VERSION 2.9

OCTOBER 28, 2019

P2PE INSTRUCTION MANUAL (PIM)
A MERCHANT GUIDE FOR DEPLOYING AND MAINTAINING NCR SECURED P2PE SOLUTIONS DEVICES

SEGMENT: NCR PAYMENT SOLUTIONS, LLC.

AN NCR COMPANY

Contents

1. P2PE Solution Information and Solution Provider Contact Details

1.1 P2PE Solution Information	
Solution name:	NCR Secured P2PE Solutions
Solution reference number per PCI SSC website:	https://www.pcisecuritystandards.org/assessors_and_solutions/point_to_point_encryption_solutions

1.2 Solution Provider Contact Information	
Company name:	NCR Payment Solutions, LLC.
Company address:	4450 Sojourn Dr Suite 500B Addison, TX 75001
Company URL:	www.NCR.com
Contact name:	David Skertich
Contact phone number:	214-420-2850
Contact e-mail address:	David.Skertich@ncr.com

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

2.1 POI Device Details

The following information lists the details of the PCI-approved POI devices approved for use in this P2PE solution. **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:	PAX COMPUTER TECHNOLOGY (SHENZEN) CO LTD
POI device model name and number:	PAX S300
Hardware version #(s):	S300(MOS)-xxx-0x4-0xxx (w/o CTLS) S300(MOS)-xxx-3x4-0xxx (with CTLS)
Firmware version #(s):	4.00.xx
PCI PTS Approval #(s):	4-30245

POI device vendor:	PAX COMPUTER TECHNOLOGY (SHENZEN) CO LTD
POI device model name and number:	PAX S500
Hardware version #(s):	S500-xxx-xx4-0xxx
Firmware version #(s):	4.00.xx
PCI PTS Approval #(s):	4-40151

POI device vendor:	PAX COMPUTER TECHNOLOGY (SHENZEN) CO LTD
POI device model name and number:	PAX S920, S920 L, S920 F
Hardware version #(s):	S920-xxx-xx4-0xxx S920-xxx-xx4-1xxx S920-xxx-xx4-2xxx S920-xxx-xx4-Axxx S920-xxx-xx4-3xxx S920-xxx-xx4-Jxxx
Firmware version #(s):	Prolin OS: 14.00.xx, Prolin Boot: 2.0.x Prolin OS: 14.01.xx xxxx Prolin OS: 14.03.xx xxxx Prolin Boot: 3.x.xx.xxxx
PCI PTS Approval #(s):	4-30159

2.2 POI Software/application Details

The following information lists the details of all P2PE certified software/applications.

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.

Application vendor, name and version #	POI device vendor	POI device model name(s) and number:	POI Device Hardware & Firmware Version #	Is application PCI listed? (Y/N)	Does application have access to clear-text account data (Y/N)
PAX COMPUTER TECHNOLOGY (SHENZEN) CO LTD COMPUTER TECHNOLOGY (SHENZEN) CO LTD S300	PAX	S300 (MOS)	**Hardware:** S300-xxx-0x4-0xxx (w/o CTLS), S300-xxx-3x4-0xxx (with CTLS) **Firmware #:** 4.00.xx Approval #(s):4-30245	No	No
PAX COMPUTER TECHNOLOGY (SHENZEN) CO LTD COMPUTER TECHNOLOGY (SHENZEN) CO LTD S500	PAX	S500	**Hardware:** S500-xxx-xx4-0xxx **Firmware:** SRED 4.00.xx PCI PTS Approval #(s): 4-40151	No	No
PAX COMPUTER TECHNOLOGY (SHENZEN) CO LTD COMPUTER TECHNOLOGY (SHENZEN) CO LTD S920	PAX	S920	**Hardware:** S920-xxx-xx4 Firmware: Prolin OS: 14.00.xx, Prolin Boot: 2.0.x, Prolin OS: 14.01.xx xxxx, Prolin OS: 14.03.xx xxxx	No	No

