



**COAST GUARD
MORALE
WELL-BEING
AND
RECREATION PROGRAM**

**PAYMENT CARD INDUSTRY (PCI)
COMPLIANCE WORKBOOK**

**PCI SAQ TYPE B
Level 4**

Stand-Alone Terminals

31 December 2011

COPYRIGHT NOTICE

Copyright © 2008-2011 by TurboPCI, Inc.

All rights reserved. No part of this TurboPCI Easy™ Workbook or the accompanying TurboPCI Easy™ Workbook CD may be reproduced or transmitted in any form by any means, electronic, mechanical or otherwise, including recording, or by any information storage and retrieval system, without the prior written consent of TurboPCI, Inc. The Products are for internal use of the purchaser or TurboPCI, Inc. authorized users of this workbook only.

To request permission or obtain additional information, please contact TurboPCI, Inc. at (407) 282-1300.

This TurboPCI Easy™ Workbook, the accompanying TurboPCI Easy™ Workbook CD and any accompanying seminar have been prepared to provide the purchaser with information on the topics covered in the workbook. The workbook is being provided with the understanding that TurboPCI, Inc. is not engaged, nor do the TurboPCI Easy™ Workbook or the accompanying TurboPCI Easy™ Workbook CD provide, legal advice or any other professional services. The TurboPCI Easy™ Workbook, the accompanying TurboPCI Easy™ Workbook CD and any accompanying seminar are not intended to be, and should not be used as a substitute for seeking professional services or advice.

Copyright © 2008-2011 TurboPCI, Inc. All rights reserved.



Warning: The unauthorized reproduction or distribution of this copyrighted work is illegal. Criminal copyright infringement, including infringement without monetary gain, is investigated by the FBI and is punishable by up to 5 years in federal prison and a fine of \$250,000.

TABLE OF CONTENTS

Introduction.....	2
Chapter 1: What is PCI DSS?	4
<i>The Payment Card Industry Security Standards Council.....</i>	<i>4</i>
<i>The Payment Card Industry Data Security Standard (PCI DSS)</i>	<i>4</i>
<i>Who Must Comply and Why.....</i>	<i>5</i>
<i>Reporting PCI DSS Compliance.....</i>	<i>6</i>
<i>Who Do You Report To?.....</i>	<i>6</i>
Chapter 2: How Does PCI DSS Affect You and Your MWR Program?	7
<i>Merchant Level Classification.....</i>	<i>7</i>
<i>SAQ Types for Merchant Levels 2, 3 and 4.....</i>	<i>8</i>
<i>SAQ B</i>	<i>8</i>
Chapter 3: SAQ B (Stand-Alone Terminal Merchants)	9
<i>What Do You Have To Prove?</i>	<i>9</i>
<i>Step-By-Step Instructions.....</i>	<i>10</i>
Chapter 4: Staying Compliant.....	Error! Bookmark not defined.
Appendix A: Definitions.....	25
Appendix B: List of Policies and PCI Templates.....	30

INTRODUCTION

This workbook is designed to provide an easy, cost-effective solution for compliance with the Payment Card Industry Data Security Standard (PCI DSS). It is written for MWR Programs accepting credit/debit cards who do not use a networked computer system to process their patrons' credit/debit cards. The authors, Dr. Suzanne Miller and E. G. "Buddy" Coley, Jr., are Qualified Security Assessors who are trained and certified by the Payment Card Industry Security Standards Council.

The TurboPCI™ Easy Workbook is divided into two parts. Part 1, "PCI DSS - What's It All About", introduces you to the Payment Card Industry, their requirements and who is responsible for overseeing your compliance. Part 2, "PCI DSS – Steps to Compliance", covers how your Coast Guard MWR Program may be classified under the PCI DSS and leads you through the steps you need to take for compliance.

A list of the provided PCI DSS policies and templates is found in Appendix B.

In addition to all the things you will learn in this text, Part 2 of the workbook has alert features designed to trigger necessary actions from you:

ALERT KEY	
	PCI Requirement
	Necessary Step

PCI DSS - What's It All About?

Before you begin your compliance work, there are some basic facts we need to cover.

In this section we will talk about the history and the basics of the Payment Card Industry Data Security Standard, commonly referred to as PCI DSS.

CHAPTER 1

What is PCI DSS?

In this chapter

- ✓ Understand what PCI DSS is
- ✓ Learn why it was established
- ✓ Discover how it affects you
- ✓ See who verifies your PCI DSS compliance

The Payment Card Industry Security Standards Council

In order to understand the Payment Card Industry Data Security Standard (PCI DSS), we begin by giving a brief history of how it came to be. Before 2006 all payment card brands, (such as Visa, MasterCard, Discover, JCB and American Express) had created and were individually managing their own programs to fight credit/debit card fraud. As credit/debit card fraud increased, costs to the brands reached billions of dollars. The brands realized they needed to band together to develop enforceable and consistent standards to protect payment card information. The Payment Card Industry Security Standards Council (PCI SSC) was formed from this united front.

Today, the PCI SSC dictates three best-practice security standards for payment card information, card swiping devices, and applications that process, store or transmit payment card information. These best-practice security standards are called the Payment Card Industry Data Security Standard (PCI DSS), Payment Application Data Security Standard (PA-DSS) and Pin Transaction Standard (PTS). These standards affect:

- merchants who accept credit/debit card information, commonly called *cardholder data*; and
- companies that have access to cardholder data from merchants because they provide services to those merchants. These service companies are called *service providers* or *processors*.

The PCI SSC also developed two certification programs for their Standards:

- **QSA** – The Qualified Security Assessor Program trains and certifies information security professionals to be experts in understanding, protecting and evaluating the use of cardholder data.
- **ASV** – The Authorized Scanning Vendor Program is designed to train and certify companies in checking for vulnerabilities that the PCI SCC deems as necessary for compliance.

For more information about the PCI SSC, visit www.pcisecuritystandards.org.

The Payment Card Industry Data Security Standard (PCI DSS)

The PCI DSS consists of twelve basic requirements. Each requirement has sub-requirements. Some of these requirements and sub-requirements may not apply to your MWR Program. The next section

tells you must comply with the PCI DSS and why. The rest of this workbook will tell you exactly which requirements MWR Program must meet.

