PCI Compliance Process Help Guide

MyTime Merchant Processing
PCI Compliance Process Help Guide

The purpose of this guide is to help you navigate and qualify through the appropriate **SAQ (Self Assessment Questionnaire)** for PCI-DSS (Payment Card Industry Data Security Standard) compliance. The SAQ includes questions you will need to answer in order to stay PCI compliant, allowing you to accept credit card payments at your business and avoiding expensive non-compliance fees.

GETTING STARTED

We highly recommend looking over this guide first to understand the types of questions you will be asked and how to prepare your business for PCI compliance so that you can positively answer this SAQ.

You will receive an email from TSYS, your merchant processor, and prompted to fill out the SAQ by going to the website mentioned in the email: www.compliance101.com

Enter your username, which will be the 16-digit Merchant ID number in the email you receive from TSYS; then use **compliance101** as the first-time password. You can then create your own password if you wish.

Once you have entered your username and password, you will see the "Compliance Overview" webpage. The graphic will display a red light indicating you are not yet compliant (simply because you haven't yet completed the questionnaire).

Click the **"Complete Questionnaire"** button within the graphic to get started with the questions.

TIP: The question mark icon  appears on every page of the SAQ. Click on it for detailed information about that page's topic and question(s). This is an additional useful tool to help answer the questions.

INTRODUCTION

This section welcomes you to the process and explains the flow. If you've already attempted to complete the questionnaire, it will welcome you back.

TIP: You can click "BACK" whenever you want to go back to a previous section and re-do it, so don't worry if you think you made an error and need to go back to fix it later! Your answers will be saved for each question you answer.

COMPANY INFORMATION

Here, you will find your company details. Your information should auto-populate. Please review and it and make sure it's up-to-date, and update your company or contact information if needed.

SERVICE PROVIDER COLLECTION

You'll see this question:

Does your company have a relationship with any other third-party agents, for example website-hosting companies, loyalty program agents, etc.?

In most cases, and if MyTime is your sole credit card payment solution, you would click **No**.

If you have a service provider, like a Paypal or Auth.net handling credit cards at point of sale, then Click "**Yes.**"

TIP: For this process a "Service Provider" is a third party that either gets involved in the transmission, processing and/or storing of cardholder data. Based on the roles they play, they can impact the security of cardholder data when acting on your behalf. Examples include companies that manage firewall services for you and website-hosting providers.

If you answer "**Yes**" to having a Service Provider, a window will then pop up asking you to fill out the contact details of that service provider.

MyTime's Point of Sale solution does NOT store full credit card numbers and is not a "QIR."

ENTER YOUR MERCHANT TYPE

You should already see your business type in the field, but if it's not there, you need click the drop down menu and find the type of business that best fits your company or operation. You can type in the box to narrow the search.

TIP: Select the category that most closely describes your business. You can select more than one option. If you do not see anything that applies to your business, select "other" and enter in your business type.

QUALIFICATION SECTION

In the this section, you will be asked a series of questions that will determine if you qualify for an abbreviated form of the SAQ. This determination is based on the method you use for processing credit card transactions. Since you use MyTime's Point of Sale solution to process payments, we'll help answer these questions as we guide you through the questionnaire.

After you complete the SAQ and any "To do" items, you can then print or download your certificate of compliance for you to file away safely until next year when you'll be asked to go through the SAQ questionnaire again.

SELECT YOUR PROCESSING METHOD

You should see the below image of MyTime's Point of Sale. Please select "MyTime Retail POS" by clicking on the circle next to it.

After a few seconds you'll be asked the following questions, for each of which, the answer should be "No."

Do you want to add another Processing Method?
Click No

Does your business electronically store credit card numbers?
Click No and then click the "Next" button.

TIP: Electronically storing credit card information means keeping at least one full credit card number saved on a computer, smartphone, or other electronic device that you own. Keeping full credit card numbers on paper does not count as electronic storage.

Eligibility

You should now have reached the next level, "Eligibility," which means you qualify to answer the shortened SAQ questionnaire!

Click "**Yes**" to each of the statements listed in the "Eligibility" section and then click the "Next" button to go to the next stage, the "Questionnaire.

