True P2PE® Instruction Manual for PCI P2PE v2.0

1. P2PE Solution Information and Solution Provider Contact Details

1.1 P2PE Solution Information	
Solution name:	*True* P2PE v2.0
Solution reference number per PCI SSC website:	

1.2 Solution Provider Contact Information	
Company name:	Shift4 Corporation
Company address:	1491 Center Crossing Road, Las Vegas, NV 89144
Company URL:	http://www.shift4.com
Contact name:	Stephen Ames
Contact phone number:	702.597.2480
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. Approved POI Devices, Applications/Software, and the Merchant Inventory

POI devices must not be purchased after the PCI PTS expiration date.

Entities should update their device inventories with newer higher version number of approved devices that will not expire for the longest amount of time possible. As a best practice, entities should plan ahead and begin to stop purchasing devices as they are approaching their expiration date.

Organizations can continue to deploy expired devices as long as the entities purchased and took delivery of the devices prior to the device's expiration date.

(Note: sponsored entities should work with their sponsoring acquirer to ensure they are following any additional device usage requirements specific to their acquirer).

As device expiration dates approach, devices become:

- More vulnerable to attacks
- More likely to be involved in device and/or account data compromise incidents

Remove expired devices at the first opportunity and replace with PCI PTS approved devices tested against the latest security version. To assist acquirers, agents, Encryption and Support Organizations (ESO) and merchants with expiring device inventories, entities should take the following steps:

- Actively plan for the replacement of devices prior to the expiration date
- Invest in devices with the highest version to reap the benefits from state–of- the-art security
- Do not sell expired devices to secondary market
- Strive to not use expired devices for new deployments
- Remove expired devices from production environments

2.1 POI Device Details

The following information lists the details of the PCI-approved POI devices approved for use in this P2PE solution. For additional device information visit: *http://www.shift4.com/dotn/integration/third-party-devices.cfm*

Note all POI device information can be verified by visiting: *https://www.pcisecuritystandards.org/approved_companies_providers/approved_pin_transaction_security.php*

POI device vendor:	**IDTech**
POI device model name and number:	SecuRED
Hardware version #(s):	IDSR-33x1xxxxx & IDSR-38xxxxxx
Firmware version #(s):	SRED: 1.07, 1.08, 2.00, V2.00, v2.01
PCI PTS Approval #(s):	4-10144 & 4-10184
POI device vendor:	**IDTech**
POI device model name and number:	SREDKey
Hardware version #(s):	IDSK-53XXXXXXX
Firmware version #(s):	SRED: 1.01
PCI PTS Approval #(s):	4-10156
POI device vendor:	**Ingenico**

POI device model name and number:	iCMP
Hardware version #(s):	ICMxxx-01Txxxxx, ICMxxx-11Txxxxx, ICMxxx-21Txxxxx, ICMxxx-31Txxxxx
Firmware version #(s):	SRED (CTLS): 820528V02.xx, 820539V01.xx
PCI PTS Approval #(s):	4-20235
POI device vendor:	**Ingenico**
POI device model name and number:	iPP310, iPP320, iPP350, iPP315
Hardware version #(s):	IPP3xx-01Txxxxx, IPP3xx-11Txxxxx, iPP3xx-21Txxxxx, iPP3xx-31Txxxxx, iPP3xx-41Txxxxx, iPP3xx-51Txxxxx
Firmware version #(s):	SRED (Non CTLS) :820157V01.xx SRED (CTLS): 820365 V02.xx, 820305V02.xx, 820528V02.xx SRED (Non CTLS): 820375V01.xx 820305 V11.xx (base firmware), 820180 V01.xx (base firmware)
PCI PTS Approval #(s):	4-20174 4-30176 4-20142
POI device vendor:	**Ingenico**
POI device model name and number:	iSC250
Hardware version #(s):	iSC2xx-01Txxxxx
Firmware version #(s):	SRED (Non CTLS): 820157 V01.xx
PCI PTS Approval #(s):	4-30054, 4-30062
POI device vendor:	**Ingenico**
POI device model name and number:	iSC350
Hardware version #(s):	ISC3xx-01Txxxxx
Firmware version #(s):	SRED (Non CTLS) : 820157V01.xx
PCI PTS Approval #(s):	4-20133