The twelve basic requirements are:

1. Install and maintain a firewall configuration to protect cardholder data
2. Don't use vendor-supplied defaults for system passwords and other security parameters
3. Protect stored cardholder data
4. Encrypt transmission of cardholder data across open, public networks
5. Use and regularly update anti-virus software or programs
6. Develop and maintain secure systems and applications
7. Restrict access to cardholder data by business need to know
8. Assign a unique ID to each person with computer access
9. Restrict physical access to cardholder data
10. Track and monitor all access to network resources and cardholder data
11. Regularly test security systems and processes
12. Maintain a policy that addresses information security for all personnel

For complete documentation of the PCI DSS requirements and sub-requirements, you can download the latest version of the PCI Data Security Standard Version 2.0 from www.pcisecuritystandards.org.

Who Must Comply and Why

All merchants, service providers, financial institutions, and transaction processors who process, store, or transmit cardholder data are required to comply with the PCI DSS. How your MWR Program processes cardholder data determines which of the requirements apply to your MWR Program. To become compliant, you need to follow the procedures set by the PCI SSC for every requirement that applies to your MWR Program.

Because the PCI DSS is a complex document, we have written this workbook to lead you through the necessary steps for your MWR Program to become compliant. If you can't meet a requirement by following the steps in the workbook, you will need to develop your own steps for meeting the requirement, and a timetable for completing the steps. This is called a remediation plan. In the documents you are required to use for reporting compliance, you will see a section referred to as "Remediation Date and Actions (if Compliance Status is NO)". If you haven't successfully completed your plan by the time you have to report your compliance, you will have to report the steps you created and the dates you've set for completion to your MWR Program Resources Specialist in Chesapeake, Virginia and/or the Loss Prevention Director in Chesapeake, immediately.

As a merchant if you do not comply with the PCI DSS, the brands will take necessary action against your MWR Program. Also, if credit/debit card fraud or identity theft occur because your MWR Program was not compliant at the time of the incident, the brands will hold your MWR Program

responsible. Your MWR Program will be subjected to financial penalties and legal action, not to mention severe loss of reputation. The brands can even take away the ability for your MWR Program to process credit/debit cards for payment.

Reporting PCI DSS Compliance

All units accepting credit/debit cards as a source of payment are required to report their compliance every year. There are two ways to report: you can complete a Self-Assessment Questionnaire (SAQ), or you can have an onsite audit by a QSA (Qualified Security Assessor).

Based on how you process credit/debit cards, the Coast Guard Community Services Command has determined that SAQ B is right for you and that you do not need an onsite audit by a QSA.

Who Do You Report To?

As a merchant, you signed a contract with a bank, credit union, merchant services company or an independent sales organization (*ISO*). In the payment card industry, these companies are referred to as *acquirers*. The brands have made the acquirers responsible for making sure merchants are compliant with the PCI DSS. If you have not already heard from your acquirer, they will be contacting you. Your acquirer is responsible for yearly reviewing and keeping a copy of your AOC.

CHAPTER 2

How Does PCI DSS Affect You and Your MWR Program?

In this chapter

- ✓ Learn how to classify your MWR Program
- ✓ Discover what you need to do to be compliant
- ✓ Discover how PCI DSS compliance affects you
- ✓ Find out how often you need to verify compliance

Merchant Level Classification

Each brand established their own method for classifying merchants. The classification is based on the number of transactions a merchant processes yearly. Below is Visa's classification for merchant levels. These levels are:

Level 1

Merchants who process greater than 6 million transactions a year

Level 2

Merchants who process at least 1 million but less than 6 million transactions per year

Level 3

eCommerce (Internet website) merchants who process at least 20,000 but less than 1 million transactions a year

Level 4

eCommerce merchants who process less than 20,000 transactions a year, and all other merchants who process up to 1 million transactions a year

If you aren't sure which level applies to your MWR Program, contact your provider.

It has been determined that your MWR Program is a LEVEL 4.

If you feel your MWR Program is not a Level 4 merchant, contact the MWR Program Resources Specialist in Chesapeake, VA and/or the Loss Prevention Director in Chesapeake immediately.

Merchants who are Level 2, 3 or 4 are required to fill out and submit a SAQ on an annual basis. However, if a Level 2, 3 or 4 merchant has a security breach that endangers cardholder data, the merchant must have an onsite audit by a QSA. Additionally, a brand or acquirer can require your MWR Program to have an onsite audit by a QSA at any time.

SAQ Types for Merchant Levels 2, 3 and 4

If you are using this workbook, it has been determined that your MWR Program is a Merchant Type SAQ B. The SAQ Merchant Type identifies for you the PCI DSS requirements that apply to your MWR Program and the SAQ you are required to fill out annually.

SAQ B

To use SAQ B (Stand-Alone Terminal Merchants), ALL of the following must be true:

- Ⓒ Your MWR Program does not store credit/debit card information electronically.
- Ⓒ Your MWR Program uses a stand-alone terminal or card swipe machine connected by phone line to your credit/debit card processor.
- Ⓒ Your stand-alone equipment which is connected by phone to your credit/debit card processor is not connected to any other systems within your MWR Program.
- Ⓒ Your stand-alone equipment which is connected by phone to your credit/debit card processor is not connected to the Internet.

After reviewing the above statements, if you feel your MWR Program does not fit into the SAQ B (Stand-Alone Terminal Merchants) classification, contact the Coast Guard MWR Program Resources Specialist in Chesapeake, VA and/or the Loss Prevention Director in Chesapeake immediately to determine your MWR Program's correct SAQ type.

If you feel your MWR Program does not meet a requirement, contact the Coast Guard MWR Program Resources Specialist in Chesapeake, VA and/or the Loss Prevention Director in Chesapeake.

Most businesses have a binder, notebook, or other way of keeping all of the master copies of official business policies and procedures together in one place. Throughout the workbook we will tell you to make certain policies and procedures are part of your formal MWR Program documents. Make sure you are retaining copies in your compliance binder.

Now that you know how to determine your MWR Program's compliance, you are ready to begin the PCI DSS compliance work. Turn the page to Part 2 of this workbook which leads you through every step necessary for your MWR Program to obtain and maintain PCI DSS compliance.

