

Security Metrics

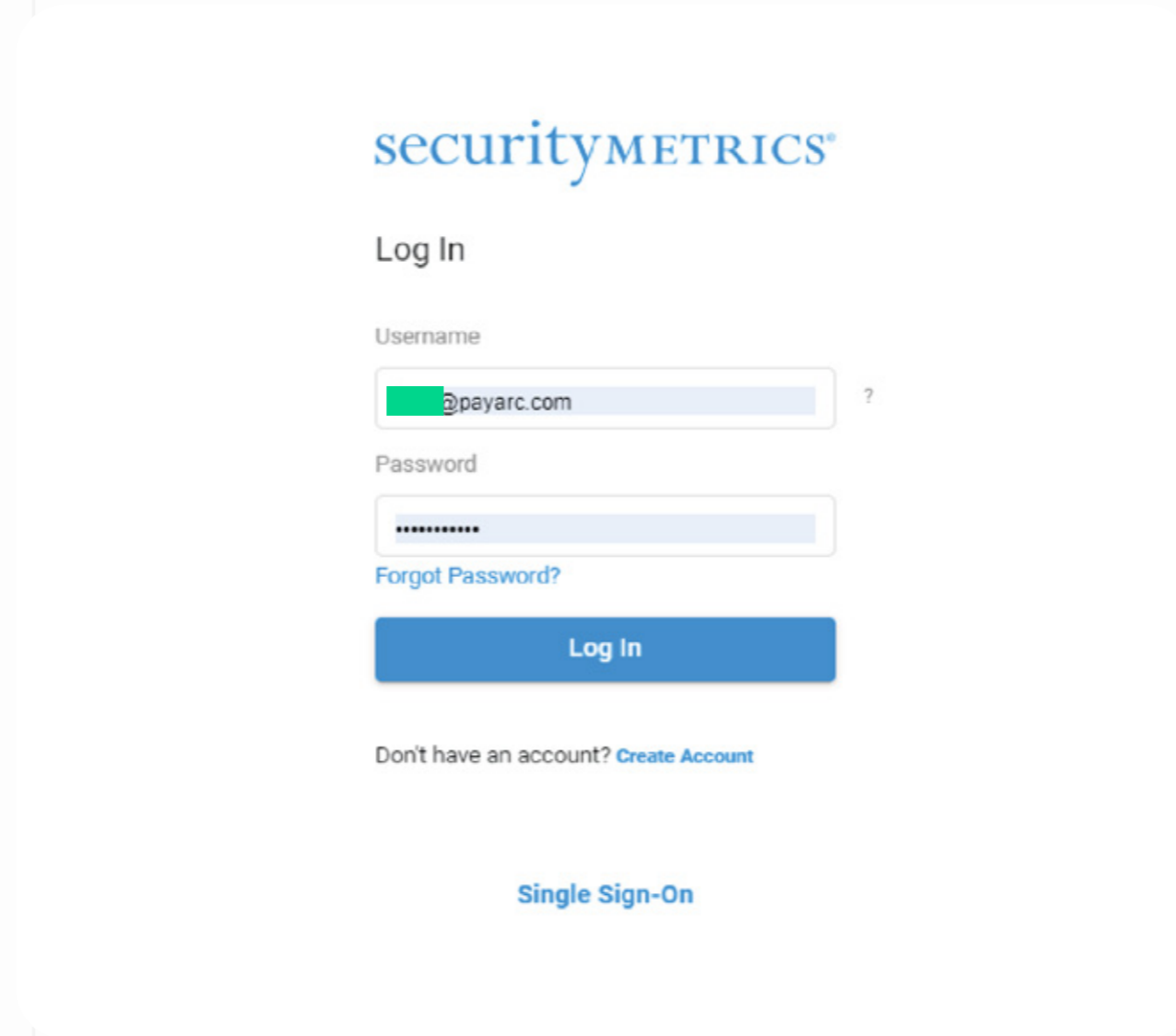
Instructions _____
to become compliant.



CP Retail/Rest Accounts: Merchants processing directly through a P2PE terminal such as a Dejavoo, Pax, Verifone, Ingenico, AMP etc.

