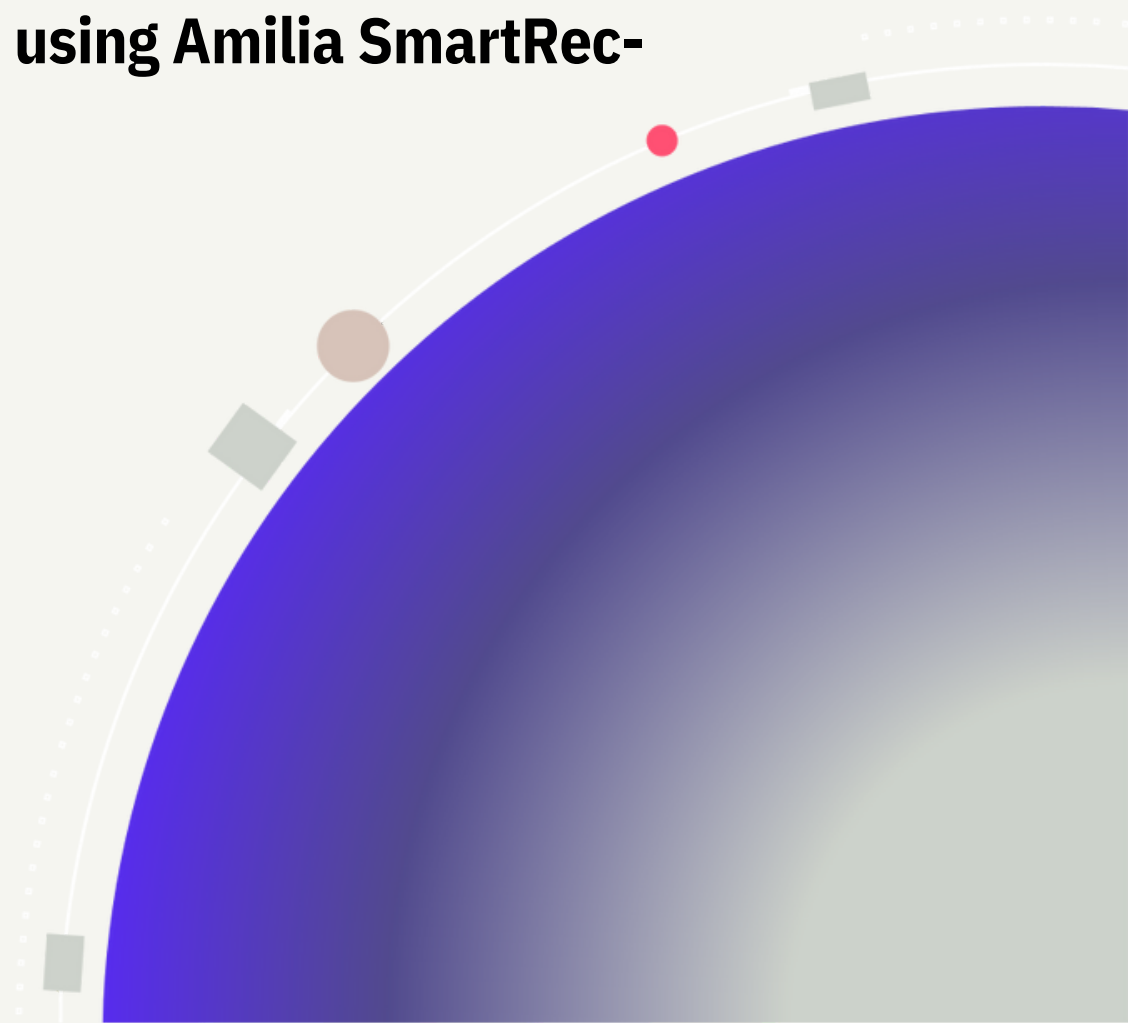


When you only accept card payments using a PAX A920 integrated terminal

-This guide is adapted to merchants using Amilia SmartRec-

SAQ P2PE User Guide
PCI v4.0