QUESTIONNAIRE

You've now qualified to answer the shortened SAQ. We'll help you answer all of the topics in the questionnaire successfully. Once complete,, you'll see a green light that will graphically display to indicate that you are certified PCI compliant.

Keep in mind that some questions may require you to make some changes at your place of work to make sure you are compliant and we'll provide you with tips along the way explaining how or why this is necessary.

Remember, the purpose of being PCI compliant is making sure your business location is handling credit card payments safely and securely according to industry standards.

Let's start the questionnaire!

1) **Anti-virus software is deployed on all systems commonly affected by malicious software.**
   Answer "**True**"

   TIP: Verify you have antivirus software running on all computers or smartphones that have access to your Internet network or the card processing environment. Install anti-virus software (many are free to use) on all systems and computers and install updates regularly.

2) **Security policies and operational procedures for encrypting transmissions of cardholder data are documented, in use, and known to all affected parties.**
   Answer "**True**"

   TIP: "Affected parties" refers to anyone who needs to be aware of the security policies and procedures. It may include employees, service providers, and other personnel.

3) **All media is physically secured (including but not limited to computers, removable electronic media, paper receipts, paper reports, and faxes).**
   Answer "True"

   TIP: Verify all media is kept as safe as possible by physically securing it (including but not limited to computers, removable electronic devices, paper receipts, paper reports, and faxes). For example, all paper receipts are placed in a locked cabinet or all equipment used for processing is locked down or stored in a locked area.

4) **All media is destroyed when it is no longer needed for business or legal reasons.**
   Answer "**True**"

   TIP: For these purposes, "media" refers to all cardholder information both on paper and electronic data. Verify all cardholder information in any form is destroyed properly when it is no longer needed for business or legal reasons set by your provider or state.

5) **For destruction, hard copy materials are cross-cut shredded, incinerated, or pulped so that cardholder data cannot be reconstructed.**
Answer "**True**"

TIP: Start destroying all hard copy materials through crosscut shredding, burning, or pulping only and all electronic media data by erasing content through securing wiping or degaussing.

6) **For destruction, containers that store information to be destroyed are secured to prevent access to the contents.**
Answer "**True**"

TIP: Verify storage containers used for information to be destroyed are secured. For example, verify that a "to-be-shredded" container has a lock preventing access to its contents.

7) **Policies and procedures require that a list is maintained of devices that capture payment card data via direct physical interaction with the card.**
Answer "**True**"

TIP: Examine documented policies and procedures to verify they include a list of devices that capture payment card data via direct physical interaction with the card. This requirement applies to card-reading devices used in card-present transactions at point of sale. This requirement is not intended to apply to manual key-entry components such as computer keyboards and POS keypads.

8) **Policies and procedures require that devices are periodically inspected to look for tampering or substitution.**
Answer "**True**"

TIP: Examine documented policies and procedures to verify they include periodically inspecting devices to look for tampering or substitution. This requirement applies to card-reading devices used in card-present transactions at point of sale. This requirement is not intended to apply to manual key-entry components such as computer keyboards and POS keypads.

9) **Policies and procedures require that personnel are trained to be aware of suspicious behavior and to report tampering or substitution of devices.**
Answer "**True**"

TIP: Make sure any employee who handles point of sale devices is aware of suspicious behavior or any attempts to tamper with the POS device.

10) **An up to date list of devices is maintained, and it includes the following:**
   - Make and model of device
   - Location of device (for example, the address of the site or facility where the device is located)
   - Device serial number or other method of unique identification

   Answer "**True**"

   TIP: This requirement applies to devices that capture payment card data via direct physical interaction with the card.

11) **The list of devices is accurate and up to date.**
   Answer "**True**"

   TIP: Keep an up-to-date list of devices to helps your organization keep track of where devices are supposed to be, and quickly identify if a device is missing or lost.

12) **The list of devices is updated when devices are added, relocated, decommissioned, etc**
   Answer "**True**"

   TIP: The method for maintaining a list of devices may be automated (for example, a device-management system) or manual (for example, documented in electronic or paper records).

13) **Device surfaces are periodically inspected to detect tampering or substitution.**
   Answer "**True**"

   TIP: This requirement applies to devices that capture payment card data via direct physical interaction with the card.

