PA DSS Implementation Guide for Childcare Manager V10 Users

© 2009 - 2011 by Personalized Software, all rights reserved

The Payment Application Data Security Standard (PA DSS) requires payment applications, like Childcare Manager, that are used to store, process, or transmit payment card information, to meet specific requirements designed to protect the security of cardholder data. These requirements are derived from the Payment Card Industry Data Security Standard (PCI DSS). Each application must go through a rigorous assessment and testing by a Qualified Security Assessor and the application must be validated by the Assessor as PA DSS-compliant before it can be used by a merchant. Childcare Manager is a PA DSS compliant payment card application.

A PA DSS-compliant application alone, however, is no guarantee of PCI DSS compliance. PCI DSS compliance comes from operating a PA DSS-compliant application in a PCI DSS-compliant environment. Our responsibility as a software vendor is to ensure Childcare Manager facilitates rather than prevents you as a merchant to meet the requirements identified in the PCI DSS. Your responsibility as the merchant is to ensure that Childcare Manager is operated in a PCI DSS-compliant environment. Only secure payment applications implemented in a PCI DSS-compliant environment can minimize the potential for security breaches leading to compromises of full magnetic stripe data, card validation codes and values, PINs and PIN blocks, and the damaging fraud resulting from these breaches.

If you use Childcare Manager at your center, this guide and the standards included within it apply to you. Failure to comply with these standards can result in significant fines should a security breach occur. This Implementation Guide has been prepared to help you minimize potential security breaches by providing you with the knowledge necessary to implement Childcare Manager in a PCI DSS-compliant environment.

Thank you for chosing Childcare Manager to fulfill your management and accounting needs and for using RapidTuition to fulfill your electronic payment processing needs.

Table of Contents

Foreword 0

Part I Introduction 3

Part II What You Need To Do To Be PCI DSS-Compliant 4

Part III What You Need To Do To Be PA DSS-Compliant 9

Part IV Windows Security 14

1 Windows Security Best Practices ... 15
2 Password Policy ... 15
3 Account Lockout Policy ... 15
4 Screensaver Lockout Policy ... 16

Part V Resources 16

Part VI Glossary of Terms, Abbreviations & Acronyms 18

Index 0

© 2009 - 2011 by Personalized Software, all rights reserved

1 Introduction

The Payment Card Industry defines a set of requirements that are applicable to merchants (you), software application vendors (Childcare Manager), service providers and acquirers (ECHO), and financial institutions. These requirements the configuration, operation, and security of payment card transactions Data Security Standard (PCI DSS) and Payment Application Data Security Standard (PA DSS)

The Payment Card Industry Data Security Standard describes 12 requirements designed to secure system components (servers, network, applications, etc.) that support cardholder data environments. PCI DSS requirements apply to all system components that are 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, including network components, servers and applications. These requirements are the shared responsibility of merchants, like yourself, service providers, software vendors and financial institutions.

The PA DSS requires payment applications, like Childcare Manager, that are used to store, process, or transmit payment card information, to meet specific requirements designed to protect the security of cardholder data. These requirements are derived from the PCI DSS. Each application must go through a rigorous assessment and testing by a Qualified Security Assessor and the application must be validated by the Assessor as PA DSS-compliant before it can be used by a merchant. Childcare Manager is a PA DSS compliant payment card application.

A PA DSS-compliant application alone is no guarantee of PCI DSS compliance. PCI DSS compliance comes from operating a PA DSS-compliant application in a PCI DSS-compliant environment. Our responsibility as a software vendor is to ensure Childcare Manager facilitates rather than prevents you as a merchant to meet the requirements identified in the PCI DSS. Your responsibility as the merchant is to ensure that Childcare Manager is operated in a PCI DSS-compliant environment. Only secure payment applications implemented in a PCI DSS-compliant environment can minimize the potential for security breaches leading to compromises of full magnetic stripe data, card validation codes and values, PINs and PIN blocks, and the damaging fraud resulting from these breaches.

If you use Childcare Manager at your center, this guide and the standards included within it apply to you. Failure to comply with these standards can result in significant fines should a security breach occur. This *Implementation Guide* has been prepared to help you minimize potential security breaches by providing you with the knowledge necessary to implement Childcare Manager in a PCI DSS-compliant environment.

This guide is updated whenever there are changes in Childcare Manager which affect the PCI-DSS, and is also updated annually to reflect changes in Childcare Manager as well as the PCI standards. Please visit Childcare Manager's secure payment gateway website at http://www.rapidtuition.com for the latest version of this guide.

> **Note:** This guide refers to Childcare Manager Version 10. Older versions of Childcare Manager do not include the capability to process payment card transactions. You must be covered by an active support plan or extended support plan, and be in the latest version of the software, to ensure that you are in compliance.

© 2009 - 2011 by Personalized Software, all rights reserved

2 What You Need To Do To Be PCI DSS-Compliant

The table below provides a list of the 12 PCI DSS requirements, a brief summary of what each requirement says, and what Childcare Manager users should do to be compliant with these requirements.