January 2024 – PCI v3.2.1



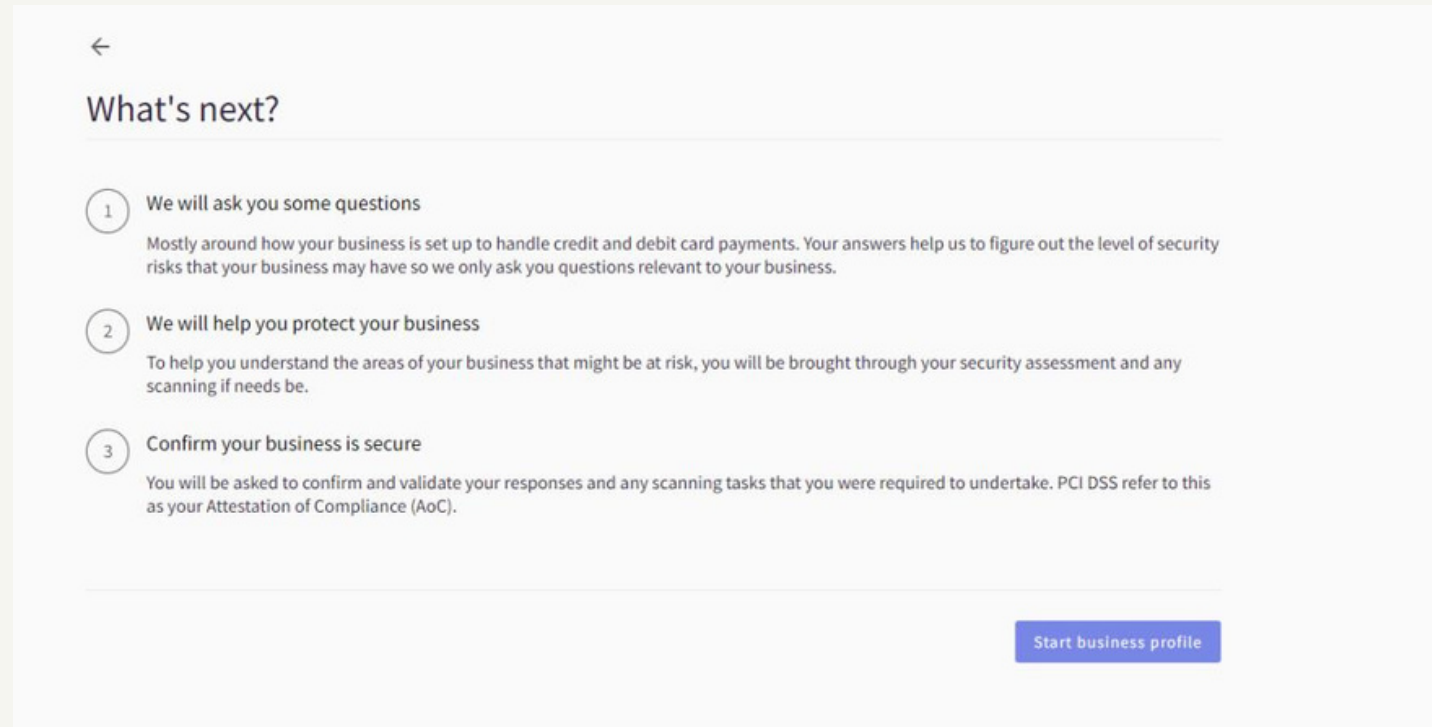
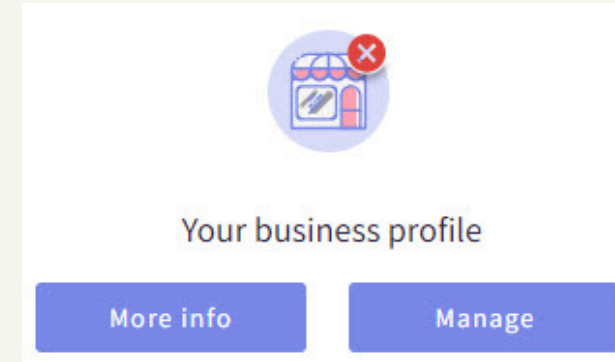
SAQ P2PE User Guide

Once your account has been boarded, you will receive log in details to your PCI Account via email.