Login

- Login Link: <https://www.securitymetrics.com/portal/app/ngsm/login>



The screenshot shows the SecurityMetrics login interface. At the top is the SecurityMetrics logo. Below it is the heading "Log In". There are two input fields: "Username" with the value "@payarc.com" and a question mark icon, and "Password" with masked characters. A "Forgot Password?" link is positioned below the password field. A blue "Log In" button is centered below the fields. At the bottom, there is a link "Don't have an account? Create Account" and a "Single Sign-On" link.

securityMETRICS®

Log In

Username

@payarc.com ?

Password

.....

[Forgot Password?](#)

Log In

Don't have an account? [Create Account](#)

[Single Sign-On](#)

User Agreement

- Click “Accept”

SECURITYMETRICS TERMS OF USE AGREEMENT

The following terms and conditions (collectively “Terms of Use Agreement”), are entered into by and between You, the customer (“Customer” or “you”), and SecurityMetrics, Inc., a Utah corporation (“SecurityMetrics”). The Terms of Use Agreement relates to SecurityMetrics’ compliance and data security programs and services, which may include but are not limited to Payment Card Industry Data Security Standard (“PCI DSS”), Health Insurance Portability and Accountability Act (“HIPAA”), Managed Firewall, and other data security and compliance services (collectively “Services”). The Terms of Use Agreement also apply to all content functionality, and services offered or purchased on or through www.securitymetrics.com (the “Website”). By use of any Services or the Website, you accept and agree to all conditions imposed in this Terms of Use Agreement. Note: THIS TERMS OF USE AGREEMENT CONTAINS ARBITRATION, WARRANTIES, AND LIMITATION OF LIABILITY CLAUSES THAT AFFECTS YOUR RIGHTS UNDER THIS TERMS OF USE AGREEMENT WITH RESPECT TO ALL SERVICES.

Services

You may select some or all of the following Services:

PCI Compliance

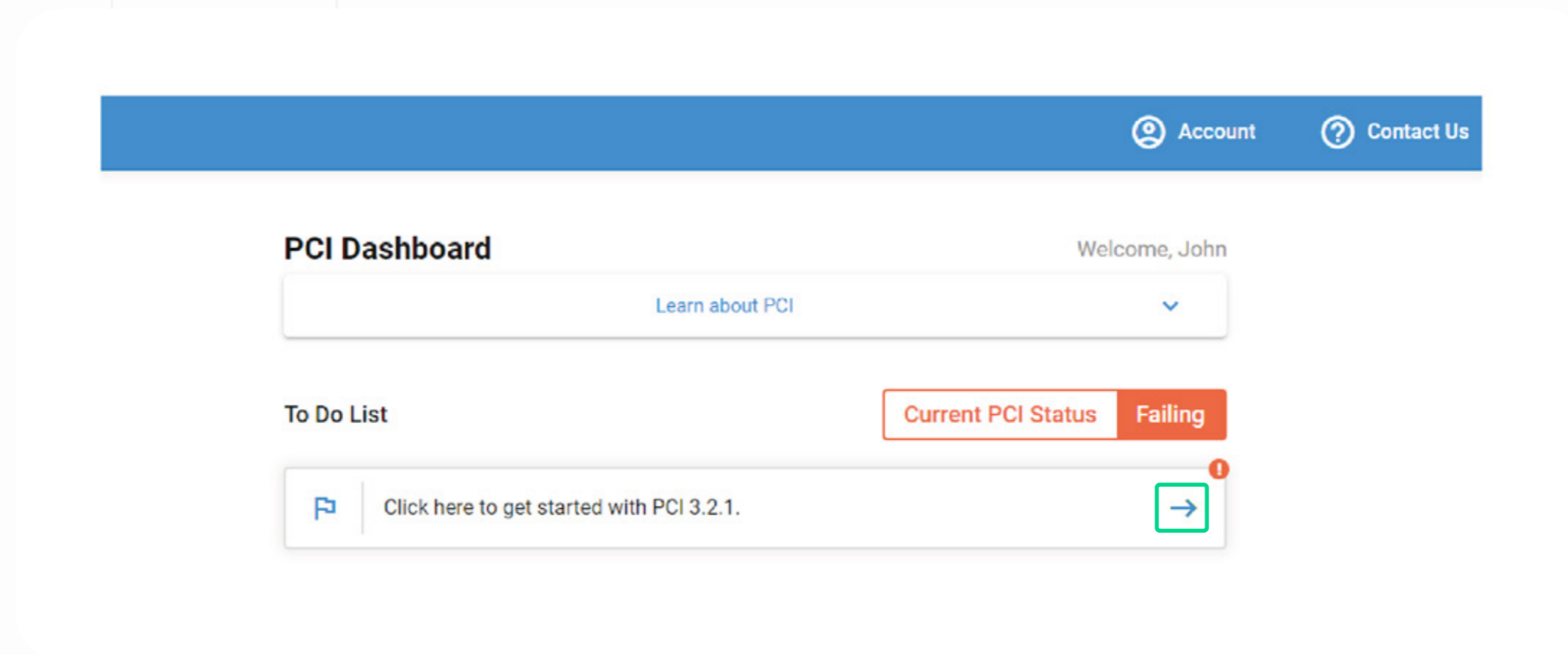
If you have selected service packages that contain PCI Compliance Services, then that package may include, but is not limited to, all or some of the Services listed below.

