



PCI Compliance – Why It’s Important to Your Business

Protect Your Business and Your Customers

- ✓ With data security compromises on the rise, it is more important than ever to take measures to safeguard your customers and your business.
- ✓ Criminals or “hackers” can pose a risk to your business both onsite and remotely ... so it’s critical to implement procedures to protect your sensitive data ... whether it is stored in a file cabinet or on a computer.

For more information, visit:

[PCISecurityStandards.org](https://www.pcisecuritystandards.org)

Understand PCI

- ✓ The card brands have joined to form the PCI Security Standards Council (PCI SSC), establishing security requirements and standards EVERY business that stores, processes or transmits payment card data MUST MEET. That means if you accept card payments you must comply with these requirements.
- ✓ Ensure you are compliant and take the first step toward avoiding costly security breaches that can include:
 - 100% responsibility for cardholder losses
 - Card brand fines up to \$500,000 per incident
 - Forensic investigations expenses as high as \$100,000

For more information, visit:

[PCISecurityStandards.org](https://www.pcisecuritystandards.org)

What You Need to Do to Be PCI Compliant

- 1. Build and Maintain a Secure Network**
- 2. Protect Cardholder Data**
- 3. Maintain a Vulnerability Management Program**
- 4. Implement Strong Access Control Measures**
- 5. Regularly Monitor and Test Networks**
- 6. Maintain an Information Security Policy**

Building and Maintaining a Secure Network

1. Build and Maintain a Secure Network

Requirement 1: Install and maintain a firewall configuration to protect cardholder data. Internet firewall security needs to be installed and functional on all computers and POS systems using IP connectivity, including those with a dial connection to the internet.

Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters. Passwords should be personalized for all users of computers and POS systems. All unnecessary services should be disabled.

Protecting Cardholder Data

2. Protect Cardholder Data

Requirement 3: Protect stored cardholder data. Do not store the contents of the track data from the magnetic stripe on the credit card or the CVV or CVC information (3-digit code on the back on the card) post authorization.

Only store cardholder account information that is essential to your business. Hard copies of batch reports and paper receipts must be placed in a secured area where only authorized personnel can enter. Implement a policy on how long data will be stored and for what it is needed (i.e. business or legal purposes). When discarding, make sure you shred or otherwise permanently destroy all documents.

Requirement 4: Encrypt transmission of cardholder data across open, public networks. Databases and files containing payment card information must be encrypted. Encryption software is required for POS systems using internet connectivity for transmission of cardholder information.

Maintaining a Vulnerability Management Program

3. Maintain a Vulnerability Management Program

Requirement 5: Use and regularly update anti-virus software. Install and maintain updated anti-virus software on all computers and POS systems. The number one reason for hacker fraud is Trojan/Backdoor virus intrusion. Business owners need to be aware that using the same server for email, web surfing and card processing is a violation of the PCI DSS and makes your business vulnerable to a cyber intrusion.

Requirement 6: Develop and maintain secure systems and applications. Check with your software dealer to ensure you are using the latest version. You can also verify if your software and version are included on the PCI Security Standards Council's Validated Payment Application list at:

https://www.pcisecuritystandards.org/approved_companies_providers/vpa_agreement.php

Old and insufficient technology is an open invitation for hackers. Don't take for granted that your dealer has informed you of possible vulnerabilities or updates. Remember it is you that will be subject to fines if your business is compromised.

If using a payment card terminal, upgrade outdated equipment or applications.



Heartland
PAYMENT SYSTEMS™

The Highest Standards | The Most Trusted Transactions

Implementing Strong Access Control Measures

4. Implement Strong Access Control Measures

Requirement 7: Restrict access to cardholder data by business need-to-know. Passwords should always be used to limit access to cardholder information by a business need-to-know.

Requirement 8: Assign a unique ID to each person with computer access. Ensure each employee has a unique user name and password to restrict access to computers and POS systems' data. Make sure you update passwords when any employee leaves.

Requirement 9: Restrict physical access to cardholder data.

Regularly Monitoring and Testing Networks / Maintaining an Information Security Policy

5. Regularly Monitor and Test Networks

Requirement 10: Track and monitor all access to network resources and cardholder data. Track and monitor all access to network resources (i.e. computers, POS systems). You must be able to show proof of tracking.

Requirement 11: Regularly test security systems and processes. Document a policy/schedule for testing of security systems and processes. You must be able to show proof of testing of your internet security and policy processes.