- Your username is your Merchant ID number.
- Please use the link within the email to select a password of your own choosing, ensuring to follow the on-screen instructions.
- Upon your first initial log in, you will need to review your contact information to ensure this is accurate.

SAQ P2PE User Guide

- To start, click 'Manage' on your **business profile**.
- The profile paints a picture of your business environment & how you accept card payments.
- Follow this (SAQ type P2PE) guide if your organization accepts card payments with an A920 PAX integrated terminal **only**.



SAQ P2PE User Guide

PLEASE READ: PCI DSS 4.0 update

We have updated our profile process to comply with the requirements of version 4.0 of the Payment Card Industry Data Security Standard (PCI DSS).

If you have Payment terminals in use completed this process previously, please re-confirm your answers. You may be required to answer some additional questions in order to correctly determine your compliance requirements under the latest version of the standard.

Please refer to the PCI Security Standards Council [PCI DSS v4.0 Resource Hub](#) for more information.

We have also made some additional resources available [here](#).

☐ I understand

Next

- The PCI standard has now changed from v3.2.1 to v.4.0. The PCI Portal has been upgraded to ensure you are validating against the latest compliance standards.
- Please read the above messaging and select 'I understand' to proceed.

SAQ P2PE User Guide

Choose an assessment method

☒ **Guide Me** - Select this option to use our profiling tool to help you determine the scope of your PCI DSS compliance requirements.

☐ **Expert** - Select this option if you already know the PCI DSS assessment type applicable to your business, and do not wish to be guided by our profiling tool. This will require you to provide responses to all of the requirements on the assessment questionnaire.

☐ **Upload** - Select this option to upload your existing currently valid PCI DSS Self-Assessment Questionnaire (SAQ) or Attestation of Compliance (AoC) from an external source.

[Previous](#) [Next](#)

- Select '**Guide me**' to complete your compliance using the PCI Portal. (Recommended)
- Select 'Expert' if you don't wish to use the profiling tool to pre-populate some of your PCI requirements. (Not Recommended)
- Select 'Upload' if you've already completed your compliance for the forthcoming year and wish to upload the required documentation.

SAQ P2PE User Guide

How do you accept payment cards? ?

Please select all of the ways you take payment cards in your business today. Please note this only refers to branded cards (e.g. Visa and MasterCard) not alternative payment types (e.g. PayPal and Google Wallet are not applicable)



Face to face



e-Commerce store



Mail or telephone order

Previous

Next

- As you only use the PAX A920 integrated terminal for card present transactions - **please select that you are accepting card payments ‘Face to face’.**
- Don't select any other option.

SAQ P2PE User Guide

As you only use the PAX A920 integrated terminal to accept card payments in the Amilia SmartRec store -

- **Please select the 4th option 'I use an integrated Point of Sale (iPOS/ePOS) system that includes an integrated card reader device'.**

Note: In the past, merchants selected the first option (standalone or portable POS terminal). However, this option leads to an SAQ B-IP with a scan (to be avoided). **Do not select the first option. You must select the 4th option.**

