PCI Compliance Checklist

Fall 2021

Table of Contents

Introduction

The Payment Card Industry Data Security Standard (PCI DSS) facilitates and enhances information security for cardholder data. It seeks to encourage the broad adoption of consistent data security measures around the world.

PCI DSS offers a baseline of twelve (12) technical and operational requirements to use as an essential part of an organization's validation process during a compliance assessment.

These requirements apply to all organizations, including merchants, processors, acquirers, issuers, and service providers, that are involved in the following activities:

- Payment card processing
- Storing, processing, or transmitting cardholder data (CHD)
- Storing, processing, or transmitting sensitive authentication data (SAD)

PCI DSS comprises a minimum set of requirements for protecting account data. In many cases, additional controls and practices are required to mitigate the full range of security risks. Further, legislation or regulatory requirements may require additional protections for specific data elements such as a cardholder's name.

This checklist provides a high-level overview of the 12 PCI DSS requirements. More detailed guidelines for each requirement, including a list of best practices, can be found in this report on the PCI Security Standards Council website.

PCI Compliance with VGS

Expedite PCI compliance by never storing sensitive data

Whether you're launching a new business that requires PCI certification or managing your own PCI CDE, VGS can help. The VGS Zero Data™ Platform allows companies to operate on sensitive data without touching it, accelerating compliances like PCI DSS and helping businesses scale faster.

Click here for more information.

Build and Maintain a Secure Network and Systems

1. Protect cardholder data with a firewall

Firewalls control network traffic between your internal enterprise networks and outside, untrusted networks. They examine data packets, block communications that do not meet specified security criteria, and deny access to unauthorized communications.

A firewall also controls traffic between more and less sensitive areas of your internal enterprise network. For PCI, it protects the cardholder data environment (CDE). Firewalls guard many possible paths that an attacker may use to attempt accessing your network, including wired connections, wireless networks, email, and web surfing.

You must include any system component (hardware or software) that provides firewall functionality for your CDE in your PCI scope and assessment.

2. Change vendor-supplied default passwords and parameters

Hackers love low-hanging fruit. Default passwords and default configurations are well-known vulnerabilities in security circles. Before password-guessing or brute-forcing an account, attackers will simply try to access your network via publicly available information, such as vendor default settings.

Always change these vendor-supplied defaults for operating systems, applications, security software, point-of-sale (POS) terminals, payment applications, and system services such as Simple Network Management Protocol (SNMP). Further, remove or disable unneeded default accounts before installing any system on your network. Even if you do not intend to use a default account, it is best to change its default password to a strong unique password before you disable it.

Protect Cardholder Data

3. Protect stored cardholder data

If an attacker successfully circumvents your security controls and breaks into your enterprise, they may access your sensitive information. In this case, a defense-in-depth strategy can still save the day. There are ways to ensure that, even if stolen, your data remains unreadable and unusable to the attacker.

There are certain types of data, such as a cardholder's full primary account number (PAN), that you should always avoid collecting, storing, or transmitting in the clear. Some examples of risk mitigation opportunities for cardholder data protection include encryption, truncation, masking, and hashing.

4. Encrypt transmission of cardholder data

To gain privileged access to your CDE, attackers take advantage of misconfigured wireless networks and exploit vulnerabilities in insecure encryption and authentication protocols. Network-based attacks occur in open, public spaces via wireless technologies such as 802.11 and Bluetooth, cellular networks, and more.

Secure transmission of cardholder data over open public networks requires strong cryptography, secure protocols, secure configurations, trusted keys, and trusted certificates. Sensitive information must be encrypted so that attackers cannot read the data while in transit or use it if they can capture it.

Maintain a Vulnerability Management Program

5. Defend against malware and keep antivirus up-to-date

Malware refers to a range of malicious software such as viruses, worms, trojans, and backdoors. Attackers use a wide variety of strategies and tactics to install malware on your network, from computer hacking to social engineering.

To varying degrees, everything is vulnerable, including corporate servers, mobile devices, and remote storage. Enterprise users may find malware on any website, in their email inbox, or on social media.