POI device vendor:	**Ingenico**
POI device model name and number:	iSC480 Touch
Hardware version #(s):	ISC4xx-01Txxxxx (no CTLS), ISC4xx-11Txxxxx (CTLS) ISC4xx-01Txxxxx, ISC4xx-11Txxxxx
Firmware version #(s):	SRED (CTLS): 820528V02.xx
PCI PTS Approval #(s):	4-30098, 4-30125
POI device vendor:	**Ingenico**
POI device model name and number:	iSMP
Hardware version #(s):	iMP3xx-01Txxxxx, iMP3x0-01Txxxxx (already approved hardware version), iMP3x2-01Txxxxx (new hardware version)
Firmware version #(s):	SRED (Non CTLS) : 820528V02.xx
PCI PTS Approval #(s):	4-20183
POI device vendor:	**Ingenico**
POI device model name and number:	iSMP4
Hardware version #(s):	IMP6xx-01Txxxxx (without contactless), IMP6xx-11Txxxxx (with contactless)
Firmware version #(s):	820305v11.xx
PCI PTS Approval #(s):	4-30220
POI device vendor:	**Ingenico**
POI device model name and number:	iUC150B
Hardware version #(s):	iUC15x-01Txxxxx
Firmware version #(s):	820168 v01.xx
PCI PTS Approval #(s):	4-30172
POI device vendor:	**Ingenico**
POI device model name and number:	iUC285

Hardware version #(s):	iUC28x-01Txxxxx
Firmware version #(s):	820177V01.xx
PCI PTS Approval #(s):	4-30161
POI device vendor:	**Ingenico**
POI device model name and number:	iUP250
Hardware version #(s):	IUP2xx-01Txxxxx
Firmware version #(s):	SRED: 820528V02.xx
PCI PTS Approval #(s):	4-30075
POI device vendor:	**Ingenico**
POI device model name and number:	IWL220, IWL250
Hardware version #(s):	IWL2xx-01Txxxxx
Firmware version #(s):	SRED (Non CTLS):820528v02.xx
PCI PTS Approval #(s):	4-20181
POI device vendor:	**Ingenico**
POI device model name and number:	iUR250, iUR250P
Hardware version #(s):	iUR2xx-01Txxxxx, iUR2xx-11Txxxxx
Firmware version #(s):	SRED: 820514V01.xx
PCI PTS Approval #(s):	4-30083
POI device vendor:	**Verifone**
POI device model name and number:	Mx925 / Mx915
Hardware version #(s):	P132-509-01-R (MX 925), P132-509-11-R (MX 925), P132-509-21-R (MX 925), P132-509-11-PF (MX 925), P132-409-01-R (MX 915), P132-509-02-R (MX 925), P132-509-12-R (MX 925), P132-509-21-R(MX 925), P132-509-22-R (MX 925), P132-509-12-PF (MX 925), P132-409-01-R (MX 925), P132-409-02-R (MX 915)
Firmware version #(s):	SRED: 1.x.x, 3.x.x; 4.x.x; 5.x.x, OP: 1.x.x, 3.x.x; 4.x.x; 7.x.x, SRED

	5.x.x.xxx
PCI PTS Approval #(s):	4-10110

2.2 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.

Note that 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.

	POI device vendor	POI device model name(s) and number:	POI Device Hardware & Firmware Version #		
	IDTech	SecuRED	Hardware: IDSR-33x1xxxxx & IDSR-38xxxxxx Firmware: SRED: 1.07, 1.08, 2.00, V2.00, v2.01		
	IDTech	SREDKey	Hardware: IDSK-53XXXXXXX Firmware: SRED: 1.01		
	Application vendor	**Name**	**Version #**	**Is application PCI listed? (Y/N)**	**Does application have access to clear-text account data (Y/N)**
	Shift4	FormAgent	30250600	N	N
	POI device vendor	**POI device model name(s) and number:**	**POI Device Hardware & Firmware Version #**		
	Ingenico	iCMP	Hardware: ICMxxx-01Txxxxx, ICMxxx-11Txxxxx, ICMxxx-21Txxxxx, ICMxxx-31Txxxxx Firmware: SRED (CTLS): 820528V02.xx, 820539V01.xx		

	Ingenico	iPP320, iPP350, iPP310, iPP315	Hardware: IPP3xx-01Txxxxx, IPP3xx-11Txxxxx, iPP3xx-21Txxxxx, iPP3xx-31Txxxxx, iPP3xx-41Txxxxx, iPP3xx-51Txxxxx Firmware: SRED (Non CTLS) :820157V01.xx, SRED (CTLS): 820365 V02.xx, 820305V02.xx, 820528V02.xx SRED (Non CTLS): 820375V01.xx, 820305 V11.xx (base firmware), 820180 V01.xx (base firmware)		
	Ingenico	iSC250	Hardware: iSC2xx-01Txxxxx Firmware: SRED (Non CTLS): 820157 V01.xx		
	Ingenico	iSC350	Hardware: ISC3xx-01Txxxxx Firmware: SRED (Non CTLS) : 820157V01.xx		
	Ingenico	iSC480 Touch	Hardware: ISC4xx-01Txxxxx (no CTLS), ISC4xx-11Txxxxx (CTLS), ISC4xx-01Txxxxx, ISC4xx-11Txxxxx Firmware: SRED (CTLS): 820528V02.xx		
	Ingenico	iSMP	Hardware: iMP3xx-01Txxxxx, iMP3x0-01Txxxxx (already approved hardware version), iMP3x2-01Txxxxx (new hardware version) Firmware: SRED (Non CTLS) : 820528V02.xx		
	Ingenico	iSMP4	Hardware: IMP6xx-01Txxxxx (without contactless), IMP6xx-11Txxxxx (with contactless) Firmware: 820305v11.xx		