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).
- The merchant is responsible for:
    - Validating that the equipment received at the merchant location has the security seal enclosure that has not been opened or tampered with.
    - Ensuring that an authorized user contacts NCR Assist at 800-834-4405, Option 2 for Customer Service to verify Bag Number.
    - Access to POI devices is restricted to authorized personnel
    - An authorized user performs an audit, at least annually of all POI devices to ensure the proper serial number POI device is logged with the correct location and status. Also review devices for authorized removal or device tampering.
    - If you are storing devices when not in use, they must be in a secure area with restricted access. Access must be restricted by key or other locking mechanism and access only allowed to designated personnel and each access must be logged and the records maintained for audit purposes.
- Any variances in inventory, including missing or substituted POI devices, must be reported to NCR 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.

It is important to identify personnel who will be responsible for maintaining the POI inventory and for inspection of devices. They will identify each POI device as being in one of five states:

- Deployed
- Awaiting Deployment
- Out of Service and/or Out for Repair
- In Transit
- Removed and returned

During the regular inventory management process, you must investigate the POI devices to identify any evidence of 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.

Indications of tampering may include, but is not limited to, attachment of 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.

Should you detect a compromised device or find that your inventory indicated a missing or substituted device, you must report this information to NCR immediately.

In addition to keeping record of device serial numbers, it is recommended that you include the following guidelines to ensure that your devices are not compromised.

- Take photographs from all angles of each device, including any labels or serial numbers on the device.
- Use the original photographs to compare devices on future inventory reviews.
- Record the location a device is deployed and match to the device serial number.
- Record how the terminal is connected, including the style, type, and color of each connector. It is recommended a photograph of the connectors.
- Mark each terminal with an ultra-violet (UV) security pen to provide a unique identifier for that terminal.

A sample inventory table is provided below.

Inventory Table Example

Device vendor	Device model name(s) and number:	Device Location	Device Status	Device Serial Number
PAX	S300	Merchant Name, Address, City, State, Zip	Deployed	112266558
PAX	S500	Merchant Name, Address, City, State, Zip	In Transit	112266599

3. POI Device Installation Instructions

Before unpacking the terminal, verify the bag number from the tamper-evident bag by contacting NCR Assist at 800-834-4405, Option 2 for Customer Service.

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.

Be cautious when attempting to change device settings or configurations, as some changes could invalidate the PCI-approved P2PE solution. If uncertain, it is best to consult with the support team. 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

S300

- Technical Requirements:
  - A standard 110-volt power plug for each device.
  - An ethernet switch port for each device.
  - The PAX S300 devices will require a fixed IP address on your internal network that is reachable from the workstation that will be used for payment processing. Your terminal is programmed and ready for use as soon as it is setup.
- Unpacking the box:
  - 1 S300 with stylus
  - 1S300 POS Connector cable and power cord.
  - 1 Ethernet cable.

1 S300 with stylus

1 S300 POS Connector cable and power cord

1 Ethernet cable

- Connecting the terminal
  - Plug an ethernet cable into the RED port on the S300 cable. The yellow and blue ports will not be used in this configuration.
  - Plug the power adapter into a nearby outlet and plug adapter A into the B adapter on the S300 cable and the device will power on.

- For assistance in setting up your terminal contact NCR Assist at 800-834-4405, Option 2 for Customer Service.

S500

- Technical Requirements:
  - A standard 110-volt power plug for each device.
  - An ethernet switch port for each device.
  - The PAX S500 devices will require a fixed IP address on your internal network that is reachable from the workstation that will be used for payment processing. Your terminal is programmed and ready for use as soon as it is setup.
- Unpacking the box:
  - 1 S500
  - 1S500 power cord.
  - 1 Ethernet cable.

1 S500

1 S500 power cord

1 Ethernet cable

- Connecting the terminal: To start using the PAX S500, you simply need to connect the device to a power source and then connect the device cable to your network.
  - Plug an ethernet cable into the LAN Port.
  - Plug the power cable into the POWER Port
- For assistance in setting up your terminal contact NCR Assist at 800-834-4405, Option 2 for Customer Service.