CHAPTER 3

SAQ B (Stand-Alone Terminal Merchants)

In this chapter

- ✓ Learn the step-by-step tasks you must do
- ✓ Find out how to create the necessary policies, procedures and forms
- ✓ Learn how to complete your SAQ
- ✓ Learn how to maintain your compliance documents

What Do You Have To Prove?

You need to meet the following PCI DSS Requirements. (Remember that you need to keep records that prove you're *in* compliance, and that you're *staying* in compliance.)

Requirement 3: Protect stored cardholder information

- Sections: 3.2, 3.2.1, 3.2.2, 3.2.3, 3.3

Requirement 4: Encrypt transmission of cardholder information across open, public networks

- Section: 4.2

Requirement 7: Restrict access to cardholder information by business need to know

Section: 7.1, 7.1.1, 7.1.2

Requirement 9: Restrict physical access to cardholder information

Sections: 9.6, 9.7, 9.7.1, 9.7.2, 9.8, 9.9, 9.10, 9.10.1

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

Sections: 12.1, 12.1.3, 12.3, 12.3.1, 12.3.3., 12.3.5, 12.4, 12.5, 12.5.3, 12.6, 12.8, 12.8.1, 12.8.2, 12.8.3, 12.8.4

Step-By-Step Instructions

Your Program's MWR Director/Officer will act as the PCI compliance officer within your MWR Program. This person will be responsible for leading your PCI DSS compliance. The MWR Director/Officer, and any staff assisting them, should be familiar with the policies and templates listed in Appendix B. These policies and templates are available on the Coast Guard MWR website at www.uscg.mil/mwr.

You will specifically need the following policies and templates:

Policies – 1000, 1010, 1200, 1300, 1700

PCI Templates – 1001, 1002, 1003, 1004, 1005, 1302, 1303, 1304, 1902

Your MWR Program will also need a compliance binder where you will keep all of the documents that prove you are meeting the requirements. Every document you retain in your compliance binder needs to be kept for at least 6 years and 3 months to provide proof that your MWR Program is maintaining compliance.

In the step-by-step instructions you will first be given the requirements and then the steps you have to take to meet these requirements. If a requirement doesn't apply to your MWR Program, or if your MWR Program uses a compensating control to meet any requirement(s), notify the MWR Program Resources Specialist or the CSC Loss Prevention Director in Chesapeake immediately.

NOTE: If you cannot meet a requirement, contact the MWR Program Resources Specialist or the CSC Loss Prevention Director in Chesapeake, VA.

Step-By-Step Instructions

📖 **Requirement 3.2 - Do not store sensitive authentication data subsequent to authorization (even if encrypted). Sensitive authentication data includes the data as cited in the following Requirements 3.2.1 through 3.2.3:**

📖 **Requirement 3.2.1 - Do not store the full contents of any track from the magnetic stripe (from the magnetic stripe on the back of a card, equivalent data contained on a chip, or elsewhere). This data is alternatively called full track, track, track 1, track 2, and magnetic stripe data.**

📖 **Requirement 3.2.2 - Do not store the card-verification code or value (three-digit or four-digit number printed on the front or back of a payment card) used to verify card-not-present transactions.**

📖 **Requirement 3.2.3 - Do not store the personal identification number (PIN) or the encrypted PIN block.**

☞ **Step 1:** Use PCI Template 1902 - Hardware System Components – Process Cardholder Data to make a list of all of the devices that your MWR Program uses to swipe your patron's credit/debit cards. To finish the form, go to pcisecuritystandards.org and click on "Approved Companies and Providers". Then go to "Approved PIN Transaction Security Devices" and look for each device your MWR Program uses. If your devices are on there, they're compliant. Put the completed form in your compliance binder.

☞ **Step 2:** Find out if the application you're using is PCI DSS compliant. Log into pcisecuritystandards.org and go to "Approved Companies and Providers". Then go to "Validated Payment Applications" and look for each application your MWR Program uses. If your applications are on there, they're compliant.

☞ **Step 3:** If any of your devices or applications aren't compliant, you need to contact your vendor to update your equipment or software. If possible, get a statement from your vendor that says the equipment or application they provided to you doesn't capture full track data. Label the top right corner of the statement with '3.2', and put it in your compliance binder. If you can't get a statement from your vendor, you'll need to have your computer system analyzed by a professional to make sure that data from the magnetic stripe isn't being stored. You aren't compliant unless you have proof.

☞ **Step 4:** Make sure you aren't keeping paper copies of the three-digit or four-digit card-validation codes printed on the front of debit/credit cards or near the signature panel. Make sure you aren't keeping paper copies of your customers' credit/debit card pin numbers as well.

NOTE: If you cannot meet a requirement, contact the MWR Program Resources Specialist or the CSC Loss Prevention Director in Chesapeake, VA.

Check if you're compliant with Requirement 3.2 _____

Check if you're compliant with Requirement 3.2.1 _____

Check if you're compliant with Requirement 3.2.2 _____

Check if you're compliant with Requirement 3.2.3 _____

Requirement 3.3 – Mask PAN when displayed. (The first six and last four digits are the maximum number of digits to be displayed.)

Step 1: If your application is on the PA-DSS list as PCI compliant, then check the compliant box for this requirement and move on to requirement 4.2 below.

Step 2: If your application isn't PCI compliant, you need to encrypt your data. If you need help, contact the MWR Program Resources Specialist or the CSC Loss Prevention Director in Chesapeake, VA.

Step 3: Once your data is encrypted, capture screen shots of the data to prove it's unreadable.

Step 4: Print, sign and date the screen shots. Label the top right corner of each one with '3.3', and put them in your compliance binder.

Check if you're compliant with Requirement 3.3 _____

Note: Before we move on to Requirement 4.2, Requirement 9, and the rest of Requirement 12, you need to complete the steps for Requirements 12.1 and 12.3.

Requirement 12.1 - Establish, publish, maintain, and disseminate a security policy that accomplishes the following:

Requirement 12.1.3 - Includes a review at least once a year and updates when the environment changes.

Step 1: Review Policy 1000 – Information Security Policy.

