology (Shenzhen) Co Ltd.	A920	A920-xxx-Rx5-3xxx (CTLS)	25.03.xxxx
4-40187	PAX Computer Technology (Shenzhen) Co Ltd.	SP30	SP30-xxx-2x4-0xxx	4.00.xx

PCI PTS approval #:	POI device vendor:	POI device model name and number	Hardware version #(s):	Firmware version #(s):
4-40184	PAX Computer Technology (Shenzhen) Co Ltd.	S80	S80-xxx-3x4-0xxx (CTLS support)	4.01.xx
4-30301	PAX Computer Technology (Shenzhen) Co Ltd.	A80	A80-xxx-Rx5-1xxx (with CTLS)	25.02.xxxx
4-30159	PAX Computer Technology (Shenzhen) Co Ltd.	S920, S920 L, S920 F	S920-xxx-xx4-Jxxx	Prolin OS: 14.03.xx xxxx Prolin Boot: 3.x.xx.xxxx
4-40188	PAX Computer Technology (Shenzhen) Co Ltd.	D220	D220-xxx-xx4-0xxx	14.00.xx xxxx
4-30162	PAX Computer Technology (Shenzhen) Co Ltd.	Px5	PX5-xxx-ax4-0xxx (a=R CTLS support	Boot: 3.0.xx.xxxx Firmware 14.02.xx xxxx
4-30297	PAX Computer Technology (Shenzhen) Co Ltd.	A930	A930-xxx-Rx5-1xxx (with CTLS)	25.01.xxxx
4-40157	PAX Computer Technology (Shenzhen) Co Ltd.	D210	D210-xxx-3x4-1xxx (CTLS)	4.01.xx
4-40272	PAX Computer Technology (Shenzhen) Co Ltd.	D210	D210-xxx-3x5-1xxx (with contactless & model 1)	5.00.xx
4-30163	PAX Computer Technology (Shenzhen) Co Ltd.	Px7	PX7-xxx-Rx4-2xxx CTLS support	Boot: 3.0.xx.xxxx 14.02.xx xxxx
4-30224	PAX Computer Technology (Shenzhen) Co Ltd.	S300	S300-xxx-3x4-0xxx (with CTLS)	14.01.xx xxxx
4-90196	PAX Computer Technology (Shenzhen) Co Ltd.	R20	R20-x61-xx0 (with CTLS)	6.00.xx
4-30388	PAX Computer Technology	D135 MSR	D135-xxx-Rx5-1xxx (with CTLS)	5.00.xx

	(Shenzhen) Co Ltd.			
PCI PTS approval #:	POI device vendor:	POI device model name and number	Hardware version #(s):	Firmware version #(s):
4-90100	PAX Computer Technology (Shenzhen) Co Ltd.	Q25	Q25-xxx-Rx5-Axxx (CTLS)	15.00.xx xxxx
4-90139	PAX Computer Technology (Shenzhen) Co Ltd.	A800	A800-xxx0x6-1xxx	26.01.xxxx
4-40340	PAX Computer Technology (Shenzhen) Co Ltd.	A3700	A3700-xxxRx6-0xxx (with CTLS	26.00.xxxx
4-40305	PAX Computer Technology (Shenzhen) Co Ltd.	A35	A35-xxxRx6-0xxx (CTLS reader)	26.00.xxxx
4-30371	PAX Computer Technology (Shenzhen) Co Ltd.	IM30	IM30-xxx-0x5-0xxx (without CTLS) IM30-xxx-Rx5-0xxx (with CTLS)	25.00.xxxx
4-40372	PAX Computer Technology (Shenzhen) Co Ltd.	IM30	IM30-xxx-0x6-Axxx (NON-CTLS) IM30-xxx-0x6-0xxx (NON-CTLS)	26.00.xxxx
4-40273	PAX Computer Technology (Shenzhen) Co Ltd.	A920Pro	A920Pro-xxx-0x5-3xxx (NON-CTLS) A920Pro-xxx-Rx5-3xxx (CTLS)	25.03.xxxx
4-40333	PAX Computer Technology (Shenzhen) Co Ltd.	A920Pro	A920Pro-xxx-0x6-0xxx (NON-CTLS) A920Pro-xxx-Rx6-0xxx (CTLS)	26.00.xxxx
4-40269	PAX Computer Technology (Shenzhen) Co Ltd.	A77	A77-xxx-Rx5-0xxx A77-xxx-0x5-0xxx A77-xxx-Rx5-1xxx A77-xxx-0x5-1xxx	25.00.xxxx 25.01.xxxx 25.02.xxxx 25.03.xxxx