- Help you determine the scope of the applicable PCI Compliance requirements. You alone are responsible for determining the scope of your PCI Compliance requirements. SecurityMetrics will not be liable for any mistake or error in determining the scope;
- Provide you with a copy of the self-assessment questionnaire determined by the scope determined above and help understanding the questions, if needed;
- Provide vulnerability scanning on IP addresses or domains specified and provided by the Customer; all vulnerability scanning is done in accordance with Warranties and Limitation of Liabilities Sections of this Terms of Use;
- Provide Customer with access to scan results and copies of the self-assessment questionnaire
- Report the status of the self-assessment questionnaire and vulnerability scans via SecurityMetrics website;
- Service Warranty (described below);
- One or more, depending on the invoice, non-exclusive, non-transferable license(s) of PANscan® during the term of this Terms of Use. PANscan® is SecurityMetrics’ software that finds unencrypted credit card numbers on computer systems;
- One or more, depending on the invoice, non-exclusive, non-transferable license(s) of PIIscan® during the term of this Terms of Use. PIIscan® is SecurityMetrics’ software that finds unencrypted personally identifiable information on computer systems;
- SecurityMetrics Mobile, a software application that scans mobile devices for vulnerabilities;
- Seats to PCI Compliance trainings; and
- Technical support.

Accept

Security Metrics Dashboard

- Click on the “arrow” to get started



Partner Confirmation

- Click “Next”

Identify Your Account

You have already been matched to the following bank:

PayArc

Please click Next to continue.

What is this for? ▼

Next

Confirm Account Information

- If anything changed, merchant should update and click “Next”

Customer Information

Company Name *		Company Phone *	
Test CNP account		8772036624	
Address *		City *	
103 Mason Street		Greenwich	
State *	Zip *	Country *	
CT	06830	United States ▼	
		Language Preference *	
		English ▼	





Back

Next

Select Your Processing Method

- Terminal – Dejavoo, Pax, VeriFone, Etc.
- Check off “Terminal”
- “My terminal features validated P2PE”
- Click “Next”

Processing
Please select your methods of processing cardholder data. Check all that apply.

	<input checked="" type="checkbox"/> Terminal	I process cardholder data using stand-alone terminals or phones.
	<input type="checkbox"/>	My terminal(s) use an Internet connection.
	<input type="checkbox"/>	My terminal is connected to an analog phone line.
	<input type="checkbox"/>	My terminal is wireless and connects to a cell tower.
	<input type="checkbox"/>	I use an imprint machine (knuckle buster) or manually enter credit card data.
	<input type="checkbox"/>	I use my acquirer's touch-tone system to process cards.
	<input checked="" type="checkbox"/>	My terminal features validated P2PE(point-to-point encrypted) hardware
	<input type="checkbox"/> Computer	I process cardholder data using a computer.
	<input type="checkbox"/> eCommerce	I have an eCommerce website.
	<input type="checkbox"/> Mobile Device	I process cardholder data using a smartphone or tablet.

ⓘ If you are a service provider, NOT a merchant, please [click here](#).

[Back](#) [Next](#)

Electronic Storage

- Click “No” – Merchants are not allowed to store CC information, unless using P2PE
- Click “Next”

Electronic Storage [Change previous answers](#)

Do you store cardholder data electronically?
Examples:
Digitally recorded phone calls,
Accepting cardholder data through email or eFax,
Cardholder data stored on a computer,
Your system does not process immediately, but batches out only periodically.

Yes No

Designated SAQ – P2PE 3.2.1

- Click “Activate and Continue”

Congratulations! Based on information you've provided, you have been assigned **SAQ**

How can I be sure this is the correct questionnaire?