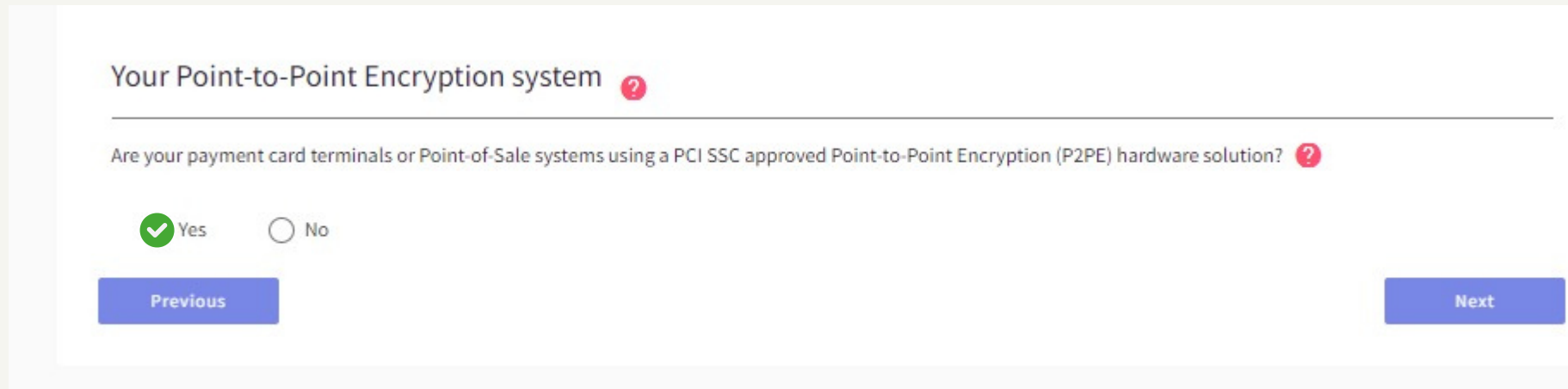
How you accept card payments ?

Please select all of the methods that you use to accept card payments in your business.

- ☐  I use a standalone counter-top or portable Point of Sale (POS) payment terminal
- ☐  I use a browser-based Virtual Terminal (or other browser-based payment page hosted by a PCI DSS compliant service provider) to manually process card payments
- ☐  I use a mobile (smartphone, tablet etc) device to accept face to face payments
- ☒  I use an integrated/electronic Point of Sale (iPOS/ePOS) system (a POS computer system running a payment application that includes an attached or integrated card reader device)
- ☐  I use a payment application that allows my company's employees to manually input card data transactions for processing using a computer (This is not a Virtual Terminal)
- ☐  I use a manual imprint machine and/or paper sales vouchers

[Previous](#) [Next](#)

SAQ P2PE User Guide



Your Point-to-Point Encryption system ?

Are your payment card terminals or Point-of-Sale systems using a PCI SSC approved Point-to-Point Encryption (P2PE) hardware solution? ?

☒ Yes ☐ No

[Previous](#) [Next](#)

- The PAX A920 integrated terminal is a Point-to-Point encrypted terminal.
Please answer ‘Yes’ to this question.

SAQ P2PE User Guide

Your Point-to-Point Encryption system 

Can you confirm that ALL of your payment terminals and/or POS systems use a PCI SSC validated Point2Point Encryption solution?

☒ Yes ☐ No

[Previous](#previous) [Next](#next)

- As you only use the PAX A920 integrated terminal, **please answer ‘Yes’ to this question.**

SAQ P2PE User Guide

Your Point-to-Point Encryption implementation 

Can you confirm that all controls specified in the P2PE Instruction Manual (PIM) have been implemented? 

☒ Yes ☐ No

[Previous](#previous) [Next](#next)

- Please answer ‘Yes’ to this question.

SAQ P2PE User Guide

Your Point-to-Point Encryption system

Please select your P2PE solution from the list

PAX

Planet Payment Group Holdings Limited - Planet PAX Solution ×

☒ Planet Payment Group Holdings Limited - Planet PAX Solution

Previous

Next

- To input your P2PE solution, please type 'PAX' in the search bar and then scroll down.
- **Please select 'Planet Payment Group Holdings Limited - Planet PAX Solution'.**

SAQ P2PE User Guide

Your Planet PAX Point-to-Point Encryption (P2PE) PTS device 

Please select your PCI PIN Transaction Security (PTS) device utilized within the PCI validated P2PE Solution.