   Signs that a device might have been tampered with or substituted include unexpected attachments or cables plugged into the device, missing or changed security labels, broken or differently colored casing, or changes to the serial number or other external markings.

14) **Personnel are aware of procedures for inspecting devices. (Including yourself if you're the only one taking payments)**
   Answer "**True**"

   TIP: This requirement applies to devices that capture payment card data via direct physical interaction with the card.

15) **Training materials for personnel at point-of-sale locations include the following:**
   - Verify the identity of any third-party persons claiming to be repair or maintenance personnel, prior to granting them access to modify or troubleshoot devices
   - Do not install, replace, or return devices without verification
   - Be aware of suspicious behavior around devices (for example, attempts by unknown persons to unplug or open devices)
   - Report suspicious behavior and indications of device tampering or substitution to appropriate personnel (for example, to a manager or security officer)

   Answer "**True**"

   TIP: Review training materials for personnel at point-of-sale locations to verify they include training in the listed requirements.

16) **Personnel at point-of-sale locations have received training, and are they aware of procedures to detect and report attempted tampering or replacement of devices.**
   Answer "**True**"

   TIP: Periodically interview personnel to verify that they have received and remember their training to detect and report attempts to tamper with or replace payment devices.

17) **Security policies and operational procedures for restricting physical access to cardholder data are documented, in use, and known to all affected parties.**
   Answer "**True**"

   TIP: Personnel need to be aware of and following security policies and operational procedures for restricting physical access to cardholder data and CDE systems on a continuous basis.

18) **Cardholder data retention and disposal policies and procedures are implemented. They include specific retention requirements for cardholder data.**
   Answer "**True**"

   TIP: Verify that your company policies include specific procedures for retention of cardholder data and outlines the business, legal and regulatory purposes for storage.

19) **Cardholder data retention and disposal policies and procedures are implemented. The amount of data and length of time it is stored is limited to what is needed for legal, regulatory, and business requirements.**
   Answer "**True**"

   TIP: Examine your data policies to verify that they limit the amount of data and the length of time it is stored to the minimum needed.

20) **Data retention and disposal policies and procedures include provisions for the secure disposal of cardholder and other data when no longer needed for legal, regulatory, or business reasons.**
Answer "**True**"

TIP: Verify that your company policies include specific procedures for secure disposal of cardholder data and when no longer needed for business, legal, or regulatory purposes.

21) **There is a quarterly process for identifying and securely deleting stored cardholder data that exceeds defined retention requirements.**
Answer "**True**"

TIP: Review your policies and procedures to ensure that they include a quarterly process for properly deleting stored cardholder data once it is no longer needed.

22) **All stored cardholder data meets the requirements defined in the data retention policy.**
Answer "**True**"

TIP: Verify that all stored credit card data complies with your data retention policy.

23) **After authorization, no systems store the card verification code or value under any circumstance, even if encrypted.**
Answer "**True**"

TIP: Verify the three or four digit card verification code or value printed on the front of the card or the signature panel (CVV2, CVC2, CID, CAV2 data) is not retained for any reason. The purpose of the card validation code is to protect transactions where the consumer and the card are not present, such as Internet or mail order/telephone order (MO/TO).

24) **Security policies and operational procedures for protecting stored cardholder data are documented, in use, and known to all affected parties.**
Answer "**True**"

TIP: Personnel need to be aware of and follow security policies and documented operational procedures for managing the secure storage of cardholder data on a continuous basis.

25) **A security policy is established, published, maintained, and disseminated to all relevant personnel.**
Answer "**True**"

TIP: This requirement applies to any personnel who are physically present at the business location or otherwise have access to the company's cardholder data environment. "Personnel" includes full-time and part-time employees, temporary employees, contractors, consultants, vendors, and business partners. You may access the complimentary PCI 1-2-3 Policy Builder in the MyControlScan portal's PCI Resources section to help with this requirement.

26) **The security policy is reviewed at least once a year and updated when the cardholder data environment changes.**
Answer "**True**"

TIP: An information security policy protects a company's most valuable assets and data. Verify the security policy is written, regularly reviewed, and distributed to all relevant personnel (including employees, vendors, and business partners).

27) **The security policy and procedures clearly define information security responsibilities for all personnel.**
Answer "**True**"

TIP: Verify your security policy clearly states all employee and contractor responsibilities for dealing with credit card information and the systems within the card processing environment.