NOTE: If you cannot meet a requirement, contact the MWR Program Resources Specialist or the CSC Loss Prevention Director in Chesapeake, VA.

- ☞ **Step 2:** Make Policy 1000 an official document for your MWR Program. Give a copy of it to all employees and contractors (processors and providers).
- ☞ **Step 3:** Make sure you review your Information Security Policy every year, or when your MWR Program environment changes. Record your reviews on PCI Template 1002 – Information Security Policy Review. Keep your Information Security Policy and PCI Templates 1002 in your compliance binder.
- ☞ **Step 4:** Every time the policy is changed, give a copy of the new policy to all employees and contractors.

Check if you're compliant with Requirement 12.1 _____

Check if you're compliant with Requirement 12.1.3 _____

📖 **Requirement 12.3 - Develop usage policies for critical technologies (for example, remote access technologies, wireless technologies, removable electronic media, laptops, tablets, personal data/digital assistants (PDAs), e-mail usage and Internet usage) and define proper use of these technologies. Ensure these usage policies require the following:**

📖 **Requirement 12.3.1 - Explicit approval by authorized parties.**

📖 **Requirement 12.3.3 - A list of all such devices and personnel with access.**

📖 **Requirement 12.3.5 – Acceptable uses of the technology.**

- ☞ **Step 1:** Review Policy 1000 – Security Information Policy to make sure explicit approval by authorized parties is required in order to use the MWR Program's critical employee-facing technologies (see the Definitions for a description of critical employee-facing technologies).
- ☞ **Step 2:** Identify all critical employee-facing technologies. Use PCI Template 1003 – Employee-Facing Technologies List to record the technologies you have identified.
- ☞ **Step 3:** Review Policy 1010 - Acceptable Use Policy. Make sure the technologies you listed on PCI Template 1003 have been included in the policy. If not, make sure you change the Acceptable Use Policy to include the technologies you use in your MWR Program.
- ☞ **Step 4:** Review and update PCI Template 1003 every year. Sign, date and keep a copy of PCI Template 1003 in your compliance binder.
- ☞ **Step 5:** Make sure every employee reads Policy 1010 - Acceptable Use Policy. When they have read it they should sign the certification page, and management should complete and sign

NOTE: If you cannot meet a requirement, contact the MWR Program Resources Specialist or the CSC Loss Prevention Director in Chesapeake, VA.

the “Witnessed by” section at the end. Then put the policy and the certification page(s) in your compliance binder.

- ☞ **Step 6:** Every new employee needs to read Policy 1010 and sign the certification page. The MWR Director/Officer should witness the signature and then put the new certification page with the others in your compliance binder.
- ☞ **Step 7:** Any time changes are made to Policy 1010 – Acceptable Use Policy, you must follow steps 5 and 6 above for the revised policy.

Check if you’re compliant with Requirement 12.3 _____

Check if you’re compliant with Requirement 12.3.1 _____

Check if you’re compliant with Requirement 12.3.3 _____

Check if you’re compliant with Requirement 12.3.5 _____

📖 Requirement 4.2 – Never send unencrypted PANs by end-user messaging technologies (for example, e-mail, instant messaging, chat, etc.).

- ☞ **Step 1:** Make sure Policy 1700 – Encryption of Transmitted Cardholder Data Policy and Policy 1010 – Acceptable Use Policy both say that unencrypted PANs must never be sent by email, instant messaging, chat, etc.
- ☞ **Step 2:** If you need to send sensitive information (especially all 16 digits of a PAN) through e-mail, the information must be encrypted. If your MWR Program uses automatic encryption, then you have to make sure your employees understand this requirement and the steps your MWR Program has taken to encrypt the information. You need to have formal training sessions and use PCI Template 1004 – Employee Training Sign-In Sheet for each session. Keep the sign-in sheets in your compliance binder.
- ☞ **Step 3:** If the encryption isn’t automatic, you must teach your employees how to encrypt e-mails. You have to make a formal list of the steps you take to encrypt the data, and prove that you’ve trained all of your employees on how to do it. Use PCI Template 1004 – Employee Training Sign-In Sheet for each training session. Have every trained employee sign a statement that they understand how and when to encrypt e-mails. Keep the list of steps you created to encrypt the information, the sign-in sheets and the employee confirmation statements in your compliance binder.

NOTE: If you cannot meet a requirement, contact the MWR Program Resources Specialist or the CSC Loss Prevention Director in Chesapeake, VA.

- ☞ **Step 4:** You will need to train every new employee on this requirement. You can use PCI Template 1004 to record the training session. And remember to put the form in your compliance binder.

Check if you're compliant with Requirement 4.2 _____

📖 **Requirement 7.1 – Limit access to system components and cardholder data to only to those individuals whose job requires such access. Access limitations must include the following:**

📖 **Requirement 7.1.1 – Restriction of access rights to privileged user IDs to least privileges necessary to perform job responsibilities.**

📖 **Requirement 7.1.2 – Assignment of privileges is based on individual personnel's job classification and function.**

- ☞ **Step 1:** Review Policy 1200 – Logical Access Policy.

- ☞ **Step 2:** Make Policy 1200 part of your official MWR Program documents. Keep a copy of it in your compliance binder.

Check if you're compliant with Requirement 7.1 _____

📖 **Requirement 9.6 – Physically secure all media.**

- ☞ **Step 1:** Locate all paper and media (such as receipts, notes, reports, faxes, CDs, backup tapes, thumb drives, and hard drives) that contain all 16 digits of your customers' credit/debit card numbers. This 16 digit number is commonly called a PAN. Don't forget that copies of emails and chats are often kept in a "Sent" folder on computers.

- ☞ **Step 2:** Decide if you need to keep the paper and media that contain your customers' full credit/debit card number (PAN). Look at your reasons for keeping the information. You shouldn't keep it if it is not required for your MWR Program. You should also take into account the risks of keeping the information, and the extra steps you have to perform if you going to keep it. See Step 3 and Requirements 9.7, 9.8, 9.9 and 9.10 below.

NOTE: If you cannot meet a requirement, contact the MWR Program Resources Specialist or the CSC Loss Prevention Director in Chesapeake, VA.