	Ingenico	iUC150B	Hardware: iUC15x-01Txxxxx Firmware: 820168 v01.xx		
	Ingenico	iUC285	Hardware: iUC28x-01Txxxxx Firmware: 820177V011.xx		
	Ingenico	iUP250	Hardware: IUP2xx-01Txxxxx Firmware: SRED: 820528V02.xx		
	Ingenico	IWL220, IWL250	Hardware: IWL2xx-01Txxxxx Firmware: SRED (Non CTLS):820528v02.xx		
	Ingenico	iUR250, iUR250P	Hardware: iUR2xx-01Txxxxx, iUR2xx-11Txxxxx Firmware: SRED: 820514V01.xx		
	Application vendor	**Name**	**Version #**	**Is application PCI listed? (Y/N)**	**Does application have access to clear-text account data (Y/N)**
	Shift4	FormAgent	30250600	N	N
	POI device vendor	**POI device model name(s) and number:**	**POI Device Hardware & Firmware Version #**		
	VeriFone	Mx925 / Mx915	Hardware version #(s): P132-509-01-R (MX 925), P132-509-11-R (MX 925), P132-509-21-R (MX 925), P132-509-11-PF (MX 925), P132-409-01-R (MX 915), P132-509-02-R (MX 925), P132-509-12-R (MX 925), P132-509-21-R(MX 925), P132-509-22-R (MX 925), P132-509-12-PF (MX 925), P132-409-01-R (MX 925), P132-409-02-R (MX 915)		

			Firmware version #(s): SRED: 1.x.x, 3.x.x; 4.x.x; 5.x.x, OP: 1.x.x, 3.x.x; 4.x.x; 7.x.x, SRED 5.x.x.xxx		
	Application vendor	**Name**	**Version #**	**Is application PCI listed? (Y/N)**	**Does application have access to clear-text account data (Y/N)**
	Shift4	FormAgent	30250600	N	N

2.3 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 the device provider.
- Sample inventory table below is for illustrative purposes only. The actual inventory should be captured and maintained by the merchant in an external document.

A device inventory is required to be maintained by the merchant in addition to any inventory maintained by a third-party support provider.

The device inventory must include at least the following:

- Make and model of device
- Location (site/facility)
- Serial number
- General description
- Status
  - Deployed
  - Awaiting deployment
  - Undergoing repair or otherwise not in use
  - In transit
- Security seals, labels, hidden markings, etc.
- Number and type of physical connections to device
- Date of last inspection
- Firmware version
- Hardware version
- Any application versions

A physical inventory must be conducted at least annually to verify the validity of the inventory and detect removal or substitution of devices. Any discrepancies must be noted and reported to the device provider immediately.

The device inventory must be secured from unauthorized access.

2.3 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** 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; and
- 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 Tempus Technologies 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);
5) Access to room must be monitored (Cameras or physical sight).

Sample Inventory Table

Device vendor	Device model name(s) and number:	Device Location	Device Status	Serial Number or other Unique Identifier

3. 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 2.1 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.
- Only P2PE approved capture mechanisms as designated on PCI's list of Validated P2PE Solutions and in the PIM can be used.

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

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

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

3.1 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 http://www.shift4.com/dotn/integration/third-party-devices.cfm.

Contact your contracted device installer.

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

Physically secure POI devices in your possession, including devices:

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

3.2 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.

3.3 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.

4. POI Device Transit

4.1 Instructions for securing 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 delivery 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.

4.2 Instructions for ensuring POI devices originate from, and are only shipped to, trusted sites/locations

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

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

- ScanSource Payment Solutions
- First Data Hardware Services
- Verifone Key Injection Service
- Portal Secure

- Ingenico US KIF
- ID Tech US KIF
- POSData KIF
- The Phoenix Group Key Injection Services

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.

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.

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.

