PCI Audit Program
# PCI Data Security Audit

## Table of Contents

PCI Compliance Security Audit Program .................................................................................................................... 2

Introduction ........................................................................................................................................................ 2

Policy - Sensitive Information Policy - Credit Card, Social Security, Employee, and Customer Data.................. 3

Policy – Record Management, Retention, and Disposition Policy ................................................................. 3

PCI DSS Applicability Information ....................................................................................................................... 4

Scope of Assessment for Compliance with PCI DSS Requirements ................................................................. 5

Instructions and Content for Report on Compliance .......................................................................................... 7

Revalidation of Open Items ................................................................................................................................ 8

Build and Maintain a Secure Network .................................................................................................................... 9

Requirement 1: Install and maintain a firewall configuration to protect cardholder data .................................. 9

Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters. ................................................................................................................................................................... 14

Protect Cardholder Data ................................................................................................................................... 18

Requirement 3: Protect stored cardholder data ........................................................................................... 18

Requirement 4: Encrypt transmission of cardholder data across open, public networks .................................. 26

Maintain a Vulnerability Management Program .............................................................................................. 28

Requirement 5: Use and regularly update anti-virus software or programs ................................................ 28

Requirement 6: Develop and maintain secure systems and applications ..................................................... 29

Implement Strong Access Control Measures .................................................................................................... 34

Requirement 7: Restrict access to cardholder data by business need-to-know ............................................. 34

Requirement 8: Assign a unique ID to each person with computer access. ................................................... 35

Requirement 9: Restrict physical access to cardholder data. ....................................................................... 41

Regularly Monitor and Test Networks .............................................................................................................. 46

Requirement 10: Track and monitor all access to network resources and cardholder data. ............................ 46

Requirement 11: Regularly test security systems and processes. ................................................................. 50

Maintain an Information Security Policy .......................................................................................................... 53

Requirement 12: Maintain a policy that addresses information security for employees and contractors. 53

Appendix A: PCI DSS Applicability for Hosting Providers (with Testing Procedures) ................................. 60

Requirement A.1: Hosting providers protect cardholder data environment .................................................. 60

Appendix B – Compensating Controls .............................................................................................................. 63

Compensating Controls – General ................................................................................................................. 63

Compensating Controls for Requirement 3.4 .................................................................................................. 63

Appendix C: Compensating Controls Completed Example/Worksheet ............................................................ 64

Compensating Controls Worksheet .............................................................................................................. 65

What’s New ...................................................................................................................................................... 67
PCI Compliance Security Audit Program

Introduction

The PCI Security Audit Procedures\(^1\) are designed for use by assessors conducting onsite reviews for merchants and service providers required to validate compliance with the Payment Card Industry (PCI) Data Security Standard (DSS) requirements. The requirements and audit procedures presented in this document are based on the PCI DSS and the most recent set of privacy mandates – including GDPR.

This document contains the following:

- Introduction
- Policy – Sensitive Information
- Policy – Record Management, Retention, and Disposition
- PCI DSS Applicability Information
- The scope of Assessment for Compliance with PCI DSS Requirements
- Instructions and Content for Report On Compliance
- Revalidation of Open Items
- Security Audit Procedures
- Appendices
  - Appendix A: PCI DSS Applicability for Hosting Providers (with Testing Procedures)
  - Appendix B: Compensating Controls
  - Appendix C: Compensating Controls Worksheet/Completed Example

With ever-increasing requirements placed by government legislatures and regulatory agencies, there are often competing and conflicting data retention/disposition requirements. For this reason, we have provided “draft” policies when can be utilized to create a customized “Sensitive Information Policy” and a “Record Management, Retention, and Disposition Policy.”

---

\(^1\) Portions of this test program were extracted from the published PCI requirements and have been enhanced by Janco Associates, Inc. Note we are not attorneys and do not express any legal nor PCI standards opinion in this document. The use of this audit program should consult with their own legal and PCI compliance staff.
PCI DSS Applicability Information

The following table illustrates commonly used elements of the cardholder and sensitive authentication data; whether the storage of each data element is permitted or prohibited; and if each data element must be protected. This table is not exhaustive but is presented to illustrate the different types of requirements that apply to each data element. At the same time compliance to Record Retention and Disposition standards (see https://www.e-janco.com/recordmanagementpolicy.html) needs to be coordinated with the PCI DSS requirements. A Sensitive Information policy (see https://www.e-janco.com/sensitive.htm) for the enterprise should be implemented.

<table>
<thead>
<tr>
<th>Data Element</th>
<th>Storage Permitted</th>
<th>Protection Required</th>
<th>PCI DSS Requirement 3.4</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Cardholder Data</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Primary Account Number (PAN)</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Cardholder Name*</td>
<td>Yes</td>
<td>Yes*</td>
<td>No</td>
</tr>
<tr>
<td>Service Code*</td>
<td>Yes</td>
<td>Yes*</td>
<td>No</td>
</tr>
<tr>
<td>Expiration Date</td>
<td>Yes</td>
<td>Yes*</td>
<td>No</td>
</tr>
<tr>
<td><strong>Sensitive Authentication Data</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Full Magnetic Stripe</td>
<td>No</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>CVC2/CVV2/CID</td>
<td>No</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>Pin / Pin Block</td>
<td>No</td>
<td>N/A</td>
<td>N/A</td>
</tr>
</tbody>
</table>

* These data elements must be protected if stored in conjunction with the PAN (Primary Account Number). This protection must be consistent with PCI DSS requirements for general protection of the cardholder environment. Additionally, other legislation (for example, related to consumer personal data protection, privacy, identity theft, or data security) may require specific protection of this data or proper disclosure of a company’s practices if consumer-related personal data is being collected during business operations. PCI DSS, however, does not apply if PANs are not stored, processed, or transmitted.