- ☞ **Step 3:** All paper and media you decide to keep *must be locked away*. Once you have locked up the items, fill out PCI Template 1302 – Cardholder Data Inventory Log to record the items you’re keeping safe. If you aren’t keeping any paper or media that contain cardholder data, state “We do not retain paper and/or media containing cardholder data” on PCI Template 1302. Be sure to sign and date the form and keep it in your compliance binder.
- ☞ **Step 4:** You’ll have to update this form every year, and whenever your MWR Program environment changes.

Check if you’re compliant with Requirement 9.6 _____

📖 **Requirement 9.7 – Maintain strict control over the internal or external distribution of any kind of media that contains cardholder data, including the following:**

- 📖 **Requirement 9.7.1 - Classify the media so the sensitivity of the data can be determined.**
- 📖 **Requirement 9.7.2 - Send the media by secured courier or other delivery method that can be accurately tracked.**

- ☞ **Step 1:** If you do not keep sensitive cardholder information (see Requirement 9.6 above), this section doesn’t apply to you. Mark it “N/A” and move on.
- ☞ **Step 2:** Identify paper or media listed on PCI Template 1302 – Cardholder Data Inventory Log that could be removed from its secure location.
- ☞ **Step 3:** Create a copy of PCI Template 1303 – Removal Log for Media for each item you identified on PCI Template 1302. You will use PCI Template 1303 to track and log the removal of the paper or media from its secure location.
- ☞ **Step 4:** Before paper or media can be removed from its secure location, it must be marked *Confidential*. Make sure you track and log the removal, copying or transporting of your confidential paper or media on PCI Template 1303.
- ☞ **Step 5:** If your confidential paper or media is transported off the premises you have to use a secure courier, or deliver it by a method that can be tracked (such as the post office). Use PCI Template 1303 to record how the transportation was tracked.

NOTE: If you cannot meet a requirement, contact the MWR Program Resources Specialist or the CSC Loss Prevention Director in Chesapeake, VA.

- ☞ **Step 6:** For convenience, keep a notebook with PCI Template 1302 and all of your copies of PCI Template 1303 with, or close to, the media you've secured. That way you or your employees won't forget to fill out the forms.

Check if you're compliant with Requirement 9.7 _____

Check if you're compliant with Requirement 9.7.1 _____

Check if you're compliant with Requirement 9.7.2 _____

Requirement 9.8 - Ensure management approves any and all media containing cardholder data that is moved from a secured area (especially when media is distributed to individuals).

- ☞ **Step 1:** Make sure PCI Template 1303 – Removal Log for Media is used every time confidential paper or media is removed from its secure location. The log must be signed by The MWR Director/Officer *before* removing the paper or media.
- ☞ **Step 2:** Sign and date PCI Template 1303 and keep it in a notebook with, or close to, the media you've secured.

Check if you're compliant with Requirement 9.8 _____

Requirement 9.9 – Maintain strict control over the storage and accessibility of media that contains cardholder data.

- ☞ **Step 1:** You'll need Policy 1300 – Physical Access Policy.
- ☞ **Step 2:** Note that Policy 1300 requires visitors to be identified with badges or tokens, but not employees. *If your employees aren't wearing badges, a visitor can easily remove his or her badge and will no longer be easily identified as a visitor.* Best-practice for companies with a large number of employees would be to issue your employees badges or other tokens that identify them as employees, and issue visitors a different kind of badge or token. It's a good idea to change Policy 1300 to add these requirements if visitors can't be easily identified without a badge or token.

NOTE: If you cannot meet a requirement, contact the MWR Program Resources Specialist or the CSC Loss Prevention Director in Chesapeake, VA.

- ☞ **Step 3:** Make Policy 1300 part of your official MWR Program documents, and put it in your compliance binder.

☞ Check if you're compliant with Requirement 9.9 _____

📖 **Requirement 9.10 – Destroy media containing cardholder data when it is no longer needed for business or legal reasons as follows:**

📖 **Requirement 9.10.1 - Shred, incinerate, or pulp hardcopy materials so that cardholder data cannot be reconstructed.**

- ☞ **Step 1:** Identify the paper or media containing cardholder data that you want to destroy.
- ☞ **Step 2:** Use PCI Template 1304 – Media Destruction Log to record the description of paper or media you have identified to destroy. If you are using holding containers to accumulate these papers or media, make sure they are secured with a lock to prevent access.
- ☞ **Step 3:** Once the paper or media is destroyed, record the date of destruction and how you destroyed it on PCI Template 1304. Make sure the person who was in charge of the destruction signs PCI Template 1304 to certify that the information on the destroyed paper or media can't be recovered.
- ☞ **Step 4:** The MWR Director/Officer needs to sign and date the bottom of PCI Template 1304, then put it in your compliance binder.

☞ Check if you're compliant with Requirement 9.10 _____

☞ Check if you're compliant with Requirement 9.10.1 _____

📖 **Requirement 12.4 – Ensure that the security policy and procedures clearly define information security responsibilities for all personnel.**

- ☞ **Step 1:** This requirement is met in Policy 1010 – Acceptable Use Policy.

☞ Check if you're compliant with Requirement 12.4 _____

NOTE: If you cannot meet a requirement, contact the MWR Program Resources Specialist or the CSC Loss Prevention Director in Chesapeake, VA.

Requirement 12.5 - Assign to an individual or team the following information security management responsibilities:

Requirement 12.5.3 - Establish, document, and distribute security incident response and escalation procedures to ensure timely and effective handling of all situations

Step 1: Refer to Commandant Instruction 5260.5, Privacy Incident Response, Notification and Reporting Procedures for Personally Identifiable Information (PII).

Step 2: Train your staff regarding Commandant Instruction 5260.5.

Step 3: Remember to train any new team members as they are assigned.

Check if you're compliant with Requirement 12.5 _____

Check if you're compliant with Requirement 12.5.3 _____

Requirement 12.6 - Implement a formal security awareness program to make all employees aware of the importance of cardholder data security.

Step 1: Refer to Commandant Instruction 5260.5, Privacy Incident Response, Notification and Reporting Procedures for Personally Identifiable Information (PII).

Step 2: Train your staff regarding Commandant Instruction 5260.5.

Step 3: Remember to train any new team members as they are assigned.

