

Payment Card Industry (PCI)
Point-to-Point Encryption

**P2PE Instruction Manual (PIM) Template**

**For Use with P2PE Version 3.0**

December 2019

# Introduction

The P2PE solution provider shall provide a P2PE Instruction Manual (PIM) in accordance with requirements in Domain 3 of the P2PE Standard. The current version of this document must be used as the template for creating the PIM.

Section 1 of this document contains instructions to facilitate populating the PIM template in Section 2. The intent is for the solution provider to only provide the completed PIM template, sans the instructions, to the merchant customers.

# Section 1 – Required PIM Content

All sections provided in the PIM Template in Section 2 must be filled out according to the instructions below.

Some sections include standardized guidance that must be included as is, with no alteration. Other sections require the solution provider to incorporate information specific to the P2PE Solution. Sections requiring input from the solution provider are identified with the notation *“<Insert details here>.”*

The solution provider may provide additional information in the PIM that the solution provider feels is useful to entities implementing and/or using the P2PE solution. The solution provider may also personalize the PIM template, such as by adding company logos, formatting, etc. However, the solution provider must not remove any sections, numbering, or content provided within this document.

All PIM requirements must be completed by the solution provider to the extent that they are applicable to the P2PE solution.

## PIM Template Instructions

| **PIM TemplateReference #** | **Instructions** |
| --- | --- |
| P2PE Solution Information and Solution Provider Contact Details |
| 1.1 | Complete the table with the PCI-approved P2PE solution details denoted.  |
| 1.2 | Complete the table with the P2PE solution provider company details.  |
| 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.* What to do if the device is received from an untrusted or unknown source location, including:
* Procedures for confirming the device is authorized
* Contact details for authorized third parties
* Procedures to ensure devices are not used unless the source location is verified as trusted
 |
| 2.2 | Instructions for confirming POI packaging and device were not tampered with, and for establishing secure, confirmed communication with the solution provider.If the solution provider uses distribution channels to distribute or sell POIs to merchants, provide guidance to the merchant for the following: * How the merchant should confirm that the device and packaging have not been tampered with, including pictures of what the device packaging should look like if not tampered with, as applicable.
 |
| 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. |
| Approved POI Devices, Applications/Software, and the Merchant Inventory  |
| 3.1 | Complete the table with all the requested POI device details. Add tables for each POI model number approved for use in the solution. Provide explicit instructions and guidance the merchant can easily follow to obtain the POI Device Details so that the merchant can compare each POI device with the details supplied within the PIM. |
| 3.2 | Complete the table with all requested POI software details for both P2PE applications and P2PE non-payment software. Add rows for each type of software used on POI devices in the solution. |
| 3.3 | Provide explicit instructions and guidance the merchant can follow easily to document and monitor its POI inventory. Highlight how the merchant can obtain the POI device specifics required for the inventory. A sample table is provided to indicate the minimum required information. |
| POI Device Installation Instructions |
| 4.1 | Provide explicit instructions detailing the approved installation and connections for all POI devices utilized in the P2PE solution, including specific instructions for any required connections to peripheral systems such as an electronic cash register, printer, etc. |
| 4.2 | Document how the merchant should select appropriate locations for deployed POI devices, for example: * How to control public access to devices such that public 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).
* How to place and install devices so they can be observed and/or monitored by authorized personnel (for example, during daily device checks performed by store/security staff).
* How to place and install devices in an environment that deters compromise attempts (for example, through use of appropriate lighting, access paths, visible security measures, etc.) to physically secure deployed devices to prevent unauthorized removal or substitution, including examples of how devices can be physically secured to prevent unauthorized removal or substitution of devices (such as wireless or handheld devices).
 |
| 4.3 | Include guidance on how the merchant should physically secure deployed POI devices to prevent unauthorized removal or substitution, including examples of how devices can be physically secured. This includes guidance to secure physical access to devices undergoing repair or maintenance while in the merchant’s possession. This guidance also covers both attended and unattended devices, as applicable to the P2PE solution (for example, kiosks, “pay-at-the-pump,” etc.)If the solution includes devices that cannot be secured physically (such as wireless or handheld devices), include additional guidance for those specific device types, which may include, for example:* 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.
 |
| POI Device Transit |
| 5.1 | Document how the merchant should secure POI devices in transit (anytime the merchant ships POI devices) to include at least the following: * Shipping via a trackable method (for example, private courier services or public shipping companies that provide status during shipping)
* Notification to the company to which the package is shipped, including package tracking details
 |
| 5.2 | Document how the merchant transports POI devices only to trusted sites/locations, including the following: * Contact details or information about authorized sites/locations to which merchants can send devices
 |
| POI Device Tamper & Modification Guidance |
| 6.1 | Provide guidance for the merchant when performing periodic physical inspections of POI devices to detect tampering or modification, to include: * How to perform physical inspections of provided devices, **including photographs or drawings** of the device illustrating what the merchant is to inspect.

**For example,** the guidance might include checking for: * Missing or altered seals or screws
* Extraneous wiring
* Holes in the device
* Addition of labels or other covering material that could be used to mask damage from device tampering
* Foreign objects attached to the device
* Altered device connections
* How to monitor devices in remote or unattended locations.