To ensure you take the correct questionnaire, we need to verify that the following is true:

- You use a PCI compliant third party provider for all of your cardholder transmission and processing
- Any cardholder data that you keep is in paper form (like receipts or copies of receipts)
- You do not store cardholder data electronically

If this doesn't describe your business, click [here](#) or call 801-705-5665 (US) or 0203.014.7820 (UK) 24 hours a day.

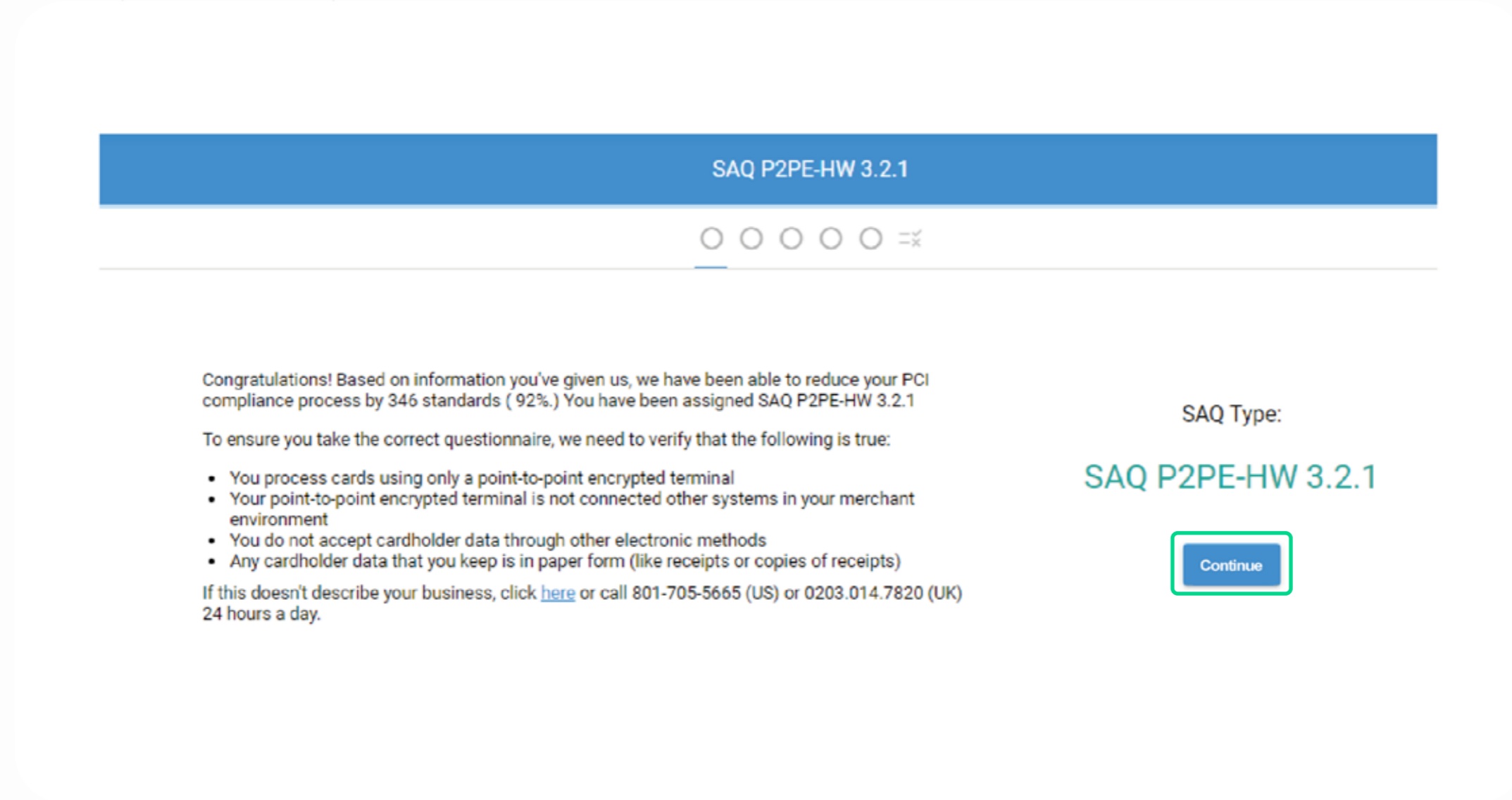
[Back](#)

Questionnaire Type:
SAQ

[Activate and Continue →](#)

Start Questionnaire

- Click “Continue”



Policy


- Answer Yes or N/A
- If the answer is N/A, you must provide an explanation.
- “This section does not apply to my business” is a valid explanation.
- After answering all the questions, scroll down, and click “Next”

Policy

Do you have a written policy which is kept up to date and disseminated to all relevant employees?