			A77-xxx-Rx5-2xxx (CTLS) A77-xxx-0x5-2xxx (NON-CTLS)	
4-10234	Innowi, Inc.	ChecOut m1	1.0	2.0.0

3.2. POI Software/Application Details

The following information lists the details of all software/applications (both P2PE applications and P2PE non-payment software) on POI devices used in this P2PE solution. Hardware and Firmware versions can be referenced in 3.1 above.

All applications with access to clear-text account data must be reviewed according to Domain 2 and are included in the P2PE solution listing. These applications may also be optionally included in the PCI P2PE list of Validated P2PE Applications list at vendor or solution provider discretion.

Application Name	Version #	Application Vendor	Is Application PCI Listed? (Y/N)	Does Application Have Access to Clear-Text Account Data (Y/N)
Form Agent	30250600	Shift4 Payments	N	N
UPP	6.80.09	Ingenico, Inc.	N	N
BroadPOS P2PE	1.01.xx	Pax Technology, Inc.	Y – 2022-00841.003	Y

3.3. POI Inventory & Monitoring

- All POI devices must be documented via inventory control and monitoring procedures, including device status (deployed, awaiting deployment, undergoing repair or otherwise not in use, or in transit).
- This inventory must be performed annually, at a minimum.
- Any variances in inventory, including missing or substituted POI devices, must be reported to Shift4 Payments via the contact information in Section 1.2 above.
- Sample inventory table below is for illustrative purposes only. The actual inventory should be captured and maintained by the merchant in an external document.

In order for you to maintain your compliance you must maintain an inventory of the provided POI devices. You must track which devices are deployed, which are awaiting deployment, those that have been removed from service for repair or otherwise not in use, and those in transit for deployment or return for repair. It is recommended that you designate a Job Role or personnel responsible for maintaining the POI inventory and for inspection of devices.

For each area identified the following information must be recorded. It is recommended that you record this information upon receipt of your POI device and then update the location of each device as it transitions from storage, transit, deployment, and repair or return.

- Manufacturer of device
- Make and Model of device
- Serial Number of Device
- Internal Inventory Number; (if applicable)
- General Description of Device (Color, Secure Seals, Labels, Hidden Marking, etc.)
- Number and type of physical connections (Network, Serial, etc.)
- Firmware version
- Hardware version
- Device Location (Storage, Where Deployed, In Transit, Awaiting Repairs or Returned)
- Date of Location Inspection (Last Date device location was confirmed)
- Date of Last Inspection (last date device was inspected for tampering)
- Name of Job Role or personnel performing inspection
- Date inventory was last updated

Device identification can be found on the PTS POI device itself. Generally this information is contained upon a manufacturer provided label located on the back or side of the device.

Device inventories are to be performed no less than annually to confirm that inventory of devices is being catalogued and performed correctly; however, inventory must be updated as device transition in and out of service and from one location to another. This inventory must also be completed to confirm that all devices identified as being within your environment are currently within your possession and not missing.

Access to device inventory and to the devices themselves must be restricted to authorized personnel. The method for maintaining a device inventory is determined by you; however the method utilized must enable you to restrict access to the inventory tracking information and allow you to record who has had access to the inventory tracking information. Failure to do so will impact your PCI DSS compliance. In addition, you must be able to restrict access to stored devices and record who has accessed said devices and when access occurred.

During your inventory process, you must investigate the POI devices to identify unauthorized removal, tampering, or substitution of devices. Detection of these events may be an indication of a compromise of your environment. Inspection of device should compare information located on the device itself with the inventory information previously recorded. In addition, the inspection should look for indications that the device has been tampered with. Indications of tampering may include, but is not limited to, attachment of unauthorized devices to the POI device, breakage of security seals, cracks within the seal of the device itself, or insertion of a "skimmer" device within the Magnetic Stripe Reader (MSR) of the device. Skimmers are devices used by attackers to capture cardholder data prior to the POI device reading the card.