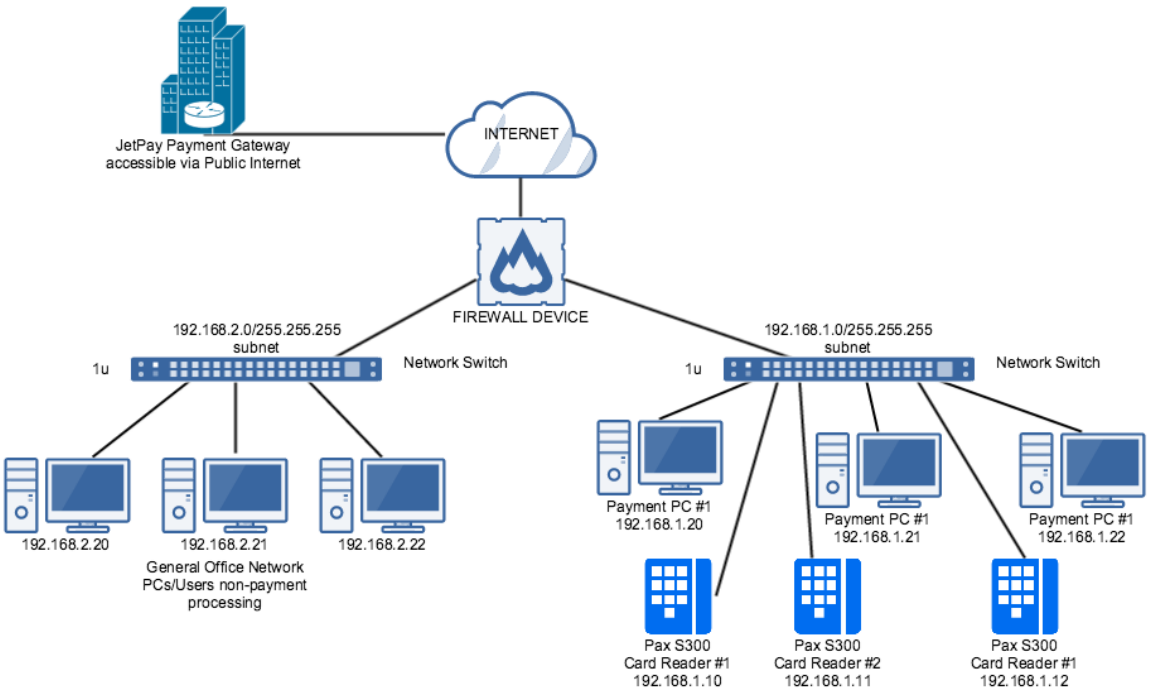
S920

Technical Requirements:

- Standard 110-volt power outlet
- An ethernet switch port for each device
- A fixed IP address on your internal network that is reachable from the workstation that will be used for payment processing
- Unpacking the Box:

- Connecting the terminal:
- Verify your bag number in your portal to ensure you have received the correct terminal.
- To charge your terminal you can either:
    - Place it on the charging dock.
    - Connect it to the charging cable.
    - You will also need to charge the charging dock with the power cord.
- For assistance in setting up your terminal contact NCR Assist at 800-834-4405, Option 2 for Customer Service.

Below is NCR's recommended network configuration for a small office, providing face to face payment options using an IP based EMV card reader.



Please coordinate with your technical staff to obtain IP address allocations inside your office network. This configuration may require additional network cabling to each potential card reader location.

One IP address is required for each reader, addresses must be configured in static mode. The card readers and PCs will require outbound TCP port 443, UDP port 53, and port 9120 for outbound communication, your local firewall network support will need to ensure this traffic is allowed.

Port 10009 should allow both inbound and outbound communications both on the credit card device and on the PCs that will be communicating with the credit card devices.

To comply with PCI best practices these computers and card reader devices should be on their own network segment. These devices are PCI P2PE compliant. In most environments this will allow you to do an annual SAQ-P2PE for the network segment that these devices are attached to.