Filter

☐ PAX Computer Technology (Shenzhen) Co Ltd, A920  **OR** 

☐ PAX Computer Technology (Shenzhen) Co Ltd, A920Pro

☐ PAX Computer Technology (Shenzhen) Co Ltd, A77

☐ PAX Computer Technology (Shenzhen) Co Ltd, A80

☐ PAX Computer Technology (Shenzhen) Co Ltd, A30

☐ PAX Computer Technology (Shenzhen) Co Ltd, IM30

[Previous](#) [Next](#)

- Please select the **A920 or A920 Pro** (depending on which one you have). They're the only integrated terminals currently supported in Amilia SmartRec.

SAQ P2PE User Guide

Printed paper receipts and reports 

Do you print, receive or have access to paper receipts or reports that contain the full payment card number?

☐ Yes ☒ No

[Previous](#) [Next](#)

- If you don't have access to paper receipts or reports that contain the full card details of your customers, **please answer 'No' to this question.**

SAQ P2PE User Guide

- You must never send, receive, transmit or store cardholder data electronically under any circumstances.

This puts your organization and your customers' data at risk of being hacked by malicious individuals who will show you no mercy.

Other uses of card numbers ?

Does anyone in your organization send or receive full card numbers via email or instant messaging?

☐ Yes ☒ No

Does your company otherwise store, transmit or receive cardholder data electronically in any other way and for any other purpose? This could be via CD-ROM, USB drive or an internet network. ?

☐ Yes ☒ No

[Previous](#) [Next](#)

- Please answer 'No' to both questions.**

SAQ P2PE User Guide

- In order to become and maintain compliance, you must have an Information Security Policy in place within your business.

You can download this document via the hyperlink as shown.

- You must read, sign and date this document, as well any other employee who handles card payments.

- This document must be always kept on the business premises and reviewed annually.

Your company policy for information security

To handle payment cards you are required by the Payment Card Industry Data Security Standard (PCI DSS) to have an Information Security Policy in place for your organization. This must cover all relevant areas of the standard. If you do not currently have one, we can provide you with a policy template below. 

☒ I do not have an Information Security Policy in place at the moment, I will implement a security policy using the template provided. [Download](#) 

☐ I already have an Information Security Policy in place that covers ALL of the relevant clauses of the Payment Card Industry Data Security Standard (PCI DSS)

☐ I do not currently have an Information Security Policy in place that covers ALL of the relevant clauses of the Payment Card Industry Data Security Standard (PCI DSS) but I do not wish to use the one provided as the basis for my policy.

[Previous](#) [Next](#)

SAQ P2PE User Guide

Password policy

Do you enforce a minimum password length of seven characters, containing both numeric and alphabetic characters, for user accounts on all POS devices, computers and systems in your business? 

☐ Yes ☐ No

Please note: After 31st March 2025, you will need to enforce a minimum password length of twelve characters (where twelve characters are supported, otherwise a minimum of eight characters is required). This also applies to passwords used by all non-customer users and administrators with access to e-commerce websites/webservers.

[Previous](#) [Next](#)

- From March 31st 2025, you will be required to update the password requirements within your business to ensure that it is protected from malicious individuals.
- Anyone who has administrator access to your website will be required to have a password length of twelve characters, rather than eight.
- As this is a future dated requirement, this question will not affect the overall status of your compliance.
- **Please answer this question as it applies to your business today.**

SAQ P2PE User Guide

Third Party Managed System Service Providers

Do you have relationships with one or more third-party service providers that manage system components included in the scope of this assessment, for example, via network security control services, anti-malware services, security incident and event management (SIEM), contact and call centers, web-hosting services, and IaaS, PaaS, SaaS, and FaaS cloud provider?

☐ Yes ☒ No

Previous

Next

- As Paysafe is your only service provider for the PAX A920 integrated terminal, **please answer ‘No’ to this question.**

SAQ P2PE User Guide

Other Third Party Service Providers that may impact cardholder data security

Do you have relationships with one or more third-party service providers that could impact the security of your company's cardholder data environment (CDE)? For example, vendors providing support via remote access, and/or bespoke software developers.

☐ Yes ☒ No

Previous

Next

- Please answer 'No' to this question.

SAQ P2PE User Guide

This is the last question in the business profile.