Skimmers may be inserted in the MSR of the device or overlaid on the device itself. It is recommended that you training personnel (Cashiers/Managers) interfacing with the POI devices on a regular basis to inspect deployed POI devices daily.

Should you detect a compromised device or find that your inventory indicated a missing or substituted device, you must report this information to the device provider immediately. For device being stored, be it prior to deployment, shipment, or awaiting repairs, they must be stored in a secure area with restricted access to ensure they are not tampered with. Though the storage location of devices within your control is your responsibility, the location must include the following measures:

1) Device must be stored in locked room or container
2) Storage location must support restricted access
3) Must restrict access to authorized personnel. Example include:
    a. Door/Container requiring key access in which defined personnel have access to the key; or
    b. Door/Container required knowledge of cipherlock code in which defined personnel have knowledge of the cipherlock code.
4) Access to room or container storing device must be logged. This logging may be manual (written access log) or automatic (proximity card system that records access)

Access to room must be monitored (Cameras or physical sight).

Sample Inventory Table

Device Vendor	Device Model Name(s) and Number(s)	Device Location	Device Status	Serial Number or Other Unique Identifier	Date of Inventory

4. POI Device Installation Instructions

Do not connect non-approved cardholder data capture devices.

The P2PE solution is approved to include specific PCI-approved POI devices. Only these devices denoted above in Table 3.1 are allowed for cardholder data capture.

If a merchant's PCI-approved POI device is connected to a data capture mechanism that is not PCI approved, (for example, if a PCI-approved SCR was connected to a keypad that was not PCI-approved):

- The use of such mechanisms to collect PCI payment-card data could mean that more PCI DSS requirements are now applicable for the merchant.

Do not change or attempt to change device configurations or settings.

Changing device configurations or settings may invalidate the PCI-approved P2PE solution in its entirety. Examples include, but are not limited to:

- Enabling any device interfaces or data-capture mechanisms that were disabled on the P2PE solution POI device.
- Altering security configurations or authentication controls on the POI device.
- Physically opening the POI device.
- Attempting to install unauthorized applications onto the POI device.

4.1. Installation and connection instructions

For detailed physical installation and connection instructions contact the Shift4 Customer Service Installations branch at +1 702.597.2480, Option 2. To find more information on Shift4 supported POI devices, visit https://www.shift4.com/our-software-hardware-partners then select Hardware Integrations for device listing. Contact your contracted device installer.

Note: *Only PCI-approved POI devices listed in the PIM are allowed for use in the Shift4 P2PE solution for account data capture.*

4.2. Guidance for selecting appropriate locations for deployed devices

Select an installation location appropriate to the device and with protection measures in mind:

- Control public access to devices such that device access is limited to only parts of the device a person is expected to use to complete a transaction (for example, PIN pad and card reader).
- Locate devices so they can be observed/monitored by authorized personnel—for example, during daily store checks of the devices performed by store/security staff.
- Locate devices in an environment that deters compromise attempts—for example, through lighting, access paths, visible security measures, etc. Do not install devices outside that are designed for indoor use only.
- The location selected should provide adequate ventilation and protection. The location should be free from excessive heat, dust, oil and moisture. The location should not be near any water source, running or standing.
- The terminal should be placed on a flat surface or mounted on a manufacturer supplied stand or wall mount per the manufacturer's instructions. The terminal should not be in direct sunlight or within 24 inches of devices that cause excessive voltage fluctuations, electrical noise or radiate heat. The terminal should be at least 6 feet from anti-theft

doorway units and at least 18 inches from surface mounted deactivator pads.

- Position the terminal on the check-stand in such a way as to make visual observation of the PIN-entry process infeasible. Examples include:
  - Visual shields designed into the check-stand. The shields may be solely for shielding purposes, or may be part of the general check-stand design.
  - Position the PIN Entry Device (device) so that it is angled in such a way that PIN spying is difficult. Installing device on an adjustable stand that allows consumers to swivel the terminal sideways and/or tilt it forwards/backwards to a position that makes visual observation of the PIN-entry process difficult.