A more detailed description of the 12 requirements, along with guidance to explain the intent of each requirement can be found in *Navigating PCI DSS --- Understanding the Intent of the Requirements*. *Navigating PCI DSS* is intended to assist merchants, service providers, and financial institutions who may want a clearer understanding of the Payment Card Industry Data Security Standard, and the specific meaning and intention behind the detailed requirements to secure system components (servers, network, applications etc) that support cardholder data environments.

You can obtain this document at:
https://www.pcisecuritystandards.org/pdfs/pci_dss_saq_navigating_dss.pdf

Payment Card Industry (PCI) Data Security Standard (DSS) Requirements			
PCI DSS Number/Topic		**What the Requirement Says**	**What You Need to Do To Be Compliant**
#1	Install and maintain a firewall configuration to protect the cardholder.	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.	To be PCI DSS-compliant, Childcare Manager users should: ➢ install and maintain a router-based firewall at the point of entry to your network or firewall software on all network computers use at your center. Your firewall should be configured to block unauthorized traffic.

© 2009 - 2011 by Personalized Software, all rights reserved

Payment Card Industry (PCI) Data Security Standard (DSS) Requirements			
PCI DSS Number/Topic		**What the Requirement Says**	**What You Need to Do To Be Compliant**
#2	Do not use vendor supplied defaults for system passwords and other security parameters.	Hackers (external and internal to a company) often use vendor default passwords and other vendor default settings to compromise systems. These passwords and settings are well known in hacker communities and easily determined via public information.	To be PCI DSS-compliant, Childcare Manager users should: ➢ create unique usernames and passwords for both your Windows accounts and for Childcare Manager. ➢ use complex passwords, especially for administrator accounts. Childcare Manager requires the use of Users Manager by default when you enroll in RapidTuition. Authentication is enabled and users must have individual accounts and passwords. If you disable Users Manager you are not in compliance.
#3	Protect stored cardholder data.	Encryption is a critical component of cardholder data protection. If an intruder circumvents other network security controls and gains access to encrypted data, without the proper cryptographic keys, the data is unreadable and unusable to that person. Other effective methods of protecting stored data should be considered as potential risk mitigation opportunities. For example: methods for minimizing risk include not storing cardholder data unless absolutely necessary; truncating cardholder data if full PAN (credit card number) is not	To be PCI DSS-compliant, Childcare Manager users should: ➢ regularly change your passwords, especially for your administrator account, to ensure that your passwords cannot be easily compromised. ➢ immediately change your passwords if you suspect that your passwords or database has been compromised. ➢ never store credit card numbers or sensitive

© 2009 - 2011 by Personalized Software, all rights reserved

Payment Card Industry (PCI) Data Security Standard (DSS) Requirements			
PCI DSS Number/Topic		**What the Requirement Says**	**What You Need to Do To Be Compliant**
		needed; not sending PAN in unencrypted e-mails. cardholder data.	data in data fields that are not designed to store this data, e.g., custom fields.
#4	Encrypt Transmission of Cardholder Data Across Open, Public Networks.	Sensitive information must be encrypted during transmission over networks that are easy and common for a hacker to intercept, modify, and divert data while in transit.	To be PCI DSS-compliant, Childcare Manager users should: ➢ maintain a secure internal network and protect sensitive cardholder data prior to entry into the computer.
#5	Use and Regularly Update Anti-Virus Software.	Many vulnerabilities and malicious viruses enter the network via employees' e-mail activities. Anti-virus software must be used on all systems commonly affected by viruses to protect systems from malicious software.	To be PCI DSS-compliant, Childcare Manager users should: ➢ install and maintain antivirus software, firewall software, and any other security software which helps to protect your computer. ➢ always make sure that this software is up to date, as security threats change often and new threats are introduced regularly.
#6	Develop and Maintain Secure Systems and Applications.	Unscrupulous individuals use security vulnerabilities to gain privileged access to systems. Many of these vulnerabilities are fixed by vendor-provided security patches. All systems must have the most recently released, appropriate software patches to protect against exploitation by employees, external hackers, and viruses. **Note:** Appropriate software	To be PCI DSS-compliant, Childcare Manager users should: ➢ ensure that Childcare Manager is always covered by a current support plan or extended support plan. ➢ keep your system up to date with software updates, operating system updates, and

© 2009 - 2011 by Personalized Software, all rights reserved

Payment Card Industry (PCI) Data Security Standard (DSS) Requirements			
PCI DSS Number/Topic		**What the Requirement Says**	**What You Need to Do To Be Compliant**
		patches are those patches that have been evaluated and tested sufficiently to determine that the patches do not conflict with existing security configurations. For in-house developed applications, numerous vulnerabilities can be avoided by using standard system development processes and secure coding techniques.	any other security patches ➢ enable the auto update feature in Childcare Manager to ensure that you have the latest version.
#7	Restrict Access to Cardholder Data by Business Need-To-Know.	This requirement ensures critical data can only be accessed by authorized personnel.	To be PCI DSS-compliant, Childcare Manager users should: ➢ configure Childcare Manager's Users Manager to only give access rights to those who need it.
#8	Assign a Unique ID to Each Person With Computer Access.	Assigning a unique identification (ID) to each person with access ensures that actions taken on critical data and systems are performed by, and can be traced to, known and authorized users.	To be PCI DSS-compliant, Childcare Manager users should: ➢ set up a unique Users Manager user account for each user of Childcare Manager ➢ do not share user accounts. ➢ set up unique user accounts in Windows. ➢ change user passwords at least every 90 days.
#9	Restrict Physical Access to Cardholder Data.	Any physical access to data or systems that house cardholder data provides the opportunity for individuals to access devices or data and to remove systems or hard copies, and should be appropriately restricted.	To be PCI DSS-compliant, Childcare Manager users should: ➢ physically secure your computers and Childcare Manager's database.