** Sensitive authentication data must not be stored subsequent to authorization (even if encrypted).
The scope of Assessment for Compliance with PCI DSS Requirements

The PCI DSS security requirements apply to all “system components.” A system component is defined as any network component, server, or application that is included in or connected to the cardholder data environment. The cardholder data environment is that part of the network that possesses cardholder data or sensitive authentication data. Network components include but are not limited to firewalls, switches, routers, wireless access points, network appliances, and other security appliances. Server types include but are not limited to the following: web, database, authentication, mail, proxy, network time protocol (NTP), and domain name server (DNS). Applications include all purchased and custom applications, including internal and external (internet) applications.

Adequate network segmentation, which isolates systems that store, process, or transmit cardholder data from the rest of the network, may reduce the scope of the cardholder data environment. The assessor must verify that the segmentation is adequate to reduce the scope of the audit.

A service provider or merchant may use a third party provider to manage components such as routers, firewalls, databases, physical security, and/or servers. If so, there may be an impact on the security of the cardholder data environment. The relevant services of the third party provider must be scrutinized either in:

1. Each of the third party provider's clients' PCI audits; or
2. The third party provider's own PCI audit.

For service providers required to undergo an annual onsite review, compliance validation must be performed on all system components where cardholder data is stored, processed, or transmitted unless otherwise specified.

For merchants required to undergo an annual onsite review, the scope of compliance validation is focused on any system(s) or system component(s) related to authorization and settlement where cardholder data is stored, processed, or transmitted, including the following:

- All external connections into the merchant network (for example; employee remote access, payment card company, third party access for processing, and maintenance)
- All connections to and from the authorization and settlement environment (for example, connections for employee access or for devices such as firewalls and routers)
- Any data repositories outside of the authorization and settlement environment where more than 500 thousand account numbers are stored. Note: Even if some data repositories or systems are excluded from the audit, the merchant is still responsible for ensuring that all systems that store, process, or transmit cardholder data are compliant with the PCI DSS
- A point-of-sale (POS) environment – the place where a transaction is accepted at a merchant location (that is, retail store, restaurant, hotel property, gas station, supermarket, or other POS location)
- If there is no external access to the merchant location (by the Internet, Wi-Fi, Bluetooth, a virtual private network (VPN), dial-in, broadband, or publicly accessible machines such as kiosks), the POS environment may be excluded.

**Wireless**

If wireless technology is used to store, process, or transmit cardholder data (for example, point-of-sale transactions, “line-busting”), or if a wireless local area network (LAN) is connected to or part of the cardholder environment (for example, not clearly separated by a firewall), the Requirements and Testing Procedures for wireless environments apply and must be performed.
**PCI Data Security Audit**

**Build and Maintain a Secure Network**

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

Firewalls are computer devices that control computer traffic allowed into and out of a company’s network, as well as traffic into more sensitive areas within a company’s internal network. A firewall examines all network traffic and blocks those transmissions that do not meet the specified security criteria.

All systems must be protected from unauthorized access from the Internet, whether entering the system as e-commerce, employees’ Internet-based access through desktop browsers, or employees’ e-mail access. Often, seemingly insignificant paths to and from the Internet can provide unprotected pathways into key systems. Firewalls are a key protection mechanism for any computer network.

<table>
<thead>
<tr>
<th>PCI DSS Requirements</th>
<th>Testing Procedures</th>
<th>In Place</th>
<th>Not in Place</th>
<th>Target Date/Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>1.1</strong> Establish firewall configuration standards that include the following:</td>
<td><strong>1.1</strong> Obtain and inspect the firewall configuration standards and other documentation specified below to verify that standards are complete. Complete each item in this section</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>1.1.1</strong> A formal process for approving and testing all external network connections and changes to the firewall configuration</td>
<td><strong>1.1.1a</strong> Verify that a formal process for approving and testing all external network connections and changes to the firewall configuration exists</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>1.1.1b</strong> Verify that security policies are in place to control changes to the firewall.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>1.1.1c</strong> Verify that logs are in place and are actively being monitored</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>1.1.2</strong> A current network diagram with all connections to cardholder data, including any wireless networks</td>
<td><strong>1.1.2a</strong> Verify that a current network diagram exists and verify that it documents all connections to cardholder data, including any wireless networks</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>1.1.2b</strong> Verify that the diagram is kept current</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
What's New

Version 3.1
- Updated to meet the latest privacy and security requirements

Version 3.0
- Update to meet the latest requirements
- Updated graphics

Version 2.1
- Added Policy – Sensitive Information
- Updated tables

Version 2.0
- Added Policy – Record Management, Retention, and Disposition
- Modified style sheet and format to be CSS compliant
- Modified audit program to be compliant to the two added policies