Check if you're compliant with Requirement 12.6 _____

NOTE: If you cannot meet a requirement, contact the MWR Program Resources Specialist or the CSC Loss Prevention Director in Chesapeake, VA.

- 📖 **Requirement 12.8 – If cardholder data is shared with service providers, maintain and implement policies and procedures to manage service providers, to include the following:**
 - 📖 **Requirement 12.8.1 – Maintain a list of service providers.**
 - 📖 **Requirement 12.8.2 – Maintain a written agreement that includes an acknowledgement that the service providers are responsible for the security of cardholder data the service providers possess.**
 - 📖 **Requirement 12.8.3 – Ensure there is an established process for engaging service providers including proper due diligence prior to engagement.**
 - 📖 **Requirement 12.8.4 – Maintain a program to monitor service providers’ PCI DSS compliance status.**
- ☞ **Step 1:** Make sure you don’t sign a contract with a service provider, processor or acquirer without making sure that the company is PCI DSS compliant. They should provide you with a copy of their yearly Attestation of Compliance (AOC).
- ☞ **Step 2:** Make sure you have a written contract with every company and person you share cardholder data with. The contract must say that these companies or people are responsible for protecting your customers’ cardholder data. (Don’t forget any company you might use to destroy papers or media.) Use PCI Template 1001 – Contract Review for PCI Security Policy to record your review of new service provider contracts. Keep copies of your contracts and your reviews in your compliance binder.
- ☞ **Step 3:** Read Policy 1000 – Information Security Policy. Make a list of who you share your customers’ cardholder data with on PCI Template 1005 – Service Provider Review List. Be sure to include all companies, and people who are not your employees. If you don’t share cardholder data right now, write “We do not share cardholder data” on PCI Template 1005 and put it in your compliance binder. Then read through the next steps to find out what you will have to do if your MWR Program needs to share cardholder data in the future.
- ☞ **Step 4:** Update the list of your service providers on PCI Template 1005 every time you sign a new contract, or an old one expires. Make sure you review and monitor every one of your service providers’ PCI DSS compliance status on a regular basis. Getting a copy of their AOC every year is the most cost-effective way to monitor their compliance. Use PCI Template 1001 – Contract Review for PCI Security Policy to record your review of service provider contracts. Log your review or monitoring on PCI Template 1005. Keep copies of PCI Template 1005 and 1001, and your providers’ annual AOCs in your compliance binder

NOTE: If you cannot meet a requirement, contact the MWR Program Resources Specialist or the CSC Loss Prevention Director in Chesapeake, VA.

Check if you're compliant with Requirement 12.8 _____

Check if you're compliant with Requirement 12.8.1 _____

Check if you're compliant with Requirement 12.8.2 _____

Check if you're compliant with Requirement 12.8.3 _____

Check if you're compliant with Requirement 12.8.4 _____

Once you have checked off all the requirements in this chapter you are ready to fill out your SAQ. You're required to complete and submit a new SAQ every year, and whenever your MWR Program changes how it processes cardholder information.

You have completed the Step-By-Step instructions.

Filling Out Your SAQ

You will use SAQ B. You may have been given the SAQ. If not, you must download it. Go to the pcisecuritystandards.org website. Click on “PCI Standards and Documents” in the bar across the top. Then click on “Documents Library” on the left. Scroll down to “PCI DSS New Self Assessment Questionnaire (SAQ)”. Find “SAQ B v2.0” and download it.

Open the file you downloaded. It’s called “pci_saq_b_v2.doc”. Read the entire document before you fill anything in.

Part 1a: Fill in all the information:

- Company Name should be the name of your Unit’s Morale Fund Account
- If you are not doing business under any other name, enter *N/A* for DBA(s) (doing business as).
- If you do not have an email address, enter *N/A* for E-mail.
- If you do not have a website, enter *N/A* for URL.

Part 1b: Do not fill out this section. If you worked with a QSA, they may want to fill out this section for you.

Part 2: Check the “Retail” box and list all the locations in your Program where you have a credit card machine (i.e., bowling alley, Club, ITT).

Part 2a: Check the “No” box for the first question. Check the appropriate box for the second question.

Part 2b: Answer the question “How does your business store, process and/or transmit cardholder data?”. A example answer would be “We do not store cardholder data. We use stand-alone terminals for processing.”

In the following table, insert the name and version number of your payment application. Visit www.pcisecuritystandards.org website to confirm that your payment application is PCI-compliant. Once at the website, click on the tab “Approved Companies and Providers”. Once you have read the page that appears, click on “Accept” at the bottom. Use the search bar, or find your application alphabetically. Insert the “Revalidation Date” into the SAQ column “Last Validated According to PABP/PA-DSS”. NOTE: If your payment application is NOT listed at the www.pcisecuritystandards.org website, contact the Coast Guard MWR Program Resources Specialist in Chesapeake, VA and/or the Loss Prevention Director in Chesapeake immediately.

Part 2c: If you performed all the steps in this workbook chapter and checked all the requirement boxes “Yes” or “N/A” in this workbook, then check all the boxes in this section. NOTE: If your MWR Program is NOT compliant, contact the Coast Guard MWR Program Resources Specialist in Chesapeake, VA and/or the Loss Prevention Director in Chesapeake immediately.

Part 3: If you performed all the steps in this workbook chapter and checked all the requirement boxes “Yes” or “N/A” in this workbook, then check the “Compliant” box. NOTE: If your MWR Program is NOT compliant, contact the Coast Guard MWR Program Resources Specialist in Chesapeake, VA and/or the Loss Prevention Director in Chesapeake immediately.

Part 3a: If you performed all the steps in this workbook chapter and checked all the requirement boxes “Yes” or “N/A” in this workbook, then check all the boxes in this section. NOTE: If your MWR Program is NOT compliant, contact the Coast Guard MWR Program Resources Specialist in Chesapeake, VA and/or the Loss Prevention Director in Chesapeake immediately. Insert the correct version of the SAQ found on the cover of the SAQ.

Part 3b: The Unit Commanding Officer, or his/her designee, must sign as the Merchant Executive Officer. *Note: The term ‘merchant’ refers to any business, or your MWR Program, that accepts credit/debit cards as forms of payment from their customers.* Type in the Unit Commanding Officer’s name (or his/her designee), title, and the date in this section.