Outbound Traffic Considerations and troubleshooting

If a network prohibits outbound traffic, the following addresses need to be allowed:

- https://gateway20.jetpay.com/jetpay
- https://gateway17.jetpay.com/jetpay

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.
- Waiting transport to designated KIF site

3.2 Guidance for selecting appropriate locations for deployed devices

- Ensure that public access to the POS device is limited to the parts of the device the customer/cardholder would need to access to complete a transaction, such as the card reader and/or PIN pad.
- To deter compromise attempts you should position the device in an area observable by authorized staff.
- Authorized personnel should complete daily checks of the device to look for indications of tampering
- Make sure any store monitoring of CCTV or cameras cannot view input of the PIN

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

- Merchants should physically secure or mount devices in such a manner that they are able to be observed at all time by staff to ensure unauthorized access or attempts at compromise.
- If devices are deployed in a remote location or unattended, it is recommended that the devices be monitored with a camera so that one may review footage to determine if there has been an attempt to tamper with the device.
- If the devices cannot be physically secured, they should be assigned to specific staff with responsibility for controlling access and preventing tampering.
- If you are storing devices when not in use, they must in a secure area with restricted access. Access must be restricted by key or other locking mechanism and access only allowed to designated personnel and each access must be logged and the records maintained for audit purposes. Note: Do NOT drill into terminals to connect cables, as this triggers security mechanisms inside the terminals, which will cause them to stop working.
- The devices should also be placed in a location that can be locked and made completely inaccessible during non-business hours.

4. POI Device Transit

4.1 Instructions for securing POI devices intended for, and during, transit

- All devices must be shipped in tamper proof packaging that will show any attempt to open the seal on the package. This includes shipping from the designated KIF to NCR or the merchant, shipping from one merchant location to another and returning a device from the merchant location to NCR or its designated KIF.
- Shipping must be done with a trusted shipping service or a designated employee/courier of the merchant. Any time a device is shipped the courier, date of pickup device (S/N) must be logged. Delivery acceptance of the device (S/N) must also be logged. The following information must be logged for device delivery:

    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 as determined by you. The recipient must be notified as to how to determine if the package has been tampered with during transit. Your deployment sites must perform the same inspection as provided upon inspection of POI device received from NCR initially.

If using internal employees for device shipment, they must be instructed to not leave devices in public areas unattended, such as 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

- To ensure there was no tampering during shipment you should confirm that the device was shipped from an authorized NCR source:

  The Phoenix Group
  6705 Keaton Corporate Parkway
  O'Fallon, MO 63368

- Upon receipt of the device and after validating the shipping source, you must also inspect the device and its security seals to make sure no tampering has occurred.

- An authorized user must contact Assist at 800-834-4405, Option 2 for Customer Service to validate that the device(s) received matches the information in the NCR system.

NOTE: If you see any evidence of tampering call NCR Assist at 800-834-4405, Option 2 for Customer Service and DO NOT deploy the device for use.

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.

Each P2PE compliant merchant is responsible for designating staff to perform inspections of devices. The designated staff must:

- Validate that serial numbers of received devices match inventory recorded.
- Perform pre-installation inspection procedures, such as; check for missing or altered seals, or the presence of decals/labels that could be hiding evidence of tampering.
- Keep the POS device in its original, tamper proof packaging and physically store it in a secure location until ready for deployment.
  - Monitor POS devices in storage locations with the use of CCTV or video recorded surveillance
  - Restrict access to authorized personnel.
  - Maintain a log of all access to device, including personnel name, company, reason for access, time in and out.

- Record Device Status in the inventory table referenced in Section 2.3.
- If anything, suspicious is detected, the device should not be used.

5.2 Instructions for responding to evidence of POI device tampering

- When the merchant or its designated staff has any suspicion that the device packaging or the device itself has been tampered with during shipping the device must not be deployed for use.

- They should contact their NCR Account Manager immediately to report any suspicious activity and instructions on next steps. This would include potential issues found during pre-installation inspection such as:

    - Evidence of tampering on the security seal
    - Serial numbers of device(s) not matching what is provided to Assist team
    - Evidence of delivery from an address other than one authorized in this document

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

NCR ships supported POI device directly to merchants. No other location will be utilized to send P2PE supported POI Devices. In order to remain compliant, you may only deploy POI devices that are shipped directly from NCR.