You must install, maintain, and regularly update antivirus and anti-malware software on all systems commonly affected by malware (particularly personal computers and servers) and all systems that lie within your PCI scope. These programs can detect and remove many classes of malware and help to prevent data compromise.

6. Develop and maintain secure systems and applications

Within your organization's information infrastructure, vulnerabilities are defined as weaknesses in design, posture, procedures, controls, or implementation that make your organization susceptible to a security threat, hazard, or harm. By exploiting one or more of these vulnerabilities, attackers seek to gain unauthorized, privileged access to your systems and network.

To successfully address a large class of these vulnerabilities, keep vendor-provided software security patches up to date for all of your systems. Patches must frequently be evaluated and tested to ensure that they do not compromise existing security configurations. Vulnerabilities may be avoided only by studying and mastering secure coding techniques for software written within your organization.

Implement Strong Access Control Measures

7. Restrict access to cardholder data by need-to-know

Within the information security discipline, you should adhere to the "principle of least privilege." This rule states that your human employees, and their computers, should be given access only to the resources they need to perform their legitimate work.

Your organization must have security policies and procedures to ensure that critical information such as cardholder data is accessible only to authorized personnel, systems, and processes.

A "need-to-know" policy is based on job responsibilities and grants rights to the least number of authorized people and systems required to perform a given task or function.

8. Identify and authenticate access to system components

Within your organization's information domain, you must enforce accountability. Each person should be assigned a unique identification number. All actions taken on critical systems, and all access of sensitive data, should be traceable to authorized users and processes.

This requirement applies to all accounts used to view or access cardholder data, including point-of-sale accounts, administrative access accounts, and those used by vendors and other third parties. It does not apply to consumer accounts, including cardholders. Depending on your use-case, it may not apply to user accounts within a point-of-sale payment application which only has access to one card number at a time.

9. Restrict physical access to cardholder data

Physical access controls, including personnel badges, help to prevent unauthorized persons from gaining access to your CDE, where they can steal, disrupt, disable, or destroy devices and sensitive data. Similarly, when your employees step away from their computers, locking console screens helps to prevent the malicious tampering of sensitive information, or system configurations. This requirement covers electronic and paper copies of information.

Physical access to sensitive areas, especially the CDE, must be limited to authorized personnel, enforced with appropriate facility controls, and monitored with video cameras. You should store collected data for at least three months (unless otherwise restricted by law), and correlate it with other data such as computer log files. This requirement does not apply to public-facing areas where only POS terminals are present.

Regularly Monitor and Test Networks

10. Monitor access to network resources and cardholder data

To determine the nature, extent, cause, and impact of a computer incident or data compromise, it is critical to maintain and to analyze log files of system activity, throughout your entire critical information infrastructure. Log files record information about users, operating systems, applications, time, type, and sometimes the content of their activities. Logs are invaluable in supporting proactive and reactive security efforts.

Common types of computer log files include “events” (e.g. logins and account lockouts), “transactions” (e.g. database modifications), and “messages” (e.g. textual communication). One widely-used standard is called syslog, which facilitates the generation, recording, tracking, filtering, alerting, and analysis of log messages.

11. Regularly test security systems and processes

The information security environment is always changing. Security researchers and black hat hackers regularly discover new vulnerabilities, build new exploits, and demonstrate that computer security threats never disappear. They simply evolve over time.

In part, this is true because your organization is also always changing, constantly introducing new hardware, software, employees, and data. Therefore, everything, including your human resources and procedures, must be tested frequently, in order to ensure that your security controls continue to be effective in such a dynamic environment.

Maintain an Information Security Policy

12. Maintain an information security policy for all personnel

The importance of information security must be clearly articulated to everyone in your organization. Each employee should know that they play a critical role in protecting sensitive data. Strong security policies set the tone for your whole enterprise, and remind personnel that they are individually responsible for helping to achieve and maintain the technical and operational requirements of the Payment Card Industry Data Security Standard (PCI DSS).

Here, the term “personnel” refers to full-time, part-time, and temporary employees, as well as contractors and consultants who are “resident” on your organization's premises. Further, it refers to any person who has access to your CDE.