6. Maintain an Information Security Policy

Requirement 12: Maintain a policy that addresses information security. Document and maintain an enforceable policy that details safeguarding of payment card information.

Compliance Depends on Levels

The card brands define various levels of compliance and validation requirements for merchants based on annual transaction volume and processing type:

- **Level 1:** Any merchant – regardless of acceptance channel – processing over 6,000,000 transactions per year per card brand requires:
 - ✓ Annual onsite review validated by a Qualified Security Assessor (QSA).*
 - ✓ Quarterly network vulnerability scan validated by an Approved Scanning Vendor (ASV).
- **Level 2:** Any merchant – regardless of acceptance channel – processing 1,000,000 to 6,000,000 transactions per year per card brand requires:
 - ✓ Annual PCI Self-Assessment Questionnaire (SAQ) validated by the merchant. It is recommended to enlist the support of a QSA to assist in answering the questionnaire.*
 - ✓ Quarterly network vulnerability scan validated by an ASV.

***Internal auditor may be used in some cases.**

MasterCard will require staff engaged in assessment to complete annual training effective 6/30/2011.

Compliance Depends on Levels

- **Level 3:** Any merchant processing 20,000 to 1,000,000 e-Commerce transactions per year per card brand requires:
 - ✓ Annual PCI SAQ validated by the merchant.
 - ✓ Quarterly network vulnerability scan validated by an ASV.
- **Level 4:** Any merchant processing fewer than 20,000 e-Commerce transactions per year per card brand, and all other merchants – regardless of acceptance channel – processing up to 1,000,000 transactions per year per card brand requires:
 - ✓ Annual PCI SAQ validated by the merchant.
 - ✓ Quarterly network vulnerability scan validated by an ASV.

The above covers Visa, MasterCard, and Discover Network. American Express only has three levels.

The PCI DSS requires that all merchants with external-facing IP addresses perform external network vulnerability scanning to achieve compliance.

Payment Card Industry Data Security Standard (PCI DSS)

- To validate compliance, you should contract with a QSA to complete the annual PCI SAQ. If you process cards over an internet connection, you must contract with an ASV to complete the quarterly network vulnerability scans.
- Heartland Payment Systems has developed a program to assist our merchants in becoming compliant. We have partnered with 403 Labs (403labs.com), a highly respected security firm in the payment card industry, to offer our merchants a security program that can help them become compliant with the PCI DSS and reduce payment card fraud risk at a significantly reduced rate. 403 Labs is a PCI approved QSA and ASV.



Heartland
PAYMENT SYSTEMS™

The Highest Standards | The Most Trusted Transactions

Self-Evaluate Your PCI Compliance With a PCI DSS Self-Assessment Questionnaire (SAQ)

The SAQ is a validation tool that will help you self-evaluate your compliance to the PCI DSS. From the [PCISecurityStandards.org](https://www.pcisecuritystandards.org) website, you can select the SAQ applicable to your business' payment card processing environment:

SAQ V2.0	Description
A	Card-not-present (e-Commerce or mail/telephone order) merchants. All cardholder data functions are outsourced. This would never apply to face-to-face merchants.
B	Imprint-only merchants with no electronic cardholder data storage or standalone, dial-out terminal merchants with no electronic cardholder data storage.
C-VT	Merchants using only web-based virtual terminals, no electronic cardholder data storage.
C	Merchants with payment applications connected to the internet with no electronic cardholder data storage.
D	All other merchants not included in descriptions for SAQ types A through C above.

PCI DSS – Frequently Asked Questions

Q: Do I have to be PCI compliant?

A: Yes, all merchants are expected to be compliant with the 12 requirements of the PCI Data Security Standard (PCI DSS).

Q: Do I have to provide documentation of my compliance with the PCI DSS?

A: While merchants are expected to be compliant with the PCI DSS, Level 4 merchants do not have to provide proof of validation to Heartland unless requested. You should complete the PCI DSS SAQ to identify any areas where you do not currently meet the requirements. If you process transactions over the internet, all internet-facing IP addresses (IP addresses directly accessible from the internet) must be scanned for vulnerabilities by a PCI SSC Approved Scanning Vendor (ASV). Level 1, 2, and 3 merchants must provide proof of their compliance with the PCI DSS requirements including an Attestation of Compliance. Heartland will contact you if you qualify as a Level 1, 2, or 3 merchant.

PCI DSS – Frequently Asked Questions

Q: How do I know my merchant level?

A: The majority of Heartland’s merchants are Level 4. The levels are defined by the transaction volume per card brand and processing method. Heartland will contact you if you qualify as a Level 1, 2, or 3 merchant to review validation requirements.