As your organization only handles card payments with a PAX A920 integrated terminal, please provide the following details:

- Describe the location(s) where card payments are accepted
- Card payments are handled with a handheld integrated terminal
- The security of your system is maintained via relevant security patches
- The # of employees that handle card payments
- The # of employees with access to the back office

A summary of how and where you handle card payments

Please provide the information requested below. This will form part of your Attestation of Compliance

List your business premises type(s) and a summary of locations that are relevant to your PCI DSS assessment (eg, retail outlets, corporate offices, data centres, call centres etc..)

X locations accepting card payments in X locations
There are X number of employees that process payments.
Online store to process payments online or via an invoice.

3/4000

How and in what capacity does your business store, process and/or transmit cardholder data?

Card payments are accepted Face to Face using the integrated A920 PAX terminal.
E-commerce store hosted by Amilia SmartRec
- payments are processed using an iFrame.

3/4000

Provide a high level description of your overall business environment, applicable to your PCI DSS assessment. For example describe the type of equipment you use for card processing, storage and transmission; such as POS devices any databases and web servers, include a description as to how they connect both externally and any internal connections.

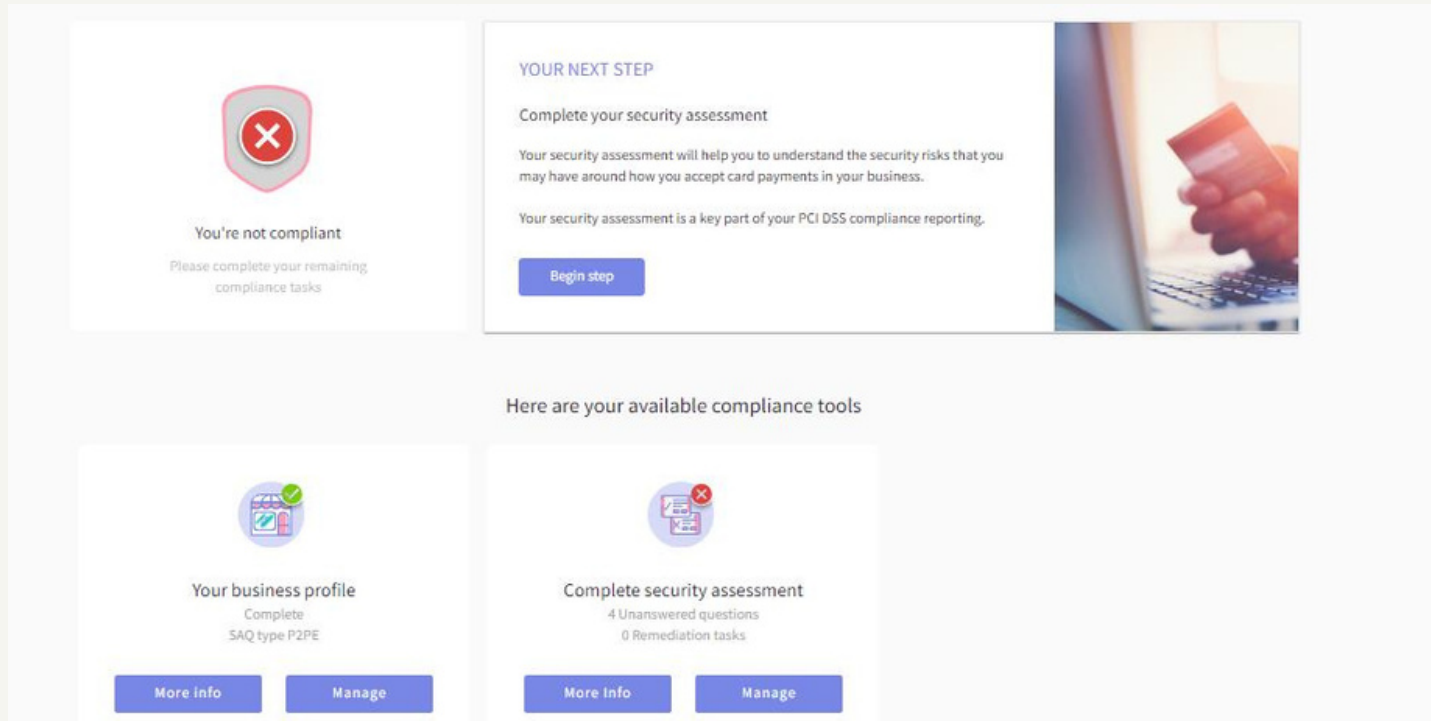
The integrated A920 PAX terminal connects via (INSERT METHOD)