Position in-store security cameras so that the PIN-entry keypad is not visible.

4.3. Guidance for physically securing deployed devices to prevent unauthorized removal or substitution

Merchants should physically secure devices to prevent unauthorized removal or substitution while devices are deployed for use.

This includes both attended and unattended devices, as applicable to the P2PE solution (for example, kiosks, “pay-at-the-pump,” etc.).

If the devices cannot be physically secured (such as wireless or handheld devices):

- Secure devices in a locked room when not in use.
- Assign responsibility to specific individuals when device is in use.
- Observe devices at all times.
- Sign devices in/out, etc.

Merchants should physically secure devices when not deployed or being used. Including devices:

- Undergoing repair or maintenance while in the merchant’s possession.
- Awaiting deployment.
- Awaiting transport between sites/locations.

Merchants should prevent unauthorized physical access to devices undergoing repair or maintenance while in their possession, to include the following:

- Verify the identity and authorization of repair personnel.
- All repair personnel must be verified and authorized prior to granting access.
- Unexpected personnel must be denied access unless fully validated and authorized.

Escort and monitor authorized personnel at all times.

5. POI Device Installation Instructions

5.1. **Instructions for securing your POI devices intended for, and during, transit**
When you are shipping devices to your location for deployment or for return, devices must be shipped securely. They must be packed in tamper-evident packaging and shipped in a secure manner. All device either being shipped to a location for deployment or for return, must be shipped using a secure transport method such as a secure courier or bonded carrier. For deployment to sites, it is permissible to use employees for transport; however, they must be authorized to deliver the devices and the recipient must be notified of who will be delivering the devices to them. Be it a bonded carrier, secure courier, or internal employee, you must log the following information: 1) Personnel providing shipping (if employee, record name and job role); 2) Date of pickup 3) Device being shipped 4) Confirmation Date of Site delivery When packaging devices for transit, they must be packed in tamper-evident packaging. You determine the type of packaging; however the recipient must be notified as to how to determine if the package has been tampered with during transit. As with your inspection of POI device received from us, your deployment sites must perform the same inspection on device shipped from your storage location. They must be notified of authorized shipping locations, notified of how the device will be shipped, and trained in how to inspect the packaging and device for tampering. For example, they must be trained to investigate for breakage of tamper-evident seals on the external packaging and to investigate the device itself for cracks or breakage of security seals. Finally, they must be instructed that if they receive devices without prior confirmation from the shipping location or they are delivered in a manner unexpected, they must confirm prior to deployment of the devices. **Special Note:** If using internal employees for device shipment, they must be instructed to not leave devices in public areas unattended, for example, in the front or back seat of a car. This may lead to unauthorized access or theft of the device.

Physically secure POI devices in your possession, including devices: • Awaiting deployment • Undergoing repair or otherwise not in use • Waiting transport between sites/locations

5.2. **Instructions for ensuring your POI devices are shipped to trusted sites/locations only**
If the device is to be returned to us for repair or replacement, you must take the following steps: 1) Perform the Steps provided to you via the support contact below or the documentation you received with the device to wipe the device of all sensitive data.

2) Pack the device within a tamper-evident packaging; and
3) Notify us that the device is being returned. You will need to provide us the serial number of the device and a tracking number of the package as provided by the carrier. We can be contacted at: Shift4 Customer Service +1 702-597-2480 Option 2

6. POI Device Tamper & Modification Guidance

6.1. **Instructions for physically inspecting POI devices and preventing skimming, including instructions and contact details for reporting any suspicious activity**

Additional guidance for inspecting POI devices can be found in the document entitled Skimming Prevention: Best Practices for Merchants, available at www.pcisecuritystandards.org.

Prior to deployment:

- Validate that serial numbers of received devices match sender records.
- Perform pre-installation inspection procedures, including physical and functional tests and visual inspection, to verify integrity of device.
- Maintain device in original, tamper-evident packaging or physically store it in a secure location until ready for deployment.
- Record device in inventory-tracking system as soon as possible.
- Restrict access to authorized personnel.
- Maintain a log of all access to device, including personnel name, company, reason for access, time in and out.
- Implement an audit trail, to demonstrate that a device is controlled, and not left unprotected, at all times from receipt through to installation.