Q: Who should I contact to become PCI compliant?

A: Heartland has partnered with 403 Labs, a highly respected security firm in the payment card industry, to offer our merchants a security program that can help them become compliant with the PCI DSS and reduce payment card fraud risk at a significantly reduced rate. To get started with the program, please visit our partner site at Heartland.403labs.com.

Q: What are the requirements for me to become PCI compliant?

A: If you are a Level 4 merchant and you process credit card transactions over an internet connection, you must complete and pass the PCI SAQ annually and perform and pass quarterly network vulnerability scans. If you do not process over the internet (for example, you use a dial terminal), you only need to complete and pass the PCI SAQ annually. Our partnership with 403 Labs is designed to help merchants who fall into either category. 403 Labs will help guide you to the proper services and requirements. To get started with the program, simply visit Heartland.403labs.com.

PCI DSS – Frequently Asked Questions

Q: If I have more than one PC at my location or have multiple locations, do I have to complete multiple SAQs?

A: Typically, no. You only have to complete one questionnaire for your business as a whole provided all locations are one type of business (such as restaurants). However, you will need to perform scans of all public-facing IP addresses at all locations, if applicable.

Q: With whom should I work to complete the SAQ?

A: You may need to consult your network support person and/or POS provider for assistance with questions about your set-up and environment. If you contract with a QSA, such as 403 Labs, they will be able to assist with understanding the questions and directing you to the appropriate network support staff to make any necessary changes.

PCI DSS – Frequently Asked Questions

Q: How often does the SAQ have to be completed to be considered PCI compliant?

A: To be compliant, the SAQ is required to be completed and passed annually. Please note, any significant changes to the business warrants updating your SAQ to appropriately reflect these changes.

Q: How often does the network vulnerability scan have to be performed to be considered PCI compliant?

A: To be compliant, the network vulnerability scan is required to be performed and passed quarterly. Please note, any significant changes to the network warrants performing a new scan to make sure the changes were made appropriately and are secure. 403 Labs will provide you with an enhanced SAQ designed to make the process easier, quarterly network vulnerability scans, access to a web portal with your results and strategies for fixing identified vulnerabilities and technical support.

PCI DSS – Frequently Asked Questions

Q: Once I validate my PCI compliance, do I have to do anything again to remain PCI compliant?

A: Your PCI compliance validation is a point-in-time measurement. True compliance requires continuous assessment and remediation to protect your business and data from new threats as they emerge. Any significant changes in your network or business processes should warrant another review of the SAQ and/or network scan to identify any vulnerabilities that may have been opened by these changes. Examples of changes would be a new software installation, upgrade to the software version, firewall rule modifications, new employee password policies and the like. Also, ongoing quarterly vulnerability scanning is a requirement as new threats emerge daily. In 2009, more than 8,000 new vulnerabilities were discovered which averages out to almost 20 each day!

PCI DSS – Frequently Asked Questions

Q: Am I PCI compliant if my point-of-sale system is compliant?

A: No. PCI compliance goes beyond the hardware or software used for payment card processing. You are expected to be compliant to the Payment Card Industry Data Security Standard (PCI DSS). The PCI DSS contains 12 requirements addressing six core principles for network architecture, cardholder data protection, vulnerability management, access controls, network security and information security policies. These include items such as policies for storing reports/receipts, physical access to data, passwords, etc.

Using a validated payment application and/or PCI approved PIN Entry Device (PED) may aide in reducing scope of potential areas requiring attention. However, to be considered PCI compliant, you must validate your compliance by completing and passing the PCI SAQ and network vulnerability scans (if applicable). 403 Labs, a highly respected security firm in the payment card industry, has partnered with Heartland to offer merchants a security program that can help them become compliant to the PCI DSS and reduce payment card fraud risk at a significantly reduced rate. To enroll in this program, please visit Heartland.403labs.com.

PCI DSS – Frequently Asked Questions

Q: Where can I obtain more information?

A: Heartland has developed an informative website where you can learn more about PCI compliance: HeartlandPaymentSystems.com/Compliance.

Full information about PCI and the necessary forms are available on the PCI Security Standards Council website: PCISecurityStandards.org.

For information about 403 Labs, please visit 403labs.com or call directly at 877.403.LABS (5227).

If you would like to get started with the process and register for the program, go to Heartland.403labs.com.

If you have any other questions, please contact Heartland Payment Systems at 888.963.3600 or email HeartlandServiceCenter@e-hps.com.