© 2009 - 2011 by Personalized Software, all rights reserved

Payment Card Industry (PCI) Data Security Standard (DSS) Requirements			
PCI DSS Number/Topic		**What the Requirement Says**	**What You Need to Do To Be Compliant**
			➢ **Special note**: If you use recurring credit card charge authorization forms and physically store these forms, you need to ensure that these forms are stored in a secure place and accessible only by those authorized to do so.
#10	Track and Monitor All Access to Network Resources and Cardholder Data.	Logging mechanisms and the ability to track user activities are critical. The presence of logs in all environments allows thorough tracking and analysis when something does go wrong. Determining the cause of a compromise is very difficult without system activity logs.	To be PCI DSS-compliant, Childcare Manager users should: ➢ never disable the C2 audit mode in Microsoft SQL Server. Childcare Manager uses this function to meet the requirement to track and monitor access to your network resources and to help you find the source of a security breach if one happens.
#11	Regularly Test Security Systems and Processes.	Vulnerabilities are being discovered continually by hackers and researchers, and being introduced by new software. Systems, processes, and custom software should be tested frequently to ensure security is maintained over time and with any changes in software.	To be PCI DSS-compliant, Childcare Manager users should: ➢ test your network connections (including wireless networks) periodically for vulnerabilities ➢ make use of network vulnerability scans at least quarterly to check for any problems. If you make any significant changes to your network, you should also test for

© 2009 - 2011 by Personalized Software, all rights reserved

Payment Card Industry (PCI) Data Security Standard (DSS) Requirements			
PCI DSS Number/Topic		**What the Requirement Says**	**What You Need to Do To Be Compliant**
			vulnerabilities. Please visit https://www.pcisecuritystandaards.org for more information.
#12	Maintain a Policy that Addresses Information Security for Employees and Contractors.	A strong security policy sets the security tone for the whole company and informs employees what is expected of them. All employees should be aware of the sensitivity of data and their responsibilities for protecting it.	To be PCI DSS-compliant, Childcare Manager users should: ➢ Maintain a written policy outlining employee responsibilities for being aware of and protecting sensitive cardholder data ➢ Review your security settings and network configuration at least once a year, or any time there is a change in your business or employees. ➢ restrict employees that no longer work at your business from accessing your network or the Childcare Manager software.

3 What You Need To Do To Be PA DSS-Compliant

The table below provides a list of PA DSS requirements that have been identified for inclusion in this *Implementation Guide*. The table also describes what Childcare Manager does to meet these requirements and what you need to do to be compliant with these requirements when you use Childcare Manager.

A more detailed description of these requirements can be found in Appendix A of the *Payment Application Data Security Standard.* You can obtain this document at: https://www.pcisecuritystandards.org/security_standards/pci_pa_dss.shtml

© 2009 - 2011 by Personalized Software, all rights reserved

Payment Application Data Security Standard (PA DSS) Requirements			
PA DSS Number/Topic		**What Childcare Manager Does For You**	**What You Need to Do To Be Compliant**
1.1.4	Delete sensitive authentication data stored by previous payment application versions.	There is never any need to remove historical data because Childcare Manager does not store or process any sensitive authentication data.	CHILDCARE MANAGER USERS ARE AUTOMATICALLY COMPLIANT
1.1.5	Delete sensitive authentication data (pre-authorization) gathered as a result of troubleshooting the payment application.	There is never any need to delete sensitive pre-authorization authentication data because Childcare Manager does not store or process any sensitive pre-authorization authentication data.	CHILDCARE MANAGER USERS ARE AUTOMATICALLY COMPLIANT
2.1	Purge cardholder data after customer-defined retention period.	There is never any need to purge cardholder data, because Childcare Manager does not store or process any sensitive cardholder data.	CHILDCARE MANAGER USERS ARE AUTOMATICALLY COMPLIANT.
2.7	Delete cryptographic key material or cryptograms store by previous payment application versions.	There is never any need to delete cryptographic key material or cryptograms because cryptographic key material and cryptograms are not used in Childcare Manager.	CHILDCARE MANAGER USERS ARE AUTOMATICALLY COMPLIANT.
3.1	Use unique user IDs and secure authentication for administrative access and access to cardholder data.	Childcare Manager controls administrative access to the program with a function called Users Manager. Users Manager allows the center to assign specific user rights to program users and to control their access through the use of unique user IDs and secure complex password authentication. Childcare Manager includes a Childcare Manager passwords are encrypted using SHA-1 cryptographic hash functions	To be PA DSS-compliant, Childcare Manager users should: ➢ ensure Users Manager is enabled; Disabling the Users Manager will result in non-compliance with PCI DSS. ➢ not use group, shared, or generic accounts and passwords. ➢ change user passwords at least every 90 days. ➢ require a minimum password length of at