Securing Devices Removed From Service

When devices are removed from service either for repair, being returned, being replaced, or being returned to storage, this must be done in a manner that allows for the tracking and security of the device. The following initial steps are required regardless of the reason a device is removed from service:

1) Removal of device must be pre-arranged prior to removal;
2) Location of device removal must confirm personnel removing device are authorized;
3) Personnel performing removal must be documented to include name, company, and time of removal; and
4) Inventory must be updated to indicate that the device was removed and reason for removal.

If the device is to remain at the deployment location for future deployment, the device must be securely stored at the location in a manner as described earlier within this manual.

If the device is to be returned to your shipping location, the device must be packed in a tamper-evident

package and shipped using an authorized source that can be tracked. Methods for shipping and tracking are described in previous sections of this manual.

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

5. POI Device Tamper Monitoring and Skimming Prevention

5.1 Instructions for physically inspecting POI devices and preventing skimming, including instructions and contact details for reporting any suspicious activity
Additional guidance for skimming prevention on POI terminals 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.

5.2 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.

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

You must implement procedures for the detection of unauthorized alterations or replacement of devices

prior to use and once deployed. This is imperative to maintaining the security of the P2PE solution and in enabling you to maintain your PCI DSS compliance.

Prior to deployment of device for use, the deployment location must validate that the device received has not been tampered with or substituted. While awaiting deployment, the device must be deployed in a secure storage location with restricted access. 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) Device must remain in its original, tamper-evident packaging or in a physically secure storage until ready for use;
3) Storage location must support restricted access;
4) 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.
5) 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);
6) Access to room must be monitored (Cameras or physical sight).

Once the device is removed from storage and is being prepped for deployment, the following steps must be implemented:

1) The serial number on the devices must be matched with the recorded serial number of the device removed from storage and shipped to the location. This information must be recorded within inventory tracking at the deployment location and at the shipping location at the time of deployment;
2) A pre-installation of the device must be performed to ensure the device has not been tampered with. This must include physical inspection of the device to search for breakage of seal and security tampering seals; and
3) Prior to finally deployment into production, functionality must be tested to ensure that the device communicates and captures data properly.

Special Note: It is recommended that a list of device and serial numbers approved for a defined location be delivered to the location separate from the devices themselves. This will circumvent an individual from being able to substitute devices with differing serial numbers and updating the inventory list to reflect the compromised devices.

Once POI devices have been deployed, periodic inspection must be made at deployment locations to ensure devices have not been tampered with or substituted. The type of location for deployment will drive the frequency for inspections. For high traffic, visible areas such as storefronts, it is recommended inspections occur twice a year. For locations that are remote or unattended, it is recommended that inspections occur every ninety (90) days.

- When inspecting devices the first step should be to compare the serial number of the device with the

serial number recorded for the location. If the serial numbers do not match, this could be the result of an unauthorized substitution. The individual should contact the personnel responsible for the storage, shipping, and installation of the POI device to confirm if the documentation is incorrect or if indeed a device has been substituted. Once the serial number has been confirmed, the device should undergo a physical inspection for tampering. Tamper and security seals should be examined to see if the seals are broken. The connection to the device should be inspected to ensure no extraneous devices are attached. The device should be inspected for missing screws, holes, or the addition of labels or covering that could be used to mask damage. Finally, the card DIP or magnetic stripe reader of the POI device should be investigated to ensure a "skimmer" or other type of device is not been inserted.

6. Device Encryption Issues

6.1 Instructions for responding to POI device encryption failures

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 Tempus Technologies or its designated partner for repair or disposal. Please see instruction within this manual regarding the returning of devices.

6.2 Instructions for formally requesting of the P2PE solution provider that P2PE encryption of account data be stopped

If upon device encryption failure, the merchant chooses to process transactions without P2PE protection, those transactions will be rejected by DOLLARS ON THE NET and you must immediately contact Shift4 Customer Service at +1 702-597-2480, Option 2.

- The security impact to the merchant's account data and potential risks associated with processing transactions without P2PE protection.
- Implementing alternative controls to protect account data in lieu of the P2PE solution.
- The merchant is no longer eligible for completing SAQ P2PE, associated with use of PCI P2PE solutions.
- Advising their acquirer that they are no longer using the P2PE solution.
- Processing transactions without P2PE protection may impact the merchant's PCI DSS compliance validation and the merchant should confirm with their acquirer or payment brand, as applicable, for all PCI payment brands affected.

7. POI Device Troubleshooting

7.1 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.

8. Additional Solution Provider Information

Third-Party Access Monitoring

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.

Disposal of 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 device for repair and return the device to us.

9. Document Update and Distribution

8.1 Document Update
This document will be reviewed at least annually and updated upon meaningful change.

8.2 Document Distribution
The most current version of this document is available on the website at http://www.shift4.com.