Part 4: If you performed all the steps in this workbook chapter and checked all the requirement boxes “Yes” or “N/A” in this workbook, then check all the “Yes” boxes in this section. NOTE: If your MWR Program is NOT compliant, contact the Coast Guard MWR Program Resources Specialist in Chesapeake, VA and/or the Loss Prevention Director in Chesapeake immediately.

Self-Assessment Questionnaire B Section: Insert the date of completion. Check all the appropriate boxes. Your response to these boxes should match the requirements you checked when you completed the Step-By-Step Instructions within this workbook.

Now that you have completed your SAQ B, send a copy of the entire SAQ to the Coast Guard MWR Program Resources Specialist in Chesapeake, VA. Keep the original SAQ along with your annual and quarterly evidence in your compliance binder for your merchant services, bank or acquirer. You are required to retain a copy of this document for a period of no less than 6 years, 3 months.

Congratulations! Now visit Chapter 4 to learn more about how your MWR Program can stay compliant throughout the year.

CHAPTER 4

Staying Compliant

In this chapter

- ✓ Discover techniques for maintaining compliance
- ✓ Learn the importance of staying compliant

It is very important for your MWR Program to be able to prove compliance at all times. You must understand that **compliance is a process, not an event!** If a breach should occur, you can reduce or eliminate liability if you can prove that you were compliant at the time of the breach. So, it is very important that you follow all the steps in this workbook and keep your compliance binder up-to-date.

We have found the best way to maintain compliance is to set up a compliance calendar. As you learned in the step-by-step instructions, there are things you need to do every quarter and every year. Review the steps and create your own calendar. It will be a valuable tool for you to stay on course with compliance.

Definitions

Acquirer: An Acquirer is a Visa/MasterCard Affiliated Bank or Bank/Processor alliance that is in the business of processing credit card transactions for businesses and is always acquiring new merchants.

Application: A software program that is designed to perform a specific function on a computer system. Examples would be accounting systems, manufacturing systems, order entry and fulfillment, ticketing, reservations, etc. The application is either purchased or built by the merchant, and must be interfaced with a credit card authorization system in order to provide on-line transaction processing.

Authorization: The process of verifying the credit card has sufficient funds (credit) available to cover the amount of the transaction. An authorization is obtained for every sale. An approval response in the form of a code sent to a merchant's POS equipment (usually a terminal) from a card issuing financial institution that verifies availability of credit or funds in the cardholder account to make the purchase. Also see Point-Of-Sale.

Authorization Code: A code that a credit card issuing bank returns in an electronic message to the merchant's POS equipment that indicates approval of the transaction. The code serves as proof of authorization.

Bankcard: A credit card issued by a Visa or MasterCard-sponsored financial institution. (American Express, Discover, Diners Club, JCB, etc., are issued directly from their respective operations, rather than through banks.)

Best-Practice: a standard way of doing things that multiple organizations can use for management, policy, and especially software systems.

Brand: A term frequently used in the Credit Card Industry that typically references a single credit card association such as: American Express, Visa, MasterCard, JCB or Discover.

Capture: The submission of an electronic credit card transaction for financial settlement. Authorized credit card sales must be captured and settled in order for a merchant to receive funds for those sales. Also see Settlement.

Cardholder: Any person who holds a payment card account (bankcard or otherwise) or that uses a credit card to purchase goods and services.

Cardholder Data: Sensitive cardholder information printed on the front and back of the card and stored in the magnetic stripe on the back of the card.

Card Issuing Bank: An EFT Network Member-Bank that runs a credit card or debit card "purchasing service" for their account holders. An example is Citibank and the Citibank Visa Card that they issue.

Card Not Present: A transaction where the card isn't present at the time of the transaction (such as mail order or telephone order). Credit card data is manually entered into the terminal, as opposed to swiping a card's magnetic stripe through the terminal.

Card Slip: A form showing an obligation on the cardholder's part to pay money (i.e., the sales amount) to the card issuer. This is the piece of paper that is signed when making the purchase. Sales draft data can be captured electronically and sent to be processed over the phone lines. Also see Electronic Data Capture.

CNP: Stands for Card Not Present.

Compensating Controls: Compensating controls may be considered when an entity cannot meet a requirement explicitly as stated, due to legitimate technical or documented business constraints but has sufficiently mitigated the risk associated with the requirement through implementation of other controls.

Compliance Binder: Binder for merchants that serves as a repository to store compliance reports and support documentation. The Binder can be ordered through the TurboPCI.com website.

Critical Employee-Facing Technology: Devices such as modems and wireless technology that must have usage policies defined for the proper use of these technologies for all employees and contractors.

Debit Card: Payment card whose funds are withdrawn directly from the cardholder's checking account at the time of sale (online debit on a Debit Network) or after batch settlement (off-line debit on a Credit Card Network).

Electronic Data Capture (EDC): Process of electronically authorizing, capturing and settling a credit card transaction.

External Network Connection: A term used to convey that a line/service has been installed externally to a merchant's network.

Full Track Data: The data that is written into the black stripe located on the back of a credit card. The data is commonly referred to as full tracked data. Full tracked data contains highly sensitive information such as: cardholder name, account number, and card expiration date.

Hosting Provider: Services offered to merchants and other service providers that range from simple to complex; from shared space on a server to a whole range of "shopping cart" options; from payment applications to connections to payment gateways and processors; and for hosting dedicated to just one customer per server.

Independent Sales Organization (ISO): An ISO is an Independent Sales Organization that represents a Bank or Bank/Processor alliance. The ISO has an agreement to sell the services of the Bank or Bank/Processor alliance, and is allowed to mark up the Fees and sign up merchants. These entities are classic Middle Men, as they are typically not performing the services sold. They typically match the banking services they sell with "Front End" solutions for accepting transactions in order to offer merchants a working system. Their Front End Systems can be anything from VeriFone or Hypercom POS Terminals to PC based Dial-Out Credit Card Processing Software, to Shopping Carts

paired with a Secure Payment Gateway. (In all cases, the Front End solution must be compatible with the Processor in order to function.)