© 2009 - 2011 by Personalized Software, all rights reserved

Payment Application Data Security Standard (PA DSS) Requirements			
PA DSS Number/Topic		**What Childcare Manager Does For You**	**What You Need to Do To Be Compliant**
		which were designed by the National Security Agency (NSA). SHA-1 is the best established of the existing SHA hash functions, and is employed in several widely used security applications and protocols. Childcare Manager also logs the user out when a session is idle for more than 15 minutes. The user must re-enter his or her password to reactivate the program.	least seven characters. ➢ use passwords containing both numeric and alphabetic characters. ➢ not allow an individual to submit a new password that is the same as any of the last four passwords he or she has used.
3.2	Use unique user IDs and secure authentication for access to PCs, servers, and databases with payment applications.	Childcare is designed for use on a PC and using Microsoft Windows operating systems.	To be PA DSS-compliant, Childcare Manager users should: ➢ configure Window to password access to Windows ➢ configure Windows account lockout policies ➢ configure windows to lock your computer after your computer has been idle for a period of time and when the screensaver is active. For a detailed account on how to use these security features see Password Policy, Account Lockout Policy and Screensaver Lockout Policy in Windows Security.
4.2	Implement automated audit trails.	Childcare Manager automatically activates the Microsoft SQL Server C2 audit mode for Childcare Manager	To be PA DSS-compliant, Childcare Manager users should:

© 2009 - 2011 by Personalized Software, all rights reserved

Payment Application Data Security Standard (PA DSS) Requirements			
PA DSS Number/Topic		**What Childcare Manager Does For You**	**What You Need to Do To Be Compliant**
		users. Activating this option configures SQL Server Express to record PA DSS required critical user activities.	➢ Ensure logs remain enabled. Disabling the logs will result in non-compliance with PCI DSS.
6.1	Securely implement wireless technology.	Childcare Manager is designed for secure use over both wired and wireless networks.	To be PA DSS-compliant, Childcare Manager users should: ➢ use a firewall. We recommend using both a hardware firewall and software firewall for maximum security. For laptops, a software firewall is highly recommended if you travel with the laptop. ➢ not use WEP (wired equivalent privacy), as it is considered insecure and can easily be circumvented. ➢ encrypt all wireless transmissions by using WiFi protected access (WPA or WPA2) technology, or SSL/ TLS. ➢ change the wireless vendor defaults, including but not limited to, default service set identifier (SSID), passwords, and Simple Network Management protocol (SNMP) community strings. Disable SSID broadcasts. ➢ install personal firewall software on any mobile and employee-owned

© 2009 - 2011 by Personalized Software, all rights reserved

Payment Application Data Security Standard (PA DSS) Requirements			
PA DSS Number/Topic		**What Childcare Manager Does For You**	**What You Need to Do To Be Compliant**
			computers with direct connectivity to the Internet (for example, laptops used by employees), which are used to access the organization's network. ➢ never use default settings or passwords for your wireless devices, as these settings are easily discovered through the public domain. Always change the default settings and passwords for your wireless network before you begin using Childcare Manager in a wireless environment.
6.2	Secure transmissions of cardholder data over wireless networks.	See 6.1 above.	See 6.1 above.
9.1	Store cardholder data only on servers not connected to the Internet.	There is never a need to store cardholder data on servers in the DMZ (demilitarized zone) or not connected to the Internet because Childcare Manager does not store or process any cardholder data.	CHILDCARE MANAGER USERS ARE AUTOMATICALLY COMPLIANT.
10.1	Securely deliver remote payment application updates.	All Childcare Manager updates delivered over the Internet are sent over secure SSL.	To be PA DSS-compliant, Childcare Manager users should: ➢ receive remote Childcare Manager updates via secure modems. ➢ receive Childcare

© 2009 - 2011 by Personalized Software, all rights reserved

Payment Application Data Security Standard (PA DSS) Requirements			
PA DSS Number/Topic		**What Childcare Manager Does For You**	**What You Need to Do To Be Compliant**
			Manager updates through a firewall, if your computer is connected via VPN or other high speed connection.
11.2	Implement two-factor authentication for remote access to payment application.	Childcare Manager is designed for local access only and therefore does not require two-factor authentication. Childcare Manager uses one-factor authentication (user ID and password) secured with SHA-1 hash encryption for local access. It is your responsibility as the user to provide for two-factor authentication if you plan to originate access to Childcare Manager from outside your network.	If you plan to originate access to Childcare Manager from outside your network you must implement two-factor authentication. Two-factor authentication requires two forms of authentication. To provide this additional security, use technologies such as remote authentication and dial-in-service (RADIUS); terminal access controller access control system (TACACS) with tokens; or VPN (based on SSL/TLS or IPSEC) with individual certificates.

4 Windows Security

We recommend that you follow the Windows security best practices listed below. We also recommend that you use the built-in security features of Microsoft Windows which that are designed to help you maintain a PCI DSS compliant environment.

These features include:

- password policies,
- account lockout policies and
- idle time and screen saver lockout.