28) **An individual or team is formally assigned responsibility for Information security management. This includes establishing, documenting, and distributing security incident response and escalation procedures to ensure timely and effective handling of all situations.**
Answer "**True**"

TIP: Verify personnel have been specifically assigned the responsibility of responding to and escalating any security breach. Confirm that all employees know exactly whom to contact if they suspect any kind of credit card data loss.

29) **An individual or team is formally assigned responsibility for administering user accounts, including additions, deletions, and modifications.**
Answer "**True**"

TIP: Verify that the responsibility for administering user accounts is formally assigned to an individual or team (it can be you or an employee). This responsibility includes additions, removals, and changes.

30) **An individual or team is formally assigned responsibility for monitoring and controlling all access to data.**
Answer "**True**"

TIP: Verify that responsibility for monitoring and controlling all access to cardholder data is assigned to an individual or team. Each person or team with responsibilities for information security management should be clearly aware of their responsibilities and related tasks, through specific policy.

31) **A formal security awareness program is in place to make all personnel aware of the importance of cardholder data security.**
Answer "**True**"

TIP: If personnel are not educated about their security responsibilities, then any security safeguards and processes that have been implemented may become ineffective through errors or intentional actions. You may access the complimentary Security Awareness Training in the MyControlScan portal's PCI Resources section to help with this requirement.

32) **A list of service providers is maintained.**
Answer "**True**"

TIP: A service provider is defined as any company other than your own that has access to the credit card information that you accept or has influence over the security measures used to keep that information safe. It is possible for the list to consist of only one service provider.

33) **A written agreement is maintained with all service providers that store, process, transmit, or impact the security of cardholder data. The agreement includes an acknowledgment that the service providers are responsible for the security of cardholder data.**
Answer "**True**"

TIP: The exact wording of an acknowledgement will depend on the agreement between the two parties, the details of the service being provided, and the responsibilities assigned to each party. The acknowledgement does not have to include the exact wording provided in this requirement.

34) **There is an established process for engaging service providers, including proper due diligence prior to engagement.**
Answer "**True**"

TIP: An established process better ensures that any engagement of a service provider is thoroughly vetted internally by the organization, lowering the risk of a data breach.

35) **Service providers' PCI DSS compliance status is monitored at least annually.**
Answer "**True**"

TIP: Verify that the compliance status of all your service providers is checked at least once a year. ControlScan recommends using PCI Validated Compliant service providers or service providers that are willing and able to share evidence of their PCI Compliance and security practices.

36) **Information is maintained about which PCI DSS requirements are managed by each service provider, and which are managed by your organization.**
Answer "**True**"

TIP: The specific information your organization maintains will depend on the particular agreement with your providers, the type of service, etc. The intent is for the assessed entity to understand which PCI DSS requirements their providers have agreed to meet.

37) **An incident response plan has been created and is ready for use in the event of system breach. (Last Question, we promise!)**
Answer "**True**"

TIP: Incident response plans help businesses react quickly to any security breach. An incident response plan should contain all the key elements to allow your company to respond effectively in the event of a breach that could impact cardholder data. These elements include designation of roles to responsible personnel, correction of system vulnerabilities, procedure for notifying card brands, and necessary steps to restore service and maintain business continuity.

After you Answer **True** and Click **Next**, you'll get this message:

All your questions have been answered!
You are able to review your questions and make changes.

If you answered True to all the SAQ statements you should be able to go straight to the final "Attestation" section.

ATTESTATION

You'll be asked to confirm a list of requirements for the PCI DSS Self-Assessment Questionnaire (SAQ D-MERCH), which is the questionnaire you completed. This should be done by an authorized representative of the company. Once completed you can download your PCI DSS compliance certificate.

You'll need to enter your name as a signature and confirm that you're an authorized representative of the company. Then click "**Next**" to finalize and lock your SAQ. You can download a report of your SAQ and/or start a new SAQ at any time in the future.

Congratulations!
You'll now get a green light for your compliance.

SUPPORT

Contact
Control Scan

Phone
Support: 800-571-3928
Fax: 800-825-2207

Hours of Operation
Mon Thurs: 8:30am 8:00pm
Friday: 8:30am 6:00pm