3/4000

Previous

Next

SAQ P2PE User Guide



- Once all steps have been completed in the business profile, you will see there are just a handful of questions outstanding in the security assessment.
- Click '**Manage**' to begin the security assessment.

SAQ P2PE User Guide

- After clicking **‘Manage’** and then **‘Answer now’**, you will see this screen.
- In the **‘Sections’** area, you will have questions relating to **‘Protecting Account Data’**, and **‘Implementing Strong Access Control Measures’**.

The screenshot displays the SAQ P2PE User Guide interface. At the top, there is a 'Show me:' dropdown menu set to 'Only unanswered questions' and a 'Show Help Text:' toggle with 'Yes' selected. The main content area is titled 'Protect Account Data' and contains 'Requirement 3: Protect Stored Account Data'. Below this, there are two text boxes: 'Processes and mechanisms for protecting stored account data are defined and understood' and 'Storage of account data is kept to a minimum.' A 'Question group 3.2.1' section is also visible, containing a 'Help answering this requirement' box with the text 'Expected Testing' and a bulleted list of tasks: 'Examine the data retention and disposal policies, procedures, and processes.', 'Interview personnel.', and 'Examine files and system records on system components where account data is'. On the right side, there is a 'Sections' panel with a list of sections: '2 Protect Account Data' (highlighted), '2 Implement Strong Access Control Measures', '✓ Maintain an Information Security Policy', and '✗ Confirm your compliance'.

SAQ P2PE User Guide

- This question is asking you to confirm if you have a data retention policy in place that covers all locations of your businesses that may store sensitive information.

- **Please answer 'N/A' to this question and write 'My organization only uses the PAX A920 integrated terminal to handle card payments' as the reason.**

3.2.1

Account data storage is kept to a minimum through implementation of data retention and disposal policies, procedures, and processes that include at least the following:

- Coverage for all locations of stored account data.
- Coverage for any sensitive authentication data (SAD) stored prior to completion of authorization. This bullet is a best practice until its effective date; refer to Applicability Notes below for details.
- Limiting data storage amount and retention time to that which is required for legal or regulatory, and/or business requirements.
- Specific retention requirements for stored account data that defines length of retention period and includes a documented business justification.
- Processes for secure deletion or rendering account data unrecoverable when no longer needed per the retention policy.
- A process for verifying, at least once every three months, that stored account data exceeding the defined retention period has been securely deleted or rendered unrecoverable.

I have implemented a compensating control

N/A

No

Yes

SAQ P2PE User Guide

- This question is asking you to confirm that you do not store the CVV/CVV2 code once the transaction has been processed.
- Please answer 'N/A' to this question and write 'The PAX A920 integrated terminal does not store cardholder data' as the answer.

3.3.1.2

The card verification code is not retained upon completion of the authorization process.

I have implemented a compensating control

i Information

Note

For SAQ P2PE, Requirement 3 applies only to merchants with paper records that include account data (for example, receipts or printed reports).

Purpose

If card verification code data is stolen, malicious individuals can execute fraudulent Internet and mail-order/telephone-order (MO/TO) transactions. Not storing this data reduces the probability of it being compromised.

Examples

SAQ P2PE User Guide

- Please answer 'N/A' to this question and write 'The PAX A920 integrated terminal does not store cardholder data' as the answer.

9.4.1.1

Offline media backups with cardholder data are stored in a secure location.

I have implemented a compensating control

N/A

No

Yes

i

Information

Note

For SAQ A, Requirements at 9.4 only apply to merchants with paper records (for example, receipts or printed reports) with account data, including primary account numbers (PANs).