© 2009 - 2011 by Personalized Software, all rights reserved

4.1 Windows Security Best Practices

We recommend following these Windows security best practices:

- Turn on Windows automatic updates and make sure that your computer is always up to date with the latest security patches and updates.
- Do not share Windows accounts between users. All users should have their own unique user accounts.
- Communicate your security and password policies to any employees that have access to your systems or to sensitive cardholder data.
- If you allow vendors or contractors to access your systems remotely, you should provide them with accounts that are only available temporarily, or change your passwords on any existing accounts that you give them access to.
- Inactive Windows user accounts should be removed at least every 90 days.
- Whenever possible, do not allow public access to computers. If you do allow public access, you should set up idle lockout policies on these computers.

4.2 Password Policy

Windows provides the ability to configure password policies. To access this configuration, go to **Start | Control Panel | Administrative Tools**, and open **Local Security Policy**. Expand **Account Policy** from the tree menu on the left, and click **Password Policy**.

The following settings are recommended by the PCI standard:

- Enforce password history: 4 passwords remembered
- Maximum password age: 90 days
- Minimum password age: 0 days
- Minimum password length: 7 characters
- Password must meet complexity requirements: Enabled
- Store password using reversible encryption: Disabled

Note that “Password must meet complexity requirements” will enforce the following requirements for all Windows passwords:

- Not contain the user's account name or parts of the user's full name that exceed two consecutive characters
- Be at least six characters in length
- Contain characters from three of the following four categories:
  - English uppercase characters (A through Z)
  - English lowercase characters (a through z)
  - Base 10 digits (0 through 9)
  - Non-alphabetic characters (for example, !, $, #, %)
- Complexity requirements are enforced when passwords are changed or created.

4.3 Account Lockout Policy

Windows provides the ability to configure account lockout policies. To access this configuration, go to **Start | Control Panel | Administrative Tools**, and open **Local Security Policy**. Expand **Account Policy** from the tree menu on the left, and click **Account Lockout Policy**.

© 2009 - 2011 by Personalized Software, all rights reserved

The PCI standard suggests the following changes:

- Account Lockout Duration: 30 (minutes)
- Account Lockout Threshold: 6 invalid login attempts
- Reset account lockout counter after: 30 (minutes)

4.4 Screensaver Lockout Policy

Windows provides the ability to lock the computer after the computer has been idle for a period of time and when the screensaver is active.

To access this configuration, right-click on the Desktop and choose **Properties**, or select Start | Control Panel | Display. Select the Screen Saver tab. Select a screen saver option (e.g. Windows XP), set the wait time, and check the box for *"n resume, password protect"* Click **Apply** or **OK** to save the changes.

5 Resources

Following is a list of resources that may be useful understanding PCI merchant requirements.

PA DSS Resource Guide	
Title	**Description and Source**
Navigating PCI DSS --- Understanding the Intent of the Requirements	This document describes the 12 Payment Card Industry Data Security Standard (PCI DSS) requirements, along with guidance to explain the intent of each requirement. This document is intended to assist merchants, service providers, and financial institutions who may want a clearer understanding of the Payment Card Industry Data Security Standard, and the specific meaning and intention behind the detailed requirements to secure system components (servers, network, applications etc) that support cardholder data environments. You can obtain this document at: **https://www.pcisecuritystandards.org/pdfs/pci_dss_saq_navigating_dss.pdf**
Prioritized Approach for DSS 1.2	This document provides guidance that will help merchants identify how to reduce risk to card holder data as early on as possible in their compliance journey. The tool groups together the requirements of PCI DSS 1.2 into six key milestones for merchants to consider in their card data security strategy. The Prioritized Approach for PCI DSS 1.2 was created with input from the PCI SSC Board of Advisors, and informed by insight from real world results of data compromises shared by the assessment community. The Prioritized Approach offers guidance on how to focus PCI DSS implementation efforts in a way that expedites the security of cardholder data. It also

© 2009 - 2011 by Personalized Software, all rights reserved

PA DSS Resource Guide	
	➢ Helps businesses identify highest risk targets ➢ Creates a common language around PCI DSS implementation efforts ➢ Enables merchants to demonstrate progress on compliance process to key stakeholders – banks, acquirers, QSAs, others You can obtain this document at: **https://www.pcisecuritystandards.org/education/prioritized.shtml**
PCI DSS Wireless Guideline	This document provides guidance and installation suggestions for testing and/or deploying 802.11 Wireless Local Area Networks (WLAN) for organizations that require Payment Card Industry's Data Security Standard (PCI DSS) v1.2 compliance. The goal is to help organizations understand how PCI DSS applies to wireless environments, how to limit the PCI DSS scope as it pertains to wireless, and practical methods and concepts for deployment of secure wireless in payment card transaction environments. You can obtain this document at: **https://www.pcisecuritystandards.org/pdfs/pci_dss_Wireless_Guidelines.pdf**
PCI DSS Requirements and Security Assessment Procedures	This document is to be used by Payment Application-Qualified Security Assessors (PA-QSAs) conducting payment application reviews, so that software vendors can validate that a payment application complies with the PCI Payment Application Security Standard (PA-DSS). You can obtain this document at: **https://www.pcisecuritystandards.org/security_standards/pci_pa_dss.shtml**
PCI DSS Security Scanning Procedures	This document explains the purpose and scope of the Payment Card Industry (PCI) Security Scan for merchants and service providers who undergo PCI Security Scans to help validate compliance with the PCI Data Security Standard (DSS). Approved Scanning Vendors (ASVs) also use this document to assist merchants and service providers determine the scope of the PCI Security Scan. You can obtain this document at: **https://www.pcisecuritystandards.org/pdfs/pci_scanning_procedures_v1-1.pdf**
(PCI) PA DSS --- Glossary of Terms, Abbreviations, and Acronyms	This document provides an extensive glossary of terms, abbreviations and acronyms used in the payment industry. You can obtain this document at: **https://www.pcisecuritystandards.org/pdfs/pci_dss_glossary.pdf**
(PCI) PA DSS --- Program Guide	This document is to be used by Payment Application-Qualified Security Assessors (PA-QSAs) to further understand the PA-DSS procedures.