- To ensure the POI device originates from and are only shipped to trusted sites and locations, the serial numbers on the terminal, the boxes the terminals are in, and the invoice provided for the terminals must all match.
- Signature upon receipt of the terminals should be required by the shipping method and the logistics provider. Only authorized signers should receive terminals.
- Before deploying a device for use, the merchant or their designated staff must ensure that the device received has not been tampered with or substituted.
- If the merchant is storing devices while awaiting deployment, the device(s) must be stored in a secure storage location with restricted access.
- If the merchant is storing devices the storage location must include the following measures:
    - The device must be stored in secured locked room
    - Keep the POS device in its original, tamper proof packaging
    - Monitor POS devices in the storage location with the use of CCTV or video recorded surveillance
    - Restrict access to authorized personnel.
    - Maintain a log of all access to device, including personnel name, company, reason for access, time in and out

- Once the device is removed from storage for use at the merchant location; the merchant or its designated staff should:
  - Validate that serial numbers of stored devices match inventory and status recorded in inventory table.
  - Perform pre-installation inspection procedures, such as; check for missing or altered seals, or the presence of decals/labels that could be hiding evidence of tampering.
  - Record the updated device status in the inventory table.
  - Test that the functionality of the device communicates and captures data properly.
- If anything, suspicious is detected, the device should not be used.

5.4 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

NCR does not use any personnel to perform on-site maintenance of devices. All devices must be returned to the designated KIF for service and any such requests for access should be denied and reported to NCR.

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.

i. Review all Point of Sale (POS) system logs and batching functions for credit authorization and any sign of clear text cardholder data.

ii. Review all POS settlement reports to ensure that no unencrypted cardholder data is present.

In the event that clear text cardholder data is found or suspected, signaling a device encryption failure, the merchant must contact NCR Assist at 800-834-4405, Option 2 for Customer Service immediately and follow the troubleshooting instructions found in Section 7 of this document. Until proper encryption functionality on the device has been restored and the device has been reauthorized by NCR, the faulty device may not be used to

process transactions unless the merchant formally requests a suspension of P2PE encryption as outlined in Section 6.2.

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 shall immediately take the device out of use and then notify NCR who will provide them a new device via swap.

The security impact to the merchant's account data and potential risks associated with processing transactions without P2PE protection is too great to allow without P2PE protection, we recommend they wait until a new P2PE device is in place to begin processing transactions.

If the merchant chooses to not follow the recommendation, they are no longer eligible for completing SAQ P2PE associated with use of PCI P2PE.

To opt-out of using the protection of the P2PE solution please contact your NCR Account Manager.

7. POI Device Troubleshooting

7.1 Instructions for troubleshooting a POI device

In the event of an issue, NCR will want 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.

If a POI device is damaged, destroyed, appears to be malfunctioning or otherwise requires servicing, NCR and the merchant must follow the following process:

1. Confirm that the end user has been authorized to troubleshoot this device. If they have not, then escalate it to someone who does.
2. If Error Code is showing on the device's display screen, using the manufacturer's resources follow the troubleshooting guidelines.
3. Verify that the cables are securely connected to the correct port.
4. Confirm that the device's indicator lights are properly illuminated.
5. Power cycle the device by unplugging all the cables and plugging them back in.
6. If success stop; else continue to STEP 7.
7. Unplug all cables from the device. Remove power plug from device.
8. Plug all cables back into the device.
9. Plug power back into the device.

8. Additional Solution Provider Information

Third-Party Access Monitoring

NCR has only one authorized vendor (The Phoenix Group) for repair/maintenance and that vendor is only authorized to perform maintenance at their physical location. NCR will not utilize any on-site 3rd party vendors to assist with P2PE equipment.

This P2PE Instruction Manual is provided pursuant to the requirements of the PCI DSS. Implementation of the controls set forth in this PIM is a requirement for the PCI DSS SAQ-P2PE-HW and Attestation of Compliance. The use of any POI device not approved by NCR and/or any failure to comply with the requirements set forth in this manual is at the merchant's sole risk and may result in non-compliance and loss of qualification for PCI DSS scope reduction and/or compromised data security.