

PDQ Guide for the PCI Data Security Standard Self-Assessment
Questionnaire C (Version 1.2)

- PDQ has created an Answer Guide for the Payment Card Industry (PCI) Data Security Standard Self-Assessment Questionnaire C to help wash operators complete questionnaires. Part of the Access Customer Management System (CMS) operator manual is the PABP Implementation Guide, which should be reviewed for specifics on Access CMS payment application site installation. PDQ Manufacturing, Inc. is not a (QSA) Qualified Security Assessor, and is not qualified to make judgments related to PCI compliance. PDQ strongly recommends wash operators consult a QSA if there is any uncertainty how to answer this questionnaire and if this questionnaire is applicable to their business operation. A list of security assessors is available at https://www.pcisecuritystandards.org/resources/qualified_security_assessors.htm.

- If you are answering Yes to these questions, it is assumed that you have read and met all the requirements of the PABP Implementation guide and the PCI Guidelines. To clarify requirements there is a document called “Navigating PCI DSS – Understanding the Intent of the Requirements” at www.pcisecuritystandards.org web site. If in doubt about how to interpret the questionnaire in regarding to your operation, please contact and consult a QSA.

- By answering Questionnaire C, you are confirming that you do not use any Custom Integration features of the Access software. If Custom Integration is used, Questionnaire D is required and must be completed.

- Please check for the latest version of this questionnaire before starting. The version may change without notice. The questionnaire can be found at www.pcisecuritystandards.org

PDQ Guide for the PCI Data Security Standard Self-Assessment
Questionnaire C (Version 1.2)

Attestation of Compliance

Part 1: Qualified Security Assessor Company Information

- Information to be filled out by Merchant if applicable

Part 2: Merchant Organization Information

- Information to be filled out by Merchant

Part 2a: Type of merchant business (check all that apply)

Part 2b: Relationships

- *1st box:* Answer Yes. PDQ has a Loyalty Club program known as WALS (Wash Access Loyalty System) no card data is involved, website and relationship to Authorize.net
- *2nd box:* Answer Yes, if you have multiple merchant accounts using separate merchant acquirers. If all merchant accounts are managed by one acquirer, answer No.

Part 2c: Transaction Processing

Payment Application in use:

Access CMS1

Access CMS2

Payment Application Version:

8

2

Part 2d: Eligibility to Complete SAQ C

If only Access CMS is used for card payment processing at the site, all the below can be checked. If other devices are processing card payments please check with manufacturer.

- *1st box:* Access CMS is a payment application and it makes use of a secure Internet connection for processing.
- *2nd box:* Access CMS does not connect to other systems such as; a central payment processor, or database on the same network for processing payments.
- *3rd box:* Access CMS does not store card holder data and is PABP validated application.
- *4th box:* Access CMS will not allow printing or producing of card holder data in any external media format.
- *5th box:* All unsecure methods for remote support are disabled on normal default mode of operation.

PDQ Guide for the PCI Data Security Standard Self-Assessment
Questionnaire C (Version 1.2)

Part 3: PCI DSS Validation

- To be filled out after questionnaire is complete

Part 3a: Confirmation of Compliant Status

- The merchant is responsible for completing the tasks listed in this section.
Check with a QSA if you feel some items do not apply to your business.
Check each box that has been completed.

Part 3b: Merchant Acknowledgement

- Appropriate merchant representatives should sign and date.

Part 4: Action Plan for Non-Compliant Status

- To be filled out after questionnaire is complete

PDQ Guide for the PCI Data Security Standard Self-Assessment
Questionnaire C (Version 1.2)

Self-Assessment Questionnaire C

Requirement 1: Install and maintain a firewall configuration to protect cardholder data

- Firewall configurations may vary from site to site depending on the services needed. Refer to the PCI guidelines under requirement 1 to ensure your firewall meets the requirements listed.
- Answer Yes, only if all requirements are met.

Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters

- Answer Yes. Access CMS software will force the user to change passwords the first time each user account is accessed.

Requirement 3: Protect stored cardholder data

- If using Access CMS1 version 8, or Access CMS2 version 2, answer Yes. The Access unit does not store any sensitive cardholder data.

Requirement 4: Encrypt transmission of cardholder data across open, public networks

- Answer Yes

Requirement 5: Use and regularly update anti-virus software

- If another system or PC is installed on the site network you must ensure they are running the latest version of anti-virus software before answering Yes to the questions under this section.
- Answer Yes. The PDQ Access is an embedded system that is not commonly affected by viruses.

Requirement 6: Develop and maintain secure systems and applications

- Answer Yes, if the latest version is installed.
- Check PDQ's website to get the latest version of software. If you are using other devices, check with your vendor for updates.
- Note: you have to sign up for the operator section of the PDQ website if you are not already a member to download updates.

PDQ Guide for the PCI Data Security Standard Self-Assessment
Questionnaire C (Version 1.2)

Requirement 7: Restrict access to cardholder data by business need-to-know

- Answer Yes
 - PDQ does not have any default passwords where anyone can log in; there is also no access to cardholder information. Make sure the site has physical locks on the Access unit and the equipment room. If you have additional site computers and routers ensure authentication is enabled and individual user accounts are created and changed regularly. Preventing physical access to PC's and other networking devices should also be limited to those who need access only.

Requirement 8: Assign a unique ID to each person with computer access

- Answer Yes
 - VPN is only enabled on an as-needed-basis for support. It must be disabled at all other times of use. Authorized login to the Access system set up is always needed to temporarily enable for remote support.

Requirement 9: Restrict physical access to cardholder data

- If the only way that you process credit cards is through Access CMS, then answer Yes to all the questions in this section 9. If not, you will need to check with the manufacturer of the device before answering. Card holder data is never displayed on the Access CMS system. The Access CMS does not supply any hard copies or media of any cardholder data.
- Answer Yes

Requirement 10: (removed from SAQ)

Requirement 11: Regularly test security systems and processes

- The answer to the questions in this section may vary based on what is required of your business. If you are required by your acquirer to be scanned and tested regularly then you may answer Yes to this question. There is a list of Approved Scanning Vendors on www.pcisecuritystandards.org website.
- Answer Yes, only if all requirements are met.

PDQ Guide for the PCI Data Security Standard Self-Assessment
Questionnaire C (Version 1.2)

Requirement 12: Maintain a policy that addresses information

- It is the responsibility of the merchant to ensure that all policies required by the PCI DSS version 1.1 are met. PDQ recommends merchants unsure of the PCI guidelines, and how to implement them, hire a consultant or Qualified Security Assessor to assist them with developing and maintaining required policies. Merchants should review the PCI Security documents and implement the policies as required based on their business. Answer Yes to all the questions in this section only if the requirements are met.