After deployment, merchants should perform periodic physical inspections of devices to detect tampering or modification, including steps such as:

- Weigh POI devices upon receipt and then periodically for comparison with vendor specifications to identify potential insertion of tapping mechanisms within devices.
- Check for missing or altered seals or screws, extraneous wiring, holes in the device, or the addition of labels or other covering materials that could be used to mask damage from device tampering.
- Monitor devices in remote or unattended locations (for example, via the use of video surveillance or other physical mechanisms to alert personnel).
- If anything suspicious is detected, the device should not be used.

Report tampered or missing POI devices and other suspicious activity immediately to local law enforcement and the device provider.

6.2. **Instructions for responding to evidence of POI device tampering**

When the merchant has any suspicion that the device or packaging has been tampered with during shipping or that a device has been compromised while deployed:

- The device must not be deployed or used.
- Contact the device provider to report suspicious activity, including but not limited to:
  - Physical device breach
  - Logical alterations to device (configuration, access controls)
  - Disconnection or reconnection of devices
  - Failure of encryption mechanism
  - Failure of any device security control
  - Connection of unrecognized device
- If a replacement is required, contact your original POI device supplier for instructions. Each POI device will have the supplier identity affixed to it. Ensure replacement POI devices are P2PE approved before completing an RMA process.
- For secure devices being returned or replaced:
  - Wipe memory/clear devices prior to destruction.

Return devices to authorized vendor for destruction.

7. Device Encryption Issues

7.1. **Instructions for responding to POI device encryption issues**

In the event of a device encryption failure, that device must not be re-enabled for use until merchant has confirmed that either:

- The issue is resolved and P2PE functions are restored and re-enabled.

  OR

- All applicable PCI DSS controls are enabled and enforced within the environment to protect account data, since the P2PE solution can no longer be used to reduce PCI DSS scope.
- The merchant has provided written notification (signed by a merchant executive officer) formally requesting stopping of P2PE protection.

Though highly unlikely, there may be occasions where a device encryption failure occurs. For this type of event, we will contact your primary point of contact regarding the failure and work with you to troubleshoot the device based on the guidelines detailed in the "Troubleshooting" section of this manual. Once contacted regarding a device encryption failure and troubleshooting has failed to remedy the situation, you have two options available to you that include removing the device from us or you may choose to opt-out of using the P2PE solution and utilize it without P2PE protection.

If you elect to remove the failing device, you must contact the location affected and instruct

them to discontinue use of the device and inform that the device will be removed from service. The removal of the device from service must follow the steps describe previously within this manual. Once the device is removed, it must be returned to the device provider for repair or disposal. Please see instruction within this manual regarding the returning of devices.

8. POI Device Troubleshooting

8.1. **Instructions for troubleshooting a POI device**

In the event of an issue, we will work with you remotely to troubleshoot the issue. Prior to any troubleshooting, we will confirm that the individual contacting us is an authorized individual within your organization for troubleshooting purposes as defined to us during the initial deployment of the solution.

Begin by contacting Shift4 Customer Service at +1 702-597-2480, Option 2.

During our troubleshooting process:

1) Primary Account Number or Sensitive Authentication Data will never be outputted to your systems;
2) We will only collect the Primary Account Number or Sensitive Authentication Data as need to resolve the issue;
3) Data collected will be encrypted upon storage;
4) Data will be stored in specific, known locations with access restricted to those individuals charged with resolving your issue;
5) We will only collect limited amounts of data needed to solve the issue; and
6) All data will be securely removed from storage immediately after use and the issue is resolved.

For more device troubleshooting instructions visit the manufacturer's website to find the most current device documentation.

9. Additional Guidance

9.1. **Instructions for Disposal of POI devices**

Disposal of devices will be handled by Shift4 or our authorized parties. If you have device for disposal, please follow the instruction regarding the removal of a device for repair and return the device to us.

9.2. Instructions for how to confirm hardware, firmware, and application versions on POI devices

As the instructions for confirming hardware, firmware, and application versions of POI devices varies by device and manufacturer, please refer to your POI device manufacturer or reseller for

instructions on confirming this information.