Purpose

If stored in a non-secured facility, backups containing cardholder data may easily be lost, stolen, or copied for malicious intent.

Good Practice

For secure storage of backup media, a good practice is to store media in an off-site facility, such as an alternate or backup site or commercial storage facility

SAQ P2PE User Guide

9.5.1.3

Training is provided for personnel in POI environments to be aware of attempted tampering or replacement of POI devices, and includes:

- Verifying the identity of any third-party persons claiming to be repair or maintenance personnel, before granting them access to modify or troubleshoot devices.
- Procedures to ensure devices are not installed, replaced, or returned without verification.
- Being aware of suspicious behavior around devices.
- Reporting suspicious behavior and indications of device tampering or substitution to appropriate personnel.

I have implemented a compensating control

 Information
Note

- **Please answer this question with ‘Yes’** and ensure now and moving forward that staff regularly check the card terminal to confirm it hasn’t been swapped out with another device and that none of its components haven’t been tampered with.
- If you don’t answer ‘Yes’ to this question, you will fail the security assessment.

SAQ P2PE User Guide

SAQ P2PE User Guide interface showing the 'Build and Maintain a Secure Network and Systems' section.

At the top, there is a 'Show me:' dropdown menu set to 'Only unanswered questions' and a 'Show Help Text:' toggle set to 'Yes'.

The main content area displays the section title 'Build and Maintain a Secure Network and Systems' and a message: 'There are no unanswered questions in this section. Attention! You may still have questions answered "No", which means that your security assessment will not be complete until you address compliance remediation tasks associated with those questions you have answered "No"'. A 'Next' button is visible at the bottom right of the main content area.

On the right side, there is a 'Sections' sidebar. The sections listed are:

- Build and Maintain a Secure Network and Systems (checked)
- Protect Cardholder Data (checked)
- Maintain a Vulnerability Management Program (checked)
- Implement Strong Access Control Measures (checked)
- Regularly Monitor and Test Networks (checked)
- Maintain an Information Security Policy (checked)
- Confirm your compliance (highlighted with a red box)

- Once all questions are answered within this section – you can then confirm your compliance and complete one final item before becoming validated for the forthcoming year.
- Please select the '**confirm your compliance**' section as highlighted in the red box

SAQ P2PE User Guide

Confirm your compliance
Please review the form below and ensure all sections are correct and complete

✓ Your organization information details ^

Company name JDTest	Contact name * Jess Donohoe
Title	Telephone numbers 1234567890
Email address	Business address 1 test Street
Country Ireland	

- You will need to review the contact information as this will be added to the e-signature of your attestation of compliance documentation.
- Please ensure to fill in all details.

SAQ P2PE User Guide

- Once you have updated the contact information, please scroll down and click the button as shown.

The screenshot displays a web interface for the SAQ P2PE User Guide. It features a vertical list of five expandable sections, each with a checkmark icon and a dropdown arrow. The sections are: 'Type of business', 'Description of environment', 'Eligibility to complete SAQ B_IP', 'Acknowledgement of status and attestation', and 'Merchant Executive Officer'. Below these is an 'Attestation' section, which is currently expanded. It contains a green box with a checkmark icon and the heading 'Information for Submission.' The text inside the green box states: 'Based on the results noted in the SAQ B-IP dated Oct 6, 2023, the signatories identified in Parts 1.1, assert(s) the following compliance status for the entity identified in Part 2 of this document as of Oct 6, 2023: Compliant: All sections of the PCI DSS SAQ are complete, all questions answered affirmatively. You are required to maintain compliance with PCI DSS at all times.' At the bottom right of the 'Attestation' section, there is a blue button labeled 'Confirm your Attestation', which is highlighted by a red rectangular box. A 'Previous' button is visible at the bottom left of the interface.

SAQ P2PE User Guide

Once all stages are completed – you will then be redirected to this screen to advise that you are now compliant for the forthcoming year.

If there is anything outstanding throughout the year, the PCI portal will email you to advise that action is required.