[Official PCI Text >](#)

12.1 YES NO N/A

 **Simplify policies requirements** ×

Many merchants struggle to create all the policies required for PCI compliance, but policies are the foundation to your data security plan. SecurityMetrics offers templates designed to simplify compliance with these requirements.

[Learn More and Buy](#)

Your policy should be reviewed at least once a year or whenever changes in business environment require, such as hiring new employees, changes in your business or risk environment or using new technologies. Is your policy reviewed appropriately?

[Official PCI Text >](#)

12.1.1 YES NO N/A

Physical Access

- Answer Yes or N/A
- If the answer is N/A, you must provide an explanation.
“This section does not apply to my business” is a valid explanation.
- After answering all the questions, scroll down, and click “Next”

Physical Access

Are all media physically secured (including but not limited to computers, removable electronic media, paper receipts, paper reports, and faxes)?
For purposes of Requirement 9, "media" refers to all paper and electronic media containing cardholder data.

9.5 YES NO N/A

All media should be destroyed when it is no longer needed for business or legal reasons. Acceptable methods to destroy paper media include cross-cut shredding, burning and/or pulping. Do you properly dispose of media to make sure that the data cannot be reconstructed?

[Official PCI Text >](#)

9.8.a-9.8.1.a YES NO N/A

Stored Data

- Answer Yes or N/A
- If the answer is N/A, you must provide an explanation.
“This section does not apply to my business” is a valid explanation.
- After answering all the questions, scroll down, and click “Next”

Stored Data

Are data-retention and disposal policies, procedures, and processes implemented as follows:

Is data storage amount and retention time limited to that required for legal, regulatory, and business requirements?

3.1.a

YES

NO

N/A

Are there defined processes in place for securely deleting cardholder data when no longer needed for legal, regulatory, or business reasons?

3.1.b

YES

NO

N/A

Choosing Your P2PE Terminal

- Under POS terminal, search for your device and select it. Ex: Pax A920
- If no results were found after entering the name, then click “Add”
- Click “Next”

How do you accept cards?

SAQ P2PE-HW 3.2.1

The following are different possible methods of processing cardholder data. Please select only the methods that you use.

Merchants are responsible to ensure the PCI compliance of any third party providers that capture, store or transmit cardholder data on their behalf. We recommend you obtain PCI compliance documentation from your provider. The scope of this SAQ does not include validation of your providers' compliance.

WARNING:
Using a non-compliant provider could result in significant financial penalties to your business in the event of a data compromise.

Please enter the details of your card processing methods. At least one third party provider must be filled out to proceed.

Points-of-Sale Terminal ⓘ

PAX Computer Technology (Shenzhen) Co Ltd A920 ✕

[BACK](#) [Restart SAQ](#) [NEXT](#)

Confirm Your Assessment

- Click “I Agree”

SAQ P2PE-HW 3.2.1

✓ ✓ ✓ ✓ ✓ ⚙

Confirm below to complete your Assessment.