© 2009 - 2011 by Personalized Software, all rights reserved

PA DSS Resource Guide	
	You can obtain this document at: **https://www.pcisecuritystandards.org/pdfs/pci_pa_dss_program_guide.pdf**
(PCI) PA DSS --- Requirements and Security Assessment Procedures	This document is to be used by Payment Application-Qualified Security Assessors (PA-QSAs) conducting payment application reviews, so that software vendors can validate that a payment application complies with the PCI DSS Payment Application Data Security Standard (PA-DSS). This document is also to be used by PA-QSAs as a template to create the Report on Validation. You can obtain this document at: **https://www.pcisecuritystandards.org/security_standards/pa_dss.shtml**

6 Glossary of Terms, Abbreviations & Acronyms

The following list is taken from the Payment Card Industry (PCI) Data Security Standard list of glossary of terms, abbreviations and acronyms.

Glossary, Abbreviations & acronyms	
Term	**Definition**
Access control	Mechanisms that limit availability of information or information processing resources only to authorized persons or applications
Account harvesting	Process of identifying existing user accounts based on trial and error. [Note: Providing excessive information in error messages can disclose enough to make it easier for an attacker to penetrate and 'harvest' or compromise the system.]
Account number	Payment card number (credit or debit) that identifies the issuer and the particular cardholder account. Also called Primary Account Number (PAN)
Acquirer	An acquirer (or acquiring bank) is a member of a Card Association, for example MasterCard and/or Visa, which maintains merchant relationships and receives all bankcard transactions from the merchant.
Anti-Virus Program	Programs capable of detecting, removing, and protecting against various forms of malicious code or malware, including viruses, worms, Trojan horses, spyware, and adware
Application	Includes all purchased and custom software programs or groups of programs

© 2009 - 2011 by Personalized Software, all rights reserved

Glossary, Abbreviations & acronyms	
	designed for end users, including both internal and external (web) applications
Approved Standards	Approved standards are standardized algorithms (like in ISO and ANSI) and well-known commercially available standards (like Blowfish) that meet the intent of strong cryptography. Examples of approved standards are AES (128 bits and higher), TDES (two or three independent keys), RSA (1024 bits) and ElGamal (1024 bits)
Audit Log	Chronological record of system activities. Provides a trail sufficient to permit reconstruction, review, and examination of sequence of environments and activities surrounding or leading to operation, procedure, or event in a transaction from inception to final results. Sometimes specifically referred to as security audit trail
Authentication	Process of verifying identity of a subject or process
Authorization	Granting of access or other rights to a user, program, or process
Backup	Duplicate copy of data made for archiving purposes or for protecting against damage or loss
Cardholder	Customer to whom a card is issued or individual authorized to use the card
Cardholder data	Full magnetic stripe or the PAN plus any of the following: • Cardholder name • Expiration date • Service Code
Cardholder data environment	Area of computer system network that possesses cardholder data or sensitive authentication data and those systems and segments that directly attach or support cardholder processing, storage, or transmission. Adequate network segmentation, which isolates systems that store, process, or transmit cardholder data from those that do not, may reduce the scope of the cardholder data environment and thus the scope of the PCI assessment
Card Validation Value or Code	Data element on a card's magnetic stripe that uses secure cryptographic process to protect data integrity on the stripe, and reveals any alteration or counterfeiting. Referred to as CAV, CVC, CVV, or CSC depending on payment