**For example,** the guidance might include:* Using video surveillance or other physical mechanisms to alert personnel of suspicious or unauthorized activity
* How to detect and report tampered or missing POI devices, and other suspicious activity, including:
* Contact details and instructions for reporting suspicious activity;
* Contact details and instructions for returning devices;
* Guidance that, if anything suspicious is detected, the device should not be used and should be reported immediately to the contacts provided.

Additionally, the solution provider should provide merchants with PCI SSC’s Information Supplement Skimming Prevention: Overview of Best Practices for Merchants and “Skimming Prevention: Best Practices for Merchants” available at [www.pcisecuritystandards.org](http://www.pcisecuritystandards.org). |
| 6.2 | Provide guidance for instances 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, including the following:* Guidance that the device must not be deployed or used
* Contact details and instructions for reporting suspicious activity
* Contact details and instructions for returning devices
 |
| 6.3 | Provide guidance for the merchant 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.  |
| Device Encryption Issues |
| 7.1 | Provide instructions for the merchant to follow in the event of a device encryption failure, including that devices must not be re-enabled for use until merchant has confirmed that either: * The issue is resolved and P2PE-encryption functions are restored and re-enabled;

**OR*** The merchant has provided written notification (signed by a merchant executive officer) formally requesting stopping of P2PE encryption.
 |
| POI Device Troubleshooting |
| 8.1 | Provide guidance for the merchant to follow if they need to troubleshoot a POI device problem, including: * To contact the solution provider or authorized third party for assistance with any troubleshooting
* Contact details
 |
| Additional Guidance |
| 9.1 | Use this section to provide additional pertinent guidance for merchants regarding the P2PE solution. |
| 9.2 | Provide instructions on how to confirm the hardware, firmware and application details on POI devices. |

**Section 2 – PIM Template**

Complete the following PIM template per the instructions above and provide the completed PIM to your merchants. The following page, the “title” page, can be populated per the solution provider’s corporate document guidelines (for example, company name, logo, date, version, etc.). Likewise, the headers and footers can follow the solution provider’s corporate document guidelines. *Solution providers must either delete or modify the headers and footers in their published* P2PE Instruction Manual*—the PCI SSC headers and footers in this PIM template must not be used by the solution provider.*

*<PIM title page for solution provider customization>*

|  |
| --- |
| P2PE Solution Information and Solution Provider Contact Details |
| P2PE Solution Information |
| Solution name: | *<Insert details here>* |
| Solution reference number per PCI SSC website: | *<Insert details here>* |

|  |
| --- |
| Solution Provider Contact Information |
| Company name: | *<Insert details here>* |
| Company address: | *<Insert details here>* |
| Company URL: | *<Insert details here>* |
| Contact name: | *<Insert details here>* |
| Contact phone number: | *<Insert details here>* |
| Contact e-mail address: | *<Insert details here>* |

|  |
| --- |
| 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. |

|  |
| --- |
| 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. |
| *<Insert details here>* |

|  |
| --- |
| 2.2 Instructions for confirming POI device and packaging were not tampered with, and for establishing secure, confirmed communications with the solution provider. |
| *<Insert details here>* |
| 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. |
| *<Insert details here>* |

|  |
| --- |
| 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*](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): |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

*<Add additional rows for each PTS POI approval listing with all the POI device types associated with that listing used in this solution, as applicable>*

| 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.  |
| *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)** |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

*<Add additional rows for each application on a POI device used in this solution, as applicable>*

|  |
| --- |
| 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 *<solution provider>* 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.
 |
| *<Solution Provider to include narrative detailing how inventory should be documented & monitored.>* |

**Sample Inventory Table**

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

|  |
| --- |
| 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 |
| *<Insert details here>* |
| ***Note:*** *Only PCI-approved POI devices listed in the PIM are allowed for use in the P2PE solution for account data capture.* |

|  |
| --- |
| 4.2 Guidance for selecting appropriate locations for deployed devices |
| *<Insert details here>* |

|  |
| --- |
| 4.3 Guidance for physically securing deployed devices to prevent unauthorized removal or substitution |
| *<Insert details here>* |

|  |
| --- |
| POI Device Transit |
| 5.1 Instructions for securing POI devices intended for, and during, transit |
| *<Insert details here>* |

|  |
| --- |
| 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 POI devices are shipped to, trusted sites/locations only |
| *<Insert details here>* |

|  |
| --- |
|  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](http://www.pcisecuritystandards.org). |
| *<Insert details here>* |

|  |
| --- |
| 6.2 Instructions for responding to evidence of POI device tampering |
| *<Insert details here>* |

|  |
| --- |
|  Device Encryption Issues |
| 7.1 Instructions for responding to POI device encryption failures |
| *<Insert details here>* |

|  |
| --- |
|  POI Device Troubleshooting |
| 8.1 Instructions for troubleshooting a POI device |
| *<Insert details here>* |

|  |
| --- |
|  Additional Guidance |
| 9.1 Instructions for troubleshooting a POI device |
| *<Instructions, guidance, or any other additional information from the solution provider>* |

|  |
| --- |
| 9.2 Instructions for how to confirm hardware, firmware, and application versions on POI devices |
| *<Instructions, guidance, or any other additional information from the solution provider>* |