



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 onsite or remotely ... so it’s critical to implement procedures to protect your data ... whether it is stored in a file cabinet or on a computer.

For more information, visit:

www.pcisecuritystandards.org



Heartland
PAYMENT SYSTEMS™

The Highest Standards | The Most Trusted Transactions

Understand PCI

- ✓ The card brands have joined to form the PCI Data Security Standards (PCI DSS) Council, establishing security requirements and standards EVERY business that accepts card payments and stores, processes or transmits payment card data MUST MEET.
- ✓ Ensure you are compliant so you avoid 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:

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**



Heartland
PAYMENT SYSTEMS™

The Highest Standards | The Most Trusted Transactions

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.



Heartland
PAYMENT SYSTEMS™

The Highest Standards | The Most Trusted Transactions

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 Counsel's Validated Payment Application list at

https://www.pcisecuritystandards.org/security_standards/pa_dss.shtml.

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.



Heartland
PAYMENT SYSTEMS™

The Highest Standards | The Most Trusted Transactions

Regularly Monitoring and Testing Networks / Maintaining an Information

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.



Heartland
PAYMENT SYSTEMS™

The Highest Standards | The Most Trusted Transactions

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
 - ✓ Quarterly network vulnerability scan validated by an Approved Scanning Vendor
- **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 validated by the merchant is currently acceptable. It is recommended to enlist the support of a Qualified Security Assessor to assist in answering the questionnaire. MasterCard will require annual onsite review validated by a Qualified Security Assessor by 12/31/10.
 - ✓ Quarterly network vulnerability scan validated by an Approved Scanning Vendor.

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 Self-Assessment Questionnaire validated by the merchant.
 - ✓ Quarterly network vulnerability scan validated by an Approved Scanning Vendor.
- **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 Self-Assessment Questionnaire validated by the merchant.
 - ✓ Quarterly network vulnerability scan validated by an Approved Scanning Vendor.

***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 Standards (PCI DSS)

- To validate compliance, you should contract with a Qualified Security Assessor to complete the annual PCI Self-Assessment Questionnaire. If you have Internet connectivity in your business, you should contract with an Approved Scanning Vendor to complete the quarterly network vulnerability scans.
- Please visit www.pcisecuritystandards.org to find a list of Qualified Security Assessors and Approved Scanning Vendors under the QSA/ASV menu.



Heartland
PAYMENT SYSTEMS™

The Highest Standards | The Most Trusted Transactions

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

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

SAQ Validation Type	Description	SAQ V1.2
1	Card-not-present (e-Commerce or Mail/Telephone Order) merchants. All cardholder data functions are outsourced. This does not apply to face-to-face merchants.	<u>A</u>
2	Imprint-only merchants with no electronic cardholder data storage.	<u>B</u>
3	Stand-alone terminal merchants with no electronic cardholder data storage.	<u>B</u>
4	Merchants with POS systems connected to the Internet with no electronic cardholder data storage.	<u>C</u>
5	All other merchants (not included in Types 1-4 above).	<u>D</u>

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 Standards (PCI DSS).

Q: Do I have to validate compliance to the PCI DSS?

A: While expected to be compliant to the PCI DSS, Level 4 merchants do not have to provide proof of validation to Heartland Payment Systems. You should complete the PCI DSS SAQ to identify any vulnerabilities. If you have external-facing IP addresses you must run network scanning.

Q: Who should I contact to become PCI compliant?

A: There are several companies that provide services. You can find a Qualified Security Assessor (QSA) to assist with the PCI SAQ and an Approved Scanning Vendor (ASV) to assist with the network vulnerability scans on the <https://www.pcisecuritystandards.org> website under the QSA/ASV menu.

PCI DSS – Frequently Asked Questions

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

A: If you have Internet in your business on a system that could store cardholder data, you must complete and pass the PCI SAQ and perform and pass quarterly network vulnerability scans.

If you do not have Internet in your business, you only need to complete and pass the PCI SAQ.

Q: If I have more than one PC, do I have to complete multiple Self-Assessment Questionnaires (SAQ)?

A: No, you only have to complete one questionnaire for your business as a whole.

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, they will be able to assist with understanding the questions.

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.

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.

Q: Once I am deemed PCI compliant, do I have to do anything again to remain PCI compliant?

A: PCI compliance is a point in time. Compliance requires continuous assessment and remediation. Any significant changes in your network or business processes should warrant another review of the SAQ and/or network scan to identify any vulnerabilities. Examples of changes would be a new software installation, upgrade to the software version, firewall rule modifications, new employee password policies and the like.



Heartland
PAYMENT SYSTEMS™

The Highest Standards | The Most Trusted Transactions

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 applications and/or approved PCI PIN Entry Device (PED) may aide in reducing scope of potential areas requiring attention. However, to be considered PCI DSS compliant, you must validate your compliance by completing and passing the PCI SAQ and network vulnerability scans.



Heartland
PAYMENT SYSTEMS™

The Highest Standards | The Most Trusted Transactions