What is PCI Compliance? 12 Requirements & More

Source: *Digital Guardian, Juliana de Groot, May 8, 2023*

What is PCI Compliance?

PCI compliance is compliance with The Payment Card Industry Data Security Standard (PCI DSS), a set of requirements intended to ensure that all companies that process, store, or transmit credit card information maintain a secure environment. It was launched on September 7, 2006, to manage PCI security standards and improve account security throughout the transaction process. An independent body created by Visa, MasterCard, American Express, Discover, and JCB, the PCI Security Standards Council (PCI SSC) administers and manages the PCI DSS. Interestingly, the payment brands and acquirers are responsible for enforcing compliance, rather than the PCI SSC.

In order to provide an extensive resource on PCI compliance, this article includes:

- A detailed overview of PCI SSC Data Security Standards (along with multiple resources for further review).
- The 12 requirements of PCI DSS Compliance listed out and explained.
- Benefits of PCI Compliance.
- Potential setbacks of being non-compliant.
- A roundup of collected tips from 18 PCS DSS experts.

AN OVERVIEW OF PCI SSC DATA SECURITY STANDARDS

In an effort to enhance payment card data security, the PCI Security Standards Council (SSC) provides comprehensive standards and supporting materials, which include specification frameworks, tools, measurements, and support resources to help organizations ensure the security of cardholder information at all times (particularly during the transmission of cardholder data). The PCI DSS is the cornerstone of the council, as it provides the necessary framework for developing complete payment card data security systems & processes that encompasses prevention, detection, and appropriate reaction to security incidents.

Tools and Resources Available from PCI SSC:

- Self-Assessment Questionnaires to assist organizations in validating their PCI DSS compliance.
- PIN Transaction Security (PTS) requirements for device vendors and manufacturers and a list of approved PIN transaction devices.
- Payment Application Data Security Standard (PA-DSS) and a list of Validated Payment Applications to help software vendors and others develop secure payment applications.
- Public resources:

- Lists of Qualified Security Assessors (QSAs)
- Payment Application Qualified Security Assessors (PA-QSAs)
- Approved Scanning Vendors (ASVs)
- Internal Security Assessor (ISA) education program

The 12 Requirements for PCI DSS Compliance

1. Use and Maintain Firewalls

Firewalls essentially block access of foreign or unknown entities attempting to access private data. These prevention systems are often the first line of defense against hackers (malicious or otherwise). Firewalls are required for PCI DSS compliance because of their effectiveness in preventing unauthorized access.

2. Proper Password Protections

Routers, modems, point of sale (POS) secure systems, and other third-party products often come with generic passwords and security measures easily accessed by the public. Too often, businesses fail to secure these security vulnerabilities. Ensuring compliance in this area includes keeping a list of all devices and software which require a password (or other security to access). In addition to a device/password inventory, basic precautions and configurations should also be enacted (e.g., changing the password).

3. Protect Cardholder Data

The third requirement of PCI DSS compliance is a two-fold protection of cardholder data. Card data must be encrypted with certain algorithms. These encryptions are put into place with encryption keys — which are also required to be encrypted for compliance. Regular maintenance and scanning of primary account numbers (PAN) are needed to ensure no unencrypted data exists.

4. Encrypt Transmitted Data

Cardholder data is sent across multiple ordinary channels (i.e., payment processors, home office from local stores, etc.). This data must be encrypted whenever it is sent to these known locations. Account numbers should also never be sent to locations that are unknown.

5. Use and Maintain Anti-Virus

Installing anti-virus software is a good practice outside of PCI DSS compliance. However, anti-virus software is required for all devices that interact with and/or store PAN. This software should be regularly patched and updated. Your POS provider should also employ anti-virus measures where it cannot be directly installed.

6. Properly Updated Software

Firewalls and anti-virus software will require updates often. It is also a good idea to update every piece of software in a business. Most software products will include security measures, such as patches to address recently discovered vulnerabilities, in their updates, which add another level of protection. These updates are especially required for all software on devices that interact with or store cardholder data.

7. Restrict Data Access

Cardholder data is required to be strictly "need to know." All staff, executives, and third parties who do not need access to this data should not have it. The roles that do need sensitive data should be well-documented and regularly updated — as required by PCI DSS.

8. Unique IDs for Access

Individuals who do have access to cardholder data should have individual credentials and identification for access. For instance, there should not be a single login to the encrypted data with multiple employees knowing the username and password. Unique IDs creates less vulnerability and a quicker response time in the event data is compromised.

9. Restrict Physical Access

Any cardholder data must be physically kept in a secure location. Both data that is physically written or typed and data that is digitally-kept (e.g., on a hard drive) should be locked in a secure room, drawer, or cabinet. Not only should access be limited, but anytime the sensitive data is accessed, it should be kept in a log to remain compliant.

10. Create and Maintain Access Logs

All activity dealing with cardholder data and primary account numbers (PAN) require a log entry. Perhaps the most common non-compliance issue is a lack of proper record keeping and documentation when it comes to accessing sensitive data. Compliance requires documenting how data flows into your organization and the number of times access is needed. Software products to log access are also needed to ensure accuracy.

11. Scan and Test for Vulnerabilities

All ten of the previous compliance standards involve several software products, physical locations, and likely a few employees. There are many things that can malfunction, go out of date, or suffer from human error. These threats can be limited by fulfilling the PCI DSS requirement for regular vulnerability scans and vulnerability testing.

12. Document Policies

Inventory of equipment, software, and employees that have access will need to be documented for attestation of compliance. The logs of accessing cardholder data will also require documentation. How information flows into your company, where it is stored, and how it is used after the point of sale will also all need to be documented.

Benefits of PCI Compliance

Complying with PCI Security Standards seems like a daunting task, at the very least. The maze of standards and issues seems like a lot to handle for large organizations, let alone smaller companies. Yet, compliance is becoming more important and may not be as troublesome as you assume, especially if you have the right tools.

According to PCI SSC, there are major benefits of compliance, especially considering that failure to comply may result in serious and long-term consequences. For example:

- PCI Compliance standards mean that your systems are secure, and your customers can trust you with their sensitive payment card information; trust leads to customer confidence and repeat customers.
- PCI Compliance improves your reputation with acquirers and payment brands – just the partners your business needs.
- PCI Compliance is an ongoing process that aids in preventing security breaches and payment card data theft in the present and in the future; PCI compliance means you are contributing to a global payment card data security solution.
- As you try to meet PCI Compliance, you're better prepared to comply with additional regulations, such as HIPAA, SOX, and others.
- PCI Compliance contributes to corporate security strategies (even if only a starting point).
- PCI Compliance likely leads to improving IT infrastructure efficiency.

Difficulties Posed by PCI Non-Compliance

PCI SSC also points to potentially disastrous results of failing to meet PCI Compliance. After working to build your brand and secure customers, don't take a chance with their sensitive information. By meeting PCI Compliance, you are protecting your customers so they can continue to be your customers. Possible results of PCI Non-Compliance include:

- Compromised data that negatively impacts consumers, merchants, and financial institutions.
- Severely damaging your reputation and your ability to conduct business effectively, not just today, but into the future.
- Account data breaches that can lead to catastrophic loss of sales, relationships, and community standing; plus, public companies often see depressed share price as result of account data breaches.
- Lawsuits, insurance claims, canceled accounts, payment card issuer fines, and government fines.

PCI Compliance, as with other regulatory requirements, can pose challenges to organizations that are not prepared to deal with protecting critical information. But, protecting data is a much more manageable task with the right software and services. Choose a data loss prevention software that accurately classifies data and uses it appropriately so you can rest more easily knowing that your cardholder data is secure.