© 2009 - 2011 by Personalized Software, all rights reserved

Glossary, Abbreviations & acronyms	
	card brand. The following list provides the terms for each card brand: • CAV Card Authentication Value (JCB payment cards) • CVC Card Validation Code (MasterCard payment cards) • CVV Card Verification Value (Visa and Discover payment cards) • CSC Card Security Code (American Express) Note: The second type of card validation value or code is the three-digit value printed to the right of the credit card number in the signature panel area on the back of the card. For American Express cards, the code is a four-digit unembossed number printed above the card number on the face of all payment cards. The code is uniquely associated with each individual piece of plastic and ties the card account number to the plastic. The following provides an overview: • CID Card Identification Number (American Express and Discover payment cards) • CAV2 Card Authentication Value 2 (JCB payment cards) • CVC2 Card Validation Code 2 (MasterCard payment cards) • CVV2 Card Verification Value 2 (Visa payment cards)
Compromise	Intrusion into computer system where unauthorized disclosure, modification, or destruction of cardholder data is suspected
Console	Screen and keyboard which permits access and control of the server or mainframe computer in a networked environment
Consumer	Individual purchasing goods, services, or both
Cookies	String of data exchanged between a web server and a web browser to maintain a session. Cookies may contain user preferences and personal information
Cryptography	Discipline of mathematics and computer science concerned with information security and related issues, particularly encryption and authentication and such applications as access control. In computer and network security, a tool for access control and information confidentiality
Database	Structured format for organizing and maintaining easily retrieved information. Simple database examples are tables and spreadsheets
Data Base Administrator	Database Administrator. Individual responsible for managing and administering

© 2009 - 2011 by Personalized Software, all rights reserved

Glossary, Abbreviations & acronyms	
(DBA)	databases
Default accounts	System login account predefined in a manufactured system to permit initial access when system is first put into service
Default password	Password on system administration or service accounts when system is shipped from the manufacturer; usually associated with default account. Default accounts and passwords are published and well known
DMZ	Domain name system or domain name server. System that stores information associated with domain names in a distributed database on networks, such as the Internet
DSS	Data Security Standard
Encryption	Process of converting information into an unintelligible form except to holders of a specific cryptographic key. Use of encryption protects information between the encryption process and the decryption process (the inverse of encryption) against unauthorized disclosure
Firewall	Hardware, software, or both that protect resources of one network from intruders from other networks. Typically, an enterprises with an intranet that permits workers access to the wider Internet must have a firewall to prevent outsiders from accessing internal private data resources
FTP	File transfer protocol
Host	Main computer hardware on which computer software is resident
Hosting Provider	Offer various services to merchants and other service providers. Services 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
HTTP	Hypertext transfer protocol. Open-internet protocol to transfer or convey information on the World Wide Web

© 2009 - 2011 by Personalized Software, all rights reserved

Glossary, Abbreviations & acronyms	
ID	Identity
IDS/IPS	Intrusion Detection System/ Intrusion Prevention System. Used to identify and alert on network or system intrusion attempts. Composed of sensors which generate security events; a console to monitor events and alerts and control the sensors; and a central engine that records events logged by the sensors in a database. Uses system of rules to generate alerts in response to security events detected. An IPS takes the additional step of blocking the attempted intrusion.
Information Security	Protection of information to insure confidentiality, integrity, and availability
Information System	Discrete set of structured data resources organized for collection, processing, maintenance, use, sharing, dissemination, or disposition of information
IP	Internet protocol. Network-layer protocol containing address information and some control information that enables packets to be routed. IP is the primary network-layer protocol in the Internet protocol suite
IP address	Numeric code that uniquely identifies a particular computer on the Internet
IP Spoofing	Technique used by an intruder to gain unauthorized access to computers. Intruder sends deceptive messages to a computer with an IP address indicating that the message is coming from a trusted host
IPSEC	Internet Protocol Security (IPSEC). Standard for securing IP communications by encrypting and/or authenticating all IP packets. IPSEC provides security at the network layer
ISO	International Organization for Standardization. Non-governmental organization consisting of a network of the national standards institutes of over 150 countries, with one member per country and a central secretariat in Geneva, Switzerland that coordinates the system
LAN	Local area network. Computer network covering a small area, often a building or group of buildings

© 2009 - 2011 by Personalized Software, all rights reserved

Glossary, Abbreviations & acronyms	
MAC	Message authentication code
Magnetic Stripe Data (Track Data)	Data encoded in the magnetic stripe used for authorization during transactions when the card is presented. Entities must not retain full magnetic stripe data subsequent to transaction authorization. Specifically, subsequent to authorization, service codes, discretionary data/ Card Validation Value/ Code, and proprietary reserved values must be purged; however, account number, expiration date, name, and service code may be extracted and retained, if needed for business
Malware	Malicious software. Designed to infiltrate or damage a computer system, without the owner's knowledge or consent
Monitoring	Use of system that constantly oversees a computer network including for slow or failing systems and that notifies the user in case of outages or other alarms
Network	Two or more computers connected together to share resources
Network Components	Include, but are not limited to firewalls, switches, routers, wireless access points, network appliances, and other security appliances
Network Security Scan	Automated tool that remotely checks merchant or service provider systems for vulnerabilities. Non-intrusive test involves probing external-facing systems based on external-facing IP addresses and reporting on services available to external network (that is, services available to the Internet). Scans identify vulnerabilities in operating systems, services, and devices that could be used by hackers to target the company’s private network
Payment applications	Refers broadly to all payment applications that store, process, or transmit cardholder data as part of authorization or settlement, where these payment applications are sold, distributed, or licensed to third parties.
Payment brands	Refers to the payment card brands that are members of the PCI SSC, currently American Express, Discover, JCB, Mastercard and Visa
Payment Cardholder Environment	That part of the network that possesses cardholder data or sensitive authentication data
PAN	Primary Account Number is the payment card number (credit or debit) that