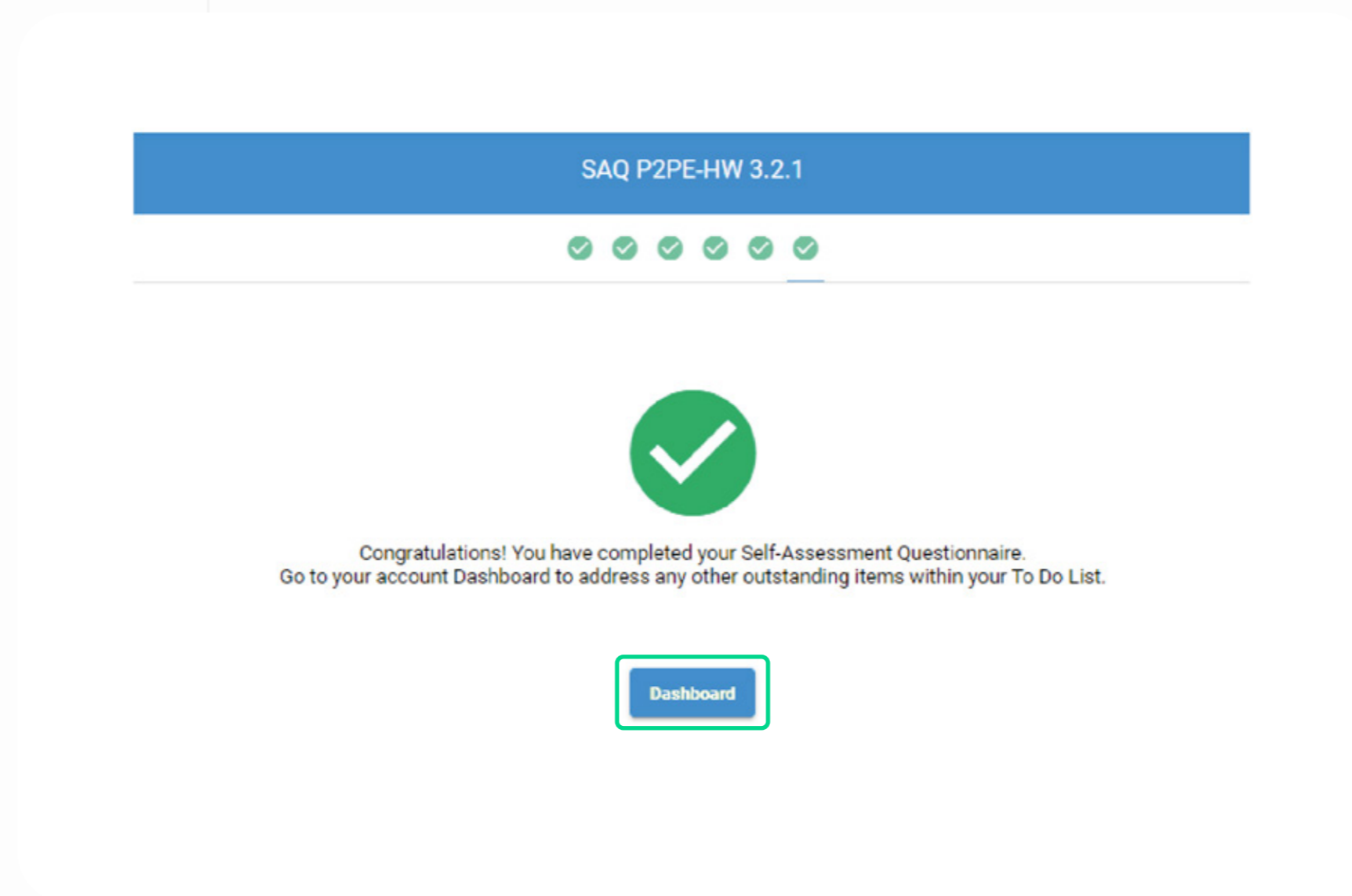
I verify that the following is true:

- PCI Self-Assessment Questionnaire P2PE-HW version 3.2.1, was completed according to the instructions therein.
- All information within the above-referenced SAQ and in this attestation fairly represents the results of my assessment in all material respects.
- I have confirmed with my payment application vendor that my payment system does not store sensitive authentication data after authorization.
- I have read the PCI DSS and I recognize that I must maintain PCI DSS compliance, as applicable to my environment, at all times.
- If my environment changes, I recognize I must reassess my environment and implement any additional PCI DSS requirements that apply.