Internet Service Provider (ISP): Internet Service Providers (ISPs) are Website Hosting companies that provide a home for a merchant's website. They typically resell and/or support the services of a Secure Gateway Provider and/or ISO or Agent or Bank.

Issuing Financial Institution: The financial institution that extends credit to a cardholder through bankcard accounts. The financial institution issues a credit card and bills the cardholder for purchases against the bankcard account. Also referred to as the cardholder's financial institution.

Merchant: A business which accepts credit/debit cards from customers for payment.

Magnetic Stripe: A strip of magnetic tape affixed to the back of credit cards containing identifying data, such as account number and cardholder name.

Mail Order/Telephone Order (MOTO): Credit card transactions initiated via mail, email or telephone. Also known as card-not-present transactions.

Network: Company and system used to authorize and capture credit card transactions.

PC Application Software: A software program that is designed to perform a specific function on a computer system. Examples would be accounting systems, manufacturing systems, order entry and fulfillment, ticketing, reservations, etc. The application is either purchased or built by the merchant, and must be interfaced with a credit card authorization system in order to provide on-line transaction processing.

Payment Application Data Security Standard (PA-DSS): PCI Security Standards Council-managed program formerly under the supervision of the Visa Inc. program known as the Payment Application Best Practices (PABP). The goal of PA-DSS is to help software vendors and others develop secure payment applications that don't store prohibited data, such as full magnetic stripe, CVV2 or PIN data, and ensure their payment applications support compliance with the PCI DSS.

Payment Card Industry Data Security Standard (PCI DSS): A set of comprehensive requirements for enhancing payment account data security, which was developed by the founding payment brands of the PCI Security Standards Council, including American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa Inc., to help facilitate the broad adoption of consistent data security measures on a global basis.

Payment Card Industry Security Standards Council (PCI SSC): An open global forum established for the ongoing development, enhancement, storage, dissemination and implementation of security standards for account data protection.

Payment Card Industry Qualified Security Assessor (PCI QSA): A certification obtained by experienced security consultants to enable them to conduct the On-Site Data Security Assessment for PCI DSS Compliance. QSAs are required to re-certify every year by attending training by PCI and passing the exam. A re-certifying QSA must obtain additional CPE's from training and other experiences in order to obtain certification.

Primary Account Number (PAN): Primary Account Number is the payment card number (credit or debit) that identifies the issuer and the particular cardholder account. Also called account number.

Point Of Sale (POS): A location where credit card transactions are performed with the cardholder present, such as a retail store. The card is read magnetically, and the cardholder's signature is obtained as insurance against the transaction. This is the most secure form of credit card commerce.

POS Terminal: Equipment used to capture, transmit and store credit card transactions at the point of sale. Examples are VeriFone terminals.

Processor: A Processor is the company that actually routes an Authorization Request from a Point of Sale device (such as a VeriFone credit card terminal) to Visa or MasterCard, and then arranges for Fund Settlement to the merchant. Such processors are traditionally accessed via direct dial out modems connecting to their system. Processors need to have a Sponsoring Bank in order to gain access to the Visa and MasterCard networks. When a Processor or other entity has made such an arrangement with a Sponsoring Bank to resell their services, they are called an Agent of that bank. Any entity that sells Visa or MasterCard must disclose themselves as an Agent of their Sponsoring Bank. Such sales entities may be a Processor, or an ISO/Agent of the Processor or Processor/Bank alliance. Many banks are also their own processors, while other banks will use a Third Party Processor to handle this processing for them (in their own brand name in some cases).

Security Officer: The security officer is responsible for the development, implementation and management of the information security. They direct staff in identifying, developing, implementing and maintaining security processes across the company to reduce risks, respond to incidents, and limit exposure to liability in all areas of financial, physical, and personal risk; establish appropriate standards and risk controls associated with intellectual property; and direct the establishment and implementation of policies and procedures related to data security.

Service Provider: Acquirers, third party processors (TPPs), data storage entities (DSEs) or any other entity that stores, processes, or transmits cardholder data.

Software: A POS Terminal Application or PC or Internet Application that runs transactions and associated administration.

Sponsoring Bank: A Sponsoring Bank is a Chartered Bank or S & L (Savings & Loan) that has obtained membership in Visa or MasterCard in order to allow a Processor access to the Visa and MasterCard networks (in order to process these types of transactions). Since only a Bank may join Visa or MasterCard, many Processors make deals with a Sponsoring Bank in order to gain access to the Visa and MasterCard networks. Because these Sponsoring agreements are usually like a partnership, the line between the Sponsoring Banks and their Processors isn't always clear; sometimes the partnership is referred to by the name of the bank, while at other times they are referred to by the name of the Processor.

Terminal: Equipment used to capture, transmit and store credit card transactions.

Third-Party Processor: A Third Party Processor is an independent processor that is contracted with by a Bank or Processor to conduct some part of the transaction processing process. Some of these Third Party Processors specialize in running and hosting networks of Point Of Sale (POS) terminals

connected to their Host via dial out modem; they produce the software in the POS terminals as well as in their host, and route authorization requests to Visa or MasterCard as needed (MAPP, MDI, FDR, for example). Other Third Party Processors specialize in the Settlement of credit card transactions with Visa and MasterCard so that merchants can be paid (FDR for example). In the world of Internet Credit Card Processing, the Secure Payment Gateway Provider is another type of Third Party Processor.

APPENDIX B

Below is a complete listing of the policies and templates provided.

Policies

Policy 1000 - Information Security Policy

Policy 1010 - Acceptable Use Policy

Policy 1200 - Logical Access Policy

Policy 1300 - Physical Access Policy

Policy 1700 - Encryption of Transmitted Cardholder Data Policy

PCI Templates

PCI Template 1001 - Contract Review – PCI Security Policy

PCI Template 1002 - Information Security Policy Review

PCI Template 1003 - Employee-Facing Technologies List

PCI Template 1004 - Employee Training Sign In Sheet

PCI Template 1005 - Service Provider Review List

PCI Template 1302 - Cardholder Data Inventory Log

PCI Template 1303 - Removal Log for Media

PCI Template 1304 - Media Destruction Log

PCI Template 1902 - Hardware System Components – Process Cardholder Data