© 2009 - 2011 by Personalized Software, all rights reserved

Glossary, Abbreviations & acronyms	
	identifies the issuer and the particular cardholder account. Also called Account Number
Password	A string of characters that serve as an authenticator of the user
Patch	Quick-repair job for piece of programming. During software product beta test or try-out period and after product formal release, problems are found. A patch is provided quickly to users
PCI	Payment Card Industry
PCI SSC	PCI Security Standards Council, LLC
PIN	Personal identification number
Policy	Organization-wide rules governing acceptable use of computing resources, security practices, and guiding development of operational procedures
POS	Point of sale
Procedure	Descriptive narrative for a policy. Procedure is the “how to” for a policy and describes how the policy is to be implemented
Protocol	Agreed-upon method of communication used within networks. Specification that describes rules and procedures that computer products should follow to perform activities on a network
Public Network	Network established and operated by a telecommunications provider or recognized private company, for specific purpose of providing data transmission services for the public. Data must be encrypted during transmission over public networks as hackers easily and commonly intercept, modify, and/or divert data while in transit. Examples of public networks in scope of PCI DSS include the Internet, GPRS, and GSM.
PVV	PIN verification value. Encoded in magnetic stripe of payment card
Router	Hardware or software that connects two or more networks. Functions as sorter

© 2009 - 2011 by Personalized Software, all rights reserved

Glossary, Abbreviations & acronyms	
	and interpreter by looking at addresses and passing bits of information to proper destinations. Software routers are sometimes referred to as gateways
Sensitive Authentication Data	Security-related information (Card Validation Codes/Values, complete track data, PINs, and PIN Blocks) used to authenticate cardholders, appearing in plaintext or otherwise unprotected form. Disclosure, modification, or destruction of this information could compromise the security of a cryptographic device, information system, or cardholder information or could be used in a fraudulent transaction
Server	Computer that providers a service to other computers, such as processing communications, file storage, or accessing a printing facility. Servers include, but are not limited to web, database, authentication, DNS, mail, proxy, and NTP
Service Code	Three- or four-digit number on the magnetic-stripe that specifies acceptance requirements and limitations for a magnetic-stripe read transaction.
Service Provider	Business entity that is not a payment card brand member or a merchant directly involved in the processing, storage, transmission, and switching or transaction data and cardholder information or both. This also includes companies that provide services to merchants, services providers or members that control or could impact the security of cardholder data. Examples include managed service providers that provide managed firewalls, IDS and other services as well as hosting providers and other entities. Entities such as telecommunications companies that only provide communication links without access to the application layer of the communication link are excluded
SHA	Secure Hash Algorithm. A family or set of related cryptographic hash functions. SHA-1 is most commonly used function. Use of unique salt value in the hashing function reduces the chances of a hashed value collision
SQL	Structured (English) Query Language. Computer language used to create, modify, and retrieve data from relational database management systems
SSH	Secure shell. Protocol suite providing encryption for network services like

© 2009 - 2011 by Personalized Software, all rights reserved

Glossary, Abbreviations & acronyms	
	remote login or remote file transfer
SSID	Service set identifier. Name assigned to wireless WiFi or IEEE 802.11 network
SSL	Secure sockets layer. Established industry standard that encrypts the channel between a web browser and web server to ensure the privacy and reliability of data transmitted over this channel
System Components	Any network component, server, or application included in or connected to the cardholder data environment
TCP	Transmission control protocol
TDES	Triple Data Encription Standard also known as 3DES. Block cipher formed from the DES cipher by using it three times
Threat	Condition that may cause information or information processing resources to be intentionally or accidentally lost, modified, exposed, made inaccessible, or otherwise affected to the detriment of the organization
TLS	Transport layer security. Designed with goal of providing data secrecy and data integrity between two communicating applications. TLS is successor of SSL
Token	Device that performs dynamic authentication
Transaction data	Data related to electronic payment
Truncation	Practice of removing data segment. Commonly, when account numbers are truncated, the first 12 digits are deleted, leaving only the last 4 digits
Two-factor authentication	Authentication that requires users to produce two credentials to access a system. Credentials consist of something the user has in their possession (for example, smartcards or hardware tokens) and something they know for example, a password). To access a system, the user must produce both factors
UserID	A character string used to uniquely identify each user of a system
Virus	Program or string of code that can replicate itself and cause modification

© 2009 - 2011 by Personalized Software, all rights reserved

Glossary, Abbreviations & acronyms	
	or destruction of software or data
VPN	Virtual private network. Private network established over a public network
Vulnerability	Weakness in system security procedures, system design, implementation, or internal controls that could be exploited to violate system security policy
Vulnerability Scan	Scans used to identify vulnerabilities in operating systems, services, and devices that could be used by hackers to target the company's private network
WEP	Wired equivalent privacy. Protocol to prevent accidental eavesdropping and intended to provide comparable confidentiality to traditional wired network. Does not provide adequate security against intentional eavesdropping (for example, cryptanalysis)
WPA	WiFi Protected Access (WPA and WPA2). Security protocol for wireless (WiFi) networks. Created in response to several serious weaknesses in the WEP protocol

© 2009 - 2011 by Personalized Software, all rights reserved