I Agree

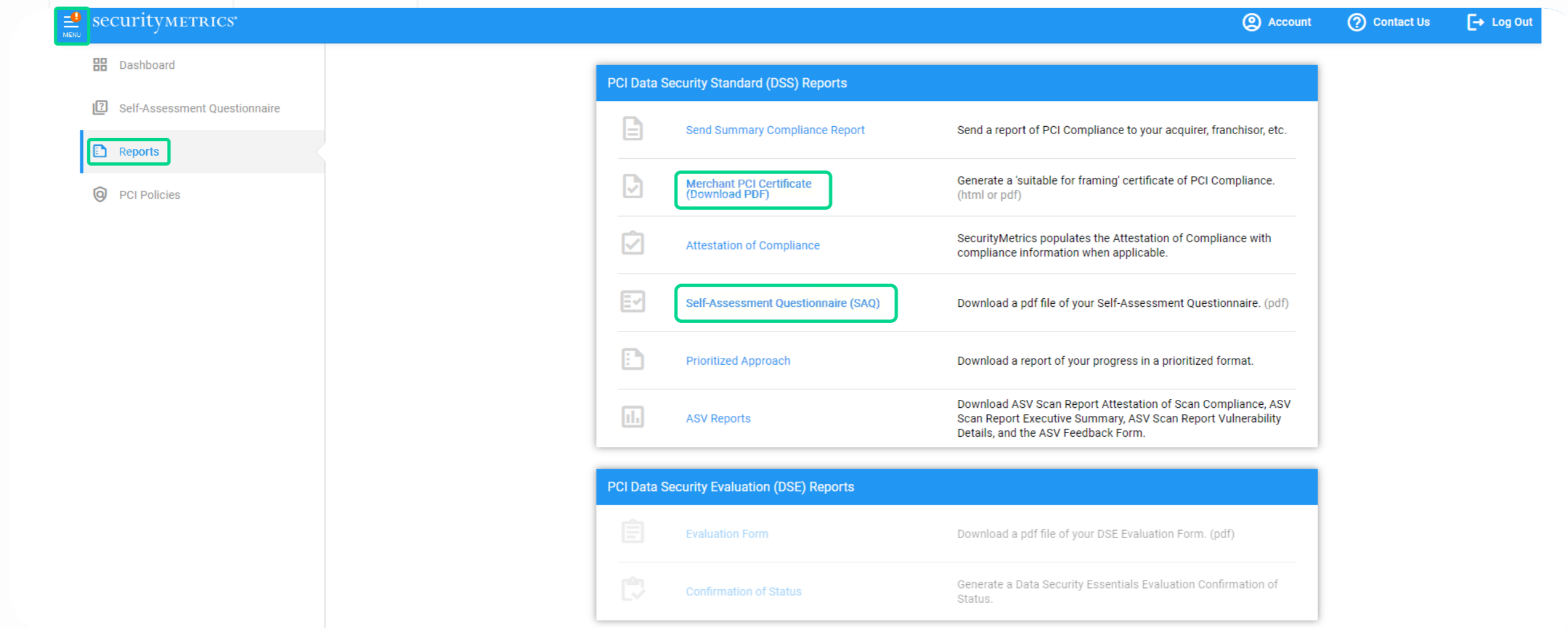
PCI-SAQ Compliance Confirmation

- To go back to the home screen, click “Dashboard”











How to retrieve your PCI Certificate & SAQ?

- From the home screen, Click “Menu” > “Reports”



The screenshot displays the SecurityMetrics dashboard interface. The top navigation bar is blue and contains the SecurityMetrics logo on the left, and links for Account, Contact Us, and Log Out on the right. A left-hand sidebar menu is visible, with the 'Reports' option highlighted in a light grey box. The main content area is divided into two sections: 'PCI Data Security Standard (DSS) Reports' and 'PCI Data Security Evaluation (DSE) Reports'. Each section contains a list of report types with icons, titles, and brief descriptions. In the DSS section, 'Merchant PCI Certificate (Download PDF)' and 'Self-Assessment Questionnaire (SAQ)' are highlighted with green boxes. In the DSE section, 'Evaluation Form' and 'Confirmation of Status' are listed.

PCI Data Security Standard (DSS) Reports		
	Send Summary Compliance Report	Send a report of PCI Compliance to your acquirer, franchisor, etc.
	Merchant PCI Certificate (Download PDF)	Generate a 'suitable for framing' certificate of PCI Compliance. (html or pdf)
	Attestation of Compliance	SecurityMetrics populates the Attestation of Compliance with compliance information when applicable.
	Self-Assessment Questionnaire (SAQ)	Download a pdf file of your Self-Assessment Questionnaire. (pdf)
	Prioritized Approach	Download a report of your progress in a prioritized format.
	ASV Reports	Download ASV Scan Report Attestation of Scan Compliance, ASV Scan Report Executive Summary, ASV Scan Report Vulnerability Details, and the ASV Feedback Form.

PCI Data Security Evaluation (DSE) Reports		
	Evaluation Form	Download a pdf file of your DSE Evaluation Form. (pdf)
	Confirmation of Status	Generate a Data Security Essentials Evaluation Confirmation of Status.

Thank You For Becoming PCI-DSS Compliant!

* SAQ Valid for 1 Year